THREAT MODELING MENGGUNAKAN PENDEKATAN STRIDE DAN DREAD UNTUK MENGETAHUI RISIKO DAN MITIGASI KEAMANAN PADA SISTEM LAYANAN PENDIDIKAN

(*THREAT MODELING USING STRIDE AND DREAD APPROACHES TO DETERMINE SECURITY RISKS AND MITIGATIONS IN EDUCATION SERVICE SYSTEMS*)

Alang Artha Iwana* [1], Raphael Bianco Huwae [1], Andy Hidayat Jatmika [1]
[1]Dept Informatics Engineering, Mataram University
Jl. Majapahit 62, Mataram, Lombok NTB, INDONESIA
Email: alangarthaiwana@gmail.com, *[*raphael.bianco.huwae, andy]@unram.ac.id

Abstract

Information system security is increasingly crucial with the rise of cyber threats. This study identifies and evaluates security risks in education service systems using STRIDE and DREAD-based Threat Modeling. STRIDE identifies threats such as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege, while DREAD assesses risk based on potential damage, ease of exploitation, affected users, and likelihood of detection. The analysis showed that information disclosure and elevation of privilege were the highest risks, mainly due to the permissive CORS configuration. Testing using Burp Suite revealed high-level vulnerabilities allowing unauthorized access and data leakage. To address this, mitigations in the form of CORS policy validation, HTTP method restrictions, data encryption, and role-based authentication were implemented. Simulation results after mitigation showed a significant reduction in security issues, such as critical issues dropping from 6 to 1. This research confirms STRIDE and DREAD are effective in identifying and evaluating security risks, providing a strong basis for designing mitigation strategies to maintain educational service security.

Keywords: *threat modeling, STRIDE, DREAD, information security, cybersecurity mitigation.*

**Correspondence Author*

1. PENDAHULUAN

Transformasi digital telah menjadi pendorong penting dalam meningkatkan kualitas pendidikan tinggi, di mana teknologi dan digitalisasi diharapkan dapat memotivasi minat belajar siswa[1]. Namun, di sisi lain, transformasi ini juga membawa tantangan baru, terutama terkait keamanan data dan privasi.

ENISA *Threat Landscape* 2024 pada laporannya mengidentifikasi ancaman utama seperti ransomware, malware, rekayasa sosial, dan ancaman terhadap data. Ransomware terus menjadi ancaman utama, sementara manipulasi informasi yang didukung AI semakin berkembang. Laporan ini juga menyoroti pentingnya mitigasi risiko melalui strategi keamanan yang kuat[2].

Tujuan penerapan keamanan informasi dinilai dalam berbagai topik, dengan fokus pada pembahasan dan penerapan semua persyaratan keamanan yang diuraikan dalam standar ISO/IEC 27001: 2013[3].

Penelitian ini berfokus pada identifikasi dan analisis ancaman keamanan dalam sistem layanan pendidikan menggunakan pendekatan *threat modeling* berbasis STRIDE dan DREAD. Model STRIDE digunakan untuk mengenali ancaman spesifik, seperti *spoofing*, *tampering*, *repudiation*, *information disclosure*, *denial of service*, dan *elevation of privilege*, sementara model DREAD digunakan untuk menilai tingkat risiko dan menentukan ancaman berisiko tinggi yang memerlukan tindakan mitigasi segera. Penelitian ini juga merumuskan langkah mitigasi untuk meningkatkan keamanan sistem, melindungi integritas data, dan memastikan kerahasiaan serta ketersediaan informasi dalam layanan pendidikan. Keamanan sistem informasi di institusi pendidikan menjadi semakin krusial, mengingat meningkatnya ancaman siber seperti pencurian data, gangguan layanan, dan kerugian finansial yang signifikan. Data akademik, informasi pribadi mahasiswa, dan hasil penelitian merupakan aset berharga yang rentan terhadap serangan, sehingga diperlukan perlindungan yang kuat untuk menjaga keandalan dan keberlanjutan sistem layanan pendidikan.

Penelitian ini memilih Universitas X sebagai studi kasus, mengingat pentingnya menjaga keamanan sistem layanan pendidikan di universitas yang tergolong baru. Universitas ini pernah melakukan analisis ancaman terkait SQL *Injection*, akan tetapi penulis menemukan celah lainnya yang belum di ekspos yaitu ancaman terkait CORS yang memang masih sangat rentan, oleh karena itu penulis mengangkat judul "*Threat Modeling* Menggunakan Pendekatan STRIDE Dan DREAD Untuk Mengetahui Risiko Dan Mitigasi Keamanan Pada Sistem Layanan Pendidikan" sebagai penelitiannya. Studi ini diharapkan dapat memberikan gambaran menyeluruh mengenai risiko yang dihadapi universitas serta memberikan rekomendasi mitigasi untuk meningkatkan keamanan sistem. Namun, cakupan sistem yang diuji dibatasi pada layanan pendidikan di jurusan teknik di universitas tersebut.

2. TINJAUAN PUSTAKA

2.1. Tinjauan Pustaka

Berbagai penelitian telah mengeksplorasi pemodelan ancaman dalam sistem berbasis kecerdasan buatan (AI) dan pembelajaran mesin (ML) menggunakan metode STRIDE dan DREAD. Mauri dan Damiani mengembangkan STRIDE-AI, metodologi berbasis aset yang mengadaptasi pendekatan STRIDE untuk domain AI-ML, serta mengintegrasikannya dengan FMEA (*Failure Modes and Effects Analysis*) untuk mengidentifikasi potensi kerentanan dalam siklus hidup ML. Pendekatan ini memungkinkan pemetaan mode kegagalan terhadap ancaman keamanan dan pemilihan kontrol yang sesuai untuk melindungi aset ML. Studi mereka juga menerapkan STRIDE-AI pada proyek TOREADOR H2020[4].

Dalam penelitian Kim et al. (2022), metode metode STRIDE dan DREAD pada Sistem Kontrol Terdistribusi (DCS), menunjukkan efektivitasnya dalam menganalisis ancaman pada elemen dan interaksi sistem. Penerapan serupa dalam sistem layanan pendidikan dianggap relevan karena kebutuhan untuk melindungi data penting[5].

Penelitian oleh Dalilah et al. (2022) menekankan pentingnya *threat modeling* dalam sistem informasi akademik untuk mengidentifikasi risiko spesifik seperti *spoofing* akun mahasiswa dan kebocoran data nilai. STRIDE digunakan untuk mengklasifikasikan ancaman, sedangkan DREAD membantu dalam mengevaluasi tingkat risiko dan menetapkan prioritas mitigasi terhadap ancaman dengan dampak paling signifikan[6].

