Pemodelan Ancaman Stride/Dread Pada Sistem Diseminasi Terintegrasi

Harry Kartono[1], Ruki Harwahyu[2]
[1) 2)] Teknik Elektro, Universitas Indonesia
E-mail: [1]**harry.kartono@ui.ac.id**, [2]ruki.h@ui.ac.id

Abstrak

Implementasi sistem yang terintegrasi seperti SDT (Sistem Diseminasi Terintegrasi) memudahkan pengguna untuk menyelesaikan pekerjaan yang sudah ada . Sistem yang terintegrasi juga membuat proses bisnis semakin cepat , efisien dan terotomasi karena adanya tukar data antar mesin . Tetapi dengan integrasinya beberapa sistem menjadi satu sistem besar maka rumit suatu sistem akan bertambah dan juga ancaman juga semakin banyak . Pemodelan ancaman adalah suatu metodologi untuk kebaikan suatu ancaman , penisian risiko , dan langkah penanggulangan agar ancaman yang timbul tidak mengganggu suatu proses bisnis dalam sistem . Pemodelan ancaman pada SDT ini memiliki beberapa tahap , tahap awal adalah dekomposisi sistem-sistem penyusun SDT, integrasi komponen antar sistem , klasifikasi ancaman berdasarkan STRIDE, penilian risiko berdasarkan DREAD, dan pemilihan perbaikan tiap kelompok komponen . Tahapan-tahapan ini menghasilkan klasifikasi ancaman , serta penisian risiko tiap komponen pada sistem-sistem di SDT. Komponen yang paling banyak ancaman dan paling berisiko terhadap ancaman adalah komponen Webserver Mediator, Webserver Diseminasi dan Webserver Portalpublikasi . Ancaman tertinggi pada tiga komponen di tersebut adalah peningkatan keistimewaan. Dari hasil klasifikasi ancaman dan penilian risiko maka ditentukan langkah pengaturan pada komponen ketiga Webserver untuk meminimalkan potensi ancaman.

.

Kata Kunci*— model ancaman , sistem terintegrasi , langkah, ketakutan.*

1. PENDAHULUAN

Saat ini, teknologi telah menjadi kebutuhan penting bagi organisasi. Transformasi digital sangat diperlukan untuk menyederhanakan proses bisnis organisasi [1]. Sistem informasi yang efektif dan berkualitas memberikan dampak positif bagi pengelola dan pengguna [2], [3]. Dalam beberapa kasus, proses bisnis tidak dapat dijalankan hanya dengan menggunakan satu sistem informasi. Beberapa sistem informasi perlu diintegrasikan untuk menjalankan proses bisnis secara efisien [4]. Sistem Diseminasi Terintegrasi (SDT) adalah sistem yang menggabungkan sistem arsip publikasi dan sistem Diseminasi. sistem mediator web tengah menjembatani sistem-sistem tersebut agar proses bisnis diseminasi berjalan dengan efisien. Awalnya, sistem arsip publikasi dan sistem diseminasi web dipisahkan. Pengolah data mengunggah publikasi ke sistem arsip publikasi, sistem diseminasi web, dan sistem lain yang memerlukan publikasi. File publikasi diunggah bersama dengan judul publikasi, gambar sampul dan abstrak publikasi . Jika terdapat 5 sistem yang membutuhkan hasil publikasi, pengolah data harus mengunggah publikasi sebanyak lima kali pada sistem yang berbeda. Pekerjaan yang berulang membuat pemroses data melakukan banyak kesalahan [5]. Mulai dari salah upload file publikasi, salah upload cover image, salah insert abstract hingga koneksi internet yang tidak stabil di kantor cabang. Di sisi server, banyak sistem yang memiliki file duplikasi, sehingga membuat sistem menjadi lambat.

SDT dibuat dengan menggunakan tiga sistem utama dengan tujuan untuk memfasilitasi publikasi pengarsipan pengolah data dan mensosialisasikannya dalam satu langkah. Mediator Web akan mendistribusikan metadata publikasi, seperti judul, gambar sampul, abstrak, dan lokasi file ke sistem yang sudah terhubung ke SDT. Di sisi server, SDT juga mengurangi duplikasi data dan sistem berjalan lebih efisien. SDT memprioritaskan integrasi pertukaran data mesin-ke-mesin untuk memastikan proses pengunggahan, penyimpanan, pengindeksan, dan penyebaran materi yang efisien dan lancar . Berbagai solusi dari literatur menawarkan model yang berbeda untuk pertukaran data mesin-ke-mesin [6]–[8]. Karena sistem terintegrasi seperti SDT menjadi lebih kompleks, demikian pula tantangan mengamankan aset pada sistem [9]untuk memastikan proses bisnis berjalan dengan lancar. Pengamanan aset pada sistem juga mempengaruhi reputasi organisasi, semakin aman aset maka semakin efisien sistem berjalan, dan reputasi organisasi terjaga dengan baik dalam pengamanan data pada sistem [10]. Oleh karena itu, analisis keamanan dan risiko sangat penting dalam menentukan mitigasi yang efektif dalam sistem yang dibangun [11].

