Pemodelan Ancaman Sistem Keamanan *E-Health* Menggunakan Metode STRIDE dan DREAD

Muhammad Khairul Faridi
17917115

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Forensika Digital
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2021

Lembar Pengesahan Pembimbing

Pemodelan Ancaman Sistem Keamanan *E-Health* Menggunakan Metode STRIDE dan DREAD

Muhammad Khairul Faridi

17917115

Yogyakarta, Juni 2021

Pembimbing Utama	Pembimbing Kedua
Dr. Imam Riadi, S.Pd., M.Kom.	Dr. Yudi Prayudi, S.Si., M.Kom.

Lembar Pengesahan Penguji

Pemodelan Ancaman Sistem Keamanan *E-Health* Menggunakan Metode STRIDE dan DREAD

Muhammad Khairul Faridi

17917115

Yogyakarta, Juni 2021

Tim Penguji,

Dr. Imam Riadi, S.Pd., M.Kom.
Ketua

Dr. Yudi Prayudi, S.Si., M.Kom.
Anggota I

Dr. Ir. Bambang Sugiantoro, S.Si., MT.
Anggota II

Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia

Izzati Muhimmah, S.T., M.Sc., Ph.D.

Abstrak

Pemodelan Ancaman Sistem Keamanan *E-Health* Menggunakan Metode STRIDE dan DREAD

Pada masa pandemi ini serangan digital sangat masif dilakukan khususnya pada fasilitas kesehatan seperti rumah sakit. Sistem Informasi Manajemen Rumah Sakit (SIMRS) berfungsi sebagai media informasi rumah sakit dan manajemen rumah sakit yang di dalamnya terdapat data rekam medis pasien yang merupakan hasil interaksi antara dokter dengan pasien. Oleh karena itu peningkatan sistem keamanan rumah sakit khususnya rekam medis sangat perlu dilakukan untuk meyakinkan pengguna atau pasien bahwa data yang tersimpan pada SIMRS aman dari *attacker*. Terdapat beberapa cara untuk meningkatkan keamanan sistem dan salah satunya yaitu dengan memodelkan ancaman. Pemodelan ancaman ini bertujuan untuk menggambarkan secara umum bagaimana sistem SIMRS berjalan, kemudian dilakukan proses identifikasi kerentanan dan penilaian ancaman yang ada pada SIMRS. Pemodelan ancaman dapat dilakukan dengan menerapkan berbagai macam metode. Pada makalah ini, pemodelan ancaman yang akan menggunakan yaitu model ancaman STRIDE dan model DREAD. Model ancaman STRIDE akan digunakan untuk mengidentifikasi dan menganalisis ancaman yang ada pada sistem e-health. Setelah proses analisis selesai dilakukan kemudian akan dilakukan perhitungan dan pemberian peringkat ancaman berdasarkan penilaian yang didapat dengan menggunakan metode DREAD. Hasil identifikasi dan analisis yang telah dilakukan dengan metode STRIDE menunjukkan terdapat sembilan kerentanan yang teridentifikasi pada sistem SIMRS seperti pada bagian pengguna terdapat satu kerentanan, web server lima kerentanan dan *database* tiga kerentanan. Kerentanan tersebut kemudian dianalisis dan ditentukan tingkat ancaman berdasarkan metode DREAD. Hasil analisis tingkat ancaman menghasilkan tiga tingkat kerentanan seperti dua kerentanan dengan tingkat ancaman rendah *(low),* empat kerentanan yang tingkat ancaman menengah *(medium).* Dan tiga kerentanan dengan tingkat ancaman tinggi *(high).* Berdasarkan tingkat ancaman tersebut dapat menjadi panduan dan urutan dalam memperbaiki dan meningkatkan sistem keamanan pada SIMRS mulai dari tingkat tertinggi sampai tingkat terendah.

Kata kunci

threat modelling, stride, dread, microsoft threat modelling tools, ehealth, simrs

Abstract

Pemodelan Ancaman Sistem Keamanan *E-Health* Menggunakan Metode STRIDE dan DREAD

During this pandemic, massive digital attacks were carried out, especially on health facilities such as hospitals. The Hospital Management Information System (SIMRS) functions as a medium for hospital information and hospital management. There are patient medical records that result from interactions between doctors and patients. Therefore, improving hospital security systems, especially medical records, really needs to be done to convince users or patients that the data stored on SIMRS is safe from attackers. There are several ways to improve system security, and one of them is by modeling threats. This threat modeling aims to describe in general how the SIMRS system runs, then the process of identifying vulnerabilities and assessing threats that exist in SIMRS is carried out. In this paper, the threat modeling used is the STRIDE threat model and the DREAD model. The STRIDE threat model will be used to identify and analyze existing threats to the e-health system. After the analysis process is complete, the calculation and ranking of threats are carried out based on the DREAD method's assessment. The identification and analysis of threats carried out using the STRIDE method show that there are nine vulnerabilities identified in the SIMRS system. On the user side, there is one vulnerability. The webserver has five the database has three vulnerabilities. The vulnerabilities are then analyzed, and the threat level is determined based on the DREAD method. The results of the threat level analysis produce three levels of vulnerability, such as two vulnerabilities with low threat levels, four vulnerabilities with medium threat levels. And three exposures with high threat levels. Based on the threat level, it can guide and sequence in improving and improving the security system at SIMRS, starting from the highest level to the lowest level.

Keywords

threat modelling, stride, dread, microsoft threat modelling tools, ehealth, simrs

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Juni 2021

Muhammad Khairul Faridi, S.Kom.

Daftar Publikasi

<u>Publikasi yang menjadi bagian dari tesis</u>

Publikasi berikut menjadi bagian dari penulisan tesis ini.

Faridi, M. K., Prayudi, Y., & Riadi, I. (2021). Pemodelan Ancaman Sistem Keamanan E-Health Menggunakan Metode STRIDE dan DREAD. *Edumatic : Jurnal Pendidikan Informatika*.

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Muhammad Khairul Faridi	Mendesain eksperimen (70%) Menulis *paper* (100%)
Imam Riadi	Memberi ide dan Saran (30%) Telaah Artikel
Yudi Prayudi	Memberi ide dan Saran (30%) Telaah Artikel

Halaman Kontribusi

Penelitian ini tidak terlepas dari kontribusi dari berbagai pihak yang berbentuk saran maupun bimbingan, mulai dari pra penelitian, seminar proposal, seminar progress, hingga seminar pendadaran. Pihak-pihak tersebut, antara lain, Dr. Imam Riadi, S.Pd., M.Kom, Dr. Yudi Prayudi,S.Si.,M.Kom, dan Dr. Ir. Bambang Sugiantoro, S.Si., MT

Halaman Persembahan

Tesis ini saya persembahkan kepada orang tua dan keluarga kecil istri dan anak saya yang telah mendukung dan menyemangati dalam menyelesaikan tugas akhir ini, tidak lupa juga saya ucapkan terima kasih kepada dosen pembimbing yang telah mengajar dan membimbing dengan sabar dan tidak lupa pula saya mengucapkan terima kasih kepada rekan-rekan dan adik tingkat yang banyak memberikan masukan dan saran dalam menyusun laporan tesis ini dan yang terakhir saya ucapkan terima kasih.

Kata Pengantar

Bismillahiwabihamdih

Assalamulaikum Wr. Wb.

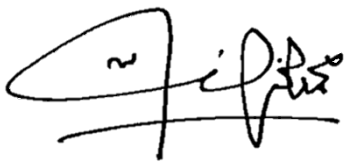
Segala puji dan syukur saya panjatkan ke hadirat Tuhan yang Maha Esa karena berkat rahmat dan hidayah serta karunia-Nya, laporan tugas akhir ini dapat terlaksana sebagaimana mestinya. Proses penyusunan tugas akhir ini dapat saya laksanakan dengan bantuan serta bimbingan dari berbagai pihak. Oleh karena itu, pada saat ini saya bermaksud untuk menyampaikan ucapan terima kasih yang sebesar besarnya kepada:

1. Allah SWT yang telah memberikan rahmat, kesehatan dan kekuatan sehingga dapat menyelesaikan penyusunan laporan tesis ini.
2. Kedua Orang tua, bapak Suriadi dan Ibu Sukini. Terima kasih telah memberikan dukungan baik dari materi, kasih sayang, perhatian dan doa kepada penulis.
3. Istri tercinta yang selalu memberikan semangat, perhatian, dan doa yang tak pernah putus.
4. Bapak Dr. Imam Riadi, S.Pd., M.Kom., dan bapak Dr. Yudi Prayudi, S.Si., M.Kom., selaku Dosen Pembimbing tesis ini yang selalu membantu serta memberikan arahan dan masukan sehingga tesis ini dapat selesai.
5. Ibu Izzati Muhimmah, S.T., M.Sc., Ph.D, selaku Ketua Program Studi Informatika – Program Pasca Sarjana Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta
6. Seluruh Dosen Informatika UII yang telah membimbing dan mengajarkan hal-hal baru.
7. Semua sahabat-sahabat yang selalu memberikan dukungan dan bersemangat untuk menyelesaikan laporan ini.

Penulis menyadari terdapat banyak kekurangan dalam proses penyampaian dan penyusunan laporan tesis ini. Oleh karena itu, saya berharap kritik, saran, dan masukan yang bersifat membangun dari pembaca untuk memperbaiki diri kedepannya. Akhir kata semoga laporan ini dapat memberikan manfaat bagi semua pihak. Amin.

Wassalaamu'alaikum Wr. Wb.

Lombok, 28 Juni 2021



Muhammad Khairul Faridi

Daftar Isi

Daftar Tabel

Daftar Gambar

Glosarium

BAB 1
Pendahuluan

1.1 Latar Belakang

Timbulnya ancaman dalam sebuah sistem aplikasi disebabkan oleh kesalahan yang muncul pada saat mendesain dan mengembangkan aplikasi(Ghafir et al., 2018). Beberapa pihak memanfaatkan kerentanan sistem tersebut untuk melakukan serangan seperti *defacing, phising, denial of service, bruteforce attack* dan lain sebagainya. Pada awal tahun 2020 lalu berdasarkan data dari kaspersky, terdapat beberapa fasilitas dan situs vital yang menangani covid-19 menjadi target serangan di Indonesia. Menurut Badan Siber dan Sandi Negara (BSSN) mencatat bahwa pada awal tahun 2020 terdapat 88 juta serangan siber yang menyerang fasilitas negara dan non negara seperti industri dan kesehatan[1]. Jumlah ini meningkat dari tahun sebelumnya yaitu 1,9 juta serangan.

Sistem *e-health* merupakan fasilitas kesehatan berupa sistem aplikasi berbasis web yang dikembangkan untuk mempermudah instansi kesehatan dalam mengelola data berkaitan rekam medis ataupun administrasi(Jaliyanti, 2018). Penerapan teknologi informasi dalam kesehatan terus berkembang karena dapat meningkatkan kualitas pelayanan dan perawatan terhadap pasien (Widiastuti, 2018). Secara garis besar *e-health* terbagi menjadi tiga bagian berdasarkan implementasi teknologi dalam layanan kesehatan yaitu *telehealth, telemedicine* dan *health informatics*. Semua jenis layanan kesehatan tersebut bertujuan untuk mempermudah pasien dan dokter dalam berkomunikasi serta mengakses layanan kesehatan. Penerapan teknologi pada layanan kesehatan tidak lepas dari isu keamanan seperti kebocoran data dan pembajakan akun merupakan ancaman yang sangat serius bagi layanan kesehatan. Oleh karena itu, keamanan informasi kesehatan seperti ini memerlukan sistem keamanan untuk menjamin informasi kesehatan seperti informasi biodata pasien dan rekam medis tetap terjaga(McDermott et al., 2019). Salah satu cara untuk menjamin informasi kesehatan dapat tetap terjaga yaitu dengan menganalisis sistem keamanan *e-health* untuk mengidentifikasi segala celah keamanan pada sistem.

Meningkatkan sistem keamanan dapat dilakukan dengan beberapa tahapan seperti mengidentifikasi celah keamanan pada sistem untuk dijadikan pedoman dalam memitigasi

[1] https://www.zettagrid.id/blog/2021/03/08/serangan-siber/

serangan (Alali et al., 2018). Sistem keamanan terbagi menjadi dua kategori yaitu sistem keamanan *software* dan sistem keamanan *hardware*(Hu et al., 2018). Permasalahan pada sistem keamanan *software* tergantung pada bagaimana sistem tersebut di bangun dan salah satu cara untuk mengetahuinya yaitu dengan mengidentifikasi ancaman dan risiko(Hussain et al., 2014). Saat ini banyak penelitian yang telah melakukan penelitian tentang pemodelan ancaman salah satunya yaitu penelitian yang dilakukan (Sivula, 2015), dalam penelitiannya terdapat beberapa uraian hasil analisis terhadap metode yang dapat diterapkan untuk memodelkan ancaman khususnya pada sistem *e-health* yaitu dengan menggunakan metode STRIDE, DREAD, DESIST, CAPEC, OWASP dan lain sebagainya.