Dalam penelitian Khairul Faridi et al. (2021) menunjukkan bahwa STRIDE dapat mengidentifikasi ancaman dalam sistem layanan pendidikan, termasuk pada level pengguna, server web, dan basis data. Mereka mengusulkan mitigasi seperti autentikasi ganda, validasi input, serta pengamanan infrastruktur jaringan, yang juga relevan untuk melindungi informasi pribadi siswa dan data akademik[7].

Laksono dalam penelitiannya menerapkan metode STRIDE dan DREAD melalui tahapan observasi, dekomposisi aplikasi, dan klasifikasi ancaman untuk sistematisasi identifikasi risiko. Analisis risiko menggunakan DREAD memungkinkan penyusunan prioritas mitigasi untuk menangani ancaman dengan risiko tertinggi, menghasilkan solusi yang dapat diterapkan untuk meningkatkan keamanan aplikasi[8].

Selanjutnya Lazar Cerovic (2024) telah mengembangkan StrideLang, sebuah bahasa spesifik domain untuk pemodelan ancaman menggunakan STRIDE dan DREAD, yang memungkinkan analisis ancaman yang lebih sistematis dan terstruktur. Pendekatan seperti ini menunjukkan bahwa STRIDE dan DREAD dapat dikombinasikan untuk menghasilkan framework analisis ancaman yang lebih mendalam dan berbasis scenario, yang dapat diadaptasi dalam berbagai konteks, termasuk sistem layanan pendidikan[9].

2.2. Teori Dasar

2.2.1. Sistem informasi akademik

Sistem informasi adalah gabungan antara perangkat keras, perangkat lunak, data, manusia, dan prosedur yang bekerja sama untuk mengolah, menyimpan, dan menyampaikan informasi[10]. Sistem informasi akademik dirancang untuk memenuhi kebutuhan peneliti dan pihak terkait dalam meningkatkan kualitas sumber daya manusia melalui layanan pendidikan berbasis komputer[11]. Sistem ini dikembangkan agar sesuai dengan proses bisnis yang terus berjalan, dengan tujuan utama mempercepat dan meningkatkan kualitas layanan di bidang akademik[12].

2.2.2. Keamanan sistem informasi

Keamanan sistem informasi adalah upaya untuk melindungi aset informasi dari potensi ancaman[13]. Tujuan dari keamanan informasi adalah untuk memastikan kerahasiaan, ketersediaan, dan integritas sumber daya informasi dalam suatu organisasi atau perusahaan[14]. Konsep dasar keamanan informasi terdapat pada setiap komponen dari Triad CIA (kerahasiaan, integritas, dan ketersediaan) [15].

2.2.3. Pemodelan ancaman

a. Definisi

Threat modeling atau pemodelan ancaman merupakan proses untuk mengidentifikasi dan meminimalkan kemungkinan ancaman yang dapat memengaruhi suatu sistem[16]. Melalui pendekatan ini, akan lebih mudah untuk memahami sejauh mana dampak dari jenis serangan yang mungkin terjadi, sekaligus menentukan langkah-langkah untuk mengurangi dampaknya atau mencegah sistem menjadi target serangan[17].

b. Metode

1. *Data Flow Diagram*

   Dalam konteks pemodelan ancaman, *Data Flow Diagram* (DFD) digunakan untuk memetakan ancaman terhadap komponen sistem yang rentan. Setiap elemen dalam DFD dianalisis menggunakan pendekatan seperti STRIDE untuk mengidentifikasi jenis ancaman yang mungkin terjadi[18].

2. STRIDE

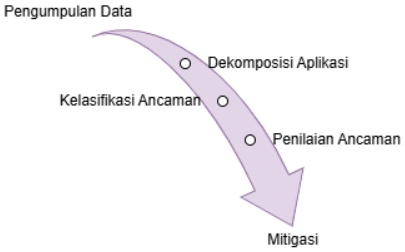
   Model STRIDE digunakan secara luas dalam pemodelan ancaman yang berpusat pada aplikasi untuk mengklasifikasikan dan mengukur risiko. Dengan menerapkan model STRIDE, tim pengembang dapat secara sistematis mengatasi sebuah ancaman, sehingga dapat meningkatkan keamanan aplikasi[19].

3. DREAD

   Model DREAD adalah kerangka kerja yang digunakan untuk menilai dan memeringkat ancaman berdasarkan risiko eksploitasi kerentanannya. Namun, kelemahan model ini terletak pada deskripsi atribut dan tingkat risikonya yang kurang konkret, sehingga dapat meningkatkan tingkat subjektivitas dalam penilaian risiko. Hal ini menjadikan hasil analisis sangat bergantung pada perspektif individu atau tim yang melakukan evaluasi[20].

3. METODE PENELITIAN

Pada penelitian ini, alur berikut digunakan sebagai pedoman dalam pelaksanaan penelitian agar tujuan yang telah ditetapkan dapat tercapai sesuai harapan. Tahapan-tahapan penelitian tersebut digambarkan pada diagram *Threat Modeling Process Flow* seperti yang di tunjukan pada gambar 1.



Gambar 1. *Threat Modeling Process Flow*, Azis Catur Laksono, 2020[8]

3.1. Pengumpulan Data

3.1.1. Studi literatur

Studi literatur adalah tahap penelitian yang bertujuan untuk mengumpulkan, menelaah, dan mempelajari referensi dari berbagai sumber seperti buku, makalah, artikel, dan situs web yang berkaitan dengan penelitian pemodelan ancaman.

3.1.2. Wawancara

Tahapan wawancara dilakukan dengan pihak pengembang sistem di Universitas X untuk memperoleh informasi terkait infrastruktur sistem, penyerangan yang pernah terjadi pada sistem serta data pendukung lainnya. Data diambil dengan rentang waktu 4 bulan mulai dari bulan September sampai akhir Desember 2024.

3.2. Dekomposisi Aplikasi

3.2.1. Identifikasi aplikasi

Langkah awal dalam proses pemodelan ancaman adalah memahami cara aplikasi berinteraksi dengan entitas eksternal, termasuk mengenali titik masuk potensial yang dapat menjadi sasaran serangan serta aset yang menarik bagi penyerang. Informasi ini kemudian didokumentasikan sebagai bagian dari proses pemodelan ancaman.

