Threat Modeling pada Sistem Informasi Akademik Menggunakan Pendekatan STRIDE dan DREAD

Azis Catur Laksono

16917203

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2020

Lembar Pengesahan Pembimbing

Threat Modeling pada Sistem Informasi Akademik Menggunakan Pendekatan STRIDE dan DREAD

Azis Catur Laksono
16917203

Yogyakarta, Desember 2020

Pembimbing

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

Lembar Pengesahan Penguji

Threat Modeling pada Sistem Informasi Akademik
Menggunakan Pendekatan STRIDE dan DREAD

Azis Catur Laksono
16917203

Yogyakarta, Desember 2020

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M.Kom.
Ketua

Dr. Ir. Bambang Sugiantoro, S.Si., M.T.
Anggota I

Dr. Imam Riadi, M.Kom.
Anggota II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Universitas Islam Indonesia

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

Abstrak

Threat Modeling pada Sistem Informasi Akademik Menggunakan Pendekatan STRIDE dan DREAD

Penerapan sistem informasi akademik ternyata membuka peluang risiko baru berupa ancaman-ancaman yang dapat mengganggu keberlangsungan sistem. Risiko ini bahkan lebih buruk dapat mengakibatkan kerugian pada organisasi. Sistem informasi akademik memiliki peran penting dalam proses bisnis Universitas XYZ, sehingga keberlangsungan sistem ini perlu dijaga dari kemungkinan ancaman dan risiko yang merugikan perguruan tinggi. *Threat modeling* (pemodelan ancaman) merupakan salah satu upaya untuk menganalisis ancaman pada sistem informasi. *Threat modeling* diterapkan dengan tahapan dekomposisi aplikasi, klasifikasi ancaman, penilaian risiko ancaman, dan penyusunan langkah mitigasi. Setiap ancaman diidentifikasi berdasarkan jenis ancaman yang telah dikategorikan pada metodologi *STRIDE*. Hasil klasifikasi ancaman selanjutnya dinilai menggunakan metodologi *DREAD* untuk mengetahui tingkat risiko setiap ancaman. Tahapan ini akan menghasilkan ranking risiko setiap ancaman sehingga dapat disusun kontrol mitigasi setiap ancaman untuk meminimalkan risiko. Melalui tahapan *threat modeling*, diketahui bahwa ancaman yang memiliki risiko tinggi pada Sistem Informasi Akademik Universitas XYZ adalah ancaman kategori *spoofing*, *tampering*, dan *repudiation*. Fokus penyusunan kontrol mitigasi dilakukan pada ketiga kategori ancaman ini karena memiliki peringkat risiko tinggi.

Kata kunci

sistem informasi, akademik, pemodelan ancaman, threat model, STRIDE, DREAD

Abstract

Threat Modeling in Academic Information Systems Using the STRIDE and DREAD Approaches

The application of academic information systems actually opens up new risk opportunities in the form of threats that can disrupt the sustainability of the system. This risk can lead to even worse harm to the organization. The academic information system has an important role in the XYZ University business process so that the sustainability of this system needs to be protected from possible threats and risks that harm the university. Threat modeling is an effort to analyze threats to information systems. Threat modeling is applied with the stages of application decomposition, threat classification, threat risk assessment, and preparation of mitigation measures. Each threat is identified based on the type of threat that has been categorized in the STRIDE methodology. The results of the threat classification are then assessed using the DREAD methodology to determine the level of risk for each threat. This step will produce a risk ranking for each threat so that mitigation controls can be arranged for each threat to minimize risk. Through the threat modeling stage, it is known that the threat that has a high risk in the Academic Information System of XYZ University is the threat of the Spoofing, Tampering, and Repudiation categories. The focus of the preparation of mitigation controls is carried out on these three threat categories because they have a high risk rating.

Kata kunci

information systems, academic, threat model, STRIDE, DREAD

Pernyataan Keaslian Tulisan

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

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

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

Yogyakarta, Desember 2020

Azis Catur Laksono, S.Kom.

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Publikasi berikut menjadi bagian dalam penulisan tesis ini.

Laksono, A. C., & Prayudi, Y. (2020). Threat Modeling Menggunakan Pendekatan STRIDE dan DREAD untuk Mengetahui Risiko dan Mitigasi Keamanan pada Sistem Informasi Akademik. Justindo, 6 (1).

Kontributor	Jenis Kontributor
Azis Catur Laksono	Mendesain eksperimen (70%) Menulis paper (100%)
Yudi Prayudi	Memberi ide dan saran (30%) Mereview artikel

Halaman Kontribusi

Penelitian ini tidak terlepas dari berbagai saran maupun bimbingan dari berbagai pihak, mulai dari pra penelitian, seminar proposal, seminar progres, hingga seminar ujian pendadaran. Pihak-pihak tersebut antara lain adalah Dr. Yudi Prayudi, S.Si., M.Kom., Dr. Ir. Bambang Sugiantoro, S.Si., M.T., dan Dr. Imam Riadi, M.Kom.

Halaman Persembahan

Dengan mengucapkan syukur Alhamdulillah, karya penelitian ini penulis persembahkan kepada orang-orang yang selama ini telah mendukung, memberikan semangat, dan motivasi penulis dalam menyelesaikan pendidikan magister di Universitas Islam Indonesia, secara khusus kepada:

1. Kedua orang tua, kakak, istri, dan kedua anak yang selalu memberi dorongan dan semangat untuk menyelesaikan studi magister.
2. Teman-teman seperjuangan konsentrasi Forensika Digital angkatan XV.

Kata Pengantar

Puji syukur kehadirat Allah Subhana wata'ala yang telah melimpahkan rahmat, taufiq dan hidayah kepada penulis sehingga dapat menyelesaikan laporan tesis dengan judul "Threat Modeling pada Sistem Informasi Akademik Menggunakan Pendekatan STRIDE dan DREAD". Semoga sholawat dan salam selalu terlimpah pada Nabi Muhammad Sholallahu'alaihi wassalam.

Atas selesainya penelitian ini penulis mengucapkan terima kasih kepada pihak-pihak yang telah mendukung dalam penyusunan tesis, yaitu:

1. Bapak Fathul Wahid, S.T., M.Sc., Ph.D., selaku Rektor Universitas Islam Indonesia yang memberikan kesempatan kepada penulis untuk mengembangkan ilmu di Universitas Islam Indonesia.
2. Bapak Prof. Hari Purnomo, M.T selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia yang memberikan fasilitas dan bantuan untuk belajar.
3. Ibu Izzati Muhimmah, ST., M.Sc., Ph.D., selaku Ketua Program Studi Informatika Program Magister Fakultas Teknologi Industri Universitas Islam Indonesia, yang selalu memberikan semangat kepada setiap mahasiswa agar segera menyelesaikan tesis.
4. Bapak Dr. Yudi Prayudi, S.Si., M.Kom., selaku dosen pembimbing yang selalu memberikan berbagai saran selama proses bimbingan.
5. Bapak Dr. Ir. Bambang Sugiantoro, S.Si., M.T., dan Bapak Dr. Imam Riadi, M.Kom., selaku Dosen Penguji Ujian Tesis yang telah memberikan berbagai saran perbaikan untuk penelitian ini.
6. Seluruh dosen, staff administrasi dan civitas Magister Informatika Universitas Islam Indonesia, baik secara langsung maupun tidak langsung telah membantu penulis selama studi.
7. Seluruh keluarga yang telah mencurahkan segenap cinta, kasih sayang, perhatian dan dukungannya.
8. Rekan-rekan mahasiswa Magister Informatika khususnya konsentrasi Forensika Digital angkatan XV yang selama ini berjuang bersama dan selalu memberikan semangat satu sama lain.
9. Semua pihak yang telah membantu dalam penyusunan tesis ini.

Penulis menyadarai bahwa penulisan tesis ini masih jauh dari sempurna. Untuk itu penulis mengharapkan kritik dan saran yang bersifat membangun sebagai bentuk perbaikan laporan penelitian ini. Akhir kata penulis mengucapkan terima kasih, semoga penyusunan laporan ini dapat memberikan inspirasi maupun manfaat bagi pembaca, khususnya bagi mahasiswa/mahasiswi Universitas Islam Indonesia.

Yogyakarta, Desember 2020

Penulis

Daftar Isi

Daftar Tabel

Daftar Gambar

BAB 1
Pendahuluan

1.1 Latar Belakang

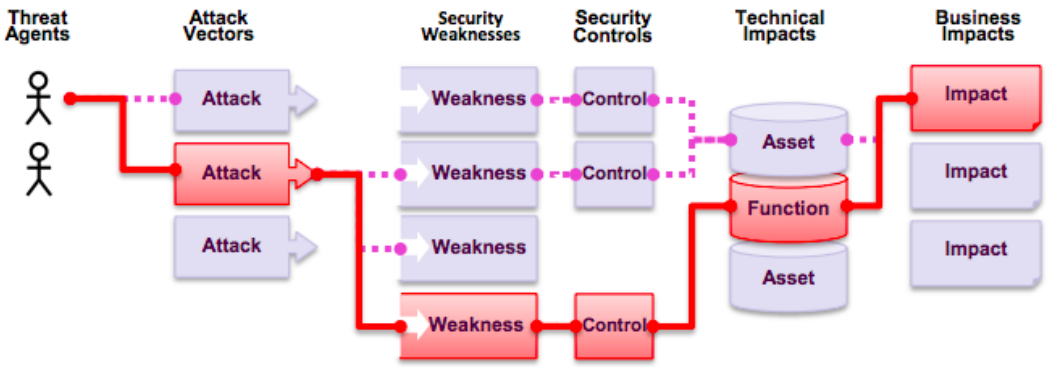
Pesatnya perkembangan teknologi informasi dan komunikasi mampu mengiring instansi pendidikan untuk mengubah model manajemen administratif akademik menjadi sistem terkomputerisasi. Kecepatan dan keakuratan data dalam penyajian informasi yang ditawarkan sistem komputer, menjadi daya tarik tersendiri bagi organisasi untuk bermigrasi dari proses administratif konvensional ke dalam bentuk sistem informasi.