Dalam SDT, data memainkan peran penting sebagai objek dalam transaksi. Beberapa data gratis, dan beberapa berbayar. Pada data berbayar hanya beberapa orang saja yang diperbolehkan mengakses data tersebut. Salah satu peran SDT adalah mengelola data gratis dan berbayar agar kedua data tersebut aman. Banyak ancaman siber yang menyerang data dan melanggar aspek *Confidentiality*, *Integrit*y, and *Availability* (CIA). karenanya setiap potongan data membutuhkan tingkat keamanan tertentu [12]. Identifikasi ancaman dan dampaknya terhadap sistem dilakukan dengan menggunakan pemodelan ancaman. SDT sangat membutuhkan pemodelan ancaman untuk mengamankan aset dan integrasi antar sistem. Literatur yang ada telah merekomendasikan perlunya model pengambilan keputusan untuk mengatasi kerentanan, ancaman, kemungkinan, dan pendekatan pendukung keputusan untuk memutuskan investasi keamanan siber yang dapat melindungi data dan jaringan. [13].

Menggunakan pemodelan ancaman dalam sistem terintegrasi dapat membantu mengidentifikasi ancaman keamanan dan potensi pelanggaran privasi di berbagai aset dalam sistem [14]. Dengan menerapkan model ancaman ke sistem terintegrasi, akan memungkinkan untuk melakukan penilaian risiko dan pengujian keamanan yang lebih efektif [15]. Menerapkan model ancaman untuk sistem terintegrasi memiliki keuntungan memperkuat fokus pada hasil serangan potensial [16]. Namun, tugas mengintegrasikan dan menganalisis semua sistem informasi yang terkait dengan ini bisa menjadi tantangan yang signifikan [17]. STRIDE/DREAD adalah metode klasifikasi serangan siber yang dikembangkan oleh Microsoft [18]. STRIDE adalah singkatan dari *Spoofing*, *Tampering*, *Repudiation*, *Information disclosure*, *Denial of service*, dan *Elevation of privileges* [19]. DREAD adalah salah satu model penilaian risiko dunia maya yang dikembangkan oleh Microsoft [20], [21]. DREAD memiliki lima variabel untuk menilai risiko [22]. Variabelnya adalah *Damage, Reproducibility, Exploitability, Affected user*, dan *Discoverability*. Klasifikasi ancaman berdasarkan model ancaman STRIDE memudahkan pengelompokan ancaman sehingga membantu pengembang sistem melindungi sistem yang telah dibuat atau yang akan dibuat [21]. Setidaknya pemodelan ancaman STRIDE telah digunakan dalam sistem tertanam otomotif untuk membantu dalam menentukan persyaratan keamanan dan langkah-langkah untuk sistem tersebut [23]. STRIDE digunakan untuk pemodelan ancaman pada

Cyber-Physical System [24]seperti jaringan distribusi air, jaringan pembangkit listrik. Sistem Informasi Manajemen Rumah Sakit menggunakan STRIDE/DREAD untuk mengidentifikasi ancaman dan penilaian risiko [25].

SDT terdiri dari sistem terintegrasi. Sistem Portalpublikasi menangani pengolahan data untuk unggah dan pengarsipan publikasi. sistem Web Mediator menangani mesin/*server* lain yang membutuhkan data publikasi dari Portalpublikasi . Web Diseminasi menangani pengguna yang membutuhkan data publikasi dari Portalpublikasi . Kompleksitas SDT membutuhkan pemodelan ancaman yang sesuai dengan sistem terintegrasi. Tidak ada literatur yang mengkaji pemodelan ancaman untuk sistem terintegrasi. Hal ini menjadikan pekerjaan ini sangat penting bagi publik untuk membangun sistem informasi yang terintegrasi dan modular. Makalah ini berisi pengantar pengantar dan latar belakang membuat karya ini. Metode penelitian berisi metode dan alat yang kami gunakan untuk menerapkan pemodelan ancaman pada SDT. Hasil dan pembahasan berisi hasil dari setiap metode yang kami gunakan, dan pembahasan untuk mengusulkan mitigasi penilaian risiko tertinggi untuk komponen. Kesimpulan berisi motivasi, kesimpulan, dan pekerjaan masa depan.

2. METODE PENELITIAN

Dalam penelitian ini, kami mengusulkan 5 metode untuk menerapkan pemodelan ancaman pada SDT. Gambar 1 adalah langkah-langkah utama yang digunakan dalam pemodelan ancaman di SDT. Langkah pertama adalah dekomposisi sistem yang membangun SDT, langkah kedua mengintegrasikan komponen antar sistem sehingga sistem dalam SDT terhubung. Langkah ketiga adalah mengklasifikasikan ancaman terhadap komponen SDT berdasarkan klasifikasi STRIDE dan kemudian penilaian risiko menggunakan metode DREAD. Langkah terakhir adalah mitigasi risiko berdasarkan jumlah ancaman tertinggi pada komponen dengan penilaian risiko tertinggi.

