e-ISSN 2549-7472
Edumatic: Jurnal Pendidikan Informatika
Vol. 5 No. 2, Desember, 2021, **Hal. 157-166**
DOI: 10.29408/edumatic.v5i2.3652

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

Muhammad Khairul Faridi*[1], Imam Riadi[2], Yudi Prayudi[3]
[1,3] Program Studi Informatika, Universitas Islam Indonesia
[2] Program Studi Sistem Informasi, Universitas Ahmad Dahlan
email: 17917115@students.uii.ac.id *[1], imam.riadi@is.uad.ac.id[2], prayudi@uii.ac.id[3]

(Received: 13 Juni 2021 / Accepted: 15 Juli 2021/ Published Online: 20 Desember 2021)

Abstrak

Sistem Informasi Manajemen Rumah Sakit (SIMRS) sebagai media informasi dan manajemen Rumah Sakit menyimpan banyak data sensitif, sehingga keamanan pada SIMRS sangat perlu ditingkatkan untuk menjaga data pengguna dan pasien tetap aman dari *attacker.* Terdapat beberapa cara untuk meningkatkan keamanan sistem yang salah satunya dengan memodelkan ancaman. Penelitian ini bertujuan untuk mengidentifikasi kerentanan dan ancaman yang ada pada SIMRS. Pada penelitian ini, pemodelan ancaman menggunakan metode STRIDE dan DREAD. Metode STRIDE digunakan untuk mengidentifikasi kerentanan yang ada pada sistem SIMRS dan metode DREAD digunakan untuk menganalisis tingkat ancaman dari setiap kerentanan yang teridentifikas. Hasil identifikasi yang telah dilakukan dengan metode STRIDE menunjukkan terdapat beberapa ancaman yang teridentifikasi seperti pada bagian pengguna terdapat satu ancaman, web server lima ancaman dan database tiga ancaman. Adapun hasil analisis tingkat ancaman dengan metode DREAD menujukan ancaman yang ada pada SIMRS bervariasi dari tingkat terendah *low* sampai tingkat tertinggi yaitu *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: Pemodelan Ancaman, STRIDE, DREAD, SIMRS, *security identification*

Abstract

The Hospital Management Information System (SIMRS) functions as a medium for hospital information and hospital management. There are patient medical record data, which is the result of interactions between doctors and sufferer. Medical records are sensitive data so that the security of the hospital management information system needs to be improved to convince users or patients that the data stored on SIMRS is safe at attackers. There are several ways to improve system security, one of which is by threat modeling. This study aims to identify vulnerabilities and threats that exist in SIMRS. In this paper, threat modeling will use the STRIDE-model. The recognition with the STRIDE-model will then be analyzed and sorted according to the modeling with the STRIDE method. After the analysis is complete, it will be calculated and given a rating based on the DREAD method's assessment. The STRIDE method's results show that there are several threats identified, such as there is one threat on the user side, the webserver is five threats, and the database is three threats. The level of the threat varies from the lowest-level (LowL) to the highest-level (HiL). Based on the threat level, it can be a guide and sequence in improving and improving the security system at SIMRS, starting from the LowL to the HiL.

Keywords: *Threat Modelling*, STRIDE, DREAD, SIMRS, *Security Identification*

PENDAHULUAN

Timbulnya ancaman dalam sebuah sistem aplikasi disebabkan oleh kesalahan yang muncul pada saat mendesain dan mengembangkan aplikasi (Hussain et al., 2014). Menurut

Badan Siber dan Sandi Negara mencatat bahwa pada bulan Mei 2019 terdapat 1,9 juta serangan siber yang menyerang fasilitas negara dan non negara seperti industri dan kesehatan.

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). Secara garis besar *e-health* terbagi menjadi tiga bagian berdasarkan implementasi teknologi dalam layanan kesehatan yaitu *telehealth, telemedicine* dan *health informatics*(Cilliers & Flowerday, 2013). 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(Mikail et al., 2016).