Threat modelling atau pemodelan ancaman merupakan suatu model yang di dalamnya terdapat beberapa tahapan seperti identifikasi sistem, identifikasi aset, dan analisis ancaman dan mitigasi dalam konteks melindungi sesuatu yang bernilai(Abomhara et al., 2015). *Threat modelling* memungkinkan IT *security* untuk mengukur risiko berdasarkan ancaman yang muncul untuk menentukan tindakan pencegahan yang paling efektif dalam evaluasi ancaman. Terdapat beberapa penelitian terdahulu yang meneliti tentang pemodelan ancaman seperti penelitian yang dilakukan oleh (Mikail et al., 2016) yaitu meneliti tentang mitigasi ancaman berdasarkan hasil identifikasi ancaman dengan metode STRIDE. Terdapat empat tahapan yang dilakukan dalam memodelkan ancaman yaitu mengidentifikasi aset *e-health*, mengidentifikasi potensi ancaman, memodelkan ancaman dan penilaian tingkat ancaman. Hasil dari pemodelan ancaman digunakan sebagai rekomendasi dalam mitigasi sistem keamanan. Terdapat dua kesimpulan yang direkomendasi dalam meningkatkan sistem keamanan yaitu otorisasi dan pembagian tugas. Penelitian sejenis juga dilakukan oleh (Cagnazzo et al., 2018) yaitu klasifikasi ancaman dengan menggunakan metode STRIDE. Tahapan-tahapan yang dilakukan dalam penelitian yaitu identifikasi bagian-bagian dalam sistem keamanan *e-health* berbasis *mobile* kemudian klasifikasi ancaman dan mengukur tingkat risiko. Hasil penelitian digunakan untuk mitigasi ancaman serangan yaitu dengan merekomendasikan penerapan proses autentikasi dan enkripsi data pada sistem.

Berdasarkan dari uraian penelitian di atas, peneliti melakukan pemodelan ancaman dengan menggunakan metode STRIDE dalam mengidentifikasi ancaman dan metode DREAD dalam penilaian ancaman. Kemudian dalam penelitian ini juga akan melakukan penilaian ancaman dengan metode STRIDE dan DREAD berdasarkan hasil dari pemodelan dengan menggunakan *microsoft threat modelling* yang di harapkan dapat membelikan informasi yang lebih akurat dibandingkan dengan penelitian sebelumnya.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka yang menjadi rumusan masalah adalah sebagai berikut:

1. Bagaimana memodelkan sistem *e-health* dengan menggunakan *tools threat modelling* yaitu *microsoft threat modelling.*
2. Bagaimana mengidentifikasi ancaman sistem keamanan *e-health* dengan menggunakan metode STRIDE.
3. Bagaimana menganalisis tingkat ancaman berdasarkan tingkat kerentanan keamanan aplikasi *e-health* dengan menggunakan metode DREAD.

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan penelitian ini adalah sebagai berikut:

1. Untuk memodelkan sistem *e-health* dengan menggunakan *tools threat modelling* yaitu *microsoft threat modelling*.
2. Untuk mengidentifikasi ancaman sistem keamanan *e-health* dengan menggunakan metode STRIDE.
3. Untuk menganalisis tingkat ancaman berdasarkan tingkat kerentanan keamanan aplikasi *e-health* dengan menggunakan metode DREAD.

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini meliputi:

1. Penelitian ini dilakukan untuk memodelkan sistem *e-health* dengan menggunakan *tools threat modelling* yaitu *microsoft threat modelling*.
2. Penelitian ini dilakukan untuk mengidentifikasi ancaman sistem keamanan *e-health* dengan menggunakan metode STRIDE.
3. Penelitian ini dilakukan untuk menganalisis tingkat ancaman pada sistem *e-health* dengan menggunakan metode DREAD.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberi kontribusi dalam kehidupan manusia dan dapat diterapkan dalam dunia nyata. Adapun manfaat penelitian ini antara lain :

1. Dengan adanya penelitian ini, diharapkan dapat menjadi acuan dalam evaluasi ancaman pada sistem aplikasi *e-health*.

2. Dengan adanya analisis dengan metode STRIDE dan DREAD, diharapkan *IT Security* dapat mengetahui kerentanan serta tingkat kerentanan dari sistem aplikasi *e-health*.
3. Dengan adanya penelitian ini juga diharapkan dapat memberikan kontribusi bagi penelitian selanjutnya.

1.6 Literatur Review

Sistem elektronik kesehatan (*E-Health system*) merupakan fasilitas kesehatan yang dikembangkan untuk memberikan kemudahan dalam memanajemen data kesehatan. Namun, untuk menjaga kerahasiaan data maka dibutuhkan sistem *e-health* yang aman dari ancaman serangan.

Telah banyak penelitian yang membahas tentang memitigasi sistem keamanan *e-health* seperti penelitian yang dilakukan oleh (Mikail et al., 2016) yaitu memitigasi sistem keamanan kesehatan dengan mengidentifikasi ancaman menggunakan pemodelan STRIDE. Dalam penelitian ini peneliti melakukan pemodelan ancaman dengan beberapa tahapan seperti mengidentifikasi aset *e-health*, identifikasi akses, identifikasi ancaman dan penilaian tingkat ancaman. Hasil identifikasi tersebut kemudian dinilai menggunakan metode *dread*. Kesimpulan dari penilaian risiko digunakan sebagai acuan dalam memitigasi risiko keamanan *e-health* seperti menggunakan kunci biometri saat akan mengakses data dan kemudian mengklasifikasikan bagian-bagian yang dapat di akses oleh pengguna. Penelitian yang sejenis juga dilakukan oleh (Cagnazzo et al., 2018) yaitu meneliti tentang bagaimana memberikan solusi untuk memitigasi risiko dari ancaman sistem keamanan *mobile health* (*m-health*). Dalam penelitiannya dilakukan tiga langkah dalam memodelkan ancaman yaitu identifikasi aset, membuat daftar ancaman, memitigasi ancaman. Daftar ancaman di dapatkan dari metode yang di terapkan yaitu dari metode STRIDE. Kemudian menilai tingkat ancaman menggunakan metode DREAD. Hasil analisis digunakan untuk mitigasi ancaman pada sistem *m-health*.

Penelitian yang dilakukan oleh (Omotosho, Haruna, & Mikail, 2019) juga meneliti tentang perangkat kesehatan yang terkoneksi dengan *Internet of things* (IoT). Penelitian ini dilakukan untuk menganalisis tingkat risiko keamanan dengan tiga tahap yaitu analisis sistem, identifikasi ancaman serta perangkat IoT, dan penilaian tingkat ancaman. Analisis sistem dilakukan untuk menganalisis desain sistem untuk menentukan ancaman dari setiap perangkat IoT. Proses identifikasi ancaman menggunakan metode STRIDE dan sedangkan penilaian tingkat ancaman menggunakan metode DREAD. Hasil dari analisis digunakan untuk meningkatkan keamanan dan memitigasi risiko dari masing-masing perangkat IoT

kesehatan. Penelitian lain juga dilakukan oleh (Vernotte, Botea, Legeard, Molnar, & Peureux, 2015) meneliti tentang proses pengujian keamanan berbasis risiko dengan pola kerentanan dan metode *Model-Based Testing* (MBT). Tujuan dari penelitian untuk meningkatkan kemampuan deteksi kerentanan aplikasi berbasis web. Metode MBT digunakan untuk menangkap perilaku aplikasi sementara identifikasi ancaman dengan basis pola kerentanan digunakan untuk penilaian risiko. Hasil penelitiannya menunjukkan bahwa proses identifikasi dengan metode MBT dan berbasis pola kerentanan sistem *e-health* dapat mendeteksi risiko secara otomatis.

Penelitian juga dilakukan oleh (Abomhara et al., 2015) meneliti tentang peningkatan potensi ancaman pada layanan kesehatan jarak jauh (*telehealth*). dalam penelitiannya memaparkan bahwa dengan adanya sistem layanan kesehatan jarak jauh dapat meningkatkan potensi ancaman. Untuk itu, dibutuhkan perlindungan terhadap ancaman. Pemodelan ancaman dapat memberikan pemahaman bagaimana cara untuk memitigasi ancaman. Dalam penelitian ini, peneliti mencoba memodelkan ancaman dengan mengidentifikasi ancaman dengan menggunakan metode STRIDE dan menilai tingkat risiko menggunakan DREAD. Hasil penelitiannya menunjukkan bahwa pemodelan ancaman dapat menjadi tolak ukur dalam memitigasi ancaman dan risiko yang akan terjadi pada sistem. Dari uraian penelitian-penelitian yang sudah dilakukan dapat disimpulkan bahwa, masing-masing peneliti meneliti tentang pemodelan ancaman pada sistem kesehatan dengan berbagai macam metode seperti STRIDE, DREAD, MBT dan metode berbasis pola kerentanan (*Pattern*). Sedangkan penelitian yang akan dilakukan yaitu meneliti tentang bagaimana menerapkan model ancaman menggunakan metode OWASP serta evaluasi sistem keamanan pada sistem *e-health* menggunakan metode DREAD.

Berikut adalah hasil tabulasi dari studi pustaka yang telah diuraikan di atas dapat dilihat pada Tabel 1.1.

Tabel 1.1 Tabulasi studi pustaka dan pengembangan yang dilakukan

No.	Peneliti	Analisa Kasus	Metode	Target Analisa
1.	(Alhassan, Abba, Mikail, & Waziri, 2016)	Melakukan analisis tingkat kerentanan sistem *elektronic health* menggunakan STRIDE	*Threat modeling with STRIDE and DREAD*	Mengetahui tingkat risiko keamanan sistem *e-health*.

No.	Peneliti	Analisa Kasus	Metode	Target Analisa
2.	(Cagnazzo, Hertlein, Holz, & Pohlmann, 2018)	Melakukan analisis tingkat kerentanan sistem *mobile health* menggunakan STRIDE	*Threat modeling with STRIDE and DREAD*	Mengetahui tingkat risiko keamanan sistem *m-health* untuk merekomendasikan solusi dalam memitigasi ancaman
3.	(Omotosho, Haruna, & Mikail, 2019)	Analisis tingkat keamanan perangkat pengguna *Internet of things* (IoT) kesehatan	*Threat modeling with STRIDE and DREAD*	Menganalisis tingkat keamanan pada pengguna IoT *health* untuk mencegah setiap ancaman
4.	(Vernotte, Botea, Legeard, Molnar, & Peureux, 2015)	Analisa tingkah laku sistem untuk mendeteksi risiko keamanan sistem *e-health*	*Threat modeling with Model-Based Testing* (MBT) dan berbasis pola kerentanan	Mengidentifikasi tingkah laku sistem *e-health* untuk dapat mendeteksi ancaman dan risiko secara otomatis
5.	(Abomhara, Gerdes, & Køien 2015)	Melakukan identifikasi ancaman terhadap sistem *telehealth*	*Threat modeling with STRIDE and DREAD*	Menganalisis tentang bagaimana meningkatkan keamanan dalam sistem layanan kesehatan jarak jauh

1.7 Metode Penelitian

Dalam penelitian perlu disusun langkah-langkah penyelesaian dalam penelitian secara sistematika. Berikut ini adalah langkah-langkah penelitian:

Gambar 1.1 Metode penelitian

1. Studi literatur

   Pada tahap ini akan dilakukan studi literatur yang bertujuan untuk mengumpulkan referensi atau bahan-bahan yang akan digunakan dalam penelitian, baik melalui buku artikel, jurnal ataupun dengan mengumpulkan bahan dari internet yang terkait dengan *threat modelling* serta teori mengenai metode-metode yang digunakan.

2. *Overview* sistem *e-health*

   Pada tahapan ini akan dilakukan proses visualisasi sistem *e-health* yaitu dengan membuat diagram arsitektur aplikasi *e-health* selain itu terdapat proses identifikasi aset seperti identifikasi jaringan, teknologi dan bagian-bagian sensitif yang menjadi konsentrasi utama dalam pemodelan ancaman ini. Visualisasi pada tahap ini hanya akan menggambarkan bagian-bagian dalam sistem secara kasar agar dapat menjadi gambaran umum aktivitas yang terjadi pada sistem *e-health.*

3. Identifikasi dan dokumentasi ancaman

   Pada tahapan ini akan dilakukan identifikasi ancaman pada sistem *e-health* yaitu SIMRS (Sistem Informasi Manajemen Rumah Sakit). Tujuan tahap ini yaitu untuk mengidentifikasi ancaman yang mungkin dapat membahayakan sistem ataupun bagian-bagian data yang sensitif seperti hak akses, data pasien, dan sebagainya. Tahapan

identifikasi ancaman akan menggunakan pendekatan metode STRIDE. Selain itu pada tahap ini juga akan dilakukan proses dokumentasi dari hasil identifikasi ancaman sebelumnya. Tahapan ini bertujuan untuk mendeskripsikan segala hasil identifikasi ancaman seperti target serangan, teknik serangan serta langkah untuk menanggulangi kerentanan keamanan pada sistem *e-health*.

4. Analisis ancaman

   Penilaian ancaman merupakan tahap akhir dalam pemodelan ancaman, pada tahap ini akan dilakukan penilaian terhadap ancaman-ancaman yang telah diidentifikasi sebelumnya, nilai dari ancaman berdasarkan pada risiko yang ditimbulkan ketika ancaman itu berhasil dilakukan. Penilaian ancaman akan menggunakan metode DREAD.

5. Mitigasi ancaman

   Pada tahap ini akan dilakukan analisis ancaman pada sistem yang telah terdeteksi sebagai ancaman pada sistem *e-health* seperti memberikan kategori, deskripsi ancaman dan cara untuk menanggulanginya.

1.8 Sistematika Penulisan

Untuk memberikan gambaran dan mempermudah dalam penyusunan penelitian ini, maka dibuat sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas. Di dalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian serta sistematika penulisan.

BAB II KAJIAN TEORI

Pada bab ini menjelaskan tentang teori-teori dasar yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang berkaitan dengan penelitian yang sedang diteliti.