Salah satu sistem informasi yang sering diimplementasikan dalam suatu perguruan tinggi adalah sistem informasi akademik. Sistem ini merupakan media untuk memanajemen kebutuhan administratif yang terkait dengan proses bisnis akademik. Penerapan sistem informasi akademik di perguruan tinggi juga dijadikan sebagai salah satu indikator kepuasan pelayanan terhadap konsumen. Selain itu penggunaan sistem informasi akademik juga diharapkan dapat meningkatkan kinerja perguruan tinggi dalam penyampaian informasi kepada peserta didik, staf pengajar, termasuk tenaga administrasi.

Dengan kelebihan seperti ini, banyak perguruan tinggi mulai mengimplementasikan sistem informasi akademik dalam kegiatan proses bisnisnya. Namun, saat beralih dari sistem konvensional ke sistem informasi, tidak selamanya pemanfaatan teknologi ini berjalan sesuai harapan. Peralihan sistem yang memanfaatkan jaringan komputer dan internet ini ternyata membuka peluang risiko baru berupa ancaman-ancaman yang dapat mengganggu keberlangsungan sistem informasi sehingga dapat mengakibatkan kerugian bagi instansi. Ancaman adalah suatu aksi atau kejadian yang dapat merugikan perusahaan dengan kerugian bias berupa uang/biaya, tenaga upaya, peluang bisnis, reputasi nama baik, dan kerugian terburuk adalah membuat perusahaan pailit (Sutabri, 2012). Penyalahgunaan teknologi informasi oleh oknum yang tidak bertanggung jawab misalnya adalah menyusup ke dalam sistem dengan maksud ingin merusak, mengubah, atau mengganti, bahkan menghapus data penting milik instansi. Ancaman-ancaman pada sistem ini merupakan risiko yang harus dicegah sebelum menjadi serangan pada sistem informasi.

Saat membangun sistem informasi, para pengembang sistem biasanya hanya fokus terhadap fitur dan fungsionalitas sistem, dan mengabaikan implementasi keamanan sistem hingga akhir pengembangan. Dalam hal ini, masalah keamanan sistem informasi sering kurang mendapat perhatian dari para pengembang sistem. Model pengembangan seperti ini

telah terbukti menjadi bencana, karena banyak kerentanan yang tidak terdeteksi sehingga aplikasi berpeluang untuk diserang dan mudah rusak. Saat ancaman benar-benar terjadi, justru keamanan sistem baru mendapat perhatian. Padahal kehilangan atau kerusakan data dan informasi merupakan hal kritis bagi suatu organisasi karena data dan informasi merupakan aset berharga yang harus terjaga keutuhannya. Gambar 1.1 menunjukkan contoh ancaman yang berpotensi menjadi serangan pada sistem (Dehalwar, Kalam, Kolhe, & Zayegh, 2018).



Gambar 1.1. Potensi ancaman sistem informasi

Tak dapat dipungkiri, data adalah salah satu aset milik instansi yang berharga, sehingga sistem informasi akademik sebagai media untuk memanajemen kebutuhan administratif harus dipastikan keamanan dan integritasnya dalam mengolah data. Hal ini merupakan upaya untuk melindungi keutuhan data tanpa mengesampingkan kinerja sistem agar dapat dimanfaatkan pengguna secara optimal. Sistem informasi yang rentan untuk disusupi oleh pihak lain tentu akan mengakibatkan keutuhan dan keakuratan datanya dipertanyakan. Di sini peran penting keamanan informasi sebagai perlindungan informasi dan sistem informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi atau pengrusakan (Syafitri, 2016).

Universitas XYZ merupakan instansi pendidikan tinggi yang menerapkan sistem informasi akademik, sehingga dengan keberadaan sistem informasi akademik secara tidak langsung membuka akses dari pihak luar walau secara kasat mata pengguna hanya melihat data tertentu yang ditampilkan. Dengan adanya fenomena berupa ancaman-ancaman tersebut, maka perlu dilakukan analisis terhadap kemungkinan ancaman dan risiko yang terjandi pada Sistem Informasi Akademik Universitas XYZ.

Untuk menganalisis ancaman secara tepat, *threat modeling* (pemodelan ancaman) dapat diterapkan sebagai upaya untuk mengidentifikasi ancaman dan risiko pada sistem informasi akademik. *Threat modeling* merupakan proses terstruktur yang dapat mendeteksi

kemungkinan kerentanan dan ancaman keamanan, mengukur tingkat keparahan dari setiap potensi risiko, dan memprioritaskan langkah perlindungan dan meminimalkan serangan terhadap infrastruktur (EC-Council, 2020). Pemodelan ancaman berguna untuk mengidentifikasi dan menilai suatu ancaman yang dapat memengaruhi sistem secara sistematis. Proses pemodelan ancaman dibagi menjadi tiga langkah utama yaitu dekomposisi aplikasi, klasifikasi ancaman, dan penentuan tindakan pencegahan untuk mengurangi risiko ancaman (Owasp.org, 2020).

Untuk keperluan analisis ancaman, *Microsoft* telah mengembangkan suatu metode klasifikasi ancaman yaitu *STRIDE*. Metode ini merupakan pengelompokan ancaman yang terdiri dari *Spoofing* (pencurian identitas), *Tampering* (modifikasi data), *Repudiation* (penyangkalan), *Information disclosure* (mengekspos informasi rahasia), *Denial of service* (gangguan layanan), dan *Elevation of priviledge* (mendapatkan hak akses lebih) (Mahmood, 2017). Menurut EC-Council (2020), metodologi STRIDE saat ini adalah metode pemodelan ancaman yang paling berkembang, yang telah berevolusi selama bertahun-tahun dengan memuat tabel baru berbasis ancaman dan varian *STRIDE-per-Interaction* dan *STRIDE-per-Element.* Metodologi *STRIDE* bertujuan untuk memastikan bahwa aplikasi memenuhi arahan keamanan dari aturan *CIA* (*Confidentiality*: kerahasiaan, *Integrity*: integritas, dan *Availability*: ketersediaan), di samping *Authentication* (autentikasi), *Authorization* (otorisasi), dan *Non-Repudiation* (Non-repudiasi).

Selanjutnya untuk mengetahui dampak yang terjadi akibat munculnya ancaman keamanan ini, perlu dilakukan rangkaian proses penilaian risiko terhadap ancaman-ancaman yang muncul dengan metodologi *DREAD*, yaitu *Damage potential* (potensi kerusakan), *Reproducibility* (reproduksibilitas), *Exploitability* (eksploitasi), *Affected user* (pengguna terdampak), dan *Discoverability* (dapat ditemukan). Dikembangkan oleh *Microsoft*, *DREAD* dipahami sebagai *add-on* model *STRIDE* yang memungkinkan bagi pemodel untuk memberi peringkat ancaman setelah diidentifikasi (Fruhlinger, 2020). Metodologi *DREAD* ini digunakan untuk menilai, membandingkan, dan memprioritaskan tingkat keparahan risiko yang disajikan oleh setiap ancaman yang telah diklasifikasikan melalui model *STRIDE* (Mahmood, 2017).

Mengingat peran sistem informasi akademik yang erat dengan proses bisnis Universitas XYZ maka keberlangsungan sistem ini perlu dijaga dari kemungkinan ancaman dan risiko yang merugikan perguruan tinggi. Dengan implementasi metodologi *threat modeling*, diharapkan ancaman dapat diminimalkan melalui penerapan tindakan pencegahan yang tepat.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang, rumusan masalah untuk penelitian ini sebagai berikut.

a. Apa saja ancaman yang teridentifikasi pada Sistem Informasi Akademik Universitas XYZ berdasarkan pemodelan *STRIDE*?
b. Jenis ancaman apa yang memiliki peringkat risiko tinggi pada Sistem Informasi Akademik Universitas XYZ berdasarkan pemodelan *DREAD*?
c. Apa saja langkah mitigasi yang perlu diterapkan untuk mengantisipasi ancaman yang memiliki peringkat risiko tinggi?

1.3 Batasan Masalah

Agar penelitian ini tidak keluar dari pokok permasalahan yang dirumuskan, maka ruang lingkup pembahasan pada penelitian ini memiliki batasan sebagai berikut.

a. Pemodelan ancaman terbatas pada Sistem Informasi Akademik Universitas XYZ
b. Penilaian risiko ancaman berdasarkan aset perangkat lunak pada Sistem Informasi Akademik Universitas XYZ
c. Klasifikasi ancaman sistem informasi akademik menggunakan pemodelan *STRIDE*
d. Penilaian risiko ancaman sistem informasi akademik menggunakan pemodelan *DREAD*
e. Fokus utama penyusunan kontrol mitigasi adalah pada ancaman yang memiliki ranking risiko tinggi.

1.4 Tujuan Penelitian

Penelitian ini memiliki tujuan sebagai berikut.

a. Mengidentifikasi dan menganalisis ancaman-ancaman yang mungkin akan muncul pada sistem informasi akademik
b. Mengetahui ranking dari setiap risiko yang berhasil diidentifikasi pada sistem informasi akademik
c. Menentukan tahapan mitigasi sebagai langkah meminimalkan risiko ancaman yang teridentifikasi memiliki peringkat risiko tinggi.

1.5 Manfaat Penelitian

Adapun manfaat yang ingin dicapai dalam penelitian ini adalah sebagai berikut.

a. Sebagai bahan kajian tentang keamanan sistem informasi akademik
b. Sebagai referensi untuk tim pengembang sistem informasi akademik terkait unsur-unsur keamanan sistem informasi dalam pengembangan perangkat lunak.