Meningkatkan sistem keamanan dapat dilakukan dengan beberapa tahapan seperti mengidentifikasi celah keamanan (Suradi & Prasetyo, 2015). Menurut (Hussain et al., 2014) sistem keamanan terbagi menjadi dua kategori yaitu sistem keamanan *software* dan sistem keamanan *hardware*. Permasalahan pada sistem keamanan *software* tergantung pada bagaimana sistem tersebut di bangun dan salah satu cara untuk mengetahuinya yaitu dengan mengidentifikasi ancaman dan risiko. Terdapat beberapa metode yang dapat digunakan untuk identifikasi ancaman (Sivula, 2015) dan (Sion et al., 2020) 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 penanggulangan dalam konteks melindungi sesuatu yang bernilai(Abomhara et al., 2015). Terdapat beberapa penelitian terdahulu yang meneliti tentang pemodelan ancaman seperti penelitian yang dilakukan oleh (Mikail et al., 2016) memitigasi sistem keamanan kesehatan dengan menggunakan pemodelan STRIDE, hasil identifikasi kemudian dinilai menggunakan metode DREAD. Hasil 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. Peneliti (Cagnazzo et al., 2018) meneliti keamanan melatah 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 penanggulangan ancaman pada sistem m-*health*. Omotosho et al., (2019) juga meneliti tentang perangkat kesehatan yang terkoneksi dengan *Internet of things* (IoT). Penelitian mereka 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.

Dua peneliti lain juga meneliti tentang keamanan sistem e-*health* dengan metode MBT(Vernotte et al., 2015) dan STRIDE(Abomhara et al., 2015), masing-masing meneliti tentang meningkatkan keamanan e-*health* berbasis web. Dan penanggulangan keamanan sistem *telehealth*.

Berdasarkan dari uraian penelitian-penelitian di atas, pada makalah ini akan melakukan pemodelan ancaman dengan menggunakan metode STRIDE dikarenakan metode ini

merupakan model ancaman yang banyak digunakan karena lebih mudah di aplikasikan, selain itu model ini lebih ringan dan efektif dalam melakukan identifikasi kerentanan (Khan et al., 2017) selain itu, metode ini sesuai dengan permasalahan yang akan diteliti. Sedangkan dalam mengidentifikasi kerentanan menggunakan metode DREAD dikerenakan selain mengidentifikasi kerentanan juga akan dilakukan penilaian tingkat ancaman dari masing-masing kerentanan.

METODE

Dalam penelitian perlu disusun langkah-langkah penyelesaian dalam penelitian secara sistematika. Berikut ini adalah langkah-langkah penelitian yang terlihat pada gambar 1. Berdasarkan gambar 1, Studi literatur bertujuan untuk mengumpulkan referensi atau bahan-bahan yang akan digunakan dalam penelitian, baik melalui buku artikel, jurnal dan segala sesuatu yang berkaitan dengan pemodelan ancaman. *Overview sistem e-health* merupakan proses visualisasi sistem e-health. 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.

Gambar 1. Alur Penelitian

Identifikasi ancaman sistem merupakan tahap untuk mengidentifikasi ancaman yang mungkin membahayakan sistem yang telah dibangun dengan menggunakan model STRIDE. Analisis ancaman merupakan penilaian ancaman menggunakan metode DREAD. Risiko akan diukur berdasarkan tingkat kerusakan yang dapat terjadi dengan konversi menjadi tiga tingkatan yaitu 1 adalah low, 2 adalah medium dan 3 adalh high. 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. Mitigasi ancaman merupakan proses identifikasi ancaman yang telah dikenali pada sistem kemudian bagaimana langkah untuk mitigasi ancaman tersebut berdasarkan mitasi dari microsoft threat modelling tools.

HASIL DAN PEMBAHASAN

Hasil

Berdasarkan hasil penelitian yang telah dilakukan terdapat beberapa temuan yang didapatkan seperti detail aktivitas pengguna beserta data yang di akses, arsitektur sistem SIMRS, teknologi yang diterapkan, pemodelan ancaman, dan ancaman-ancaman yang terdapat pada sistem. Berikut ini adalah gambaran dan penjelasan dari hasil penelitian yang telah dilakukan.