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat lunak, perangkat keras dan bahan penelitian yang digunakan serta alat-alat yang akan digunakan dalam melakukan pengujian.

BAB IV PEMBAHASAN

Pada Bab ini membahas tentang hasil dan pembahasan, terkait dengan pembahasan penyelesaian masalah yang diangkat, penentuan hasil analisis dan evaluasi dari penelitian yang diangkat.

BAB V PENUTUP

Pada bab ini memuat kesimpulan akhir dari semua proses penelitian sampai kepada hasil implementasi metode dan saran yang perlu diperhatikan karena keterbatasan dalam mendapatkan materi yang dibuat selama melakukan penelitian dan rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.

BAB 2
Tinjauan Pustaka

2.1 Electronic Health

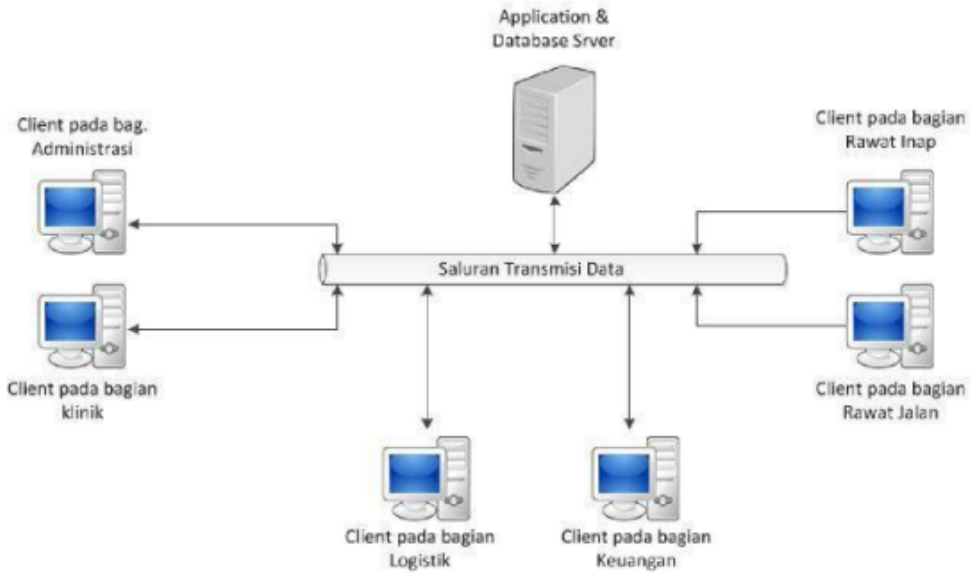
Sistem *e-health* merupakan fasilitas kesehatan berupa sistem aplikasi berbasis web yang dikembangkan untuk mempermudah instansi kesehatan dalam mengelola data berkaitan rekam medis ataupun administrasi (Jaliyanti, 2018). Sistem kesehatan elektronik yang merupakan kegiatan mengomputerisasi isi rekam medis kesehatan dan proses yang berhubungan dengannya. *Electronic Health Record* adalah rekaman atau catatan elektronik informasi terkait kesehatan (*health-record-Information*) seseorang yang mengikuti standar *interoperabilitas* nasional dan dapat dibuat, dikumpulkan, dikelola, digunakan, dan dirujuk oleh dokter atau tenaga kesehatan yang berhak (*authorized*) pada lebih dari satu organisasi pelayanan kesehatan (Widayanti, 2015).

Menurut tipe penggunaannya *e-health* terbagi menjadi tiga bagian yaitu *consumer informatics, clinical informatics, bioinformatics* (Amelia, 2016).

1. *Consumer informatics* merupakan sistem *e-health* yang ditujukan untuk masyarakat umum. Pada umumnya tipe ini digunakan hanya untuk memberikan informasi kesehatan bagi pasien serta memfasilitasi komunikasi antara praktisi kesehatan dengan pasien di luar jam praktik.
2. *clinical informatics* merupakan Rekam medis elektronik (EMR) yang mengelola data terkait informasi kesehatan pasien. *e-health* dalam tipe ini membantu meningkatkan akurasi diagnosis dan terapi dalam bentuk *telemedicine*. *e-health* juga digunakan sebagai sarana pendidikan jarak jauh misalnya melalui pembelajaran *online*.
3. Bioinformatika (*bioinformatics*) untuk para akademisi dan peneliti. Pada tipe ini, aplikasi *e-health* utamanya dimanfaatkan untuk manajemen, distribusi, dan pengolahan data kesehatan (misalnya data sebaran penyakit). Hasil olahan data tersebut umumnya dipakai sebagai dasar pembuatan kebijakan kesehatan maupun pengobatan untuk kepentingan masyarakat umum.

Saat ini kementerian kesehatan telah mengeluarkan aplikasi layanan manajemen rumah sakit yang disebut SIMRS GOS. SIMRS GOS merupakan sebuah sistem informasi manajemen rumah sakit yang dikembangkan oleh Kementerian Kesehatan Republik Indonesia dan dapat diperoleh secara gratis (markoferdiansalim, 2019). Aplikasi ini dapat di rubah sesuai dengan model layanan rumah sakit, sebelum menerapkan aplikasi ini ada

beberapa persyaratan yaitu jaringan harus sesuai dengan jaringan yang direkomendasikan oleh kemenkes. Berikut ini adalah arsitektur jaringan yang dapat digunakan dalam menjalankan aplikasi SIMRS GOS.



Gambar 2.1 Arsitektur sistem aplikasi dalam jaringan *multi-tried*

Berdasarkan gambar di atas, teknologi arsitektur di atas setiap pengguna hanya memerlukan koneksi internet atau jaringan komputer untuk dapat mengakses sistem informasi layanan SIMRS GOS.

2.2 Microsoft Threat Modelling Tools

Microsoft Threat Modelling Tools merupakan Alat yang dapat digunakan untuk pemodelan ancaman, *tools* ini dapat mempermudah pemodelan bagi semua pengembang aplikasi. *Microsoft Threat Modelling Tools* memiliki notasi yang standar dalam memvisualisasikan komponen sistem aplikasi, aliran data, dan batas keamanan. Pemodelan ini menerapkan *Security Development Lifecycle* (SDLC) yang dimaksudkan untuk membantu dalam mengidentifikasi semua ancaman, serangan dan kerentanan pada aplikasi.

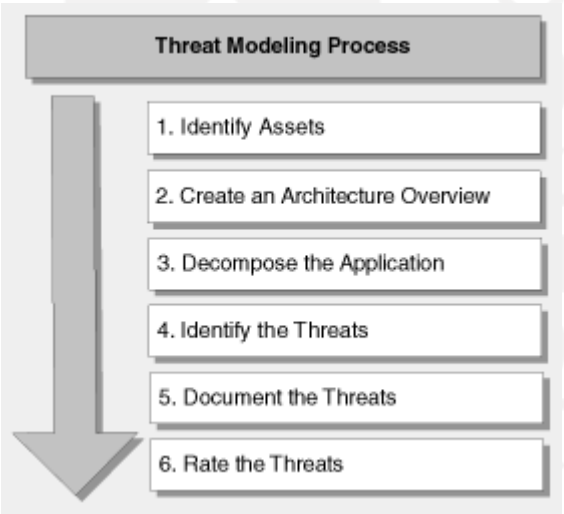
Terdapat tiga kelebihan dari *microsoft threat modelling tools* dalam pemodelan Ancaman perangkat lunak yaitu:

1. Desain arsitektur aplikasi lebih mudah karena memiliki notasi yang sederhana.
2. Analisis potensi keamanan menggunakan metodologi yang telah terbukti.
3. Memiliki saran mitigasi dari setiap hasil identifikasi ancaman.

2.3 *Threat Modelling*

Threat modelling merupakan proses identifikasi ancaman atau kerentanan pada sistem yang tidak memiliki sistem keamanan yang baik. Menurut (Hussain et al., 2014) *Threat Modelling* merupakan sebuah konsep atau *framework* dalam mengintegrasikan keamanan dalam sistem aplikasi dengan mengidentifikasi bagian-bagian yang rentan terhadap serangan sehingga membutuhkan perbaikan keamanan. *Threat modelling* memungkinkan IT *security* untuk mengukur risiko berdasarkan ancaman yang muncul untuk menentukan tindakan pencegahan mana yang paling efektif dalam memitigasi ancaman.

Terdapat enam tahapan untuk memodelkan ancaman yaitu *identify assets, Create an architecture overview, Decompose the application, Identify the threat, Document the threat dan rate the threat*(Meier et al., 2003).



Gambar 2.2 *Threat modeling process*

Identify assets bertujuan untuk mengidentifikasi aset yang akan dilindungi seperti *user*, server dan lain-lain. *Create an architecture overview* merupakan perancangan ilustrasi bagian-bagian dari aplikasi yang akan di analisis. *Decompose the application* merupakan tahap menguraikan bagian-bagian dalam bentuk alur diagram beserta arsitektur jaringan. *Identify the threat* merupakan tahap untuk mengidentifikasi bagian-bagian yang berpotensi memiliki kerentanan dan membaca pola pikir *attacker* dan pada tahapan ini akan digunakan model STRIDE dalam mengidentifikasi ancaman pada sistem aplikasi. *Document the theat* merupakan mencatat dan mendokumentasikan proses identifikasi menggunakan bagan. Dan

yang terakhir yaitu proses *rate the threat* merupakan proses penilaian tingkat ancaman pada aplikasi dengan menggunakan metode-metode yang telah tersedia seperti DREAD.

2.4 STRIDE

STRIDE merupakan sebuah singkatan dari *Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of Privilege*. STRIDE merupakan model yang digunakan dalam memodelkan ancaman. Model ini sangat cocok digunakan bagi pengembang aplikasi untuk menganalisis kelemahan sistem sebelum dilakukan publik aplikasi.

Tabel 2.1 *Desired property of* STRIDE

Threat	*Desired property*
Spoofing	*Authenticity*
Tampering	*Integrity*
Repudiation	*Non-repudiability*
Information disclosure	*Confidentiality*
Denial of Service	*Availability*
Elevation of Privilege	*Authorization*

2.5 DREAD

DREAD atau singkatan dari (*Damage, Potential, Reproducibility, Exploitability, Affected users, and Discoverability*) merupakan pemodelan ancaman yang digunakan untuk menilai tingkat keamanan dari sebuah sistem (Mikail et al., 2016). Model ini dibagi menjadi lima kategori penilaian yaitu berapa luas kerusakan jika terjadi serangan, seberapa mudah serangan dapat terjadi kembali, seberapa mudah melakukan serangan, seberapa luas dampak bagi pengguna dan seberapa mudah menemukan kerentanan. Hasil dari lima kategori tersebut kemudian akan digunakan untuk menghitung peringkat keamanan dari sistem dengan tiga peringkat yaitu rendah, menengah dan tinggi. Berikut adalah tabel dari deskripsi dari DREAD.

Tabel 2.2 Deskripsi DREAD

NO	Kata	Deskripsi
1	**D** = *Demage*	Kerusakan berdiri hanya untuk keseriusan serangan

2	**R** = *Reproducibility*	Apakah serangan berulang dan betapa mudahnya akan mengulangi serangan
3	**E** = *Exploitability*	*Explotabilitas* berarti kemudahan serangan
4	**A** = *Affected Users*	Pengguna yang terpengaruh mewakili semua orang yang terkena dampak serangan
5	**D** = *Discoverability*	*Discoverability* berarti betapa mudahnya untuk menemukan mengeksploitasi

Berikut adalah tabel penilaian ancaman menggunakan metode DREAD seperti pada tabel 2.3.

Tabel 2.3 Penilaian ancaman DREAD (Meier et al., 2003)

DREAD	**Rating**	**High (3)**	**Medium (2)**	**Low (1)**
D	*Damage potential*	Sistem lumpuh; Dapat mengakses administrator; Sistem diambil alih; Dapat menambah konten	Bocornya informasi sensitif	Bocornya informasi biasa
R	*Reproducibility*	Serangan dapat terjadi setiap saat dan berulang-ulang	Serangan dapat terjadi pada saat tertentu	Serangan sulit dilakukan walaupun memiliki kerentanan
E	*Exploitability*	Serangan dengan mudah dilakukan	Serangan berhasil namun membutuhkan beberapa kali percobaan	Membutuhkan orang yang sangat ahli dalam melakukan serangan.
A	*Affected users*	Semua pengguna, konfigurasi *default*, pelanggan	Beberapa pengguna, konfigurasi non-*default*	Persentase yang sangat kecil dari pengguna, fitur tidak jelas;
D	*Discoverability*	Informasi kesalahan sistem dapat terlihat dengan jelas. Kerentanan ditemukan dengan mudah.	*Bug* sistem jarang terlihat.	Kesalahan sulit di identifikasi.