1.6 Literatur Review

Penelitian yang mengangkat tema risk assessments atau manajemen risiko keamanan sistem informasi sudah pernah dilakukan oleh peneliti-peneliti sebelumnya. Seperti penelitian milik Gita Mustika Rahmah, membahas manajemen risiko penerapan sistem informasi perguruan tinggi menggunakan metode NIST. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis risiko pada penerapan sistem informasi, serta menilai risiko yang ditemukan untuk dapat ditindak lanjuti langkah pencegahannya. Analisis risiko diawali dengan penentuan lingkup karakteristik sistem untuk mengetahui batasan sistem, sumber daya, dan informasi terkait sistem sebagai acuan dasar penilaian risiko. Tahap selanjutnya adalah mengidentifikasi sumber ancaman yang diperkirakan akan menyerang kelemahan-kelemahan sistem, termasuk identifikasi kerentanan pada sistem untuk mengetahui seberapa mudah sumber ancaman menyerang sistem. Untuk meminimalkan atau mengeliminasi serangan pada kelemahan sistem maka dilakukan melalui tahap analisis pengendalian. Selain itu juga dilakukan tahap penentuan kemungkinan serangan untuk memberikan gambaran seberapa mudah atau seberapa sering sumber ancaman melakukan serangan pada kerentanan sistem. Tahap selanjutnya adalah menganalisis dampak atas terjadinya serangan pada kerentanan sistem termasuk dampak akibat serangan terhadap operasional dan tujuan organisasi. Kemudian tahapan penentuan risiko diterapkan untuk menilai tingkat risiko sistem sebagai dasar penentuan tindakan yang perlu dilakukan agar ancaman dapat dihilangkan, atau memperkecil dampak ancaman yang mungkin terjadi sehingga ancaman dapat diabaikan. Hasil penilaian ini akan menjadi bahan pertimbangan pengambilan keputusan pada tahap rekomendasi pengendalian. Setiap risiko yang teridentifikasi akan diberikan rekomendasi apakah risiko dapat diterima organisasi atau perlu mitigasi risiko sehingga dampak risiko dapat ditekan ke tingkat yang dapat diterima (Rahmah, 2019).

Penelitian yang dilakukan oleh Prasetyowati et al., membahas tentang Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013. Indeks KAMI dengan dasar ISO/IEC 27001:2013 digunakan sebagai kerangka penelitian untuk mengolah hasil analisis. Indeks KAMI diterapkan untuk menilai tingkat kematangan, dan tingkat kelengkapan penerapan ISO/IEC 27001: 2013 serta gambaran tata kelola keamanan informasi pada organisasi. Hasil penilaian Indeks KAMI termasuk kepatuhan terhadap ISO/IEC 27001:2013 disajikan dalam bentuk diagram jaring laba-laba (spider chart). Hasil penilaian selanjutnya digunakan untuk

membuat saran-saran perbaikan pada sistem (Prasetyowati, Gamayanto, Wibowo, & Suharnawi, 2019).

Penelitian yang dilakukan oleh Endang Kurniawan dan Imam Riadi, membahas tentang analisis tingkat keamanan sistem informasi akademik sesuai standar ISO 27002:2013 menggunakan SSE-CMM. SSE-CMM adalah Capability Maturity Model (CMM) untuk System Security Engineering (SSE). SSE-CMM menjelaskan karakteristik penting dari suatu proses rekayasa keamanan organisasi yang harus ada untuk memastikan teknik keamanan yang baik dengan tidak menganjurkan proses tertentu atau berurutan, namun mengambil praktek secara umum yang diamati dalam industri. Penelitian ini dilakukan untuk mengetahui tingkat keamanan informasi dalam sistem informasi akademik dan memberikan rekomendasi perbaikan dalam manajemen keamanan informasi. Analisis tingkat keamanan dilakukan melalui penilaian hasil pengolahan jawaban atas pertanyaan kuesioner yang mengacau pada standar ISO 27002 tentang intruksi pelaksanaan manajemen keamanan informasi. Lingkup pemeriksaan keamanan sistem informasi akademik dilakukan dengan menentukan tujuan pengendalian yang akan digunakan, melalui kesepakatan yang dibuat sebelumnya. Hasil pengolahan data dan wawancara dengan pengelola sistem informasi akademik selanjutnya digunakan sebagai temuan penelitian yaitu berupa gap untuk menentukan nilai yang diharapkan atas rekomendasi perbaikan di setiap tujuan pengendalian (Kurniawan & Riadi, 2018).

Penelitian lain dilakukan oleh Hidayatul Ikhsan dan Nanda Jarti tentang manajemen risiko sistem informasi akademik perguruan tinggi menggunakan pendekatan *OCTAVE Allegro*. *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (*OCTAVE*) merupakan seperangkat peralatan, teknik dan metode untuk menilai dan merencanakan keamananan sistem informasi berbasis risiko. Metoda *OCTAVE* memiliki tiga varian yaitu *OCTAVE*, *OCTAVE-S* dan *OCTAVE Allegro*. *OCTAVE Allegro* merupakan metode yang disederhanakan dengan fokus pada aset informasi. Langkah yang dilakukan peneliti terdiri dari beberapa tahapan mulai dari penentuan kriteria pengukuran risiko, identifikasi profil aset informasi dan penentuan aset kritis termasuk kontainer dimana aset berada, identifikasi area yang bermasalah, identifikasi skenario ancaman, dan identifikasi risiko dari skenario ancaman. Tahapan selanjutnya adalah menganalisis ancaman risiko untuk mengetahui proses mitigasi risiko (Ikhsan & Jarti, 2018).

Penelitian yang dilakukan oleh Anggariyona Saputra et al., memaparkan penilaian ancaman aplikasi berbasis web menggunakan metode DREAD. Penelitian dilakukan dengan mengidentifikasi aset informasi pada aplikasi berserta jenis ancamannya, menganalisis

skenario serangan yang mungkin terjadi pada aplikasi, melakukan uji keamanan website, dan langkah terakhir adalah penentuan tingkat ancaman. Dari proses ini diperoleh suatu laporan berupa peringkat ancaman yang akan digunakan sebagai dasar penyusunan dokumen ancaman. Berdasarkan dokumen ancaman ini selanjutnya disusun *security report* yang berisi tentang deskripsi ancaman, tingkat risiko ancaman, target ancaman, jenis serangan yang terjadi, dan langkah pencegahannya (Saputra, Nelmiawati, & Sitorus, 2017).

Penelitian oleh Raden Budiarto, membahas manajemen keamanan sistem informasi menggunakan FMEA dan ISO 27001. Penelitian dimulai dengan menganalisis aliran data dan proses pada diagram *flowchart* dan *data flow diagram* sistem informasi, menganalisis potensi kegagalan yang mungkin terjadi, baik kegagalan selama proses pengolahan data maupun kegagalan di luar proses pengolahan data. Tahap penelitian selanjutnya adalah menganalisis dan menghitung penyebab, dampak, dan frekuensi dari setiap daftar potensi kegagalan dalam skala ordinal untuk mengetahui nilai RPN (*Risk Priority Number*). Berdasarkan nilai RPN, selanjutnya disusun prosedur mitigasi berdasarkan standar ISO 27001. Hasil penelitian berupa laporan pengelolaan manajemen risiko yang memuat daftar prioritas analisis risiko serta sebab permasalahan dan pengendalian risiko sesuai dengan standar ISO 27001. Dalam penerapan prosedur mitigasi, nilai RPN kemudian dihitung ulang untuk mengetahui tingkat risiko, apakah mengalami perubahan secara signifikan atau tidak (Budiarto, 2017).

Penelitian oleh Chalifa Chazar dan Moch. Ali Ramdhani, mengusulkan perencanaan keamanan sistem informasi dengan pendekatan OCTAVE dan ISO 27001:2005. Awal perencanaan keamanan sistem diawali dengan langkah analisis menggunakan pendekatan OCTAVE, yang menghasilkan dua fase analisis. Pertama adalah fase membangun aset berdasarkan profil ancaman, meliputi penentuan aset penting organisasi, identifikasi ancaman yang mungkin terjadi, tindakan perlindungan aset penting, kerentanan organisasi dan prasyarat keamanan. Fase kedua adalah identifikasi kerentanan infrastruktur informasi dan identifikasi kelemahan teknologi yang digunakan. Hasil dari analisis kedua fase ini kemudian digunakan untuk menentukan perancangan strategi keamanan dan penerapannya, sesuai dengan dokumen Standar Manajemen Keamanan Informasi (SMKI) berdasarkan ISO 27001:2005 sehingga dihasilkan dokumen SKMI yang terarah terhadap kebutuhan pengamanan aset-aset penting perusahaan (Chazar & Ramdani, 2016).

Penelitian yang dilakukan oleh Ucu Nugraha memaparkan tentang manajemen risiko sistem informasi pada perguruan tinggi menggunakan kerangka kerja NIST SP 800-30. *National Institute of Standards and Technology* (NIST) merilis rekomendasi manajemen

risiko melalui publikasi khusus yaitu NIST *Special Publication* 800-30 tentang *Risk Management Guide for Information Technology Systems*. Dalam penelitian ini diuraikan tentang proses manajemen risiko pada sistem informasi melalui tiga tahapan, yaitu penilaian risiko (*risk assessment*), peringanan risiko (*risk mitigation*), dan evaluasi risiko (*risk evaluation*). Sesuai dengan kerangka kerja NIST SP 800-30, pada tahap penilaian risiko (*risk assessment*) akan menghasilkan informasi berupa dampak risiko, penentuan risiko, dan rekomendasi risiko. Dampak risiko dihasilkan dari adanya kemungkinan-kemungkinan risiko yang dianggap mengancam keberlangsungan sistem informasi. Penentuan risiko merupakan tahapan untuk menilai tingkat risiko terhadap sistem, dengan mengacu pada kemungkinan risiko dan dampak risiko yang telah disusun sebelumnya. Adapun rekomendasi risiko adalah langkah rekomendasi pencegahan terhadap risiko yang muncul. Selanjutnya tahap peringanan risiko (*risk mitigation*), merupakan kegiatan mitigasi risiko yang meliputi prioritas aksi dengan mengacu pada hasil akhir penilaian risiko, dengan harapan dapat mengatasi permasalahan yang mengganggu keberlangsungan sistem informasi. Risiko yang memiliki tingkat penilaian tertinggi harus dijadikan sebagai prioritas utama dalam proses peringanan risiko. Adapun tahap terakhir yaitu evaluasi risiko (*risk evaluation*), merupakan saran-saran yang direkomendasikan terhadap keberlangsungan sistem informasi perguruan tinggi agar berjalan dengan baik sesuai harapan (Nugraha, 2016).