Gambar 1. Pemodelan Ancaman pada SDT

2.1. Dekomposisi Sistem di SDT

Langkah awal dalam pemodelan ancaman SDT adalah dekomposisi sistem yang membangun SDT. DFD (Data Flow Diagram) digunakan dalam melakukan langkah ini. Data Flow Diagram (DFD) adalah metode untuk menganalisis desain terstruktur [26]. DFD adalah cara visual untuk menggambarkan model logis yang menunjukkan transformasi data. Tujuan dari dekomposisi sistem adalah untuk mengidentifikasi semua aset, terutama yang penting, di dalam sistem [27]. Selain itu, dekomposisi sistem juga bertujuan untuk mengidentifikasi potensi kerentanan keamanan pada komponen seperti aliran data, penyimpanan data, dan batas kepercayaan sistem. DFD digunakan untuk memfokuskan aliran data pada perangkat lunak dan mengidentifikasi potensi kerentanan keamanan pada komponen seperti aliran data, penyimpanan data, dan batas kepercayaan sistem karena banyaknya serangan yang menyerang data pada perangkat lunak [28].

2.2. Integrasi Komponen Antar Sistem pada SDT

Integrasi komponen antara sistem ini adalah langkah selanjutnya setelah dekomposisi. Tidak semua komponen dalam suatu sistem terhubung dengan komponen dalam sistem lain. Dengan adanya integrasi komponen antar sistem menjadi multi sistem sesuai keinginan pengembang aplikasi. Integrasi komponen ini memanfaatkan hasil dekomposisi sistem menggunakan DFD pada langkah sebelumnya dan mengintegrasikan komponen pada sistem tersebut dengan komponen pada sistem lainnya sesuai aliran data. Integrasi ini juga membentuk SDT yang akan dibahas pada langkah selanjutnya tentang klasifikasi ancaman.

2.3. Klasifikasi Ancaman Berdasarkan Metode STRIDE

Setelah integrasi dan pembentukan SDT, langkah selanjutnya adalah memetakan ancaman ke setiap komponen SDT. Pemodelan ancaman STRIDE adalah salah satu metode populer yang digunakan untuk analisis keamanan sistem yang telah dibuat [30]. Metode STRIDE memanfaatkan DFD untuk merepresentasikan sistem yang akan dianalisis dan dapat diterapkan pada berbagai domain [31], baik dalam sistem tunggal maupun sistem ganda seperti SDT. Model ancaman STRIDE terdiri dari 6 kategori ancaman: *spoofing*, *tampering*, *repudiation*, *information disclosure*, *denial of service*, dan *elevation of privilege* [28], [32]–[34]. Microsoft mengembangkan metode klasifikasi serangan yang bertujuan untuk memahami maksud dan tujuan serangan tersebut [35]. Tabel 2 adalah jenis serangan berdasarkan akronim STRIDE.

Microsoft Threat Modeling Tool adalah aplikasi pemodelan ancaman pada sistem yang mengimplementasikan STRIDE sebagai panduan dalam menemukan ancaman pada sistem [36]. STRIDE adalah model ancaman yang banyak digunakan dalam mengidentifikasi ancaman dan dikembangkan oleh Microsoft[37] Pemodelan ancaman diakui sebagai aktivitas penting dalam mengamankan perangkat lunak dan membantu mengatasi masalah keamanan dalam pengembangannya [38]. Aplikasi ini digunakan untuk menentukan kontrol keamanan dan tindakan pencegahan untuk potensi serangan pada sistem yang akan diidentifikasi. Alat Pemodelan Ancaman Microsoft adalah aplikasi pemodelan ancaman yang bebas digunakan dan digunakan untuk mengotomatisasi pemodelan ancaman, terutama pada SDT sebagai objek penelitian kami.

Tabel 2. Klasifikasi STRIDE

Klasifikasi STRIDE	Sasaran Diserang	Serangan Sampel
Spoofing	Autentikasi	Pengguna peniruan
Tampering	Integritas data	Manipulasi data.
Repudiation	penolakan	individu menyangkal telah melakukan tindakan atau transaksi
Information disclosure	Kebocoran data	Mencuri data
Denial of service	Ketersediaan	Membatasi akses ke suatu layanan
Elevation of privilege	Otorisasi	Memperoleh hak akses yang bukan haknya.

2.4. Rumus Penilaian Risiko Berdasarkan Metode DREAD

Selanjutnya menilai risiko dari masing-masing komponen yang ancamannya telah dipetakan berdasarkan klasifikasi STRIDE. Langkah ini menggunakan metode DREAD untuk mendapatkan penilaian risiko dari setiap komponen. Metode penilaian DREAD ini dikembangkan oleh Microsoft [39]. Metode ini menggunakan 5 variabel dalam menghitung risiko ancaman [22] yaitu kerusakan, reproduktifitas, eksploitasi, pengguna yang terpengaruh, dan kemampuan untuk ditemukan.