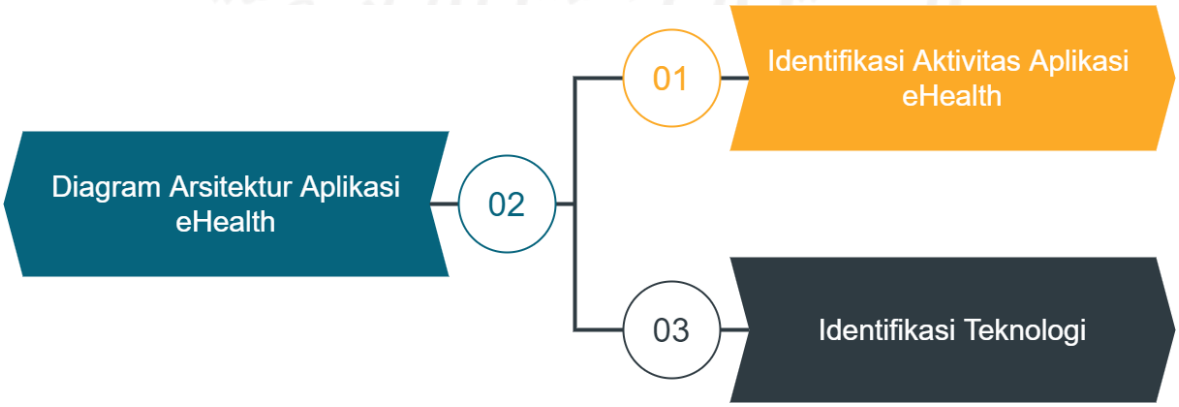
BAB 3
Metodologi

3.1 Studi Literatur

Studi literatur yang akan dilakukan yaitu mengumpulkan informasi dari berbagai sumber tertulis berupa buku-buku, artikel dan jurnal ataupun bersumber dari artikel *online* yang relevan dengan permasalahan yang dikaji yaitu tentang *threat modelling* beserta teori-teorinya. Setelah informasi dikumpulkan kemudian dilakukan analisis terhadap setiap literatur untuk mengetahui teknik dan langkah-langkah dalam menyelesaikan permasalahan. Selain itu tahap ini juga bertujuan untuk dapat menjadi wawasan dan rujukan untuk memperkuat argumentasi yang ada dalam penelitian.

3.2 *Overview* Sistem *E-Health*

Pada tahapan ini akan dilakukan proses visualisasi sistem *e-health* yaitu dengan menggambarkan diagram arsitektur aplikasi *e-health* yang di dalamnya terdapat aktivitas pengguna terhadap aplikasi yang kemudian akan dilakukan proses identifikasi teknologi yang digunakan. Selain itu pada tahap ini akan dilakukan identifikasi aktivitas pengguna dengan aplikasi seperti aktivitas pasien saat mendaftar, aktivitas bagian administrasi dan lain sebagainya, tentunya bagian-bagian yang dapat mengakses aplikasi *e-health* serta yang dapat mempengaruhi data secara langsung. Proses visualisasi pada tahap ini akan menggambarkan bagian-bagian dalam sistem secara kasar agar dapat menjadi gambaran umum aktivitas yang berjalan pada sistem *e-health*.



Gambar 3.1 *Overview* sistem *e-health*

Berdasarkan gambar di atas, digambarkan terdapat 3 langkah yang akan dilakukan untuk menggambarkan sistem aplikasi serta jaringan yang digunakan seperti identifikasi aktivitas aplikasi *e-health*, membuat diagram arsitektur aplikasi *e-health* untuk mempermudah dalam proses identifikasi teknologi. Kemudian hasil dari setiap langkah akan digunakan dalam proses identifikasi ancaman.

3.2.1 Identifikasi Aktivitas Aplikasi *e-health*

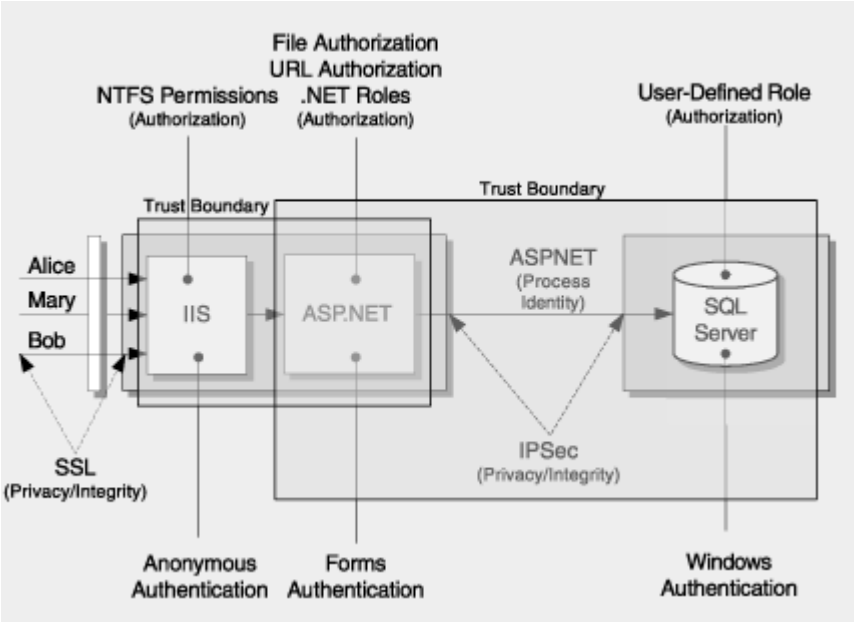
Penerapan teknologi pada pelayanan kesehatan khususnya teknologi SIMRS GOS sudah diterapkan hampir di seluruh bagian, oleh karena itu tahap identifikasi aktivitas pengguna aplikasi ini akan dibatasi hanya beberapa bagian saja yaitu pada bagian pasien, dokter, administrasi, rekam medis dan administrator. Aktivitas yang akan identifikasi yaitu aktivitas yang memiliki dampak langsung kepada sistem baik dalam pengolahan data ataupun manajemen hak akses pengguna. Berikut ini adalah tabel identifikasi aktivitas yang akan dilakukan seperti pada tabel berikut.

Tabel 3.1 Identifikasi aktivitas aplikasi

No	Aktivitas	Pengguna	Data
1	.....	.....	.....
2	.....	.....	.....
3	.....	.....	.....

3.2.2 Diagram Arsitektur Aplikasi *e-health*

Diagram arsitektur aplikasi *e-health* merupakan proses menggambarkan bagian-bagian dalam struktur aplikasi *e-health* serta untuk mengidentifikasi bagaimana penerapan sistem yang digunakan. Berikut ini adalah contoh diagram arsitektur aplikasi *e-health* seperti pada gambar 3.2.



Gambar 3.2 Diagram arsitektur aplikasi (sumber: docs.microsoft.com)

Berdasarkan gambar di atas, dapat dilihat terdapat beberapa teknologi yang saling terhubung seperti sistem keamanan, *framework* aplikasi, web server, serta basis data yang digunakan pada saat aplikasi di jalankan atau diakses oleh pengguna sistem aplikasi tersebut.

3.2.3 Identifikasi Teknologi

Identifikasi teknologi digunakan untuk mengidentifikasi teknologi yang telah diimplementasikan pada arsitektur sistem *e-health*. Proses ini akan sangat membantu dalam proses identifikasi ancaman pada teknologi yang diterapkan dikemudian hari. Teknologi yang akan di identifikasi yaitu teknologi yang diterapkan langsung pada sistem *e-health* maupun teknologi pendukung lainnya. Berikut ini adalah tabel teknologi yang diterapkan.

Tabel 3.2 Identifikasi teknologi

No	Teknologi	Detail Implementasi
1	.....	.....
2	.....	.....
3	.....	.....

3.3 Identifikasi dan Dokumentasi Ancaman

Identifikasi ancaman sistem merupakan tahap untuk mengidentifikasi ancaman yang mungkin membahayakan sistem yang telah dibangun. Identifikasi dilakukan berdasarkan

dari berbagai macam sudut pandang dan idealnya terdiri dari semua aspek seperti developer sampai dengan yang mengimplementasikan sistem. Semua tahapan pada identifikasi ini akan mengidentifikasi semua potensi ancaman pada sistem baik ancaman pada aplikasi. Dokumentasi ancaman merupakan proses pengolahan hasil dari identifikasi ancaman yang akan mendeskripsikan ancaman sesuai dengan model STRIDE. Selain itu, tahapan ini juga akan mengidentifikasi target dari semua ancaman serta dampak yang akan ditimbulkan dari ancaman tersebut. Terdapat beberapa tahapan yang akan dilakukan seperti identifikasi teknik serangan, target serangan, serta tindakan yang harus dilakukan untuk menghalau atau mencegah ancaman tersebut agar tidak terjadi. Berikut ini adalah tabel dokumentasi ancaman seperti pada tabel berikut:

Tabel 3.3 Dokumentasi ancaman

Ancaman 1	
Deskripsi ancaman	....
Target Ancaman	....
Teknik Serangan	....
Penanggulangan	....

3.4 Analisis Ancaman

Tahap ini merupakan tahap terakhir yaitu penilaian ancaman. Penilaian ancaman akan menggunakan metode DREAD yaitu setiap ancaman akan dikelompokkan berdasarkan risiko yang akan diakibatkan jika ancaman tersebut benar-benar terjadi. Risiko akan diukur berdasarkan tingkat kerusakan yang dapat terjadi dengan konversi menjadi tiga tingkatan yaitu rendah, sedang dan tinggi. DREAD sendiri singkatan dari *Damage potensial* (besaran kerusakan), *Reproducibilit* (seberapa sering serangan), *Exploitabilitas*: Seberapa mudah serangan), *Affected user* (efek serangan), dan *Discoverability* (seberapa mudah menemukan kerentanan). Setelah ditemukan tingkatan ancaman kemudian akan diberikan nilai berdasarkan hasil kalkulasi dari tingkat kerusakan dan potensi serangan dengan interval berikut yaitu interval 12–15 sebagai risiko Tinggi, 8–11 sebagai risiko Sedang, dan 5–7 sebagai risiko Rendah.

Tabel 3.4 Analisis ancaman

Ancaman	***D***	***R***	***E***	***A***	***D***	Total	Tingkat
.....							

Ancaman	***D***	***R***	***E***	***A***	***D***	Total	Tingkat
.....							
.....							

3.5 Mitigasi Ancaman

Tahap ini merupakan proses identifikasi ancaman yang telah dikenali pada sistem kemudian bagaimana langkah untuk mitigasi ancaman tersebut berdasarkan hasil identifikasi dengan menggunakan metode STRIDE dan DREAD.

Tabel 3.5 Mitigasi ancaman

Risk	
Deskripsi Ancaman	
Target Ancaman	
Penanggulangan	

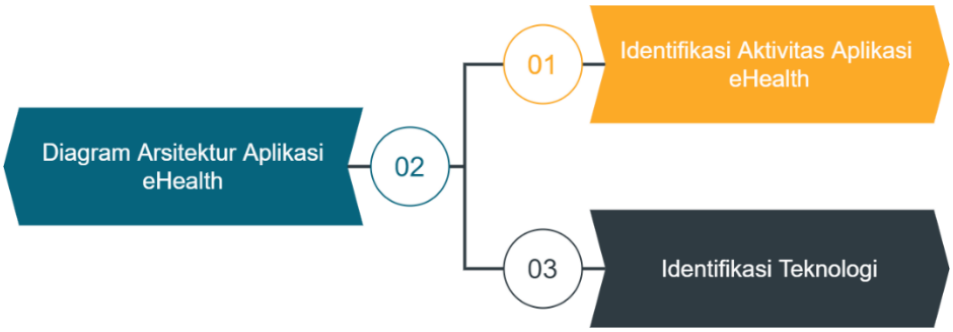
BAB 4
Hasil dan Pembahasan

4.1 Studi Literatur

Pada tahapan ini akan dilakukan kajian terhadap literatur dan penelitian terkait dengan pemodelan ancaman (*thread modelling*), metode STRIDE dan DREAD. Terdapat beberapa penelitian yang telah dilakukan dalam pemodelan ancaman seperti penelitian yang dilakukan oleh (Mikail et al., 2016) menyatakan bahwa pemodelan ancaman merupakan metode yang digunakan untuk mengidentifikasi ancaman sebelum aplikasi di publikasikan. Hasil identifikasi akan menjadi rujukan dalam proses pemeliharaan sistem. Terdapat beberapa metode yang dapat digunakan dalam melakukan pemodelan ancaman pada sistem e-health (Sivula, 2015), salah satu metode yang dapat digunakan yaitu STRIDE. STRIDE merupakan singkatan dari (*Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service and Elevation of Privilege*), metode ini merupakan model ancaman yang banyak digunakan kerena lebih mudah di aplikasikan, selain itu model ini lebih ringan dan efekti dalam melakukan identifikasi kerentanan serta merumuskan langkah dalam menanggulanginya (Khan et al., 2017). Dalam proses identifikasi ancaman, metode ini mengunakan pendekatan pemodelan ancaman berbasis Data Flow Diagram (DFD) (Sion et al., 2020) dan pada penelitian model ancaman STRIDE akan digunkan dalam menklasifikasikan ancaman pada sistem. Setelah identifikasi ancaman selesai kemudian akan diidentifikasi kembali untuk melakukan penilaian terhadap ancaman yang ditemukan dengan menggunakan model DREAD. Hasil dari identifikasi dan penilaian dapat digunakan sebagai rekomendasi dalam melakukan perbaikan sistem ehealth.

4.2 *Overview* Sistem *E-Health*

Overview sistem e-health akan melakukan analisis terhadap sistem aplikasi e-health yaitu aplikasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) yang telah diimplentasikan di disebagian besar rumah sakit di Indonesia dan salah satunya di rumah sakit XYZ. Sistem aplikasi tersebut akan menjadi objek penelitian untuk dilakukan identifikasi dan pemodelan ancaman. Sebelum dilakukan pemodelan ancaman, terdapat beberapa tahapan yang akan dilakukan seperti identifikasi aktivitas pengguna, membuat arsitektur sistem aplikasi dan mendeskripsikan teknologi yang digunakan.