Penelitian oleh RA Fitria Hamzah et al., membahas analisis risiko keamanan sistem informasi menggunakan metode *OCTAVE*. Penelitian diawali dengan langkah penentuan aset berdasarkan profil ancaman untuk mencari ancaman-ancaman yang dapat terjadi pada sistem. Pada tahap ini dilakukan pendataan aset kritis instansi, identifikasi kebutuhan keamanan aset kritis, identifikasi ancaman pada aset kritis, identifikasi kelemahan instansi. Hasil dari identifikasi tersebut digunakan untuk mengidentifikasi kerentanan infrastruktur melalui penentuan komponen kunci aset kritis termasuk mengevaluasi kerentanan komponan kunci tersebut. Langkah berikutnya adalah mengukur risiko sekaligus melakukan perencanaan mitigasi yang terdiri dari tahapan identifikasi risiko, penilaian risiko, dan perencanaan mitigasi risiko. Penelitian ini akan menghasilkan rekomendasi SOP (*Standard Operating Procedures*) tentang risiko keamanan sistem informasi perguruan tinggi yang dapat digunakan sebagai acuan mitigasi (Hamzah, Jaya, & Putri, 2020).

Penelitian lain yang dilakukan oleh Rusydi Umar et al., membahas analisis keamanan sistem informasi berdasarkan *framework COBIT-5* menggunakan *Capability Maturity Model Integration* (*CMMI*). Framework *COBIT-5* diterapkan sebagai standar kontrol keamanan teknologi informasi, sedangkan *CMMI* diperlukan untuk mencapai standar level

pencapaian keamanan teknologi informasi. COBIT-5 memiliki 5 domain utama. Adapun domain yang berhubungan dengan keamanan teknologi informasi adalah domain DSS (*Deliver, Service and Support*) sebagai domain untuk menganalisis teknologi informasi. Tahap awal penelitian adalah melakukan observasi untuk menganalisis keamanan sistem informasi yang dijalankan. Setiap aktivitas berupa tindakan pencegahan, deteksi, dan perbaikan untuk perlindungan pada sistem informasi dipetakan berdasarkan *framework COBIT-5*. Dari hasil pemetaan ini kemudian disusun sebuah kuesioner yang dikombinasikan dengan kriteria sesuai standarisasi *CMII* untuk memperoleh bentuk kuesioner yang mampu menjawab kebutuhan terkait keamanan sistem informasi yang dijalankan. Dari hasil kuesioner selanjutnya digunakan untuk menghitung *maturity level* (tingkat kematangan) sistem yang berjalan. Dari hasil perhitungan ini maka diperoleh informasi *maturity level gap* yang dapat dijadikan dasar penyusunan langkah rekomendasi untuk meningkatkan kualitas keamanan sistem informasi (Umar, Riadi, & Handoyo, 2019).

Tabel 1.1 menyajikan rangkuman dan perbandingan dari setiap penelitian yang sudah pernah dilakukan sebelumnya.

Tabel 1.1. Literatur Review

NO	PENULIS	METODE	TAHAPAN IDENTIFIKASI RISIKO	HASIL
1	Gita Mustika Rahmah (2019)	NIST	1. Penentuan lingkup karakteristik sistem 2. Identifikasi sumber ancaman dan kerentanan sistem 3. Analisis pengendalian risiko 4. Penentuan kemungkinan serangan pada kerentanan sistem 5. Analisis dampak atas terjadinya serangan 6. Penentuan risiko untuk menilai tingkat risiko 7. Rekomendasi pengendalian risiko	Rekomendasi berupa pengendalian risiko dan mitigasi risiko untuk menekan dampak risiko ke tingkat yang dapat diterima oleh organisasi.
2	Desy Dwi Prasetyowati, Indra Gamayanto, Sasono Wibowo, Suharnawi (2019)	1. Indeks Keamanan Informasi (Indeks KAMI) 2. ISO/IEC 27001:2013	1. Klasifikasi peran sistem elektronik di instansi terkait untuk mengelompokan instansi ke dalam ukuran tertentu 2. Penilaian kelima area yang terdapat pada Indeks KAMI termasuk nilai kepatuhan terhadap ISO/IEC 27001:2013 3. Penyusunan saran-saran perbaikan pada setiap area atas hasil penilaian Indeks KAMI	Penilaian berdasarkan Indeks KAMI untuk menyusun saran-saran perbaikan pada sistem
3	Endang Kurniawan, Imam Riadi (2018)	1. ISO 27002: 2013 2. SSE-CMM	1. Pengumpulan data melalui kuesioner yang disusun dengan acuan standar ISO 27002 tentang intruksi pelaksanaan manajemen keamanan informasi 2. Lingkup pemeriksaan keamanan sistem informasi akademik dilakukan dengan menentukan tujuan pengendalian yang akan digunakan, melalui kesepakatan yang dibuat sebelumnya	Penilaian berupa gap yang dapat digunakan sebagai rekomendasi perbaikan keamanan sistem informasi sesuai kontrol keamanan ISO 27002 yang telah ditetapkan sebelumnya

NO	PENULIS	METODE	TAHAPAN IDENTIFIKASI RISIKO	HASIL
			3. Hasil pengolahan data dan wawancara dengan pengelola sistem informasi akademik selanjutnya digunakan sebagai temuan penelitian yaitu berupa gap untuk menentukan nilai yang diharapkan atas rekomendasi perbaikan di setiap tujuan pengendalian	
4	Hidayatul Ikhsan, Nanda Jarti (2018)	OCTAVE Allegro	1. Menentukan kriteria pengukuran risiko 2. Identifikasi profil aset informasi, kontainer dari aset informasi, area bermasalah, skenario ancaman, dan risiko 3. Analisis ancaman risiko dan penilaian risikonya 4. Menentukan pendekatan mitigasi untuk setiap risiko	Informasi tentang semua aset kritis beserta syarat keamanan untuk aset tersebut
5	Anggariyona Saputra, Nelmiawati, Maya Armys Roma Sitorus (2017)	DREAD	1. Identifikasi aset informasi pada aplikasi beserta jenis ancamananya 2. Analisis skenario serangan yang mungkin terjadi 3. Uji keamanan website 4. Penentuan tingkat ancaman 5. Penyusunan langkah pencegahan	Dokumen berupa *security report* yaitu laporan tentang deskripsi ancaman, tingkat risiko ancaman, target ancaman, jenis serangan yang terjadi, dan langkah pencegahan ancaman
6	Raden Budiarto (2017)	1. FMEA 2. ISO 27001	1. Analisis aliran data dan proses pada diagram flowchart dan *data flow diagram* sistem informasi 2. Analisis potensi kegagalan yang mungkin terjadi, baik kegagalan selama proses pengolahan data maupun kegagalan di luar proses pengolahan data 3. Analisis dan perhitungan penyebab, dampak, dan frekuensi dari setiap daftar potensi kegagalan dalam	Laporan hasil pengelolaan manajemen risiko yang memuat daftar prioritas analisis risiko beserta sebab permasalahan dan pengendalian risiko sesuai dengan standar ISO 27001

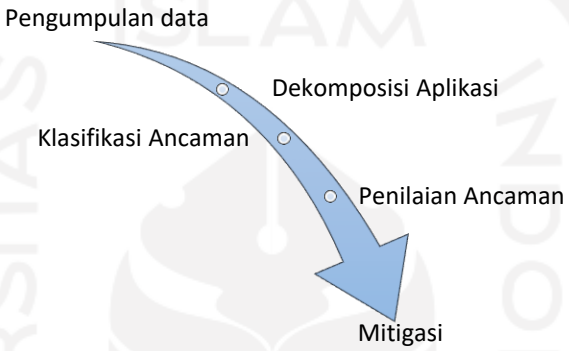
NO	PENULIS	METODE	TAHAPAN IDENTIFIKASI RISIKO	HASIL
			skala ordinal untuk mengetahui nilai RPN (*Risk Priority Number*) 4. Menyusun prosedur mitigasi berdasarkan ISO 27001 5. Menghitung ulang nilai RPN setelah penerapan prosedur penanggulangan untuk mengetahui berkurangnya risiko	
7	Chazar Chalifa, Moch. Ali Ramdhani (2016)	1. OCTAVE 2. ISO 27001: 2005	1. Identifikasi kerentanan organisasi, mulai dari aset penting organisasi, ancaman yang muncul, langkah perlindungan terhadap aset, kerentanan organisasi, prasyarat keamanan 2. Identifikasi kerentanan infrastruktur informasi 3. Penentuan rancangan strategi keamanan dan penerapannya sesuai dokumen Standar Manajemen Keamanan Informasi (SMKI) berdasarkan ISO 27001:2005	Dokumen SMKI berupa perancangan strategi keamanan berdasarkan kebutuhan pengamanan aset-aset penting organisasi
8	Ucu Nugraha (2016)	NIST SP 800-30	1. Penilaian risiko (*risk assessment*), yang menghasilkan informasi dampak risiko, penentuan risiko, dan rekomendasi risiko 2. Peringanan risiko (*risk mitigation*), adalah langkah evaluasi permasalahan berdasarkan hasil analisis penilaian risiko 3. Evaluasi risiko (*risk evaluation*), merupakan saran rekomendasi terhadap keberlangsungan sistem informasi berdasarkan hasil analisis risiko	*Risk mitigation* berupa profil risiko dengan rekomendasi solusi untuk mengurangi dampak risiko, dan evaluasi risiko berupa saran terhadap sistem agar berjalan dengan baik

NO	PENULIS	METODE	TAHAPAN IDENTIFIKASI RISIKO	HASIL
9	RA Fitria Hamzah, Irfan Dwi Jaya, Utami Mizani Putri (2020)	1. OCTAVE 2. FMEA	1. Penentuan aset berdasarkan profil ancaman, mulai dari pendataan aset kritis perusahaan, identifikasi kebutuhan keamanan aset, identifikasi ancaman pada aset, dan identifikasi kelemahan perusahaan 2. Identifikasi kerentanan infrastruktur melalui penentuan komponen kunci aset kritis 3. Mengukur risiko sekaligus menyusun perencanan mitigasi risiko, meliputi tahapan identifikasi risiko, penilaian risiko, dan perencanaan mitigasi risiko	Rekomendasi SOP (*Standard Operating Procedures*) tentang risiko keamanan sistem informasi sebagai acuan mitigasi
10	Rusydi Umar, Imam Riadi, Eko Handoyo (2019)	1. COBIT-5 2. CMMI	1. Observasi terhadap keamanan sistem informasi yang dijalankan 2. Pemetaan setiap aktivitas tindakan pencegahan, deteksi, dan perbaikan untuk perlindungan sistem informasi dan teknologi dari perangkat lunak perusak berdasarkan framework *COBIT-5* 3. Penyusunan kuesioner berdasarkan aktivitas tindakan pencegahan, deteksi, dan perbaikan, yang dikombinasikan dengan kriteria pada *capability* level *CMMI* 4. Menghitung *maturity level* (tingkat kematangan) keamanan sistem informasi yang sedang dijalankan 5. Menganalisis *maturity level gap* dengan memperbandingkan *maturity* saat ini dengan target 6. Menyusun rekomendasi tata kelola keamanan sistem informasi	Rekomendasi langkah-langkah peningkatan kualitas keamanan sistem informasi di setiap domain framework COBIT-5