Aktivitas pengguna

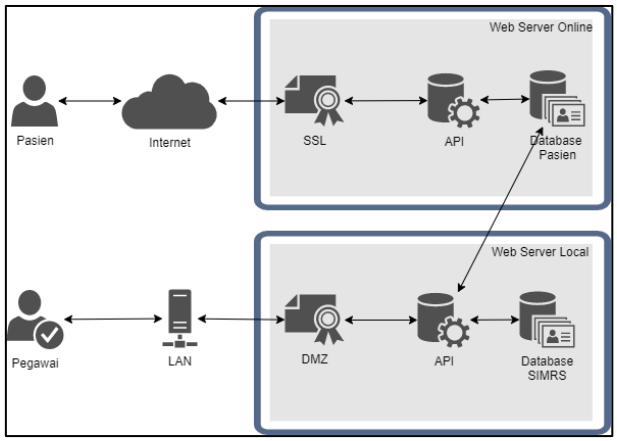
Berikut adalah hasil identifikasi aktivitas pengguna pada aplikasi *e-health* seperti pada tabel 1 di bawah ini

Tabel 1. Aktivitas Aplikasi E-*Health*

Pengguna	***Aktivitas***	***Data***
Karyawan	*Mengelola data pegawai*	*Pegawai*
	Mengelola data pembayaran	*keuangan*
	Mengelola data pasien	*Pasien*
Dokter	*Mengelola data hasil diagnosa*	*Rekam medis*
	Mengelola resep obat	*Obat*
	Mengelola data rekam medis	*Rekam medis*
	Melihat data pasien	*Pasien*
Pasien	*Melakukan registrasi pasien*	*Pasien*
Admin	*Mengelola data pengguna*	*Pengguna*
	Mengelola log aktivitas pengguna	*Log*

Diagram Arsitektur Sistem Aplikasi SIMRS

Berikut ini adalah hasil *overview* arsitektur sistem SIMRS seperti tampak pada gambar 2.



Gambar 2. Diagram Arsitektur

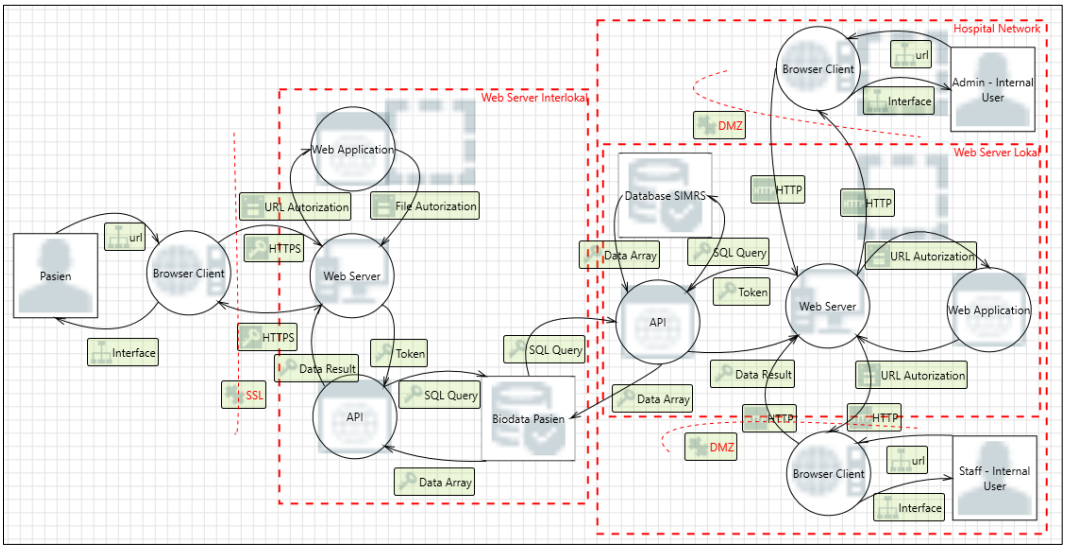
Teknologi

Berdasarkang gambar 1 dapat disimpulkan terdapat beberapa teknologi yang di terapkan pada sistem SIMRS seperti yang terlihat pada tabel 2.