Gambar 4.1 *Overview* Sistem *E-Health*

Berdasarkan gambar di atas, digambarkan terdapat 3 langkah yang akan dilakukan untuk menggambarkan sistem aplikasi serta jaringan yang digunakan seperti identifikasi aktivitas aplikasi e-*health*, membuat diagram arsitektur aplikasi e-*health* untuk mempermudah dalam proses identifikasi teknologi. Kemudian hasil dari setiap langkah akan digunakan dalam proses identifikasi ancaman.

4.2.1 Identifikasi Akitivitas Aplikasi eHealth

Sistem aplikasi SIMRS merupakan sistem yang menjadi standar aplikasi manajemen rumah sakit di Indonesia. Di dalamnya terdapat banyak fitur dan pengguna seperti pada aplikasi tersebut, terdapat 39 pengguna yang dibedakan berdasarkan bagian dan fungsinya masing-masing seperti apoteker, dokter, rekam medis, kepegawaian dan lain sebagainya. Pada penelitian ini, identifikasi aktivitas pengguna akan dikelompokkan menjadi empat bagian besar yaitu staf (karyawan), dokter, pengguna umum, dan admin. Staf yaitu bagian yang mengolah data administrasi rumah sakit seperti bagian pendaftaran, pembayaran, jamkesmas dan lain sebagainya. Kemudian bagian dokter yaitu bagian yang mengelola data pasien seperti perawat dan dokter yang memasukkan hasil diagnosa sampai dengan rekam medis. Selanjutnya admin yaitu pengguna yang dapat mengelola aplikasi atau yang mengawasi jalankan aplikasi. Kemudian yang terakhir adalah pengguna umum yaitu pengguna aplikasi yang tidak terkait langsung dengan rumah sakit seperti karyawan rumah sakit akan tetapi pengguna yang menggunakan aplikasi seperti pengunjung rumah sakit (calon pasien) dan pasien.

Berikut ini adalah tabel identifikasi aktivitas pada aplikasi SIMRS berdasarkan aktivitas pengguna serta data yang dapat di akses.

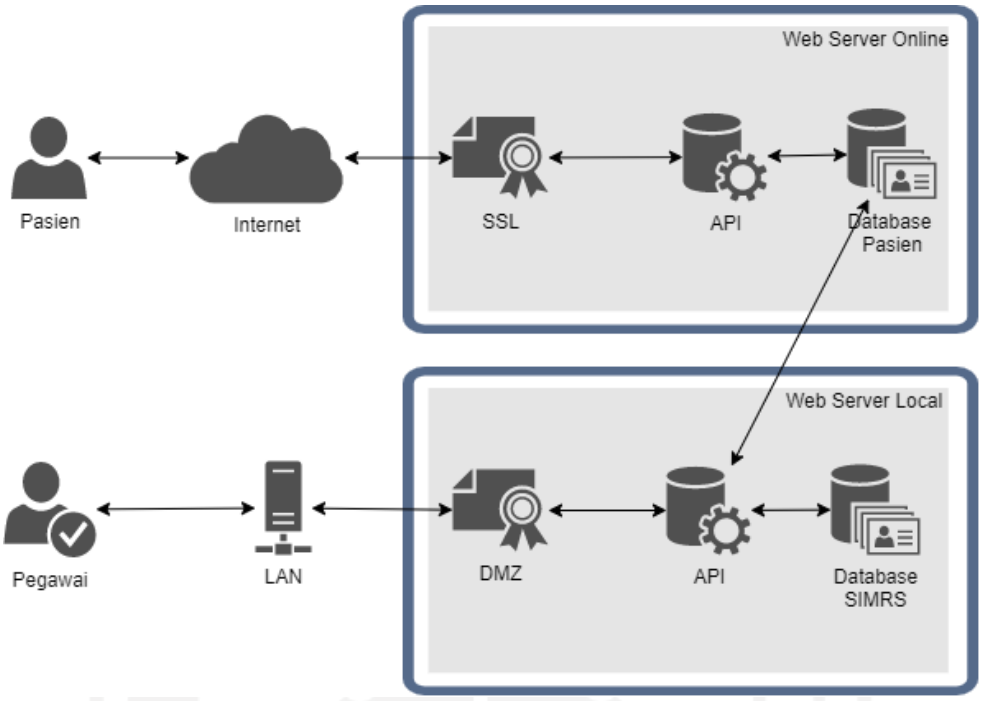
Tabel 4.1 Identifikasi aktivitas aplikasi

No	Pengguna	Aktivitas	Data
1	Karyawan	Mengelola data pegawai	Pegawai
		Mengelola data pembayaran	keuangan
		Mengelola data pasien	Pasien
2	Dokter	Mengelola data hasil diagnosa	Rekam medis
		Mengelola resep obat	Obat
		Mengelola data rekam medis	Rekam medis
		Melihat data pasien	Pasien
3	Pengguna umum	Melakukan registrasi pasien	Pasien
		Melihat biodata pasien	Pasien
4	admin	Mengelola data pengguna	Pengguna
		Mengelola log aktivitas pengguna	Log

Tabel aktifitas di atas merupakan aktifitas pengguna pada aplikasi, aktifitas tersebut merupakan sebagian besar aktifitas pengguna aplikasi yang di pilih secara garis besar.

4.2.2 Diagram Arsitektur Sistem Aplikasi SIMRS

Diagram arsitektur sistem aplikasi SIMRS pada rumah sakit XYZ memiliki dua kondisi untuk dapat mengakses SIMRS yaitu web server yang dapat diakses pada jaringan lokal dan web server *online*. Adapun yang dapat mengakses SIMRS dengan menggunakan jaringan lokal ialah semua pegawai dan dokter di rumah sakit tersebut termasuk admin dan sedangkan yang dapat mengakses sistem SIMRS menggunakan jaringan internet yaitu hanya pasien. Untuk lebih jelasnya dapat dilihat pada diagram arsitektur sistem SIMRS di bawah ini.



Gambar 4.2 Diagram arsitektur sistem

Pada Gambar 4.2 diagram arsitektur sistem di atas terdapat dua kelompok pengguna yang dapat mengakses aplikasi yaitu pasien dan pegawai rumah sakit termasuk dokter dan admin. Pada gambar di atas juga dapat diidentifikasi terdapat dua kondisi yaitu aplikasi yang terdapat pada web server *online* dan web server yang lokal. Aplikasi yang *online* dapat di akses oleh pasien dan sedangkan aplikasi yang berada di lokal hanya dapat di akses oleh pegawai di sekitar rumah sakit yang memiliki aksesnya terbatas.

4.2.3 Identifikasi Teknologi

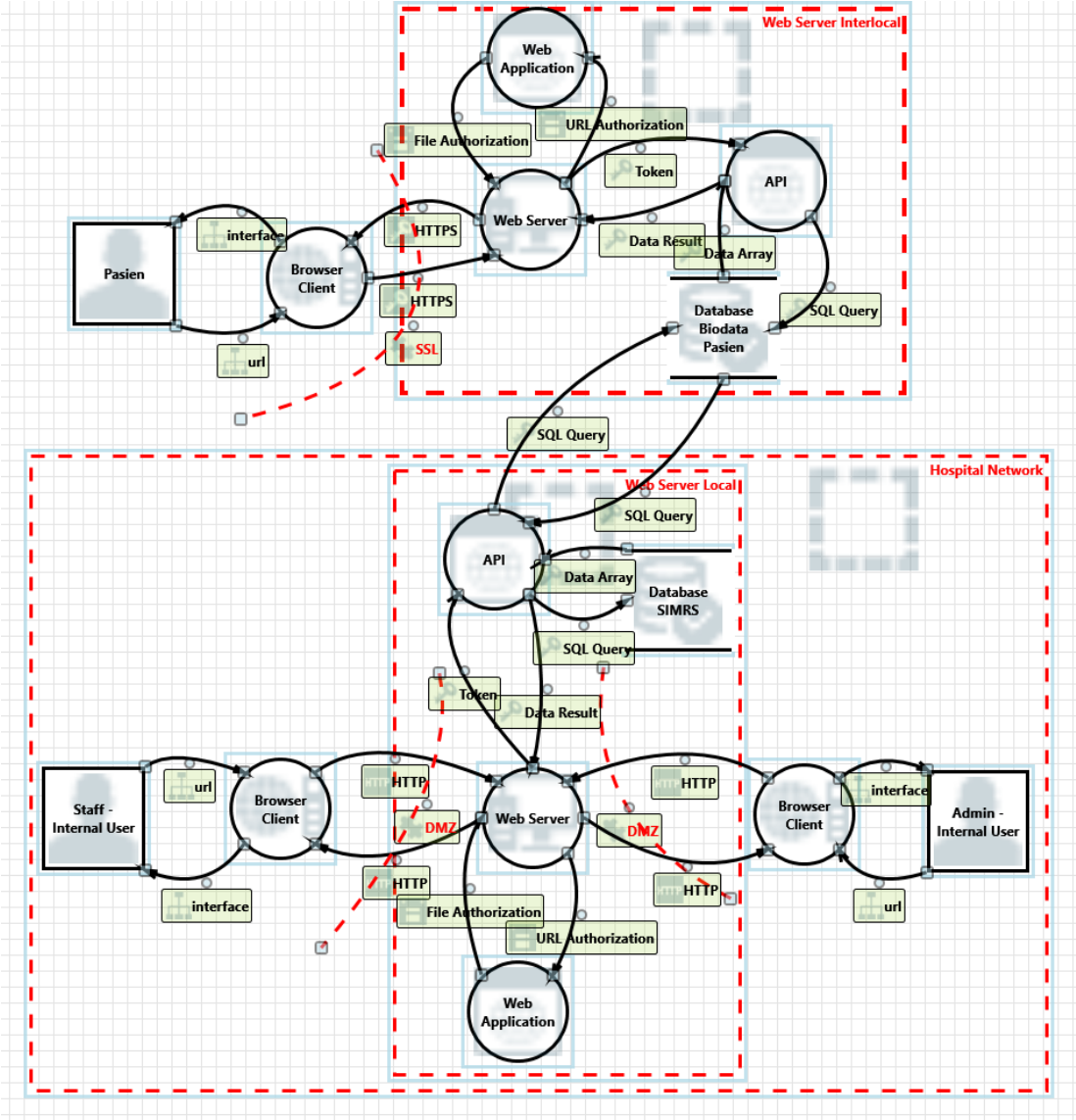
Identifikasi teknologi bertujuan untuk mengidentifikasi teknologi yang diimplementasikan pada arsitektur sistem *e-health*. Teknologi yang akan di identifikasi yaitu teknologi yang diterapkan langsung pada sistem *e-health* maupun teknologi pendukung lainnya. Berdasarkan gambar pada 4.2 dapat dilihat beberapa teknologi yang digunakan dalam menjalankan aplikasi SIMRS yaitu seperti pada Tabel 4.2

Tabel 4.2 Identifikasi teknologi

No	Teknologi	Detail Implementasi
1	SSL	Digunakan untuk melindungi informasi sensitif seperti informasi nama pasien, kata sandi, biodata pasien dan lain-lain. Protokol keamanan internet ini sangat umum digunakan (Chung et al., 2016) karena sebagian besar *website* menerapkan SSL pada domainnya.
2	DMZ	Merupakan singkatan dari *demilitarized zone* (zona demiliterisasi), dmz diimplementasikan sebagai sebuah *host* komputer yang berfungsi untuk menghubungkan jaringan lokal dan jaringan publik(Ikhwan & Elfitri, 2014). Selain sebagai *firewall* dmz juga memiliki fungsi sebagai penyaring agar pengguna dari luar tidak dapat mengakses aplikasi SIMRS secara langsung akan tetapi hanya dapat dilakukan ketika terkoneksi dengan jaringan lokal saja.
3	API	API merupakan sebuah *interface* yang dapat menghubungkan aplikasi satu dengan aplikasi lainnya(Destian Wijaya et al., 2015) seperti pada Gambar 4.2 api berfungsi untuk menghubungkan aplikasi yang berada pada server lokal dengan aplikasi yang berada pada server *online*.
4	PHP	Bahasa pemrograman yang digunakan dalam mengembangkan aplikasi SIMRS adalah PHP 5.
5	SQL	*Database* yang diterapkan pada aplikasi SIMRS adalah SQL-*based*.

4.3 Identifikasi dan Dokumentasi Ancaman

Sebelum melakukan dokumentasi ancaman terlebih dahulu akan dilakukan identifikasi ancaman dengan pemodelan ancaman STRIDE dan identifikasi ancaman dengan menggunakan *microsoft threat modeling tools*. Aplikasi ini merupakan aplikasi yang digunakan untuk memodelkan ancaman dan analisis ancaman secara otomatis. Hasil analisis ancaman tersebut kemudian akan didokumentasi untuk mengetahui bagian-bagian dari aplikasi yang memiliki ancaman. berikut ini merupakan pemodelan dengan menggunakan *microsoft threat modelling tools*. Berikut ini merupakan hasil pemodelan yang dilakukan.