3.2.2. Diagram alur data (*data flow diagram*)

Setelah informasi disusun dalam dokumen *threat model*, selanjutnya adalah menyusun *Data Flow Diagram* untuk memudahkan dalam memahami aplikasi ketika memproses data.

3.3. Klasifikasi Ancaman

Daftar ancaman kategori STRIDE ditunjukkan pada Tabel 1[8]. Penerapan model STRIDE untuk mengklasifikasikan ancaman potensial yang dapat memengaruhi sistem. STRIDE membantu mengidentifikasi ancaman seperti *spoofing*, *tampering*, *repudiation*, *information disclosure*, *denial of service*, dan *elevation of privilege*.

TABEL I. KATEGORI STRIDE

Tipe	Jenis Ancaman
Spoofing	Tindakan ancaman yang ditujukan untuk memperoleh dan memanfaatkan kredensial milik pengguna lain, seperti nama pengguna dan kata sandi.
Tampering	Ancaman yang bertujuan untuk memodifikasi data, baik dengan mengubah data yang tersimpan dalam *database* maupun data yang sedang ditransmisikan melalui jaringan.
Repudiation	Ancaman yang bertujuan melakukan tindakan terlarang dalam sistem yang tidak memiliki kemampuan untuk mencatat atau melacak aktivitas tersebut.
Information disclosure	Ancaman yang bertujuan untuk mengakses file tanpa izin atau membaca data yang sedang dikirimkan.
Denial of service	Ancaman yang berusaha mencegah akses bagi pengguna yang sah, misalnya dengan membuat server web sementara tidak tersedia atau tidak bisa digunakan.
Elevation of priviledge	Ancaman yang bertujuan memperoleh akses khusus ke sumber daya untuk mendapatkan akses ilegal ke informasi atau merusak sistem.

3.4. Penilaian Ancaman

3.4.1. Analisis risiko

Metode DREAD digunakan untuk menilai tingkat risiko dari setiap ancaman yang telah diklasifikasikan. Penilaian diberikan berdasarkan tingkat risiko yang terjadi, yaitu rendah untuk peringkat 1, sedang untuk peringkat 2, dan tinggi untuk peringkat 3. Penilaian ini didasarkan pada beberapa kategori, yaitu: *Damage Potential* (besar potensi kerusakan yang dapat ditimbulkan), *Reproducibility* (kemudahan untuk menggandakan serangan), *Exploitability* (banyaknya waktu dan sumber daya yang dibutuhkan untuk melakukan serangan), *Affected Users* (jumlah pengguna yang terpengaruh), dan *Discoverability* (kemudahan dalam menemukan ancaman dalam sistem).

3.4.2. Peringkat risiko

Seperti yang telah dijelaskan sebelumnya, model DREAD mengharuskan pemberian nilai antara satu hingga tiga pada setiap lima aspek utama. Dengan demikian, setiap ancaman akan memiliki total nilai antara 1 hingga 3.

Menurut model DREAD, ancaman yang memiliki nilai antara 1.0–1.5 adalah risiko rendah, rentang nilai antara 1.6–2.5 adalah risiko sedang, dan rentang nilai antara 2.6–3.0 adalah risiko tinggi[20].

3.5. Mitigasi

Berdasarkan peringkat risiko, dilakukan penyusunan rencana mitigasi untuk setiap ancaman dengan prioritas lebih tinggi. Tindakan mitigasi dapat mencakup autentikasi ganda, validasi input, dan pemberian izin yang diperlukan.

4. HASIL DAN PEMBAHASAN

Analisis ancaman menggunakan model STRIDE menunjukkan adanya beberapa risiko keamanan pada sistem layanan pendidikan Universitas X. Beberapa risiko telah termitigasi, sementara lainnya masih membutuhkan penanganan lebih lanjut.

Penggunaan *Cloudflare* telah diterapkan sebagai langkah mitigasi untuk menghadapi risiko *Denial of Service* (DoS) dan *Repudiation*. *Cloudflare* membantu melindungi sistem dengan fitur *rate limiting* dan deteksi dini serangan DDoS, yang memastikan layanan tetap tersedia meskipun menghadapi volume permintaan yang tinggi. Untuk *Repudiation*, *Cloudflare* menyediakan validasi asal permintaan melalui *whitelist*, namun mitigasi di sisi aplikasi masih terbatas karena belum diterapkannya pencatatan jejak aktivitas yang memadai dan autentikasi berbasis token kriptografis.

Sementara itu, risiko lain seperti *Spoofing*, *Tampering*, *Information Disclosure*, dan *Elevation of Privilege* belum sepenuhnya dimitigasi. Oleh karena itu, direncanakan implementasi tambahan seperti autentikasi berbasis peran, validasi input yang lebih ketat, dan penggunaan token sesi yang terenkripsi guna meningkatkan keamanan sistem secara keseluruhan. Langkah-langkah ini diharapkan dapat mengurangi risiko dan melindungi integritas sistem layanan pendidikan.

4.1. Dekomposisi Aplikasi

4.1.1. Identifikasi aplikasi

Aplikasi yang dirancang dapat dipecah menjadi beberapa komponen utama seperti pada tabel berikut:

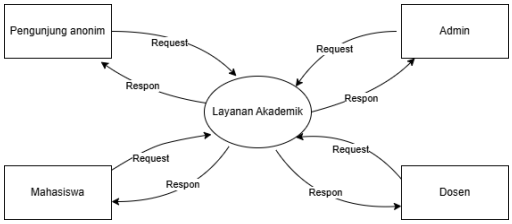
TABEL II. KOMPONEN UTAMA

Komponen	Fungsi	Teknologi	Framework /Library
Frontend	Menyediakan antarmuka pengguna untuk akses informasi dan formulir.	HTML, CSS, JavaScript	Bootstrap atau library lainnya
Backend	Mengelola logika bisnis, autentikasi, dan pemrosesan data.	PHP, Laravel, atau framework lain	-
Database	Menyimpan data utama, seperti informasi pengguna dan hasil evaluasi.	MySQL/PostgreSQL atau *database* lain	-
API	Menghubungkan aplikasi dengan layanan eksternal atau modul internal.	REST API	-
Web Server	Melayani permintaan pengguna dan mengelola sumber daya aplikasi.	Apache atau Nginx	-

4.1.2. *Data flow diagram*

Untuk memahami bagaimana data mengalir dalam aplikasi yang dibuat, setiap bagian dalam proses pengolahan data telah diidentifikasi. Setiap bagian memiliki peran dan fungsi masing-masing untuk memastikan data dapat dikelola dengan baik, mulai dari interaksi pengguna hingga pengolahan di server dan penyimpanan di *database*.