- *Damage* atau kerusakan: variabel ini mengukur tingkat kerusakan yang diakibatkan oleh suatu ancaman yang diimplementasikan pada sebuah layanan. Semakin besar dampak kerusakan maka semakin tinggi pula tingkat risikonya.
- *Reproducibility*: variabel ini mengukur seberapa mudah ancaman dapat direplikasi atau diimplementasi pada sebuah layanan. Semakin mudah ancaman tersebut direplikasi pada suatu komponen maka tingkat risiko pada variabel ini semakin tinggi.
- *Exploitability*: variabel ini menghitung tingkat keahlian, waktu dan alat yang dibutuhkan oleh peretas dalam mengeksploitasi suatu komponen. Semakin mudah proses eksploitasi maka nilai variabel ini semakin tinggi.
- *Affected user*: pada variabel ini menghitung jumlah pengguna yang terpengaruh akibat serangan pada suatu layanan. Semakin menyeluruh tingkat pengguna yang terganggu maka variabel ini bernilai semakin tinggi.
- *Discoverability*: variabel ini menghitung tingkat kemudahan suatu celah pada layanan ditemukan oleh peretas dan kemudian dijadikan jalan untuk meretas suatu layanan. Semakin mudah celah tersebut ditemukan maka semakin tinggi nilai variabel ini.

Setiap atribut risiko dapat dikategorikan ke dalam empat level kualitatif: kritis, tinggi, sedang, dan rendah sehingga salah satu dari empat level kualitatif dapat diterapkan pada setiap atribut risiko sesuai dengan sifat ancaman yang sebenarnya. Lima aspek yang terkandung dalam model perlu diperhatikan untuk mengevaluasi risiko suatu ancaman. Rentang risiko ancaman adalah dari 0 hingga 10. Perhitungan penilaian risiko menggunakan metode DREAD adalah sebagai berikut. Risiko direpresentasikan sebagai Rs(t), *Damage*(D), *Reproducibility*(R), *Exploitability*(E), *Affected User*(A), dan *Discoverability* (Di).

$$Rs_{(t)} = \frac{D_{(t)}+R_{(t)}+E_{(t)}+A_{(t)}+Di_{(t)}}{5} \quad (1)$$

2.5. Mitigasi Resiko

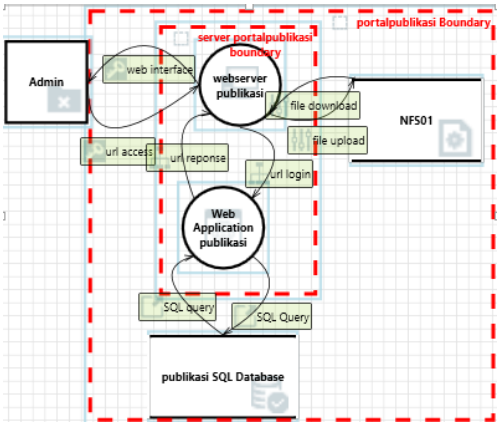
Langkah terakhir dari pemodelan ancaman adalah mitigasi risiko. Dalam SDT, mitigasi risiko dibuat secara berkelompok tergantung pada fungsi masing-masing komponen, dan jumlah ancaman tertinggi dengan prioritas tertinggi memiliki nilai risiko tertinggi. Dengan menggunakan *risk assessment range* pada langkah sebelumnya, diperoleh komponen dengan risiko tertinggi dan harus diprioritaskan untuk mitigasi komponen tersebut jika terjadi serangan. Mitigasi risiko ini mengikuti dari fasilitas organisasi tempat penulis melakukan penelitian pemodelan ancaman ini.

3. HASIL DAN PEMBAHASAN

Tahap pertama adalah dekomposisi sistem pembangun SDT. SDT ini terdiri dari 3 sistem utama Portalpublikasi , Web Mediator dan Web Diseminasi. Portalpublikasi digunakan oleh pengolah data untuk mengunggah publikasi dari data yang telah diproses, baik publikasi gratis maupun publikasi berbayar. Publikasi yang berhasil diunggah akan digunakan oleh sistem internal di SDT dan sistem SDT eksternal. Gambar 2 merupakan hasil dekomposisi Portalpublikasi

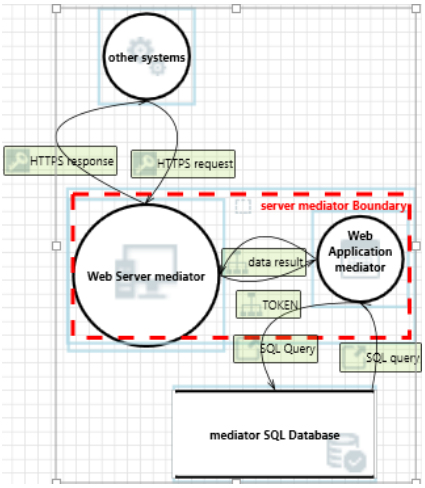
P-ISSN: 2089-676X
E-ISSN: 2549-0796

menggunakan DFD. Portalpublikasi terdiri dari 4 komponen, *webserver*, aplikasi web, *database* SQL publikasi, dan NFS01. Setiap komponen memiliki fungsi yang berbeda, *webserver* merupakan layanan agar aplikasi web dapat diakses oleh admin dan pengolah data. Aplikasi web berisi skrip aplikasi Portalpublikasi . Publikasi *database* SQL untuk menyimpan query SQL dilakukan oleh aplikasi web untuk menyimpan data berupa teks dan angka. NFS01 berfungsi sebagai tempat penyimpanan dokumen publikasi yang diunggah oleh pengolah data.