Gambar 4.3 Pemodelan sistem *e-health*

Pada Gambar 4.3 terdapat dua kondisi yaitu *online* dan *local*, server *online* hanya dapat di akses oleh pengguna umum atau pasien dan sedangkan server *local* hanya dapat di akses oleh pegawai yang tersambung dengan jaringan rumah sakit. Setelah pemodelan dibuat kemudian akan dilakukan identifikasi ancaman berdasarkan hasil identifikasi oleh *microsoft threat modelling tools.*

Berikut merupakan tabel hasil identifikasi ancaman yang teridentifikasi dengan menggunakan aplikasi *microsoft threat modelling* seperti pada Tabel 4.3:

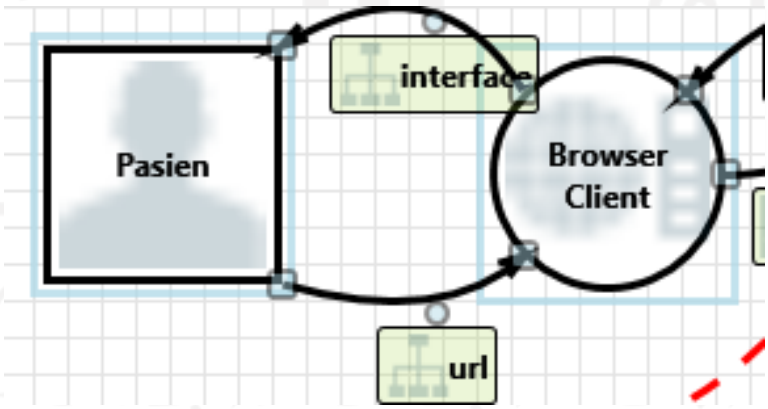
Tabel 4.3 Dokumentasi ancaman

No.	***Name***	***Category***
1	*Elevation Using Impersonation*	*Elevation Of Privilege*

2	*Data Flow HTTPS Is Potentially Interrupted*	*Denial Of Service*
3	*Potential Data Repudiation by Web Server*	*Repudiation*
4	*Cross Site Scripting*	*Tempring*
5	*Spoofing the Web Server Process*	*Spoofing*
6	*Elevation by Changing the Execution Flow in Web Server*	*Elevation Of Privilege*
7	*Data Flow SQL Query Is Potentially Interrupted*	*Denial Of Service*
8	*Potential SQL Injection Vulnerability for Database Biodata Pasien*	*Tampering*
9	*Spoofing of Destination Data Store Database Biodata Pasien*	*Spoofing*

4.3.1 Identifikasi ancaman pada bagian pengguna

Identifikasi ancaman pada bagian pengguna dilakukan dengan mengambil satu sampel yaitu pada bagian pasien dikarenakan sistem yang ada memiliki konfigurasi yang sama dengan pengguna lainnya. Untuk lebih jelasnya berikut adalah sampel interaksi pengguna dengan sistem SIMRS.



Gambar 4.4 Hasil identifikasi pada bagian pengguna

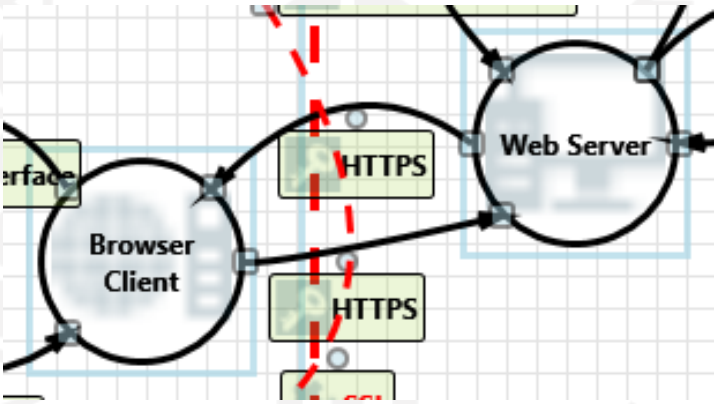
Pada Gambar 4.4 dapat dilihat seluruh pengguna saat mengakses aplikasi memiliki aktivitas yang sama, yang membedakannya hanya data yang disajikan oleh aplikasi ke pengguna. Hasil identifikasi bagian pengguna terdapat satu ancaman yaitu *Elevation Of Privilege*. *Elevation Of Privilege* yaitu sebuah metode serangan yang digunakan pengguna

untuk mengelabuhi sistem dengan mengubah hak akses pengguna sehingga dapat mengakses halaman dengan level yang lain.

4.3.2 Identifikasi ancaman pada bagian Web server

Berdasarkan hasil modeling ancaman pada Gambar 4.3, terdapat dua web server yang berjalan pada sistem SIMRS yaitu web server yang berada di jaringan lokal dan web server yang berada pada *cloud.* Masing-masing web server memiliki peran dan terhubung dengan menggunakan teknologi API yaitu teknologi yang mampu mengintegrasikan dua server atau lebih.

Fungsi utama dari server lokal yaitu sebagai pusat data, baik data informasi rumah sakit maupun data rekam medis pasien. Sedangkan server interlokal hanya memiliki fungsi sebagai media informasi rumah sakit dan media penyimpanan biodata pasien.



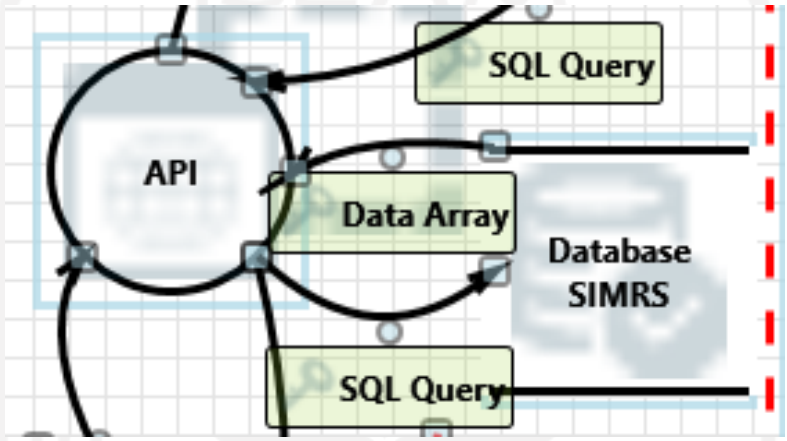
Gambar 4.5 Hasil identifikasi pada bagian web server

Pada Gambar 4.5 terdapat beberapa sistem keamanan dasar yaitu seperti penggunaan protokol HTTPS yang bertujuan untuk melindungi web server dari serangan. Selain itu pada web server juga terdapat teknologi API yaitu teknologi yang digunakan untuk menghubungkan server lokal dan interlokal. Dalam kasus ini API digunakan sebagai teknologi backup data seperti data yang ada pada server interlokal ke data server lokal. Setelah dilakukan modeling ancaman, hasil identifikasi menunjukkan terdapat beberapa kerentanan yaitu *Denial Of Service, Repudiation, Tempering Spoofing* dan *Elevation Of Privilege*.

Serangan DDos merupakan metode serangan dengan membanjiri server dengan *request packet* dari penyerang dengan bertujuan untuk membuat server target menjadi *down*(Prajapati et al., 2019). Hasil identifikasi ditemukan bahwa ancaman DDos pada server sangat tinggi sehingga serangan ini sangat mungkin dilakukan pada sistem SIMRS.

4.3.3 Identifikasi ancaman pada bagian *Database*

Identifikasi yang terakhir yaitu identifikasi ancaman pada bagian *database*. *Database* menjadi sumber data yang valid bagi semua aktivitas pada sistem. Pada sistem SIMRS terdapat dua bagian *database* yaitu *database* yang terdapat pada server lokal dan *database* yang terdapat pada sistem *interloka*. *Database* yang ada pada server lokal berfungsi sebagai media penyimpanan semua data baik itu data pengguna, pasien dan rumah sakit. Sedangkan *database* yang tersimpan pada jaringan interlokal memiliki fungsi untuk menyimpan data pasien khususnya biodata pasien dan informasi rumah sakit.



Gambar 4.6 Hasil identifikasi pada bagian web server

Pada Gambar 4.6 data dilihat untuk mengakses *database* sistem harus melakukan validasi token untuk dapat mengakses data yang ada pada *database*. Hasil identifikasi, terdapat tiga ancaman yang di identifikasi pada sistem *database* yaitu *Denial Of Service*, *Tampering* dan *spoofing*.

4.4 Analisis Ancaman

Analisis ancaman merupakan proses akhir yang akan dilakukan dalam proses identifikasi ancaman. Analisis ancaman yang akan dilakukan yaitu proses penilaian ancaman yang telah diidentifikasi untuk menentukan tingkat ancaman dari semua kerentanan yang telah ditemukan. Proses penilaian akan dilakukan dengan menggunakan model DREAD. Perhitungan dengan model ini selalu akan menghasilkan angka antara 1-10. Semakin tinggi angkanya berarti semakin serius risikonya. Untuk detail penilaian ancaman dapat dilihat pada lampiran 1.

Penilaian potensi kerusakan ini diberikan setelah dikakukan pengujian sederhana pada sistem SIMRS dengan teknik ancaman yang telah diidentifikasi. Setelah dilakukan penilaian potensi kerusakan kemudian akan dilakukan penilaian ancaman yaitu dengan menggunakan rumus berikut.

***DREAD Risk* = (*Damage* + *Reproduciblity* + *Exploitability* + *Affected Users* + *Discoverability*) / 5**

Setelah hasil ancaman diperoleh kemudian akan diberikan peringkat sesuai dengan tingkat ancaman dari setiap kerentanan. Berikut adalah tingkat ancaman yang ada pada penilaian menggunakan model DREAS yaitu 1=*low*, 2=*medium*, dan 3=*high*.

4.4.1 Pengguna

Pengguna yang diidentifikasi merupakan seluruh pengguna yang mengakses aplikasi, baik pengguna yang mengakses pada jaringan lokal maupun interlokal. Terdapat kerentanan yang telah teridentifikasi dalam bagian pengguna yaitu *Elevation of privilege. Elevation of privilege* merupakan teknik serangan berbasis *shell* yang bertujuan untuk mengambil hak akses administrator untuk mendapatkan informasi dari target serangan(Sim et al., 2017). Berikut adalah deskripsi penilaian ancaman seperti pada Tabel 4.4

Tabel 4.4 Deskripsi dan penilaian *Elevation of privilege* pada pengguna

Kategori	Deskripsi	Nilai
Damage	Seperti yang digambarkan pada pemodelan ancaman, pada saat *request* dikirimkan ke server, teknologi SSL akan memvalidasi permintaan tersebut sebelum data dikirimkan lagi pengguna sehingga secara otomatis dampak serangan ini **tidak ada**	1
Reproducibility	Serangan **sangat sulit** dilakukan dikarenakan penyerang harus melakukan konfigurasi lebih untuk melakukan serangan	1
Exploitability	Serangan ini **membutuhkan pengetahuan yang lebih tinggi** atau tidak bisa dilakukan oleh orang awam	1
Affected Users	Serangan ini memiliki dampak pada **sebagian pengguna** saja tidak yang memiliki level yang lebih rendah	2
Discoverability	Ancaman ini mudah ditemukan hanya dengan **memantau dan memanipulasi HTTP *request*** namun karena adanya teknologi SSL tidak semua ancaman tersebut berhasil dilakukan	2

Berdasarkan tabel di atas kemudian akan dilakukan penilaian tingkat ancaman dari kerentanan seperti pada Tabel 4.5

Tabel 4.5 Penilaian ancaman pengguna

Ancaman	**D**	**R**	**E**	**A**	**D**	**Total**	***Grade***
Elevation Of Privilege	1	1	1	2	2	7	*medium*

Berdasarkan pada tabel di atas dapat diketahui bahwa ancaman *elevation of provilage* pada pengguna medium dikarenakan hasil dari penjumlahan tingkat ancaman mendekati nilai dua yang artinya *Elevation Of Privilege* memiliki tingkat ancaman medium.

4.4.2 Web server

Hasil pemodelan dan identifikasi kerentanan pada bagian web server yaitu terdapat lima kerentanan yang teridentifikasi seperti *Denial Of Service, Repudiation, Tempering, Spoofing* dan *Elevation Of Privilege*.