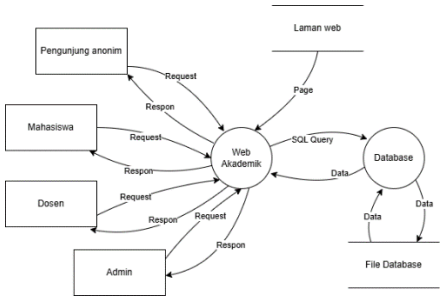
a. *Context diagram* sistem layanan pendidikan



Gambar 2. *Context Diagram* Sistem Layanan Pendidikan

Gambar di atas merupakan diagram konteks sistem layanan pendidikan akademik yang menggambarkan interaksi antara sistem dengan aktor-aktor eskternal. Setiap aktor mengirimkan permintaan kepada sistem sesuai kebutuhan mereka, dan sistem memproses serta memberikan tanggapan berdasarkan hak akses dan jenis layanan yang diminta.

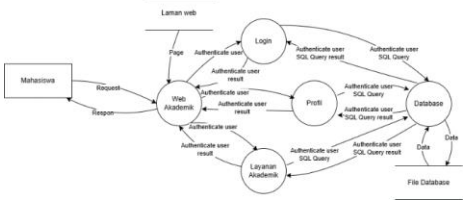
b. *Data flow diagram* sistem layanan pendidikan level -1



Gambar 3. DFD Sistem Layanan Pendidikan Level 1

Gambar di atas merupakan DFD level 1 dari sistem web akademik yang menjelaskan aliran data antara aktor eksternal, sistem utama, dan *database*. Aktor eksternal mengirimkan *request* ke web kemudian di proses dan memberikan *response.* Sistem juga berinteraksi dengan *database* menggunakan *query* SQL untuk mengambil atau menyimpan data yang dibutuhkan. Untuk laman web berfungsi sebagai antarmuka pengguna untuk menampilkan informasi sesuai permintaan.

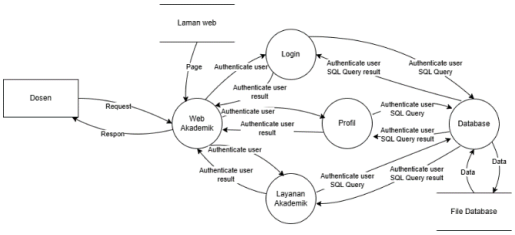
c. *Data flow diagram* sistem layanan pendidikan level -2 pengguna mahasiswa



Gambar 4. DFD Sistem Layanan Pendidikan Level 2 Pengguna Mahasiswa

Gambar di atas merupakan DFD level 2 dari sistem web akademik yang berfokus pada interaksi pengguna yaitu mahasiswa. Mahasiswa mengirimkan *request* ke web akademik, yang kemudian memproses permintaan tersebut melalui tiga proses utama, yaitu *login*, profil, dan layanan akademik. Setiap proses berkomunikasi dengan *database* untuk mengautentikasi pengguna dan mengambil atau menyimpan data menggunakan *query* SQL. Laman web menampilkan hasil autentikasi dan informasi yang diminta kepada mahasiswa.

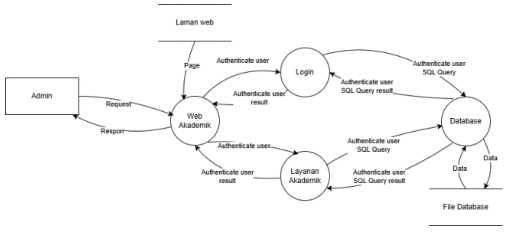
d. *Data flow diagram* sistem layanan pendidikan level -2 pengguna dosen



Gambar 5. DFD Sistem Layanan Pendidikan Level 2 Pengguna Dosen

Gambar di atas merupakan DFD level 2 dari sistem web akademik yang berfokus pada interaksi pengguna yaitu dosen. Dosen mengirimkan *request* ke web akademik, yang kemudian memproses permintaan tersebut melalui tiga proses utama, yaitu *login*, profil, dan layanan akademik. Setiap proses berkomunikasi dengan *database* untuk mengautentikasi pengguna dan mengambil atau menyimpan data menggunakan *query* SQL. Laman web menampilkan hasil autentikasi dan informasi yang diminta kepada dosen.

e. *Data flow diagram* sistem layanan pendidikan level -2 pengguna admin program studi



Gambar 6. DFD Sistem Layanan Pendidikan Level 2 Pengguna Admin Prodi

Gambar di atas merupakan DFD level 2 dari sistem web akademik yang berfokus pada interaksi pengguna yaitu admin. Admin mengakses web akademik untuk mengautentikasi melalui modul *login*, yang memverifikasi data dengan *database* menggunakan SQL *query*. Jika berhasil, akses ke layanan akademik diberikan dengan proses autentikasi serupa. *Database* menyimpan dan mengelola data pengguna dalam file *database* untuk kebutuhan sistem. Laman web menampilkan hasil autentikasi dan informasi yang diminta kepada admin.

Dari beberapa DFD sistem layanan pendidikan diatas menunjukkan aliran data antara pengguna (mahasiswa, dosen, admin), *backend*, dan *database*. Setiap interaksi, seperti *login* dan pengelolaan data, menjadi potensi ancaman, terutama jika *API endpoint* atau kebijakan CORS terlalu permisif. Hal ini dapat memicu risiko seperti *spoofing*, *tampering*, dan *information disclosure*. Untuk mengurangi kerentanan, diperlukan mitigasi seperti validasi CORS yang ketat, pembatasan *origin*, dan penggunaan enkripsi.