Pemodelan ancaman sistem *e-health*

Hasil perancangan pemodelan ancaman sistem *e-health* didapatkan dari *overview* sistem *e-health* seperti hasil identifikasi aktivitas pengguna, diagram arsitektur sistem dan teknologi yang digunakan. Untuk lebih jelas berikut ini adalah gambar pemodelan ancaman sistem e-health. Pada gambar 3, SIMRS memiliki dua kondisi server yaitu server interlokal dan local, server interlokal hanya dapat di akses oleh pengguna umum atau pasien. Sedangkan server local dapat di akses oleh pegawai dan staff yang tersambung dengan jaringan rumah sakit. Masing-masing server telah menerapkan sistem keamanan dasar seperti penggunaan SSL pada server interlokal dan DMZ pada server lokal. Kedua server tersebut terhubung dengan penggunakan teknologi API yaitu teknologi yang menghubungkan database lokal dengan database interlokal.

Berdasarkan hasil analisis dengan menggunakan pemodealan STRIDE didapatkan sembilan kerentanan yang teridentifikasi yang tersebar pada beberapa bagian seperti pengguna, webserver dan database.



Gambar 3. Hasil Pemodelan SIMRS

Tabel 2. Identifikasi Teknologi

Teknologi	Detail Implementasi
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.
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).
API	API merupakan sebuah interface yang dapat menghubungkan aplikasi satu dengan aplikasi lainnya(Destian Wijaya et al., 2015) seperti pada gambar 3 api berfungsi untuk menghubungkan aplikasi yang berada pada server lokal dengan aplikasi yang berada pada server online.
PHP	Bahasa pemrograman yang digunakan dalam mengembangkan aplikasi SIMRS adalah PHP 5.
SQL	Database yang diterapkan pada aplikasi SIMRS adalah SQL-based.

Pengguna

Hasil identifikasi pada bagian pengguna terdapat satu ancaman yaitu *elevation of privilege.* Ancaman ini dapat menyebabkan hilangnya integritas pada pengguna. Adapun tingkat ancaman pada bagian pengguna yaitu *medium* berdasarkan perhitungan pada analisis ancaman.

Web server

Hasil identifikasi pada bagian web server terdapat satu ancaman yaitu *denial of service, repudiation, tempering spoofing dan elevation of privilege.* Adapun tingkat ancaman pada web server yaitu *medium* berdasarkan perhitungan pada analisis ancaman.

Database

Hasil identifikasi pada bagian database terdapat satu ancaman yaitu *Denial Of Service, Tampering dan spoofing*. Adapun tingkat ancaman pada database adalah *medium* berdasarkan perhitungan pada analisis ancaman.

Berdasarkan hasil identifikasi pemodelan yang telah dibuat terdapat perbedaan hasil penelitian yang dilakukan oleh peneliti sebelumnya (Mikail et al., 2016) yaitu hasil identifikasi pada penelitian sebelumnya hanya terbatas pada ancaman yang ada pada aplikasi saja sehingga saran yang diberikan terbatas pada perbaikan pada sistem aplikasi, sedangkan hasil penelitian ini memiliki cakupan yang lebih luas, identifikasi tidak hanya dilakukan pada sisi aplikasi saja namun juga dari sisi arsitektur dan sistemnya.

Pembahasan

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 diimplantasikan di sebagian 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.

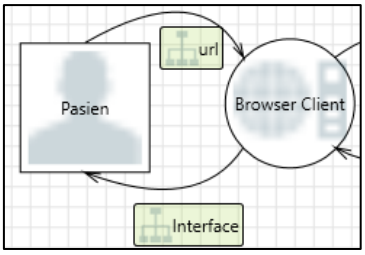
Identifikasi aktivitas pengguna pada sistem SIMRS memiliki banyak pengguna namun pada penelitian ini akan disederhanakan menjadi beberapa pengguna seperti karyawan, dokter, pasien dan admin. Semua pengguna adalah pengguna yang mengakses aplikasi SIMRS secara langsung. Diagram Arsitektur Sistem Aplikasi 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. Untuk lebih jelasnya dapat dilihat pada diagram arsitektur sistem SIMRS pada gambar 2. Pada diagram tersebut 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

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.