NO	PENULIS	METODE	TAHAPAN IDENTIFIKASI RISIKO	HASIL
Usulan Penelitian		1. STRIDE 2. DREAD	1. Pengumpulan informasi tentang Sistem Informasi Akademik 2. Dekomposisi aplikasi sistem informasi akademik untuk menyusun dokumen *Threat Model* 3. Klasifikasi ancaman pada sistem informasi akademik menggunakan *STRIDE* 4. Penilaian ancaman yang telah diklasifikasikan pada langkah keempat menggunakan *DREAD* 5. Penyusunan mitigasi ancaman berdasarkan ranking risiko ancaman	Rekomendasi tindakan mitigasi terhadap ancaman yang teridentifikasi pada sistem informasi akademik berdasarkan ranking risiko ancaman

1.7 Metodologi Penelitian

Penelitian dilakukan melalui tahapan sistematis sebagai pedoman dalam penelitian, mulai dari studi literatur untuk mengumpulkan dan mengkaji bahan-bahan penelitian *tentang threat modeling*, wawancara dengan pihak pengembang sistem, dekomposisi aplikasi untuk menguraikan aplikasi sebagai bentuk pemahaman karakter aplikasi, penerapan model *STRIDE* untuk mengklasifikasikan ancaman, dan penilaian ancaman berdasarkan model *DREAD*, serta penentuan langkah mitigasi untuk mengurangi dampak dari ancaman. Tahapan penelitian threat modeling disajikan pada Gambar 1.2.



Gambar 1.2. Metodologi penelitian *Threat Modeling*

1.8 Sistematika Penelitian

Gambaran secara ringkas terkait kerangka penyusunan penelitian diuraikan dalam sistematika penulisan sebagai berikut.

BAB I PENDAHULUAN

Bab ini berisi uraian latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, dan manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tinjauan pustaka yang memaparkan hasil-hasil penelitian sebelumnya yang relevan dengan penelitian ini, dan menguraikan teori-teori atau konsep yang dibutuhkan untuk menyusun penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini berisi gambaran secara umum langkah analisis kerentanan sistem informasi dan proses perankingan ancaman yang muncul.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil penelitian dan pembahasan dalam menyelesaikan masalah yang diteliti.

BAB V PENUTUP

Bab ini memuat kesimpulan hasil analisis keamanan sistem informasi dan saran yang diharapkan bermanfaat untuk penelitian selanjutnya.

BAB 2
Kajian Pustaka

2.1 Sistem

Menurut Mulyani et al., (2018) sekumpulan subsistem, komponen ataupun elemen yang saling bekerja sama dengan tujuan untuk menghasilkan output yang sudah ditentukan sebelumnya.

Menurut Ahmad & Munawir (2018) sistem adalah suatu susunan yang teratur dari kegiatan yang saling berkaitan, prosedur yang saling berhubungan, sinergi dari semua unsur dan elemen di dalamnya untuk menunjang pelaksanaan dan mempermudah pencapaian kegiatan utama suatu organisasi. Sistem memiliki ciri-ciri yang diklasifikasikan sebagai berikut.

1. *Component*: suatu sistem memiliki beberapa elemen/unsur/unit tersendiri namun terintegrasi dalam satu kesatuan sistem
2. *Boundary*: batas sistem yaitu area pemisah dengan sistem yang lain
3. *Environmen*: lingkungan luar, sisi/bagian yang bukan termasuk dalam bagian suatu sistem
4. *Interface*: media penghubung antar elemen luar dengan sistem
5. *Input*: masukan yang akan diproses
6. *Output*: keluaran atau hasil dari pengolahan sistem
7. *Process*: pengolah yang terdapat pada sistem
8. *Objective*: sesuatu yang menjadi sasaran atau tujuan sistem

2.2 Informasi

Informasi adalah data yang telah diklasifikasi atau diinterpretasi untuk proses pengambilan keputusan. Informasi bersumber dari data, yaitu suatu bentuk yang masih mentah yang belum dapat bercerita banyak sehingga perlu diolah lebih lanjut melalui suatu model hingga menghasilkan informasi (Sutabri, 2012).

Definisi lain dari informasi adalah data yang telah diolah untuk menghasilkan suatu luaran yang bermanfaat bagi penerimanya (Setyawan & Munari, 2020).

Menurut Jogiyanto dalam bukunya Prehanto (2020), mengemukakan bahwa informasi dikatakan berkualitas jika memenuhi tiga aspek yaitu:

1. Akurat: informasi harus bebas dari kesalahan-kesalahan dan tidak bias atau menyesatkan
2. Tepat waktu: informasi yang datang pada penerimanya tidak boleh terlambat
3. Relevan: informasi tersebut mempunya manfaat untuk pemakainya.

2.3 Sistem Informasi

Definisi sistem informasi adalah sebuah rangkaian prosedur formal berupa pengelompokan data, pemrosesan data menjadi informasi, dan pendistribusian informasi kepada pemakai (Hartono, 2020).

Definisi lain dari sistem informasi menurut Hendry Lucas dalam bukunya Habibi (2020) yaitu suatu kegiatan dari prosedur-prosedur yang diorganisasikan, bilamana dieksekusi akan menyediakan informasi untuk mendukung pengambilan dan pengendalian di dalam.

Sistem informasi juga didefinisikan sebagai sistem yang terdiri dari pengguna dan komputer yang memproses atau menafsirkan informasi, meliputi perangkat keras, perangkat lunak, infrastruktur, dan pengguna yang digabung untuk merencanakan, mengendalikan, mengkoordinir, dan cara pengambilan keputusan untuk suatu kegiatan (Mulyani et al., 2018).

2.4 Sistem Informasi Akademik

Sistem informasi akademik adalah suatu sistem yang dirancang untuk mengolah data akademik agar proses kegiatan akademik dapat dikelola dengan baik sehingga menjadi informasi yang bermanfaat untuk manajemen perguruan tinggi dan pengambilan keputusan (Homaidi, 2016).

Definisi lain tentang sistem informasi akademik adalah suatu sistem untuk mengelola data akademik dengan penerapan teknologi komputer sehingga seluruh proses kegiatan akademik dapat terkelola menjadi informasi yang bermanfaat dalam pengelolaan manajemen perguruan tinggi dan pengambilan di lingkungan perguruan tinggi (Sevima.com, 2018).

2.5 Keamanan Informasi

Seiring berjalannya tren penyimpanan digital, banyak pihak baik individu maupun instansi mengubah model penyimpanan data menjadi bentuk digital, sehingga peran keamanan informasi menjadi poin penting untuk memastikan validitas data digital tersebut.

Keamanan informasi adalah suatu kondisi yang menjamin kerahasiaan, integritas, dan ketersediaan informasi melalui penerapan langkah-langkah dan standar yang ditentukan (Klaić, 2010). Keamanan informasi juga didefinisikan sebagai perlindungan informasi dan

sistem informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi atau pengrusakan (Syafitri, 2016). Definisi lain dari keamanan informasi adalah perlindungan terhadap informasi yang mencakup kerahasiaan, integritas, dan ketersediaan informasi, termasuk perlindungan terhadap sistem dan perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi tersebut (Whitman & Mattord, 2010).

Lebih lanjut, ketiga aspek keamanan informasi yaitu kerahasiaan, integritas, dan ketersediaan dijabarkan sebagai berikut (Chazar & Ramdani, 2016).

1. *Confidentiality* (kerahasiaan)

   Adalah aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang, dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.
2. *Integrity* (integritas)

   Adalah aspek yang menjamin bahwa data tidak dapat diubah tanpa adanya izin dari pihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya.
3. *Availability* (ketersediaan)

   Merupakan aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, dan memastikan pengguna yang berhak dapat menggunakan informasi dan perangkat terkait.

2.6 Keamanan Sistem Informasi

White (dalam Syafitri, 2016) menyebutkan bahwa, *United Stated National Information System Security* mendefinisikan keamanan sistem informasi sebagai bentuk perlindungan sistem informasi terhadap akses yang tidak sah ataupun modifikasi informasi, baik yang terjadi saat penyimpanan, pemprosesan, ataupun transit, penolakan layanan terhadap pengguna resmi atau pemberian layanan kepada pengguna yang tidak sah, juga termasuk tindakan-tindakan yang diperlukan untuk mendeteksi dan melawan ancaman tersebut.

Menurut Techopedia (2012), keamanan sistem informasi mengacu pada proses dan metodologi yang terlibat dalam menjaga kerahasiaan informasi, tersedia, dan memastikan integritasnya. Hal ini juga mengacu pada kontrol akses yang mencegah pihak tidak berwenang untuk masuk dan mengakses sistem, perlindungan terhadap informasi di manapun lokasinya baik dalam penyimpanan atau pengiriman informasi, serta identifikasi dan pemulihan terhadap adanya serangan keamanan termasuk dokumentasi atas insiden tersebut.

2.7 Ancaman, Kerentanan, dan Serangan

Ancaman adalah suatu aksi atau kejadian yang dapat merugikan perusahaan dengan kerugian bias berupa uang/biaya, tenaga upaya, peluang bisnis, reputasi nama baik, dan kerugian terburuk adalah membuat perusahaan pailit (Sutabri, 2012).

Definisi lain dari ancaman adalah segala bentuk kejadian berbahaya yang berpotensi dapat merusak aset. Dengan kata lain, ancaman adalah segala hal buruk yang terjadi pada aset. Selanjutnya, kerentanan didefinisikan sebagai kelemahan yang memungkinkan terjadinya ancaman. Kerentanan ini bisa muncul karena buruknya desain sistem, adanya kesalahan konfigurasi, atau teknik pengkodean yang tidak tepat dan tidak aman. Lemahnya validasi pada input formulir adalah salah satu contoh kerentanan lapisan aplikasi yang memungkinkan munculnya serangan melalui input formulir. Adapun serangan, didefinisikan sebagai tindakan mengeksploitasi kerentanan atau ancaman yang terdapat pada sistem, misalnya mengirim kode berbahaya pada input formulir suatu aplikasi, atau sengaja membanjiri jaringan untuk melumpuhkan layanan sistem (Meier et al., 2003).