Gambar 2. Dekomposisi Portalpublikasi

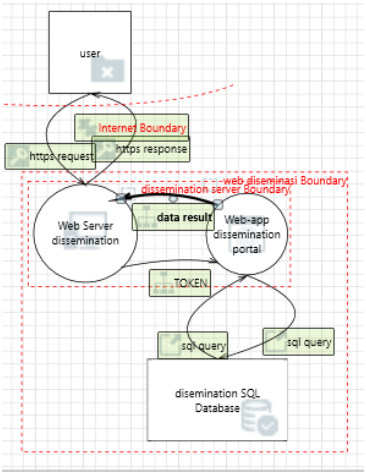
Web Mediator adalah sistem web yang menjembatani PortalPublikasi dengan Web Diseminasi dan sistem organisasi lain yang terhubung dengan Web Mediator (dapat berupa aplikasi web atau desktop). Web Mediator juga digunakan sebagai jembatan bagi website internal yang belum terkoneksi dengan SDT agar dapat menggunakan publikasi dari Portalpublikasi . Perbedaan utama dalam cara kerja Mediator Web dalam menangani sistem SDT internal dan eksternal adalah otomatisasi pertukaran data antar mesin. Pada SDT internal, Web Mediator bekerja secara otomatis segera setelah pengolah data mengunggah publikasi, Web Mediator mengirimkan informasi *metadata* seperti nama file dan deskripsi dari Portalpublikasi ke sistem yang terhubung ke SDT. Sedangkan sistem eksternal SDT tidak secara otomatis mendapatkan informasi file publikasi yang telah diunggah oleh pengolah data. Gambar 3 merupakan hasil dekomposisi web mediator. Mediator web ini memiliki 3 komponen: *webserver*, aplikasi web, dan *database* SQL mediator.



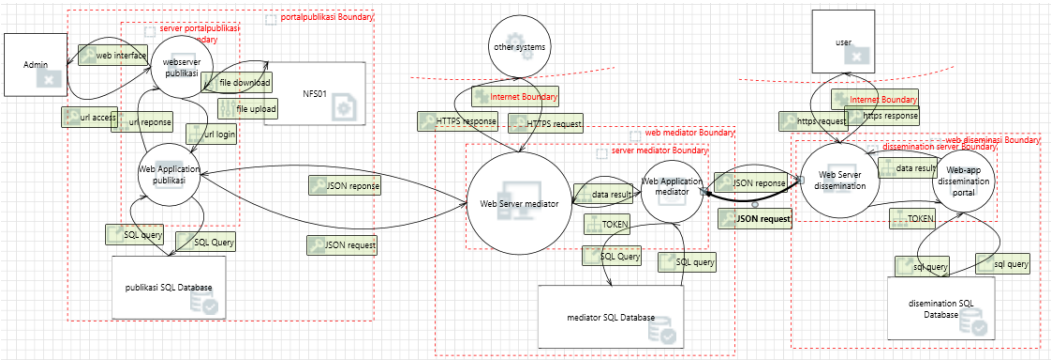
Gambar 3. Dekomposisi Web Mediator

P-ISSN: 2089-676X
E-ISSN: 2549-0796

Diseminasi Web adalah sarana untuk menyebarluaskan hasil publikasi yang telah dibuat dan diunggah oleh pengolah data pada portal publikasi. Sosialisasi Web ini langsung berinteraksi dengan pengguna yang akan menggunakan data tersebut. File publikasi dalam tampilan Diseminasi Web berasal dari Portalpublikasi . Diseminasi Web menggunakan Web Mediator sebagai jembatan dalam pengambilan publikasi untuk ditampilkan di Web Diseminasi. Gambar 4 merupakan Web Diseminasi yang telah didekomposisi menggunakan DFD. Ini memiliki 3 komponen, dan 1 komponen langsung berinteraksi dengan pengguna yang akan mengunduh dan menggunakan data publikasi. Jumlah Diseminasi Web ini adalah 549 domain yang terdiri dari 1 domain pusat dan 548 domain cabang.



Gambar 4. Dekomposisi Web Diseminasi



Gambar 5. Sistem SDT

Pada SDT, setelah mendekomposisikan masing-masing sistem, komponen-komponen yang terdapat di dalamnya saling berhubungan dan berinteraksi membentuk suatu integrasi dari sistem-sistem tersebut seperti terlihat pada Gambar 5. Pada sistem Portalpublikasi terdapat integrasi antara web server dari sistem Web Mediator dengan Web Application Publikasi di Portalpublikasi . Kedua komponen tersebut saling berinteraksi dan berkomunikasi, misalnya saat admin/pengolah data mengunggah publikasi baru, Aplikasi Web Portalpublikasi akan berkomunikasi dengan *webserver* Mediator dan bertukar data. Selanjutnya *webserver* Mediator akan berkomunikasi dengan Web Aplikasi Mediator untuk mengolah data dari Portalpublikasi .

Komponen web aplikasi Mediator dan *webserver* Diseminasi merupakan bagian dari sistem Web Diseminasi yang terhubung ke sistem Web Diseminasi dan terjadi pertukaran data, ditunjukkan pada Gambar 5. Setelah mengolah data dari *webserver* Diseminasi, aplikasi web Diseminasi akan berinteraksi kembali dengan *webserver* Diseminasi untuk menampilkan data yang telah diolah. Informasi yang ditampilkan pada aplikasi web diseminasi dapat dimanfaatkan oleh pengguna.