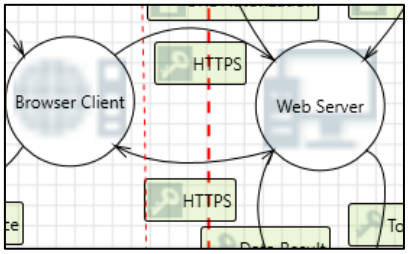
Identifkasi dan Dokumentasi Ancaman

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*.

Hasil pemodelan kerentanan yang telah dilakukan sebelumnya dapat dilihat terdapat tiga bagian yang teridentifikasi rentan yitu bagian pengguna, web server dan pada database. Hasil identifikasi pada bagian pengguna terdapat satu kerentanan yaitu *Elevation Of Privilege.* Pada gambar 4 terdapat pengguna dengan level pasien mengases SIMRS dengan mengirimkan url ke browser client dan bowser client merespon dengan menampilkan intaface. Pada proses ini *attacker* dapat melakukan penyerangan kedalam sistem dengan melakukan pengamatan pada url dan kemudian merubah url tersebut menjadi url pengguna lain. Hal tersebut diakibatkan oleh tidak adanya peroses autorisasi level pengguna serta format url yang mudah ditebak.

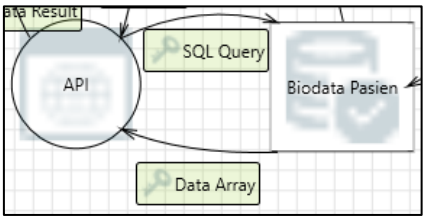


Gambar 4. Hasil Identifikasi pada Bagian Pengguna



Gambar 5. Hasil Identifikasi pada Bagian Web Server

Berdasarkan hasil identifikasi dengan metode STRIDE terdapat beberapa kerentanan yaitu *Denial Of Service, Repudiation, Tempering Spoofing dan Elevation Of Privilege.* Seperti pada gambar 5, kerentantanan tersebut teridentifikasi dikareankan tidak adanya sistem keamanan seperti form validation pada browser client untuk menanggulangi DDoS, penggunaan anti click jacking pada browser client sebelum mengirimkan request ke webserver.



Gambar 6. Hasil Identifikasi pada Bagian Database

Pada bagian database yang Nampak pada gambar 6, terdapat 3 ancaman yang di identifikasi pada sistem database yaitu *Denial Of Service, Tampering* dan *spoofing.* Kerentanan tersebut disebabkan oleh API Key yang dipublikasiskan dan API Key yang mudah ditebak sehingga data yang tersimpan pada database dapat diakses oleh orang lain.

Analisis Ancaman

Penilaian ancaman merupakan proses akhir yang akan dilakukan dalam makalah ini. Berikut adalah penilaian terhadap ancaman-ancaman yang telah di identifikasi. Penilaian akan menggunakan model DREAD. Penilaian DREAD merupakan penilaian berdasarkan skala yang telah ada pada DREAD. Pemberian skala dilakukan berdasarkan pada hasil analisis dan asumsi peneliti. Skala diberikan berdasarkan tingkat ancaman dan kerusakan pada sistem seperti 1 yaitu ancaman sulit dilakukan; 2 yaitu ancaman agak sulit dilakukan dan membutuhkan orang memiliki pengetahuan lebih untuk melakukan ancaman tersebut; 3 yaitu ancaman mudah diterapkan dan tidak membutuhkan orang yang ahli untuk melakukakan penyerangan tersebut. Setalah skala DREAD diberikan kemudian dilakukan proses peringkat dari masing-masing ancaman dengan total skala dibagi lima. Jika hasil bagi adalah 1 maka gradenya adalah low. Jika hasil bagi mendekati 2 maka gradenya adalah medium dan jika hasil bagi mendekati 3 grade nya adalah high (Sivula, 2015).