2.8 Pemodelan Ancaman

Pemodelan ancaman berguna untuk mengidentifikasi dan menilai suatu ancaman yang dapat memengaruhi sistem secara sistematis. Dengan tahapan tersebut diharapkan ancaman dapat diatasi dengan menerapkan tindakan pencegahan yang tepat, dimulai dari ancaman dengan nilai risiko terbesar.

Pemodelan ancaman memiliki pendekatan terstruktur yang jauh lebih efektif dan efisien daripada menerapkan fitur keamanan secara sembarangan tanpa mengetahui dengan tepat ancaman apa yang seharusnya ditangani oleh setiap fitur. Dengan model pendekatan keamanan yang sembarangan, tentunya sulit untuk mengetahui kondisi aman suatu aplikasi dan sulit untuk mengetahui area sistem yang masih memiliki kerentanan (Meier et al., 2003).

Proses pemodelan ancaman dapat dibagi menjadi tiga langkah utama, yaitu (Owasp.org, 2020):

1. Dekomposisi aplikasi, adalah tahapan pertama untuk memperoleh pemahaman tentang aplikasi dan bagaimana aplikasi tersebut berinteraksi dengan entitas eksternal.
2. Penentuan ancaman, adalah tahapan untuk mengidentifikasi dan mengklasifikasikan ancaman menggunakan suatu metodologi tertentu, salah satunya metodologi STRIDE.
3. Penentuan tindakan pencegahan dan mitigasi, adalah tahapan untuk mengidentifikasi tindakan sebagai langkah mengurangi risiko ancaman, termasuk penentuan tindakan mitigasi sesuai prioritas risiko.

Terdapat terminologi pemodelan ancaman, sebagai berikut (Owasp, 2016).

1. Pihak pengancam (*a threat agent*), adalah seseorang atau kelompok yang mampu melakukan suatu bentuk ancaman tertentu. Dalam hal ini perlu untuk mengidentifikasi siapa yang ingin mengeksploitasi aset organisasi, bagaimana pengancam menggunakan aset untuk menyerang organisasi, dan apakah pengancam mampu untuk melakukan hal tersebut.
2. Dampak (*impact*), merupakan ukuran potensi kerusakan yang disebabkan oleh ancaman tertentu. Dampak dan kerusakan ini dapat terjadi dalam berbagai bentuk. Ancaman dapat mengakibatkan kerusakan pada aset fisik, atau dapat mengakibatkan kerugian secara finansial. Selain itu, ancaman juga dapat mengakibatkan kerugian secara tidak langsung, yang perlu dipertimbangkan sebagai bagian dari dampak adanya ancaman.
3. Kemungkinan (*likelihood*), merupakan ukuran kemungkinan terjadinya suatu ancaman. Berbagai faktor dapat memengaruhi adanya kemungkinan ancaman termasuk seberapa sulit penerapan ancaman tersebut, dan seberapa besar hasil yang akan diperoleh penyerang apabila berhasil mengeskploitasi ancaman.
4. Kontrol (*controls*), merupakan bentuk pengamanan atau tindakan pencegahan yang dilakukan untuk menghindari, mendeteksi, menangkal, atau meminimalkan potensi ancaman terhadap informasi, sistem, atau aset lainnya.
5. Pencegahan (*preventions*), merupakan kontrol yang sepenuhnya dapat mencegah adanya kemungkinan serangan tertentu.
6. Mitigasi (*mitigation*), merupakan kontrol yang diterapkan untuk mengurangi kemungkinan atau dampak dari suatu ancaman.
7. *Data Flow Diagram* (Diagram Aliran Data), adalah penggambaran tentang aliran informasi pada suatu sistem yang menunjukkan setiap titik masuk dan keluarnya data dari setiap proses atau subsistem, termasuk lokasi penyimpanan data dalam sistem.
8. Batas kepercayaan (*trust boundary*) adalah lokasi pada Diagram Aliran Data ketika data mengalami perubahan pada level kepercayaan. Secara umum, setiap tempat yang dilewati data di antara dua proses merupakan batas kepercayaan. Jika suatu aplikasi membaca file dari disk, maka terdapat batas kepercayaan antara aplikasi dan file tersebut karena proses dan pengguna luar dapat memodifikasi data dalam file tersebut.

2.9 Data Flow Diagram

Menurut Kristanto (dalam Muslihudin & Oktafianto, 2016) *Data Flow Diagram* (Diagram Aliran Data) adalah suatu model logika data atau proses yang dibuat untuk menggambarkan

dari mana asal data dan kemana tujuan data yang keluar dari sistem, di mana data tersimpan, proses apa yang menghasilkan data tersebut dan interkasi antara data tersimpan dan proses yang dikenakan pada data tersebut.

Dalam lingkup pemodelan ancaman, fokus *Data Flow Diagram* adalah untuk mengetahui bagaimana data bergerak melalui aplikasi, dan mengetahui apa yang terjadi pada data saat bergerak. *Data Flow Diagram* memiliki struktur hierarki, sehingga dapat digunakan untuk menguraikan aplikasi menjadi subsistem dan subsistem tingkat yang lebih rendah. *Data Flow Diagram* tingkat tinggi akan mampu memperjelas ruang lingkup aplikasi yang dimodelkan. Iterasi tingkat yang lebih rendah memungkinkan untuk fokus pada proses spesifik yang terlibat saat memproses data tertentu (Owasp.org, 2020).

Terdapat sejumlah komponen *Data Flow Diagram* untuk pemodelan ancaman, sebagai berikut (Owasp.org, 2020).

1. *External entity* (entitas eksternal), digunakan untuk mewakili entitas apa pun di luar aplikasi, yang berinteraksi dengan aplikasi melalui titik masuk.
2. *Process* (proses), merepresentasikan tugas yang menangani data di dalam aplikasi. Tugas dapat berupa pemrosesan data atau melakukan tindakan berdasarkan data tersebut.
3. *Multiple process*, digunakan untuk menyajikan kumpulan subproses. Berbagai proses dapat dipecah menjadi beberapa subproses di DFD lain.
4. *Data store*, digunakan untuk merepresentasikan lokasi penyimpanan data.
5. *Data flow*, merepresentasikan pergerakan data di dalam aplikasi yang diwakili oleh anak panah.
6. *Privilege Boundary*, digunakan untuk mewakili perubahan tingkat hak akses saat data mengalir melalui aplikasi.

2.10 STRIDE

Microsoft telah mengembangkan metode klasifikasi ancaman yaitu *STRIDE*, yang dapat diterapkan pada jaringan, host, dan aplikasi. Dengan menerapkan model *STRIDE* memungkinkan untuk mengetahui karakterisasi ancaman sesuai dengan tujuan serangan (Jouini, Rabai, & Aissa, 2014). Singkatan *STRIDE* sendiri dibentuk dari huruf pertama dari masing-masing kategorinya, yaitu *Spoofing*, *Tampering*, *Repudiation*, *Information disclosure*, *Denial of service*, dan *Elevation of priviledge*.

Setiap kategori ancaman *STRIDE* memiliki kaitan dengan bidang keamanan seperti ditunjukkan pada Tabel 2.1 (Shevchenko, 2018).

Tabel 2.1. Kategori Ancaman STRIDE

Bidang Keamanan	Klasifikasi *STRIDE*	Contoh kasus
Authentication	*Spoofing*	Menggunakan akun milik orang lain untuk mengakses sistem
Integrity	*Tampering*	Memodifikasi data secara ilegal
Confirmation	*Repudiation*	Menyangkal perbuatan yang telah dilakukan
Confidentiality	*Information disclosure*	Mengekspos informasi kepada pihak yang tidak berhak
Availability	*Denial of service*	Menghambat pelayanan pengguna
Authorization	*Elevation of priviledge*	Memperoleh hak akses lebih tinggi tanpa otorisasi yang tepat

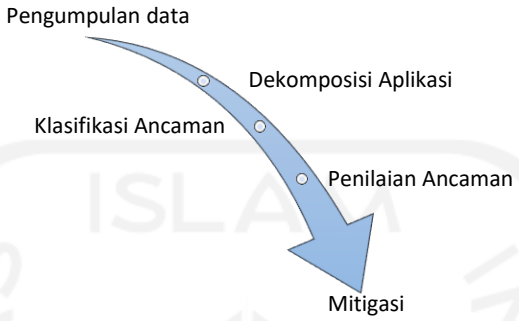
2.11 DREAD

DREAD merupakan model perankingan risiko yang dikembangkan oleh *Microsoft* untuk menghitung risiko yang dapat menghasilkan informasi peringkat risiko suatu ancaman yang terjadi. Istilah *DREAD* merupakan akronim dari *Damage Potential*, *Reproducibility*, *Exploitability*, *Affected user*, dan *Discoverability*, dengan definisi sebagai berikut (Owasp.org, 2020).

a. *Damage potential* yaitu seberapa besar potensi kerusakan yang terjadi jika serangan berhasil dilakukan
b. *Reproducibility* yaitu seberapa mudah untuk mereproduksi serangan
c. *Exploitability* yaitu berapa banyak waktu, tenaga, dan keahlian yang dibutuhkan untuk mengeksploitasi ancaman
d. *Affected user* yaitu seberapa banyak pengguna yang terpengaruh jika ancaman dieksploitasi
e. *Discoverability* yaitu seberapa mudah bagi seorang penyerang untuk menemukan ancaman pada sistem.

BAB 3
Metodologi Penelitian

Penelitian ini dilakukan melalui tahap-tahap sistematis sebagai pedoman dalam penelitian, seperti disajikan pada Gambar 3.1.



Gambar 3.1. Tahapan penelitian *Threat Modeling*

3.1 Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian diuraikan sebagai berikut.

1. Studi literatur

   Studi literatur merupakan tahap penelitian sebagai langkah untuk mengumpulkan, mengkaji dan mempelajari bahan-bahan referensi dari berbagai sumber seperti buku, makalah, paper, artikel, dan situs web yang terkait dengan penelitian *threat modeling*.