Berikut adalah rincian proses alur data berdasarkan setiap bagiannya:

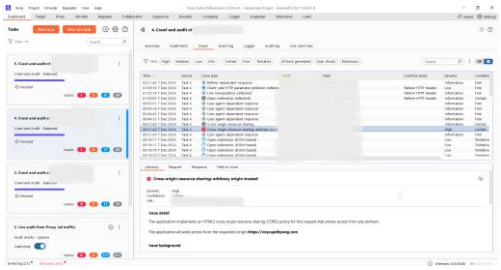
TABEL III. PROSES ALUR DATA

Komponen	Deskripsi Proses	Data yang terlibat	Aktor
Laptop, *Smartphone*	Pengguna mengakses website melalui browser pada perangkat mereka.	Permintaan HTTP, *input* seperti *login* atau pendaftaran.	Mahasiswa, Dosen, Admin/staff
Apache/Nginx, SSL/TLS	Mengelola permintaan pengguna, melayani file statis, dan memastikan koneksi aman.	Permintaan dan respons HTTP/HTTPS.	Administrator Jaringan
Halaman *Login*, Formulir Registrasi	Menerima input pengguna, validasi sisi klien, dan mengirimkan data ke *backend*.	Data *login* dan pendaftaran pengguna.	Mahasiswa, Dosen, Admin/staff
Logika Bisnis, Validasi Data, API	Memproses dan memvalidasi data pengguna	*Input* pengguna, respons validasi,	*Backend Developer, Sistem Aplikasi*

Komponen	Deskripsi Proses	Data yang terlibat	Aktor
	serta mengirimkan data ke *database*.	*query database*.	
Tabel Data Mahasiswa, Pendaftaran	Menyimpan dan mengelola data yang diterima dari *backend*, seperti data mahasiswa dan pendaftaran.	Data mahasiswa, evaluasi, status pendaftaran.	*Database* Administrator

4.2. Klasifikasi Ancaman

Untuk memahami ancaman yang dapat memengaruhi sistem informasi akademik Universitas X, pendekatan STRIDE digunakan untuk mengklasifikasikan jenis-jenis ancaman. Ancaman tersebut mencakup *spoofing*, *tampering*, *repudiation*, *information disclosure*, *denial of service*, dan *elevation of privilege*. Setiap ancaman memiliki karakteristik dan potensi dampak tertentu terhadap sistem, yang dijelaskan lebih rinci dalam tabel berikut. Misalnya, *spoofing* merujuk pada ancaman di mana pengguna dari *origin* yang tidak terpercaya dapat memalsukan permintaan ke server, sedangkan *tampering* melibatkan modifikasi data yang tidak sah. Dengan klasifikasi ini, diharapkan dapat diperoleh gambaran menyeluruh tentang risiko yang dihadapi oleh sistem.



Gambar 7. Analisis Kerentanan CORS

Gambar di atas merupakan tampilan dari *Burp Suite* yang digunakan untuk melakukan pengujian kemanan aplikasi web. Terdapat hasil pemindaian dengan metode *Crawl and Audit-Balanced*, yang mendeteksi beberapa jenis kerentanan salah satunya adalah *Cross-Origin Resource Sharing (CORS): Arbitrary Origin Trusted* dengan tingkat tinggi (*High*).

Akibat kerentanan ini memungkinkan pihak yang tidak terpercaya mengakses data atau berintraksi dengan sistem secara tidak aman, seperti mencuri informasi pengguna. Tingkat keparahan masalah ini ditandai sebagai tinggi (*high*) dengan keyakinan pasti (*certain*), yang berarti ini adalah masalah serius yang segera diperbaiki.

Gambar 8. Analisis Konfigurasi CORS dalam PHP

Berikut penjelasan dari ancaman berdasarkan kode konfigurasi CORS dari Gambar 8.

a. Line 1: ‘paths’ => [‘api/*’, ‘sanctum/csrf-cookie’],
   Ancaman terhadap T4 yaitu *Information Disclosure*, tidak adanya pembatasan yang jelas dalam mengakses jalur API sehingga menyebabkan kebocoran data sensitif, seperti token atau informasi pengguna, jika *origin* tidak terpercaya.
b. Line 2: ‘allowed_methods’ => [‘*’],
   Ancaman terhadap T2 yaitu *Tampering,* mengizinkan semua metode HTTP, termasuk yang sensitive seperti *PUT*, *DELETE*, dan *POST*, sehingga penyerang dapat memodifikasi data atau manipulasi permintaan yang tidak aman.
c. Line 5: ‘allowed_origins’ => [‘*’],
   Ancaman terhadap T1 yaitu *Spoofing,* mengizinkan semua *origin* (‘*’) tanpa batas sehingga *origin* yang tidak terpercaya dapat mengirimkan permintaan berbahaya yang dapat memalsukan identitas sehingga menjadi pengguna yang sah.
d. Line 7: ‘max_age’ => 0,
   Ancaman terhadap T5 yaitu *Denial of Service*, tidak mengatur waktu *cache* untuk *preflight request* dapat menyebabkan server terus memproses permintaan yang berulang, sehingga meningkatkan potensi serangan DoS.
e. Line 8: ‘supports_credentials’ => false,
   Ancaman terhadap T3 yaitu *Repudiation* dan T6 yaitu *Elevation of Privilege,* karena kredensial tidak diizinkan untuk disertakan dalam permintaan, sehingga penyerang memungkinkan mengakses sumber daya tanpa batas dengan sah (T6) dan melakukan tindakan berbahaya (T3).

Untuk memahami Ancaman yang diidentifikasi dalam konfigurasi CORS, tabel di bawah ini menyajikan klasifikasi Ancaman berdasarkan model STRIDE.

TABEL IV. KLASIFIKASI ANCAMAN

ID	Deskripsi	STRIDE
T1	Pengguna dari *origin* tidak terpercaya dapat memalsukan permintaan ke server karena kebijakan CORS mengizinkan *arbitrary origin*.	*Spoofing*
T2	Penyerang memodifikasi permintaan atau respons HTTP yang melewati *origin* tidak terpercaya yang diizinkan oleh kebijakan CORS.	*Tampering*
T3	Tidak adanya validasi *origin* yang jelas dalam kebijakan CORS memungkinkan penyerang mengklaim bahwa tindakan mereka dilakukan oleh pihak yang sah.	*Repudiation*
T4	Data sensitif seperti token atau informasi pengguna dapat bocor karena *origin* tidak terpercaya diizinkan oleh kebijakan CORS.	*Information Disclosure*
T5	Penyerang mengirimkan permintaan terus-menerus dari *origin* yang diizinkan untuk membebani server dan menyebabkan layanan terganggu.	*Denial of Service*
T6	Penyerang memanfaatkan kebijakan CORS untuk mendapatkan akses istimewa terhadap data atau fungsi yang seharusnya terbatas.	*Elevation of Privilege*