Langkah selanjutnya setelah dekomposisi sistem dan mengintegrasikan hasil dekomposisi sistem adalah mengklasifikasikan ancaman dari setiap komponen menggunakan klasifikasi STRIDE. Berikut adalah ancaman terhadap setiap komponen di setiap sistem berdasarkan Alat Pemodelan Ancaman Microsoft.

Tabel 3 adalah daftar ancaman pada sistem Portalpublikasi dengan menggunakan metode klasifikasi STRIDE dan Microsoft Threat Modeling Tools sebagai aplikasi untuk mengidentifikasi ancaman tersebut. Pada kolom kiri Tabel 3 adalah komponen Portalpublikasi sedangkan baris komponen adalah jumlah ancaman berdasarkan Microsoft Threat Modeling Tools dari setiap klasifikasi STRIDE. S didefinisikan sebagai *spoofing*, T sebagai *tampering*, R sebagai *repudiation*, I sebagai *information disclosure*, D sebagai *denial of service*, dan E sebagai *elevation of privilege.*

Tabel 3. Klasifikasi STRIDE pada Portalpublikasi

Komponen PortalPublikasi	Kode	Jumlah Ancaman					
		S	T	R	I	D	E
Webserver Publikasi	WSP	2	5	2	2	5	6
Web Aplikasi Publikasi	WAP	1	7	2	1	5	6
Publikasi SQL *database*	PDB	2	3	5	3	3	-
NFS01	NFS	2	2	5	2	3	-

Tabel 4 mencantumkan ancaman terhadap Komponen Web Mediator. Klasifikasikan daftar ancaman menggunakan STRIDE dan gunakan Microsoft Threat Modelling Tools untuk mengidentifikasi ancaman yang berpotensi mengancam komponen Web Mediator. Mediator Web komponen yang terdiri dari 3 komponen yaitu *webserver* Mediator, Web Applikasi Mediator , dan Mediator SQL database sangat penting untuk SDT. Di bawah ini adalah jumlah potensi ancaman di setiap Komponen Web Mediator.

Tabel 4. Klasifikasi STRIDE pada Web Mediator

Komponen Web Mediator	Kode	Jumlah Ancaman					
		S	T	R	I	D	E
Webserver Mediator	WSM	2	3	2	1	4	7
Web Aplikasi Mediator	WAM	4	7	2	1	5	6
Mediator SQL *database*	MDB	1	3	5	1	2	-

Klasifikasi ancaman untuk setiap komponen Web Diseminasi dapat dilihat pada Tabel 5. Web Diseminasi yang melayani pengguna data memiliki tiga komponen, yaitu webserver Diseminasi, Web aplikasi Diseminasi, dan Diseminasi SQL database. 549 Web Diseminasi memiliki arsitektur dan komponen yang sama yang memudahkan administrator infrastruktur dan pengembang

aplikasi untuk membangun dan memelihara sistem. Berikut adalah jumlah potensi ancaman pada setiap Komponen Web Diseminasi berdasarkan klasifikasi STRIDE menggunakan Microsoft Threat Modeling Tools.

Tabel 5. Klasifikasi STRIDE pada Diseminasi Web

Komponen Web Diseminasir	Kode	Jumlah Ancaman					
		S	T	R	I	D	E
Webserver Diseminasi	WSD	1	3	2	1	5	7
Web Aplikasi Diseminasi	WAD	1	5	1	1	3	3
Diseminasi SQL *database*	DDB	2	3	5	3	3	-

Tahap selanjutnya adalah penilaian risiko dengan menggunakan metode DREAD untuk setiap komponen sistem SDT. Penilaian ini diperoleh dari kuisioner yang telah dibuat berdasarkan ancaman dan jumlah masing-masing komponen pada masing-masing sistem. Koresponden kuesioner ini adalah pengembang aplikasi dan tim infrastruktur server dan jaringan yang mengembangkan dan memelihara sistem agar berjalan dengan baik. Penilaian risiko pada komponen ini didasarkan pada 4 level. Tabel 6 memuat nilai tingkat risiko beserta kisaran nilai yang diperoleh dari penilaian risiko.

Tabel 6. Tingkat Penilaian Risiko

Kategori Risiko	Kisaran Skor Risiko
Rendah	0 - 3,00
Sedang	3,01 - 6,00
Tinggi	6,01 – 8,00
Kritis	8,01 – 10,0