2. Wawancara

   Wawancara dilakukan dengan pihak internal pengembang sistem di Universitas XYZ untuk memperoleh informasi terkait infrastruktur sistem informasi akademik, tindak kejahatan yang pernah terjadi pada sistem, dan segala kebutuhan yang diperlukan dalam penelitian *threat modeling*. Data diambil dalam rentang waktu satu tahun selama semester genap 2018/2019 dan semester ganjil 2019/2020.

3. Observasi

   Metode observasi dilakukan dengan menjalankan dan mengamati secara langsung proses kerja dari sistem informasi akademik untuk mengetahui informasi-informasi terkait sistem sebagai data pendukung penelitian.

3.2 Dekomposisi Aplikasi

Langkah pertama dalam proses pemodelan ancaman adalah dengan memahami aplikasi dan bagaimana aplikasi berinteraksi dengan entitas eksternal. Hal ini meliputi pemahaman tentang bagaimana aplikasi digunakan, identifikasi titik masuk untuk melihat potensi serangan ketika berinteraksi dengan aplikasi, identifikasi aset yang akan diminati penyerang, dan identifikasi level kepercayaan terkait hak akses yang diberikan aplikasi kepada entitas eksternal. Tahap identifikasi aplikasi ini dituangkan dalam bentuk dokumen *Threat Model*.

Setelah informasi tentang aplikasi berhasil dihimpun melalui dokumen *threat model,* selanjutnya adalah menyusun *Data Flow Diagram*. Representasi visual *Data Flow Diagram* memungkinkan untuk memperoleh pemahaman yang lebih baik mengenai aplikasi ketika memproses data. Menurut Fruhlinger (2020), salah satu teknik untuk mendekompisisi aplikasi adalah dengan menyusun *Data Flow Diagram,* sebagai cara untuk memvisualkan pergerakan data di sekitar aplikasi atau sistem, dan untuk mengetahui lokasi di mana data tersebut diubah atau disimpan oleh berbagai komponen.

3.3 Klasifikasi Ancaman

Proses klasifikasi ancaman dilakukan dengan mengadopsi kategorisasi ancaman pada metodologi *STRIDE*. Dikembangkan oleh *Microsoft*, metodologi ini berguna untuk mengetahui kategori ancaman berdasarkan maksud dan tujuan serangan (Jouini et al., 2014). Singkatan *STRIDE* dibentuk dari huruf pertama dari masing-masing kategorinya, yaitu *Spoofing*, *Tampering*, *Repudiation*, *Information disclosure*, *Denial of service*, dan *Elevation of priviledge*.

Menurut EC-Council (2020), metodologi *STRIDE* saat ini adalah metode pemodelan ancaman yang paling berkembang, yang telah berevolusi selama bertahun-tahun dengan memuat tabel baru berbasis ancaman dan varian *STRIDE-per-Interaction* dan *STRIDE-per-Element*. Metodologi *STRIDE* bertujuan untuk memastikan bahwa aplikasi memenuhi arahan keamanan dari aturan *CIA* (*Confidentiality*: Kerahasiaan, *Integrity*: Integritas, dan *Availability*: Ketersediaan), di samping *Authentication* (Autentikasi), *Authorization* (Otorisasi), dan *Non-Repudiation* (Non-Repudiasi).

STRIDE menyediakan sekumpulan kategori ancaman dengan contoh yang sesuai, sehingga proses identifikasi ancaman dapat dilakukan secara sistematis dengan cara yang terstruktur dan berulang. Daftar ancaman kategori *STRIDE* ditunjukkan pada Tabel 3.1 (Owasp.org, 2020).

Tabel 3.1. Kategori Ancaman *STRIDE*

Tipe	Jenis Ancaman
Spoofing	Tindak ancaman yang ditujukan untuk mengakses dan menggunakan kredensial pengguna lain secara ilegal, seperti nama dan sandi pengguna
Tampering	Tindak ancaman yang bertujuan untuk mengubah data, baik mengubah data yang tersimpan dalam database maupun mengubah data pada saat transit melalui jaringan
Repudiation	Tindak ancaman berupa perbuatan ilegal dalam suatu sistem yang tidak memiliki kemampuan untuk melacak tindakan yang telah dilakukan
Information disclosure	Tindak ancaman berupa perbuatan membaca file secara tidak sah, atau membaca data pada saat transit
Denial of service	Tindak ancaman yang bertujuan untuk menolak akses ke pengguna yang valid, seperti dengan membuat server web tidak tersedia untuk sementara waktu
Elevation of priviledge	Tindak ancaman yang mempunyai tujuan untuk memperoleh hak akses yang lebih tinggi, agar dapat mengakses informasi atau menyusup ke sistem secara tidah sah

3.4 Penilaian Ancaman

Dikembangkan oleh *Microsoft*, *DREAD* dipahami sebagai *add-on* model *STRIDE* yang memungkinkan bagi pemodel untuk memberi peringkat ancaman setelah diklasifikasikan berdasarkan *STRIDE* (Fruhlinger, 2020). Penerapan metode *DREAD* digunakan untuk menilai, membandingkan, dan memprioritaskan tingkat risiko yang ditimbulkan dari setiap ancaman. Istilah *DREAD* merupakan singkatan dari setiap kategori risiko yaitu *Damage potential*, *Reproducibility*, *Exploitability*, *Affected user*, dan *Discoverability*, dengan definisi sebagai berikut (Owasp, 2016).

a. *Damage potential* yaitu seberapa besar potensi kerusakan yang terjadi jika serangan berhasil dilakukan
b. *Reproducibility* yaitu seberapa mudah untuk mereproduksi serangan
c. *Exploitability* yaitu berapa banyak waktu, tenaga, dan keahlian yang dibutuhkan untuk mengeksploitasi ancaman
d. *Affected user* yaitu seberapa banyak pengguna yang terpengaruh jika ancaman dieksploitasi
e. *Discoverability* yaitu seberapa mudah bagi penyerang untuk menemukan ancaman pada sistem.

Ancaman dapat dinilai dari perspektif faktor risiko. Melalui penentuan faktor risiko yang ditimbulkan oleh berbagai ancaman yang teridentifikasi, dimungkinkan untuk menyusun daftar ancaman yang diprioritaskan dalam strategi mitigasi, seperti memutuskan ancaman mana yang harus ditangani terlebih dahulu.

Tabel 3.2 menunjukkan skema yang biasa digunakan untuk acuan penilaian ancaman (Alhassan, Abba, Olaniyi, & Waziri, 2016). Ancaman dengan peringkat tinggi dinilai sama dengan 3, peringkat sedang dinilai sama dengan 2, dan ancaman dengan peringkat rendah dinilai sama dengan 1 (Fruhlinger, 2020). Peringkat ancaman kemudian dihitung dari penjumlahan nilai setiap kategori. Setiap kategori ancaman memiliki nilai minimal 1 dan nilai maksimal 3. Apabila kelima kategori ancaman mendapat penilaian minimal yaitu 1, maka hasil perhitungan dari kelima ancaman akan mendapatkan nilai total 5. Sebaliknya apabila kelima kategori ancaman mendapat penilaian maksimal yaitu 3, maka hasil perhitungan dari kelima ancaman akan mendapatkan nilai total 15. Berdasarkan metode perhitungan ini maka dari total 5 kategori ancaman akan diperoleh hasil nilai antara 5 s.d 15.

Tabel 3.2. Peringkat Ancaman

Kategori	Tinggi (3)	Sedang (2)	Rendah (1)
D	Penyerang menerobos sistem keamanan, memperoleh otorisasi penuh; memiliki akses sebagai admin; mampu mengupload konten	Membocorkan informasi yang penting	Membocorkan informasi yang sepele
R	Serangan dapat dilakukan secara berulang setiap saat tanpa jeda waktu	Serangan dapat diulangi, tetapi dalam waktu tertentu	Serangan sulit untuk diulangi, walaupun celah keamanan diketahui penyerang
E	*Programmer* pemula mampu membuat serangan dalam waktu singkat	*Programmer* terlatih mampu membuat serangan berulang kali	Serangan memerlukan seseorang yang sangat terampil dan memiliki pengetahuan lebih
A	Seluruh pengguna, konfigurasi default, pelanggan utama	Hanya beberapa pengguna, konfigurasi non-default	Pengguna terdampak hanya sedikit, mengaburkan fitur
D	Adanya informasi yang menjelaskan serangan. Kerentanan ditemukan pada fitur yang umum dipakai dan terlihat jelas	Kerentanan di bagian yang jarang dipakai dan hanya pengguna tertentu yang menemukan, butuh pemikiran lebih untuk mengeksploitasi	*Bug* tidak diketahui, pengguna tidak akan menemukan potensi kerusakan

Hasil total perhitungan setiap kategori ancaman yang memiliki rentang nilai 12–15 dikategorikan sebagai risiko Tinggi, total nilai 8–11 sebagai risiko Sedang, dan total nilai 5–7 sebagai risiko Rendah, seperti ditunjukkan pada Tabel 3.3 (Logixconsulting, 2019).

Tabel 3.3. Peringkat Risiko

Rentang Nilai	Peringkat Risiko
5 – 7	Rendah
8 – 11	Sedang
12 – 15	Tinggi

3.5 Mitigasi

Setelah peringkat risiko setiap ancaman ditetapkan, dimungkinkan untuk mengurutkan ancaman dari risiko tertinggi hingga terendah, dan memprioritaskan upaya mitigasi pada ancaman tersebut. Mitigasi merupakan usulan rencana mekanisme kontrol untuk mencegah dan mengurangi dampak ancaman yang telah teridentifikasi sesuai tingkat risikonya.

BAB 4
Hasil dan Pembahasan

Penelitian tentang *threat modeling* ini dilakukan dengan objek berupa Sistem Informasi Akademik milik Perguruan Tinggi Universitas XYZ. Aplikasi berbasis web perguruan tinggi ini menyediakan layanan secara online bagi mahasiswa, dosen, pihak akademik, dan pihak program studi untuk mendukung proses bisnis perguruan tinggi.