4.3. Penilaian Ancaman

Tahap penilaian ancaman bertujuan untuk menentukan ranking risiko berdasarkan ancaman yang telah diklasifikasikan pada Tabel V menggunakan pendekatan DREAD. Prosesnya meliputi:

a. Penilaian ancaman dilakukan pada tiap kategori DREAD dengan skala yaitu tinggi (3), sedang (2), dan rendah (1)[20].
b. Contoh ancaman T1: "Pengguna dari *origin* tidak terpercaya dapat memalsukan permintaan ke server."
    1. (D) *Damage potential*, ancaman T1 diberikan nilai potensi kerusakan sebesar 3 karena dapat menyebabkan kebocoran kredensial pengguna, serta memungkinkan akses tidak sah ke sistem.
    2. (R) *Reproducibility*, ancaman T1 diberikan nilai reproduksi sebesar 3 karena jika penyerang berhasil memperoleh kredensial *login* milik pengguna, serangan dapat dengan mudah dilakukan secara berulang.
    3. (E) *Exploitability* ancaman T1 dinilai memiliki tingkat *exploitability* sedang (nilai 2), karena diperlukan upaya atau langkah tertentu untuk mendapatkan kredensial yang diperlukan untuk memalsukan permintaan ke server. Namun langkah-langkahnya relatif sederhana.
    4. (A) *Affected users* ancaman T1 diberikan nilai sebesar 3 karena serangan ini memungkinkan pemalsuan permintaan dari *origin* tidak terpercaya, sehingga dapat mengakses banyak akun sekaligus.
    5. (D) *Discoverability* ancaman T1 dinilai memiliki tingkat *discoverability* tinggi (nilai 3) karena sifatnya yang mudah dikenali, di mana penyerang dapat dengan cepat menemukan kelemahan dengan alat otomatis seperti Burp Suite.
c. Berdasarkan proses penilaian ancaman setiap kategori DREAD pada langkah ketiga, diperoleh nilai setiap kategori yaitu D = 3, R = 3, E = 2, A = 3, dan D = 3, sehingga dihasilkan perhitungan $\frac{3+3+2+3+3}{5}$.

TABEL V. KLASIFIKASI ANCAMAN

Kategori	Tinggi(3)	Sedang(2)	Rendah(1)
D	Penyerang dapat menguasai system keamanan secara penuh, mendapatkan akses penuh sebagai admin, dan mampu melakukan tindakan seperti menunggah konten	Informasi penting bocor tetapi kerugiannya masih bisa dikelola.	Kebocoran informasi yang sepele atau tidak signifikan.

Kategori	Tinggi(3)	Sedang(2)	Rendah(1)
	tanpa batas.		
R	Serangan bisa diulangi tanpa batas dan kapan saja untuk mengkesploitasi sistem	Serangan dapat diulangi, tetapi hanya dalam jangka waktu tertentu atau dengan persyaratan khusus.	Serangan sulit diulangi, meskipun celah kemanan sudah diketahui oleh penyerang.
E	Serangan dilakukan oleh individu yang masih pemula dalam waktu singkat.	Serangan dilakukan oleh individu yang terampil dalam waktu yang lama.	Serangan dilakukan oleh individu yang berpengalaman.
A	Dampak dari serangan memengaruhi banyak pengguna.	Dampak dari serangan memengaruhi sebagian dari pengguna,	Dampak dari serangan terbatas pada jumlah kecil.
D	Informasi tentang celah kemanan sangat jelas dan mudah ditemukan oleh penyerang.	Kerentanan ditemukan di bagian sistem yang jarang digunakan, membutuhkan upaya lebih untuk menemukannya.	Kerentanan sulit ditemukan karena bug hampir tidak terlihat, dan potensi kerusakannya sangat kecil.

d. Hasil perhitungan total nilai ancaman kemudian diranking sesuai aturan peringkat ancaman seperti pada Tabel V, yaitu rentang nilai antara 1.0–1.5 adalah risiko rendah, rentang nilai antara 1.6–2.5 adalah risiko sedang, dan rentang nilai antara 2.6–3.0 adalah risiko tinggi[20]. Perhitungan pada langkah ketiga menghasilkan total nilai 2.8, sehingga dapat dikatakan bahwa ancaman T1 merupakan ancaman dengan risiko tinggi.

e. Seluruh ancaman akan dinilai dengan langkah-langkah tersebut. Penilaian setiap kategori DREAD untuk setiap ancaman yang teridentifikasi disajikan pada Tabel VI.

TABEL VI. PENILAIAN DREAD

ID	Deskripsi	D	R	E	A	D	Total	Risiko
T1	Pengguna dari *origin* tidak terpercaya dapat memalsukan permintaan ke server.	3	3	2	3	3	2.8	Tinggi
T2	Penyerang memodifikasi permintaan atau respons HTTP melalui *origin* tidak terpercaya.	2	3	2	2	2	2.2	Sedang
T3	Tidak adanya validasi *origin* memungkinkan penyerang mengklaim tindakan mereka dilakukan oleh pihak sah.	2	2	2	2	2	2.0	Sedang
T4	Data sensitif seperti token atau informasi pengguna dapat bocor karena *origin* tidak terpercaya.	3	3	3	3	3	3.0	Tinggi
T5	Penyerang mengirimkan permintaan terus-menerus dari *origin* yang diizinkan untuk	3	3	2	3	2	2.6	Tinggi

ID	Deskripsi	D	R	E	A	D	Total	Risiko
	membebani server.							
T6	Penyerang memanfaatkan kebijakan CORS untuk mendapatkan akses istimewa terhadap data atau fungsi yang terbatas.	3	3	3	3	3	3.0	Tinggi

4.4. Mitigasi

Setelah ancaman diidentifikasi dan diklasifikasikan, langkah berikutnya adalah menentukan strategi mitigasi untuk mengurangi dampak dari ancaman tersebut. Tabel berikut menyajikan berbagai strategi mitigasi yang disesuaikan dengan ancaman yang telah diidentifikasi sebelumnya. Setiap ancaman dikaitkan dengan potensi dampaknya terhadap sistem, serta solusi yang dapat diterapkan untuk meningkatkan keamanan. Misalnya, ancaman *spoofing* dapat dimitigasi dengan menerapkan validasi ketat pada kebijakan CORS, sedangkan ancaman *denial of service* (DoS) dapat diatasi dengan membatasi jumlah permintaan dari *origin* tertentu. Berdasarkan OWASP: *Cross-Origin Resource Policy* (CORP), kebijakan yang tidak tepat dalam konfigurasi CORS dapat menyebabkan kebocoran data sensitif dan meningkatkan risiko eksploitasi oleh pihak yang tidak sah. Strategi mitigasi ini memberikan panduan praktis bagi pengelola sistem untuk melindungi data dan memastikan keberlanjutan layanan.