- *Denial of service* merupakan serangan yang memfokuskan serangan ke sumber daya jaringan sehingga sumber daya tersebut menjadi *down* atau mati(Jamal et al., 2018) sehingga pengguna lain tidak bisa mengakses server atau alamat web tersebut. Berikut adalah deskripsi penilaian ancaman *denial of service* seperti pada Tabel 4.6

Tabel 4.6 Deskripsi dan penilaian *denial of service* pada web server

Kategori	Deskripsi	Nilai
Damage	Serangan ini dapat mengakibatkan server yang *online* tidak dapat di akses oleh pasien sehingga **attacker dapat melihat kerentanan lainnya** walaupun server lokal tidak akan terdampak apa-apa dikarenakan hanya dapat di akses oleh jaringan lokal saja	2
Reproducibility	Serangan ini **mudah dilakukan** dikarenakan penyerang tidak harus melakukan konfigurasi lebih untuk melakukan serangan atau bisa dengan bantuan *tools* DDOS.	3
Exploitability	Serangan ini tidak membutuhkan seorang yang ahli dalam melakukan serangan dikarenakan **alat ddos bisa di dapatkan dengan mudah di internet.**	3
Affected Users	Serangan ini memiliki dampak hanya pada **sebagian pengguna** saja yaitu pasien	2
Discoverability	Untuk saat ini DOS **sangat sulit** ditemukan dikarenakan sebagian server sudah mengantisipasi serangan ini dengan menambahkan *capta* pada *form* mereka termasuk sistem SIMRS	1

- *Repudiation* merupakan serangan yang memanfaatkan kekurangan aplikasi dalam memanajemen *cookie* dengan baik yaitu ketika aplikasi tidak menyimpan segala aktivitas pengguna saat mengakses aplikasi. Berikut adalah deskripsi penilaian ancaman *repudiation* seperti pada Tabel 4.7

Tabel 4.7 Deskripsi dan penilaian *repudiation* pada web server

Kategori	Deskripsi	Nilai
Damage	Dalam aplikasi SIMRS tidak memiliki sistem manajemen web *history* sehingga sangat memungkinkan teknik ini digunakan. Seperti saat pegawai mengakses aplikasi di sembarangan *device* sehingga riwayat *browsing* dapat **diambil dengan mudah** oleh orang yang tidak bertanggung jawab untuk **menyusup ke dalam sistem**.	3
Reproducibility	Serangan ini **membutuhkan cara yang kompleks** dikarenakan penyerang harus menganalisis dan mengetahui pola yang tersimpan pada *cookie*.	2
Exploitability	Serangan ini **membutuhkan orang yang ahli** untuk melakukan analisis riwayat yang sudah ada pada browser	1
Affected Users	Serangan ini memiliki dampak hanya **beberapa pengguna** saja seperti pengguna yang mengakses aplikasi di fasilitas umum	2
Discoverability	Serangan ini **mudah temukan di web browser** dikarenakan cookie tersimpan pada memori web browser sehingga analisis dapat dilakukan dengan mudah	3

- *Tempering* merupakan serangan yang menargetkan logika aplikasi yang sederhana seperti parameter alamat situs saat mengakses suatu halaman. Berikut ini adalah penilaian dari *tempering* seperti pada Tabel 4.8

Tabel 4.8 Deskripsi dan penilaian *tempering* pada web server

Kategori	Deskripsi	Nilai
Damage	**Semua pengguna dapat terdampak** oleh serangan ini karena logika aplikasi yang dikembangkan sangat mudah ditebak	3
Reproducibility	Serangan ini **sangat mudah** dilakukan untuk mengelabui sistem dikarenakan pada aplikasi SIMRS tidak memiliki proses autentikasi pengguna	3
Exploitability	Serangan ini **tidak membutuhkan orang yang ahli** dalam bidang teknologi	3
Affected Users	**Semua pengguna termasuk admin** dapat merasakan efek dari serangan ini karena ketika seseorang mengetahui logika alamat webnya maka semua halaman dapat diakses oleh penyerang	3
Discoverability	Serangan **sangat mudah** ditemukan dikarenakan dalam aplikasi SIMRS terdapat **beberapa formulir yang tidak terproteksi** sehingga serangan seperti *Tempering* dapat dilakukan dengan mudah.	3

- *Spoofing* merupakan serangan yang menduplikasi suatu halaman atau menyisipkan *malicious code* ke dalam *form*. Ketika seseorang memasukkan data di *form* tersebut

kemudian data tersebut akan terkirim ke *attacker*. Berikut ini adalah penilaian dari *tempering* seperti pada Tabel 4.9

Tabel 4.9 Deskripsi dan penilaian *spoofing* pada web server

Kategori	Deskripsi	Nilai
Damage	Serangan ini dapat **menyebabkan informasi kerentanan** pada sistem dapat dilihat dikarenakan sistem formulir yang tidak diproteksi.	2
Reproducibility	Serangan ini **sangat mudah** dilakukan dikarenakan pada aplikasi SIMRS tidak memiliki perlindungan dari malicious code	3
Exploitability	Serangan ini **membutuhkan orang yang sangat ahli** untuk melakukan ini karena harus memahami dengan baik aplikasi yang akan di serang	1
Affected Users	Serangan ini memiliki dampak hanya **beberapa pengguna** saja seperti pasien	2
Discoverability	Serangan ini **merupakan kerentanan umum yang mudah ditemukan pada bagian formulir** yang tidak terproteksi dengan baik sehingga serangan seperti *spoofing* dapat dengan mudah dilakukan.	3

- *Elevation Of Privilege* pada web server berbeda dengan ancaman pada bagian pengguna. Ancaman ini berfokus untuk mendapatkan hak akses penuh terhadap server. Berikut ini adalah penilaian dari *elevation of privilege* seperti pada Tabel 4.10

Tabel 4.10 Deskripsi dan penilaian *tempering* pada web server

Kategori	Deskripsi	Nilai
Damage	Serangan ini **tidak ada** potensi kerusakan dikarenakan untuk mengambil akses secara penuh harus masuk ke server lokal	1
Reproducibility	Serangan **sangat sulit** dilakukan karena sistem SIMRS memili dua server yang saling terpisah	1
Exploitability	Serangan ini **membutuhkan pengetahuan yang lebih tinggi** atau tidak bisa dilakukan oleh orang awam	1
Affected Users	Serangan ini memiliki **dampak pada sebagian pengguna** saja seperti pasien	2
Discoverability	kerentanan ini **sangat sulit** ditemukan karena akses server hanya dipegang oleh administrator	1

Berdasarkan beberapa deskripsi ancaman pada sistem SIMRS di atas dapat disimpulkan penilaian ancaman pada web server seperti pada Tabel 4.11

Tabel 4.11 Penilaian ancaman web server

Ancaman	**D**	**R**	**E**	**A**	**D**	**Total**	***Grade***
Denial Of Service	2	3	3	2	1	11	*high*
Repudiation	3	2	1	2	3	11	*high*
Tempering	2	3	1	2	2	10	*medium*
Spoofing	3	3	3	3	3	15	*high*
Elevation Of Privilege	1	1	1	2	1	7	*low*

Berdasarkan pada tabel di atas dapat diketahui kerentanan pada web server memiliki beberapa tingkatan seperti *Denial Of Service, Repudiation* dan *Spoofing* memiliki tingkatan *high,* kemudian *Elevation Of Privilege* memiliki tingkat ancaman *low* dan ancaman Tempering memiliki tingkatan *medium*. Tingkatan tersebut menunjukkan tingkat ancaman yang ada pada web server.

4.4.3 *Database*

Hasil identifikasi kerentanan pada *database* yaitu terdapat tiga kerentanan yang teridentifikasi yaitu *Denial Of Service, Tempering,* dan *Spoofing.*

- *Denial of service* merupakan serangan yang memfokuskan serangan dengan mengirim perintah simpan sehingga kapasitas database menjadi penuh. Berikut adalah deskripsi penilaian ancaman *denial of service* seperti pada Tabel 4.12

Tabel 4.12 Deskripsi dan penilaian *denial of service* pada *database*

Kategori	Deskripsi	Nilai
Damage	Serangan ini sulit dilakukan dikarenakan setiap proses pengiriman data ke *database* dibatasi teknologi API sehingga serangan ini **tidak menjadi potensi kerusakan** pada *database*	1
Reproducibility	Serangan ini bisa dilakukan namun **membutuhkan cara yang kompleks** dikarenakan terdapat dua *database* yang terpisah	2
Exploitability	Serangan ini **membutuhkan seorang yang ahli** dalam melakukan serangan	1
Affected Users	Serangan ini memiliki dampak hanya pada **sebagian pengguna saja yaitu pasien**	2
Discoverability	Kerentanan ini **sulit ditemukan** dikarenakan sebagian ada beberapa fungsi yang dapat diterapkan sebelum data tersimpan ke *database*	1

- *Tempering* merupakan serangan yang menargetkan logika aplikasi saat melakukan penyimpanan data ke *database* dengan memantau dan menganalisis parameter alamat

situs saat menyimpan data. Berikut ini adalah penilaian dari *tempering* seperti pada Tabel 4.13

Tabel 4.13 Deskripsi dan penilaian *tempering* pada *database*

Kategori	Deskripsi	Nilai
Damage	**Tidak ada** dampak yang diakibatkan dari teknik ini karena proses simpan data harus melalui API yang memiliki *token*	1
Reproducibility	Serangan ini **sangat sulit** dilakukan dikarenakan pada aplikasi SIMRS memiliki proses autentikasi yaitu menggunakan *token*	1
Exploitability	Serangan ini **membutuhkan orang yang ahli** dalam bidang teknologi untuk melakukan serangan	1
Affected Users	Hanya **sebagian pengguna** yang akan terganggu dengan serangan ini seperti *user* pasien	2
Discoverability	Serangan **sangat sulit** dilakukan kecuali *attacker* memiliki token untuk mengakses *database*	1

- *Spoofing* merupakan serangan yang menduplikasi suatu halaman atau menyisipkan *malicious code* ke dalam *form* sehingga pada saat menyimpan data *code* tersebut akan berjalan sesuai perintah. Berikut ini adalah penilaian dari *tempering* seperti pada Tabel 4.14

Tabel 4.14 Deskripsi dan penilaian *tempering* pada *database*

Kategori	Deskripsi	Nilai
Damage	Dampak dari serangan ini yaitu mengakibatkan data pasien dapat dicuri dan **digunakan untuk mengidentifikasi kerentanan** pada sistem dengan masuk menggunakan akun pasien dan mengirimkan malicious code ke dalam *database*	2
Reproducibility	Serangan ini **sangat sulit** dilakukan karena membutuhkan *token* setiap mengirim data ke *database*	1
Exploitability	Serangan ini **membutuhkan orang yang sangat ahli** untuk melakukan ini karena harus memahami dengan baik aplikasi yang akan di serang dan memiliki *token*	1
Affected Users	Serangan ini memiliki dampak hanya **beberapa pengguna** saja seperti pasien	2
Discoverability	Serangan ini **sangat sulit** dilakukan dikarenakan untuk melakukan serangan harus memiliki *token*	1

Berikut ini adalah penilaian ancaman dari semua kerentanan yang telah teridentifikasi.

Tabel 4.15 Penilaian ancaman *database*

Ancaman	**D**	**R**	**E**	**A**	**D**	**Total**	***Grade***
Denial Of Service	1	2	1	2	1	7	*medium*
Tempering	1	1	1	2	1	6	*low*
Spoofing	2	1	1	2	1	7	*medium*

Berdasarkan pada tabel di atas dapat dilihat terdapat beberapa tiga kerentanan pada *database*, dua di antaranya memiliki tingkat ancaman *medium* dan satu memiliki tingkat ancaman *low*.

Setelah proses penilaian tingkat ancaman selesai dilakukan, kemudian tahap selanjutnya yaitu proses analisis risiko keamanan yang ada pada masing-masing bagian yang dimodelkan dengan menggunakan rumus:

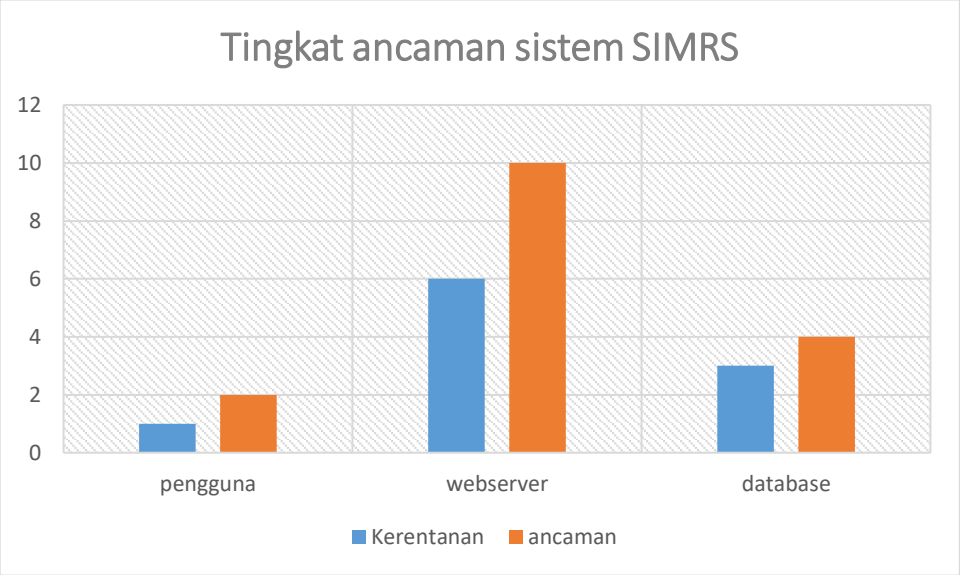
Risk = Probability * Damage Potential

Tabel 4.16 Analisis risiko ancaman

No	***Category***	***Probability***	***Damage Potential***	**Risiko Ancaman**
1.	*Spoofing*	2	10	20
2.	*Tampering*	2	10	20
3	*Repudiation*	1	10	10
4.	*Information Disclosure*	0	10	0
5.	*Denial Of Service*	2	10	20
6.	*Elevation Of Privilege*	2	10	20

Pada Tabel 4.16 dapat dilihat hasil analisis tingkat risiko yang ada pada sistem SIMRS. Terdapat enam kerentanan yang teridentifikasi yaitu *spoofing, tempring, repudation, danial of service, dan elevation of privelege*. Empat kategori memiliki risiko 20, satu kategori memiliki risiko 10 dan satu kategori tidak memiliki risiko pada sistem SIMRS dikarenakan pada tahap identifikasi kerentanan pada pemodelan ancaman, category informastion disclosure tidak ditemukan sehingga nilai probabilitas adalah nol.

Berikut adalah grafik tingkat ancaman berdasarkan bagian-bagian yang telah teridentifikasi memiliki kerentanan yaitu:



Gambar 4.7 Grafik tingkat ancaman sistem SIMRS

Berdasarkan gambar grafik di atas dapat dilihat pada bagian web server memiliki tingkat ancaman yang paling banyak dibandingkan dengan bagian yang lain dikarenakan memiliki jumlah kerentanan yang paling tingi dibandingkan dengan yang lain. Pada bagian *database* dan pengguna memiliki ancaman lebih sedikit dikarenakan kerentanan yang teridentifikasi pada bagian tersebut memiliki jumlah yang lebih sedikit dibandingkan dengan bagian web server.