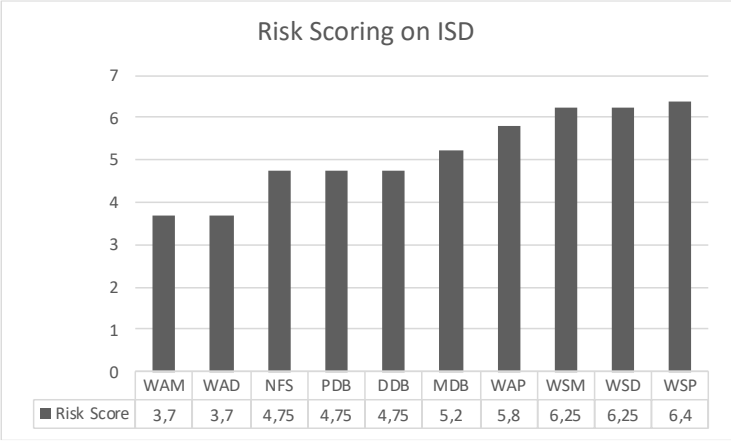
Tabel 7 berisi hasil penilaian risiko dengan menggunakan metode DREAD. D adalah penilaian kerusakan jika ancaman menyerang komponen dalam sistem, dan R adalah tingkat reproduksi/implementasi ancaman terhadap komponen tersebut. Dalam menilai tingkat keahlian, waktu, dan alat yang digunakan oleh peretas dalam mengeksploitasi suatu komponen, dilambangkan dengan huruf E, A sebagai tingkat/jumlah pengguna yang terpengaruh oleh ancaman yang diterapkan, dan D diakhir sebagai penilaian terhadap seberapa mudah ancaman ditemukan oleh peretas. Nilai Risiko diperoleh dengan menggunakan persamaan (1).

Tabel 7. Penilaian Risiko Pada Komponen SDT

Komponen SDT	DREAD *scoring*					Nilai Risiko
	D	R	E	A	D	
WAM	8,5	2,5	1	5,5	1	3,7
WAD	5,5	4	1	5,5	2,5	3,7
NFS	7,75	1,75	1,75	10	2,5	4,75
PDB	6,25	2,5	2,5	10	2,5	4,75
DDB	5,5	4	1,75	10	2,5	4,75
MDB	6,25	4	3,25	8,5	4	5,2

WAP	5,5	4	5,5	10	4	5,8
WSM	7,75	7	3,25	10	3,25	6,25
WSD	7	7	3,25	10	4	6,25
WSP	8,5	6,25	2,5	10	4,75	6,4

Gambar 6 adalah grafik penilaian risiko komponen SDT. Gambar 6 dan Tabel 7 menunjukkan 3 komponen berada pada tingkat risiko tinggi yaitu *Webserver* Publication (WSP) dengan nilai risiko 6,4, *Webserver* Mediator (WSM), dan *Webserver* Disemination (WSD) dengan nilai risiko sebesar 6,25 masing-masing. Komponen lainnya termasuk dalam kategori sedang dengan nilai risiko bervariasi dari 3,7 hingga 5,8.



Gambar 6. Grafik Tingkat Risiko Komponen SDT.

Pada tahap terakhir adalah mitigasi yang harus dilakukan untuk mencegah maupun mengurangi risiko pada tiap komponen dari ancaman yang telah diklasifikasikan. Mitigasi ini sangat dibutuhkan supaya organisasi tidak mengalami kerugian yang besar ketika adanya ancaman pada SDT. Usulan mitigasi dibagi menjadi tiga bagian webserver, web aplikasi dan media penyimpanan. Pada komponen-komponen webserver ancaman terbanyak adalah elevation of privilege. Pada komponen-komponen database repudiation sebagai ancaman paling banyak dan di komponen-komponen media penyimpanan ancaman tampering merupakan ancaman paling banyak. Berikut tabel 8 berisi usulan mitigasi dari komponen pembangun SDT.

Tabel 8. Usulan Mitigasi

Ancaman	Komponen	Usulan mitigasi
Elevation of privilege	WSP, WSM, WSD	- Pemasangan IPS(Intrusion Prevention System) dan IDS(Intrusion Detection System) - Menggunakan VPN(Virtual Private Network) atau teknik khusus seperti port dinamis untuk mengakses sistem webserver pada jarak jauh. - Pergantian Password untuk masuk ke sistem secara rutin
Repudiaton	PDB, DDB, MDB, NFS	- Menerapkan proses logging pada aktivitas komponen tersebut

		- Audit secara rutin aktivitas dan data yang tersimpan pada komponen tersebut.
Tampering	WAP, WAM, WAD	- Penggunaan Enkripsi yang kuat pada data yang sensitif - Melakukan pembaruan skrip aplikasi yang digunakan sehingga dapat menutup celah dari fungsi skrip aplikasi yang telah usang - Menggunakan metode hash untuk integrity pada data yang dikirim maupun diterima.

4. KESIMPULAN

Motivasi dari dibuatnya SDT ini adalah untuk menggabungkan sistem yang awalnya berjalan secara terpisah tetapi menggunakan data yang sama. Selain itu juga untuk memudahkan dan mempercepat waktu untuk pengolah data dalam mengunggah hasil publikasi yang telah dibuat. Selain pengolah data, pengguna data, sistem lain dipermudah dengan adanya Web Mediator sebagai jembatan untuk mengambil hasil publikasi. Tetapi dengan semakin kompleksnya suatu sistem informasi maka semakin banyak pula ancaman pada sistem tersebut. Dengan menggunakan klasifikasi ancaman STRIDE, ditemukan 181 potensi ancaman yang dapat saja menyerang SDT. Dengan risiko tertinggi ada pada komponen Webserver masing-masing sistem karena merupakan pintu masuk dari pengguna maupun sistem lain untuk mengakses data di dalam sistem. Keterbatasan dari penelitian ini adalah hanya menggunakan tiga sistem yang terintegrasi di dalam SDT. Pada penelitian selanjutnya diharapkan mampu menggunakan lebih dari tiga sistem pada SDT sehingga SDT dapat tergambar lebih kompleks. Dengan kompleksnya SDT maka penilian risiko dapat menambahkan nilai gangguan pada sistem lain yang terintegrasi apabila satu komponen tertentu terdampak ancaman.