TABEL VII. STRATEGI MITIGASI

STRIDE	Ancaman	Dampak	Mitigasi
Spoofing	Pengguna dari *origin* tidak sah memalsukan permintaan ke server.	Manipulasi data yang merusak integritas sistem dan reputasi.	Validasi kebijakan CORS secara ketat, izinkan hanya *origin* terpercaya, tambahkan header CSP.
Tampering	Modifikasi permintaan atau *respons* HTTP oleh penyerang.	Data menjadi tidak valid, menyebabkan sistem berfungsi tidak semestinya.	Gunakan *whitelist* untuk validasi *origin* dan blokir akses tidak sah dengan status 403.
Repudiation	Penyerang menyamar sebagai pihak sah karena kurangnya validasi *origin*.	Tidak ada jejak yang dapat dipercaya, merusak kepercayaan sistem.	Verifikasi *origin* dengan *whitelist* dan validasi menggunakan token atau kredensial pengguna.
Information Disclosure	Kebocoran data sensitif melalui *origin* tidak terpercaya.	Data pribadi dapat disalahgunakan, mengakibatkan pelanggaran privasi.	Enkripsi data dengan TLS saat transit, batasi akses data berdasarkan prinsip "*least privilege*".
Denial of Service	Permintaan berulang dari *origin* sah membebani server.	Layanan terganggu, mengurangi kualitas layanan dan potensi kerugian.	Terapkan *rate limiting* dan mekanisme deteksi serangan DDoS.
Elevation of Privilege	Penyerang memperoleh akses ke fungsi atau data terbatas.	Penyalahgunaan data atau pelanggaran sistem.	Gunakan autentikasi berbasis peran dan tambahkan header keamanan seperti *X-Content-Type-Options*.

Mitigasi langsung dilakukan dengan merubah kode konfigurasi CORS yang sebelumnya sudah dijelaskan pada bagian klasifikasi ancaman.

Berikut penjelasan kode konfigurasi CORS yang sudah diperbaharui:

a. Line 1: ‘paths’ => [‘api/*’, ‘sanctum/csrf-cookie’],

Pengaturan *endpoint* diterapkan dalam aturan CORS pada semua rute di bawah "api/*" dan rute "sanctum/csrf-cookie".

b. Line 2: 'allowed_methods' => [],
Jika kosong maka akan dibatasi metode HTTP yang diizinkan yaitu "GET dan POST".

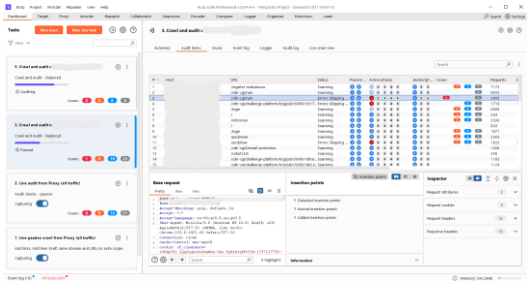
c. Line 5: 'allowed_origins' => [],
Menggunakan *whitelist origin* untuk memastikan hanya domain yang terpercaya yang diizinkan mengakses *API*.

d. Line 7: 'max_age' => 3600,
Cache preflight diatur selama 1 jam untuk mengurangi *overhead* server.

e. Line 8: 'supports_credentials' => true,
Izinkan kredensial jika diperlukan, sehingga penyerang memungkinkan mengakses sumber daya terbatas dengan sah dan menyangkal tindakan berbahaya yang dilakukan.

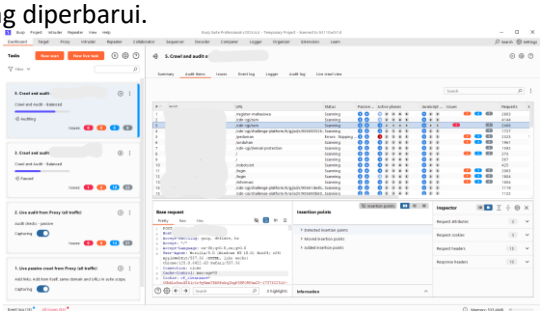
Gambar 9. Pembaharuan Kode Konfigurasi CORS dalam PHP

Berikut perbedaan hasil konfigurasi CORS sebelum (Gambar 10) dan sesudah (Gambar 11) dilakukan mitigasi:



Gambar 10. Sebelum Mitigasi

Pada Gambar 10 dan Tabel VIII sebelum mitigasi, ditemukan sejumlah kelemahan pada konfigurasi CORS yang memungkinkan akses lintas asal tanpa pembatasan yang memadai. Terdeteksi 6 isu kritikal, 19 isu *medium*, dan 23 isu *low*, yang menunjukkan bahwa server berpotensi rentan terhadap serangan, seperti eksploitasi oleh pihak ketiga akibat kebijakan *origin* yang terlalu permisif dan pengaturan kredensial yang tidak aman. Selain itu, konfigurasi waktu *cache* yang tidak tepat dapat meningkatkan risiko serangan berulang terhadap server. Sebaliknya, Gambar 11 dan Tabel VIII sesudah mitigasi, menunjukkan peningkatan signifikan dalam keamanan, dengan berkurangnya jumlah isu menjadi 1 isu kritikal, 4 isu *medium*, dan 1 isu *low*. Hal ini menandakan bahwa panduan OWASP mengenai pengujian CORS menekankan pentingnya validasi yang ketat terhadap origin yang diizinkan dan pembatasan metode HTTP yang diperbolehkan untuk mencegah potensi penyalahgunaan, serta OWASP: CORS *Request Preflight Scrutiny* membahas pentingnya mengatur ulang waktu *cache* dan kredensial agar lebih aman. Dengan perbaikan ini, server kini lebih terlindungi dan hanya mengizinkan akses dari sumber yang terpercaya sesuai dengan kebijakan keamanan yang diperbarui.