Berikut merupakan hasil identifikasi ancaman secara menyeluruh seperti yang terlihat pada tabel 3. Berdasarkan pada tabel 3, dapat diketahui bahwa ancaman *elevation of provilage*

pada pengguna medium. Selanjutnya Berdasarkan pada tabel 4, dapat diketahui bahwa ancaman pada web server tinggi. Dikarenakan begaian ancaman dapat diterapkan dan sebagian memiliki tingak ancaman low dan medium

Tabel 3. Penilaian Ancaman Pengguna

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

Tabel 4. 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*

Tabel 5. 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 5, dapat diketahui bahwa ancaman pada web sever medium. Dikarenakan sebagian ancaman dapat ditemukan namun harus memiliki pengetahuan yang lebih untuk melakukan serangan. Setelah hasil analisis ancaman selesai kemudian akan dilakukan identifikasi risiko keamanan dengan menggunakan rumus atau persamaan (1).

$$\text{Risk} = \text{Probability} * \text{Damage Potential} \quad (1)$$

Tabel 6. Nilai Risiko Ancaman

Category	Probability	Damage Potential	Risiko Ancaman
Spoofing	2	10	20
Tampering	2	10	20
Repudiation	1	10	10
Information Disclosure	0	10	0
Denial of Service	2	10	20
Elevation of Privilege	2	10	20

Pada tabel 6 dapat dilihat hasil identifikasi ancaman menemukan beberapa ancaman seperti *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 e-health.

Mitigasi ancaman

Tahapan ini berisi mitigasi ancaman dari ancaman terdeteksi menggunakan *microsoft threat modelling tools*. Berikut adalah jenis ancaman serta mitigasi atau penanggulangannya. Tabel 7, merupakan deskripsi ancaman dengan teknik serangan *elevation of privilage* yaitu teknik untuk mengelabui sistem berdasarkan hak akses yang dimiliki pengguna. Adapun langkah memitigasi serangan tersebut dengan melakukan doble *autentifikasi* saat melakukan *login.*

Tabel 7. Mitigasi Ancaman *elevation of privilege*

Category	***Probability***
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 8. Mitigasi Ancaman *denial of service*

Category	***Probability***
Deskripsi ancaman	*Potential Excessive Resource Consumption for API or Database SIMRS*
Target Ancaman	*Web Server, database*
Penanggulangan	*Secure Your Network Infrastructure*

Tabel 8 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 agar database yang digunakan SIMRS menjadi penuh dan *error*. Cara menanggulanginya yaitu dengan meningkatkan keamanan infrastruktur jaringan.

Tabel 9. Mitigasi Ancaman *tempering*

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

Tabel 9 merupakan tabel ancaman yang ketiga dengan teknik serangan yaitu *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 otentikasi.

Tabel 10. Mitigasi Ancaman *Spoofing*

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

Tabel 10 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.

SIMPULAN

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.

REFERENSI

Abomhara, M., Køien, G. M., & Gerdes, M. (2015). A STRIDE-Based Threat Model for Telehealth Systems. *NISK Journal*, 82–96.

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

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.

Cilliers, L., & Flowerday, S. V. (2013). Health information systems to improve health care: A telemedicine case study. *SA Journal of Information Management*, *15*(1), 1–5.

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.

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.

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.

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.

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.

Omotosho, A., Ayemlo Haruna, B., & Mikail Olaniyi, O. (2019). Threat modeling of Internet of Things health devices. *Journal of Applied Security Research*, *14*(1), 106–121.

Sion, L., Yskout, K., Van Landuyt, Di., Van Den Berghe, A., & Joosen, W. (2020). Security Threat Modeling: Are Data Flow Diagrams Enough?. *International Conference on Software Engineering Workshops, ICSEW 2020*, 254–257. IEEE.

Sivula, A. (2015). *S*ecurity Risk and Threat Models for Health Care Product Development Processes. *Master Thesis*. JAMK Unviersity of Applied Sciences.

Suradi, A., & Prasetyo, H. J. (2015). Contingency Planning pada Website Universitas Widya Dharma. *Jurnal Teknologi Informasi*, *10*(29), 1–12.

Vernotte, A., Botea, C., Legeard, B., Molnar, A., & Peureux, F. (2015). Risk-Driven Vulnerability Testing: Results from eHealth Experiments Using Patterns and Model-Based Approach. *International Workshop on Risk Assessment and Risk-Driven Testing*, *3*, 93–109.