4.5 Mitigasi ancaman

Mitigasi ancaman merupakan tahapan yang dilakukan untuk menanggulangi dari setiap ancaman yang telah diidentifikasi menggunakan *microsoft threat modelling tools*. Saran penanggulangan ancaman ini berdasarkan mitigasi ancaman pada *microsoft threat modelling tools*. Berikut adalah jenis ancaman serta langkah mitigasi atau penanggulangannya.

- *Elevation Of Privilege*

Tabel 4.17 Mitigasi ancaman *elevation of privilege*

Elevation Of Privilege	
Deskripsi Ancaman	Browser Client may be able to impersonate the context of Admin - Internal User in order to gain additional privilege.
Target Ancaman	Pengguna, web server
Penanggulangan	*Use secured authentication*

Tabel di atas merupakan deskripsi ancaman dengan teknik serangan *elevation of privilage* yaitu teknik mengelabui sistem berdasarkan hak akses yang dimiliki pengguna. Adapun langkah memitigasi serangan tersebut dengan melakukan doble *autentifikasi* saat melakukan *login*.

- *Denial Of Service*

Tabel 4.18 Mitigasi ancaman *denial of service*

Denial Of Service	
Deskripsi Ancaman	*Potential Excessive Resource Consumption for API or Database SIMRS*
Target Ancaman	*Web Server, database*
Penanggulangan	*Secure Your Network Infrastructure*

Tabel 4.18 merupakan tabel ancaman dengan teknik serangan *Denial of service* atau biasa disebut DDOS, target serangan yaitu web server, dan database. Teknik ini mengirimkan data ke server agar server atau database yang digunakan SIMRS menjadi penuh dan error. Cara menanggulanginya yaitu dengan meningkatkan keamanan infrastruktur jaringan.

- *Tempering*

Tabel 4.19 Mitigasi ancaman *tempering*

Tempering	
Deskripsi Ancaman	*Potential SQL Injection Vulnerability for Database SIMRS.*
Target Ancaman	*Database, web server*
Penanggulangan	*Use secured authentication*

Tabel 4.19 merupakan tabel ancaman dengan teknik serangan tempering. Teknik ini paling umum digunakan karena serangan dapat dilakukan tanpa menggunakan aplikasi langsung atau dengan menyisipkan kode ke dalam *form* untuk mendapat respons dari server. Target dari serangan ini adalah web server dan *database*. Adapun langkah untuk menanggulanginya yaitu dengan menggunakan validasi *form* dan autentikasi.

- *Spoofing*

Tabel 4.20 Mitigasi ancaman *spoofing*

Spoofing	
Deskripsi Ancaman	*Spoofing of Destination Data Store Database Biodata Pasien.*
Target Ancaman	*Database, web server*
Penanggulangan	*Don't use standard authentication mechanism*

Tabel 4.20 merupakan tabel ancaman yang terakhir yaitu ancaman yang menggunakan teknik *spoofing*, teknik ini mengelabui server dengan menempelkan halaman di depan *form input* seperti XXS dan lain sebagainya. Adapun langkah untuk menanggulanginya yaitu dengan menggunakan autentikasi yang unik atau berubah-ubah setiap waktu agar tidak dapat terdeteksi musuh.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Penelitian ini dilakukan untuk memodelkan sistem *e-health* yaitu sistem SIMRS untuk mengidentifikasi ancaman serta menganalisis tingkat ancaman pada sistem SIMRS dengan menggunakan pemodelan ancaman STRIDE dan model DREAD. Dapat disimpulkan bahwa:

1. Hasil pemodelan ancaman menggunakan *microsoft threat modelling* mampu memberikan informasi mengenai kerentanan yang ada pada sistem SIMRS seperti kerentanan pada bagian pengguna, web server dan *database*. Hanya saja terdapat beberapa notasi penghubung sistem yang masih kurang yang membutuhkan pemahaman yang baik mengenai penggunaan *microsoft threat modelling tools*.
2. Penerapan model STRIDE dan model DREAD pada penelitian ini terbukti dapat memberikan informasi terkait tingkat ancaman dari masing-masing kerentanan pada setiap bagian sehingga dapat menjadi acuan bagi pengembang aplikasi dalam meningkatkan keamanan pada sistem SIMRS.

Berdasarkan hasil identifikasi ancaman menggunakan model STRIDE dan penilaian ancaman menggunakan metode DREAD dapat disimpulkan bahwa tingkat ancaman pada masing-masing bagian seperti pengguna, web server, dan *database* memiliki tingkat ancaman paling banyak yaitu medium dan *low*. Sedangkan tingkat ancaman tertinggi *high* terdapat pada bagian *database* dengan ancaman *denial of service*. Berdasarkan hasil identifikasi dan penilaian tersebut, penanggulangan ancaman pada sistem SIMRS dapat dimulai dengan tingkat ancaman yang paling tinggi sampai tingkat ancaman yang terendah.

5.2 Saran

Dalam penelitian ini peneliti banyak menyadari bahwa masih banyak kekurangan terkait penelitian tentang pemodelan ancaman seperti,

1. Identifikasi notasi penghubung pada desain pemodelan ancaman masih kurang sehingga untuk peneliti berikutnya perlu pemahaman yang lebih tentang bagaimana mendesain *overview* sistem yang lebih baik.
2. Hasil penelitian mengidentifikasi bahwa masih banyaknya kerentanan pada sistem SIMRS saat ini sehingga dirasa perlu untuk menerapkan sistem keamanan terbaru berupa penerapan teknologi dan bahasa pemrograman yang lebih aman terhadap serangan.

Daftar Pustaka

Abomhara, M., Gerdes, M., & Køien, G. M. (2015). A STRIDE-Based Threat Model for Telehealth Systems. *NISK Journal*, *8*(January 2016), 82–96. https://www.researchgate.net/profile/Mohamed_Abomhara/publication/291766457_A_STRIDE_Based_Threat_Model_for_Telehealth_Systems/links/56a5de3208ae1b6511345e4a.pdf

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers and Security*, *74*, 323–339. https://doi.org/10.1016/j.cose.2017.09.011

Cagnazzo, M., Hertlein, M., Holz, T., & Pohlmann, N. (2018). Threat modeling for mobile health systems. *2018 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2018*, 314–319. https://doi.org/10.1109/WCNCW.2018.8369033

Chung, T., Liu, Y., Choffnes, D., Levin, D., Maggs, B. M., Mislove, A., & Wilson, C. (2016). Measuring and applying invalid SSL Certificates: The silent majority. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, *14-16-Nove*, 527–541. https://doi.org/10.1145/2987443.2987454

Destian Wijaya, B., E.M.A, F., & Fiade, A. (2015). Implementasi JSON Parsing Pada Aplikasi Mobile E-commerce Studi Kasus : CV V3 Tekno Indonesia. *Jurnal Pseudocode*, *2*(1), 1–9. https://doi.org/10.33369/pseudocode.2.1.1-9

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *Journal of Supercomputing*, *74*(10), 4986–5002. https://doi.org/10.1007/s11227-018-2337-2

Hu, W., Ardeshiricham, A., Gobulukoglu, M. S., Wang, X., & Kastner, R. (2018). Property specific information flow analysis for hardware security verification. *IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD*, 1–8. https://doi.org/10.1145/3240765.3240839

Hussain, S., Kamal, A., Ahmad, S., Rasool, G., & Iqbal, S. (2014). Threat Modelling Methodologies: a Survey. *Sci.Int.(Lahore)*, *26*(4), 1607–1609.

Ikhwan, S., & Elfitri, I. (2014). Analisa Delay Yang Terjadi Pada Penerapan Demilitarized Zone (DMZ) Terhadap Server Universitas Andalas. *Jurnal Nasional Teknik Elektro*, *3*(2), 118. https://doi.org/10.25077/jnte.v3n2.75.2014

Jaliyanti, D. (2018). Analisis Penerapan E-Health Sebagai Perwujudan Pelayanan Prima di Puskesmas Peneleh Kecamatan Genteng Kota Surabaya. *Jurnal Administrasi*

Perkantoran, *6*(2), 26–34. https://jurnalmahasiswa.unesa.ac.id/index.php/JPAPUNESA/article/view/25679/23542

Jamal, T., Haider, Z., Butt, S. A., & Chohan, A. (2018). *Denial of Service Attack in Cooperative Networks*. 10–13. https://doi.org/10.31224/osf.io/smdax

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017). STRIDE-based Threat Modeling for Cyber-Physical Systems. *IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 1–6. https://doi.org/10.1109/ISGTEurope.2017.8260283

Markoferdiansalim. (2019, Juli 17). *SIMRS dan Strategi Pengadaannya*. Diambil kembali dari Menara Ilmu Manajemen Informasi Kesehatan Universitas Gadjah Mada: https://mik.sv.ugm.ac.id/2019/07/17/simrs-dan-strategi-pengadaannya/

McDermott, D. S., Kamerer, J. L., & Birk, A. T. (2019). *Electronic Health Records : A Literature Review of Cyber Threats and Security Measures*. *1*(2), 42–49. https://doi.org/10.4018/IJCRE.2019070104

Meier, J. D., Mackman, A., Vasireddy, S., Dunner, M., Escamilla, R., & Murukan, A. (2003). *Improving Web Application Security : Threats and Countermeasures* (1st ed.). Microsoft Corporation. https://www.microsoft.com/en-us/download/confirmation.aspx?id=1330

Mikail, O. O., Alhassan, J., Abba, E., & Waziri, V. O. (2016). Threat Modeling of Electronic Health Systems and Mitigating Countermeasures Big Data & Cyber-Physical Systems in Water, Energy and Food Nexus View project Online System for Vehicle Ownership Tracking and Theft Alert With Community Participation View proje. *Conference: International Conference on Information and Communication Technology and Its Applications*, 82–89. https://www.researchgate.net/publication/311238739

Prajapati, P., Patel, N., & Shah, P. (2019). A review of recent detection methods for HTTP ddos attacks. *International Journal of Scientific and Technology Research*, *8*(12), 1693–1696.

Sim, C. J., Kim, W. Il, Kim, H. J., & Lee, C. H. (2017). A Method of Detecting Real-Time Elevation of Privilege Security Module Using User Credentials. *KIPS Transactions on Computer and Communication Systems*, *6*(5), 247–254. https://doi.org/10.3745/ktccs.2017.6.5.247

Sion, L., Yskout, K., Van Landuyt, Di., Van Den Berghe, A., & Joosen, W. (2020). Security Threat Modeling: Are Data Flow Diagrams Enough? *Proceedings - 2020 IEEE/ACM*

42nd International Conference on Software Engineering Workshops, ICSEW 2020, 254–257. https://doi.org/10.1145/3387940.3392221

Sivula, A. (2015). *Security Risk and Threat Models for Health Care Product Development Processes* [School of Technology and Transport]. https://core.ac.uk/download/pdf/38131677.pdf

LAMPIRAN

1. Pedoman penilaian dengan model DREAD

Berikut ini adalah pedoman perhitungan sistematis dalam model DREAD berdasarkan pada penelitian yang dilakukan (Sivula, 2015) yaitu:

- Potensi Kerusakan (*Damage*) merupakan potensi kerusakan jika ancaman terjadi.

Tabel 1 Potensi Kerusakan (*Damage*)

Nilai	Potensi Kerusakan
1	Tidak ada
2	Mendapatkan informasi terkait kerentanan lainnya
3	Data pengguna yang mudah disusupi, Data admin dapat di ambil dengan mudah, dan Data bisa dihapus atau Aplikasi tidak bisa di akses

- Dapat direproduksi (*Reproduciblity*) adalah seberapa mudah dalam melakukan eksploitasi ancaman.

Tabel 2 Dapat direproduksi (*Reproduciblity*)

Nilai	Potensi Kerusakan
1	Sangat sulit atau tidak mungkin
2	Membutuhkan cara yang kompleks untuk melakukan serangan
3	Mudah untuk pengguna yang di autentikasi, Hanya dengan browser web atau manipulasi alamat web

- Kemampuan eksploitasi (Exploitability) adalah tingkat pengetahuan seseorang yang dibutuhkan untuk melakukan serangan

Tabel 3 Kemampuan eksploitasi (*Exploitability*)

Nilai	Potensi Kerusakan
1	Membutuhkan pengetahuan pemrograman dan jaringan tingkat lanjut, dengan alat serangan khusus atau lanjutan
2	Menggunakan *backdoor* atau alat bantu serangan yang sudah ada
3	Alat Proksi Aplikasi Web atau Hanya dengan browser web

- Pengguna yang terkena dampak (*Affected Users*) merupakan apakah serangan berdampak langsung bagi pengguna.

Tabel 4 Pengguna yang terkena dampak (*Affected Users*)

Nilai	Potensi Kerusakan
1	Tidak ada
2	Hanya individu, Beberapa pengguna tetapi tidak semua
3	Semua pengguna termasuk admin

- Kemampuan menemukan (*Discoverability*) merupakan tingkat kemudahan dalam menemukan ancaman.

Tabel 5 Kemampuan menemukan (*Discoverability*)

Nilai	Potensi Kerusakan
1	Sangat sulit
2	Dapat diketahui dengan memantau dan memanipulasi HTTP *request*
3	Kerentanan sudah umum dan dapat ditemukan dengan mudah menggunakan mesin pencari dan Informasi terlihat di bilah alamat browser web atau dalam formulir