Gambar 11. Sesudah Mitigasi

Sebagai tambahan, berikut adalah perbandingan kerentanan yang terdeteksi sebelum dan sesudah mitigasi:

TABEL VIII. PERBANDINGAN KERENTANAN

Kondisi	Isu Kritikal	Isu Medium	Isu Rendah
Sebelum mitigasi	6	19	23
Sesudah mitigasi	1	4	1

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Penelitian ini berhasil mengidentifikasi dan mengevaluasi berbagai ancaman yang terdapat pada sistem layanan pendidikan Universitas X dengan menggunakan pendekatan *threat modeling* berbasis STRIDE dan DREAD. Ancaman dengan tingkat risiko tinggi, seperti *information disclosure* dan *elevation of privilege*, DREAD menunjukkan bahwa ancaman T4 dan T6 telah diidentifikasi memiliki skor tertinggi, sehingga mitigasi harus diprioritaskan. Beberapa langkah mitigasi yang diusulkan meliputi validasi ketat pada kebijakan CORS, penerapan enkripsi data, serta pembatasan akses berbasis peran. Berdasarkan hasil analisis akhir, implementasi mitigasi pada kebijakan CORS menunjukkan penurunan signifikan dalam jumlah isu kerentanan yang terdeteksi.

5.2. Saran

Penelitian di masa mendatang dapat memperluas ruang lingkup analisis dengan memanfaatkan teknologi keamanan terbaru, seperti kecerdasan buatan (AI) untuk mendeteksi ancaman secara *real-time*, atau dengan menerapkan kerangka kerja *Zero Trust*. Selain itu, pendekatan yang digunakan dalam penelitian ini juga dapat diterapkan pada sistem layanan pendidikan lainnya untuk menciptakan solusi keamanan yang lebih menyeluruh.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak Universitas X atas dukungan dan kerja sama yang diberikan selama proses penelitian ini. Ucapan terima kasih juga disampaikan kepada dosen pembimbing, rekan-rekan, dan semua pihak yang telah memberikan kontribusi dalam penyusunan artikel ini. Dukungan dan masukan yang diberikan sangat membantu dalam menyelesaikan penelitian ini dengan baik.

DAFTAR PUSTAKA

[1] H. Putri, N. P. Hariani, T. Febrianti, and T. Sutabri, "IJM: Indonesian Journal of Multidisciplinary Teknologi Pendidikan dan Tranformasi Digital di Indonesia Selama Pandemi," 2023. [Online]. Available: https://journal.csspublishing/index.php/ijm

[2] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2024," https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. .

[3] S. Paramita, S. A. Siregar, R. A. Damanik, and M. Dedi Irawan, "Bulletin of Information Technology (BIT) Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013," vol. 3, no. 4, pp. 374–379, 2022, doi: 10.47065/bit.v3i1.

[4] L. Mauri and E. Damiani, "Modeling Threats to AI-ML Systems Using STRIDE †," *Sensors*, vol. 22, no. 17, Sep. 2022, doi: 10.3390/s22176662.

[5] K. H. Kim, K. Kim, and H. K. Kim, "STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery," *ETRI Journal*, vol. 44, no. 6, pp. 991–1003, Dec. 2022, doi: 10.4218/etrij.2021-0181.

[6] D. Dalilah, D. Syamsuar, and Y. N. Kunang, "EVALUASI RESIKO KEAMANAN MENGGUNAKAN MODEL DREAD TERHADAP SISTEM INFORMASI AKADEMIK UNIVERSITAS XYZ."

[7] M. K. Faridi, I. Riadi, and Y. Prayudi, "Pemodelan Ancaman Sistem Keamanan E-Health menggunakan Metode STRIDE dan DREAD," *Edumatic: Jurnal Pendidikan Informatika*, vol. 5, no. 2, pp. 157–166, Dec. 2021, doi: 10.29408/edumatic.v5i2.3652.

[8] A. C. Laksono, "Threat Modeling pada Sistem Informasi Akademik Menggunakan Pendekatan STRIDE dan DREAD."

[9] L. Cerovic, "StrideLang: Creation of a Domain-Specific Threat Modeling Language using STRIDE, DREAD and MAL," 2022.

[10] A. Frisdayanti, "Peranan Brainware Dalam Sistem Informasi Manajemen," *JEMSI (Jurnal Ekonomi dan Manajemen Sistem Informasi)*, vol. vol.1, 2019, doi: 10.31933/JEMSI.

[11] H. A. Salsabila and I. Iriyadi, "Evaluasi Atas Penerapan Sistem Informasi Akademik Dan Keuangan Terhadap Tingkat Kepuasan Mahasiswa," *JAS-PT (Jurnal Analisis Sistem Pendidikan Tinggi Indonesia)*, vol. 4, no. 2, p. 137, Dec. 2020, doi: 10.36339/jaspt.v4i2.348.

[12] W. Krisna Hamid Jumasa Muhammad Ambadar Nadia, "RANCANG BANGUN SISTEM INFORMASI AKADEMIK MENGGUNAKAN FRAMEWORK CODEIGNITER PADA UNIVERSITAS MUHAMMADIYAH PURWOREJO," 2022.

[13] A. N. Puriwigati, "Sistem Informasi Manajemen-Keamanan Informasi." [Online]. Available: https://www.researchgate.net/publication/341293613

[14] S. Nurul, S. Anggrainy, and S. Aprelyani, "FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM)," vol. 3, no. 5, 2022, doi: 10.31933/jemsi.v3i5.

[15] M. Betty Yel and M. K. M Nasution, "KEAMANAN INFORMASI DATA PRIBADI PADA MEDIA SOSIAL," *JIK)*, vol. 6, no. 1, 2022.

[16] S. M. Khalil, H. Bahsi, and T. Korõtko, "Threat modeling of industrial control systems: A systematic literature review," *Comput Secur*, vol. 136, Jan. 2024, doi: 10.1016/j.cose.2023.103543.

[17] J. D. S. Y. N. I. A. Andriyan Dwi Putra, "ANALISIS ANCAMAN SMISHING PADA SMARTPHONE MENGGUNAKAN STRIDE SEBAGAI PEMODELAN ANCAMAN," *Jurnal Teknologi Informasi dan Komputer*, vol. 8, pp. 173–179, Oct. 2022.

[18] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies," *IEEE Access*, vol. 9, pp. 29775–29818, 2021, doi: 10.1109/ACCESS.2021.3058403.

[19] A. Hammami, "The Art of Threat Modeling," *Journal of Computer Sciences and Informatics*, vol. 1, no. 1, p. 1, 2024, doi: 10.5455/jcsi.20240710052550.

[20] L. Zhang, A. Taal, R. Cushing, C. de Laat, and P. Grosso, "A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces," *Int J Inf Secur*, vol. 21, no. 3, pp. 509–525, Jun. 2022, doi: 10.1007/s10207-021-00566-3.