DAFTAR PUSTAKA

[1] A. Hanelt, R. Bohnsack, D. Marz, and C. Antunes Marante, 'A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change', *Journal of Management Studies*, vol. 58, no. 5, pp. 1159–1197, Jul. 2021, doi: 10.1111/JOMS.12639.

[2] A. Abugabah, L. Sanzogni, and A. Poropat, 'The impact of information systems on user performance: A critical review and theoretical model', 2009. [Online]. Available: https://www.researchgate.net/publication/45109460

[3] C. Tam, A. Loureiro, and T. Oliveira, 'The individual performance outcome behind e-commerce Integrating information systems success and overall trust', 2020, doi: 10.1108/INTR-06-2018-0262.

[4] R. Lawan, 'Why you need to integrate Information Systems in your business'. https://www.linkedin.com/pulse/why-you-need-integrate-information-systems-your-business-lawan (accessed Feb. 09, 2023).

[5] C.-C. Osman, 'Robotic Process Automation: Lessons Learned from Case Studies', *Informatica Economica*, vol. 23, no. 4/2019, pp. 66–71, Dec. 2019, doi: 10.12948/ISSN14531305/23.4.2019.06.

[6] F. Yahya, B. M. Fazli, M. F. Abdullah, and H. Zulkifli, 'Extending the national lake database of Malaysia (MyLake) as a central data exchange using big data integration', *ACM International Conference Proceeding Series*, pp. 30–35, Jul. 2019, doi: 10.1145/3352411.3352417.
[7] L. A. Al-Juboori and A. A. Duroobi, 'CAD/CAM integration verification process based on data exchange method on free form surfaces', *2020 Advances in Science and Engineering Technology International Conferences, ASET 2020*, vol. 2020-January, Feb. 2020, doi: 10.1109/ASET48392.2020.9171372.
[8] A. Luder, K. Kirchheim, J. Pauly, S. Biffl, F. Rinker, and L. Waltersdorfer, 'Supporting the data model integrator in an engineering network by automating data integration', *IEEE International Conference on Industrial Informatics (INDIN)*, vol. 2019-July, pp. 1229–1234, Jul. 2019, doi: 10.1109/INDIN41052.2019.8972174.
[9] L. Garber, 'The challenges of securing the virtualized environment', *Computer (Long Beach Calif)*, vol. 45, no. 1, pp. 17–20, Jan. 2012, doi: 10.1109/MC.2012.27.
[10] T. Subatri, *Konsep Sistem Informasi*. Andy Publisher, 2012.
[11] Victoria Drake, 'Threat Modeling | OWASP Foundation'. https://owasp.org/www-community/Threat_Modeling (accessed Feb. 04, 2023).
[12] M. Aminzade, 'Confidentiality, integrity and availability – finding a balanced IT framework', *Network Security*, vol. 2018, no. 5, pp. 9–11, May 2018, doi: 10.1016/S1353-4858(18)30043-6.
[13] R. Goel, A. Kumar, and J. Haddow, 'PRISM: a strategic decision framework for cybersecurity risk assessment', *Information and Computer Security*, vol. 28, no. 4, pp. 591–625, Oct. 2020, doi: 10.1108/ICS-11-2018-0131/FULL/PDF.
[14] M. S. Ferdous, S. Chowdhury, and J. M. Jose, 'Privacy threat model in lifelogging', *UbiComp 2016 Adjunct - Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp. 576–581, Sep. 2016, doi: 10.1145/2968219.2968324.
[15] M. G. Jaatun, K. Bernsmed, D. S. Cruzes, and I. A. Tøndel, 'Threat modeling in agile software development', *Exploring Security in Software Architecture and Design*, pp. 1–14, Jan. 2019, doi: 10.4018/978-1-5225-6313-6.CH001.
[16] T. Omitola, A. Rezazadeh, and M. Butler, 'Making (Implicit) security requirements explicit for cyber-physical systems: A maritime use case security analysis', *Communications in Computer and Information Science*, vol. 1062, pp. 75–84, 2019, doi: 10.1007/978-3-030-27684-3_11/COVER.
[17] D. Ha, S. Upadhyaya, H. Ngo, S. Pramanhik, R. Chinchani, and S. Mathew, 'Insider threat analysis using information-centric modeling', *IFIP International Federation for Information Processing*, vol. 242, pp. 55–73, 2007, doi: 10.1007/978-0-387-73742-3_4/COVER.
[18] 'Threats - Microsoft Threat Modeling Tool - Azure | Microsoft Learn'. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats (accessed Feb. 09, 2023).
[19] J. Straub, 'Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATTCK and STRIDE Frameworks as Blackboard Architecture Networks', in *Proceedings - 2020 IEEE International Conference on Smart Cloud, SmartCloud 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 148–153. doi: 10.1109/SmartCloud49737.2020.00035.
[20] 'Threat modeling for drivers - Windows drivers | Microsoft Learn'. https://learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers (accessed Feb. 10, 2023).