Layanan yang disediakan untuk mahasiswa meliputi pendataan profil mahasiswa, pengisian kartu rencana studi persemester, informasi jadwal perkuliahan, informasi kartu hasil studi, transkrip nilai, pembimbingan, pendaftaran yudisium, pendaftaran wisuda, dan layanan administratif lainnya. Layanan yang dapat dimanfaatkan oleh dosen meliputi data profil dosen, *upload* informasi perkuliahan, *upload* materi perkuliahan, *upload* informasi nilai sebagai bahan kroscek nilai mahasiswa, termasuk *download* daftar peserta dari kelas mata kuliah yang diampu. Adapun layanan untuk pihak akademik dan program studi meliputi manajemen data administratif transaksi akademik mahasiswa.

Dalam perjalanannya, aplikasi ini pernah mengalami serangan salah satunya adalah perubahan data nilai mahasiswa yang telah diunggah dosen pengampu mata kuliah. Hal ini dirasa mengkhawatirkan karena perubahan nilai tidak hanya terjadi pada satu transaksi nilai dosen, tetapi terjadi pada beberapa transaksi nilai yang telah diunggah dosen. Sebagai langkah mitigasi serangan, maka perlu dilakukan tahapan *threat modeling* untuk mengidentifikasi ancaman-ancaman yang akan terjadi pada sistem informasi akademik.

Threat modeling pada Sistem Informasi Akademik Universitas XYZ dilakukan melalui tahapan dekomposisi aplikasi, identifikasi ancaman sesuai kategori *STRIDE*, penilaian ancaman yang teridentifikasi menggunakan *DREAD*, dan tahapan akhir adalah penyusunan langkah mitigasi serangan.

4.1 Dekomposisi Aplikasi

Proses dekomposisi aplikasi adalah tahapan *threat modeling* untuk memahami bagaimana sistem informasi akademik digunakan, identifikasi titik masuk pada sistem untuk melihat potensi serangan ketika berinteraksi dengan aplikasi, identifikasi aset pada sistem informasi yang akan diminati penyerang, dan identifikasi level kepercayaan terkait hak akses yang diberikan aplikasi kepada entitas eksternal.

Dokumentasi *threat model* disajikan pada Tabel 4.1 sampai Tabel 4.5. Hasil dari pengumpulan informasi aplikasi dalam bentuk thread model ini selanjutnya digunakan untuk bahan penyusunan *Data Flow Diagram*. Dalam lingkup pemodelan ancaman, fokus *Data Flow Diagram* adalah untuk mengetahui bagaimana data bergerak melalui aplikasi, dan mengetahui apa yang terjadi pada data saat bergerak.

4.1.1 Dokumen Threat Model

Dokumen *threat model* disusun sebagai acuan awal tahapan *threat modeling*. Menggunakan standarisasi dari Owasp.org, dokumen ini disusun dari dokumentasi pengumpulan informasi tentang aplikasi yang menjadi objek pemodelan ancaman (*threat model information*), dokumentasi depedensi ekternal, dokumentasi titik masuk pada aplikasi, dokumentasi aset-aset pada sistem, dan dokumentasi level kepercayaan yang merepresentasikan batasan akses ke aplikasi dari entitas luar. Dokumen *threat model* diuraikan sebagai berikut.

1. Informasi *Threat Model*

Dokumentasi dimulai dengan penyusunan informasi singkat tentang aplikasi yang akan menjadi objek dalam *threat modeling*, yaitu Sistem Informasi Akademik Universitas XYZ. Dokumen ini memuat info tentang nama aplikasi, deskripsi tentang aplikasi, pemilik dokumen, partisipan, dan peninjau dokumen model ancaman, disajikan pada Tabel 4.1.

Tabel 4.1. Informasi *Threat Model*

Informasi *Threat Model*	
Aplikasi	Sistem Informasi Akademik
Deskripsi	Merupakan situs web perguruan tinggi yang menyediakan layanan *online* bagi mahasiswa, dosen, pihak akademik, dan pihak program studi. Layanan untuk mahasiswa meliputi pendataan profil mahasiswa, pengisian kartu rencana studi persemester, informasi jadwal perkuliahan, informasi kartu hasil studi, transkrip nilai, pembimbingan, yudisium, wisuda, dan layanan administratif lainnya. Layanan untuk dosen meliputi data profil dosen, *upload* informasi perkuliahan, upload materi perkuliahan, *upload* informasi nilai sebagai bahan kroscek nilai mahasiswa, termasuk *download* daftar peserta dari kelas mata kuliah yang diampu. Adapun layanan untuk pihak akademik dan program studi meliputi manajemen data administratif transaksi akademik mahasiswa.
Pemilik Dokumen	Azis Catur Laksono
Peninjau	Dr. Yudi Prayudi, S.Si., M.Kom.

2. Dependensi Eksternal

Dependensi eksternal didefinisikan sebagai objek lain di luar kode aplikasi yang keberadaannya dapat menimbulkan ancaman bagi aplikasi. Dependensi eksternal untuk sistem informasi akademik Universitas XYS didokumentasikan dengan memberikan nomor unik dan deskripsi untuk setiap dependensi, seperti disajikan pada Tabel 4.2.

Tabel 4.2. Dependensi Eksternal

Dependensi Eksternal	
ID	Deskripsi
1	Situs web layanan akademik perguruan tinggi berjalan pada server *Linux* yang menjalankan *Apache* sebagai *web server*
2	*Database server* yang digunakan adalah *MySQL*
3	Koneksi antara *server web* dan *database server* menggunakan jaringan pribadi
4	Protokol komunikasi menggunakan TLS (*Transport Layer Security*)

3. Titik Masuk

Titik masuk merupakan antarmuka pada aplikasi sebagai media interaksi antara penyerang potensial dengan aplikasi atau data. Titik masuk ini didokumentasikan dengan memberikan nomor unik, nama antarmuka, deskripsi titik masuk, dan level kepercayaan dari setiap hak akses.

Setiap titik masuk pada aplikasi sistem informasi akademik akan diidentifikasi dan akan dicari keterkaitannya dengan level kepercayaan pengguna sistem. Sebagai contoh, titik masuk aplikasi yaitu *port https* yang merupakan protokol komunikasi pada jaringan komputer memiliki keterkaitannya dengan setiap pengguna web yang mengakses sistem informasi akademik. Jika dilihat lebih detail lagi maka pengguna web dalam lingkup ini terdiri atas pengguna web secara umum dan pengguna web yang memiliki akun untuk login ke aplikasi. Sebagai standarisasi penentuan pengguna, maka jenis-jenis pengguna ini telah ditetapkan sebagai Level Kepercayaan (LK) pada sistem informasi akademik yang diatur pada Tabel 4.5. Proses identifikasi titik masuk sistem informasi akademik akan dikaitkan dengan level kepercayaan yang merujuk pada Tabel 4.5.

Hasil identifikasi titik masuk pada aplikasi sistem informasi akademik selengkapmya disajikan pada Tabel 4.3.

Tabel 4.3. Identifikasi Titik Masuk pada Aplikasi

Titik Masuk			
ID	Nama	Deskripsi	Level Kepercayaan
1	*Port* HTTPS	Situs web sistem informasi akademik hanya dapat diakses melalui protokol TLS	(LK1) Pengguna web anonim (LK2) Pengguna dengan kredensial login yang valid (LK3) Pengguna dengan kredensial login yang tidak valid (LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi
1.1	Halaman *login*	Pengguna wajib *login* untuk dapat mengakses layanan akademik	(LK1) Pengguna web anonim (LK2) Pengguna dengan kredensial login yang valid (LK3) Pengguna dengan kredensial login yang tidak valid (LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi
1.2	Fungsionalitas *login*	Fungsionalitas *login* menerima kredensial dari pengguna dan akan membandingkan kredensial tersebut dengan data yang ada di *database*	(LK2) Pengguna dengan kredensial login yang valid (LK3) Pengguna dengan kredensial login yang tidak valid (LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi

4. Aset

Aset dapat berupa hal fisik atau abstrak yang dimiliki oleh sistem dan merupakan sesuatu yang diminati oleh penyerang. Aset pada dasarnya adalah target ancaman, yaitu sesuatu yang menjadi alasan munculnya sebuah ancaman. Aset didokumentasikan dengan memberikan nomor unik, nama aset, deskripsi aset, dan level kepercayaan dari setiap hak akses.

Setiap aset pada aplikasi sistem informasi akademik akan diidentifikasi dan akan dicari keterkaitannya dengan level kepercayaan pengguna sistem. Sebagai contoh, aset berupa Detail *Login* Pengguna yang berfungsi sebagai kredensial pengguna agar dapat menggunakan layanan aplikasi memiliki keterkaitannya dengan pengguna web yang

mengakses sistem informasi akademik. Jika dilihat lebih detail lagi maka pengguna web di sini terdiri atas pengguna web pada umumnya, dan pengguna yang memiliki akun untuk *login* ke aplikasi. Setiap identifikasi aset pada aplikasi akan dikaitkan dengan level kepercayaan yang merujuk pada Tabel 4.5.

Hasil identifikasi aset aplikasi sistem informasi akademik selengkapmya disajikan pada Tabel 4.4.

Tabel 4.4. Identifikasi Aset pada Sistem

Aset			
ID	Nama	Deskripsi	Level Kepercayaan
A1	Pengguna layanan situs akademik	Aset yang berkaitan dengan pengguna	
A1.1	Detail Login Pengguna	Kredensial login yang akan digunakan pegguna untuk masuk ke situs web Sistem Informasi Akademik	(LK2) Pengguna dengan kredensial login yang valid (LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi (LK7) Administrator server database (LK9) Proses server web (LK10) Database read user (LK11) Database read/write user
A1.2	Data pribadi mahasiswa	Situs web akademik akan menyimpan informasi pribadi yang berkaitan dengan mahasiswa	(LK2) Pengguna dengan kredensial login yang valid (LK5) Admin akademik (LK6) Admin prodi (LK7) Administrator server database (LK8) Administrator situs web (LK9) Proses server web (LK10) Database read user (LK11) Database read/write user

Aset			
ID	Nama	Deskripsi	Level Kepercayaan
A1.3	Data pribadi dosen	Situs web akademik akan menyimpan informasi pribadi yang berkaitan dengan dosen	(LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi (LK7) Administrator server database (LK8) Administrator situs web (LK9) Proses server web (LK10) Database read user (LK11) Database read/write user
A2	Sistem	Aset yang berkaitan dengan sistem	
A2.1	Ketersediaan situs web	Situs web layanan akademik harus tersedia selama 24 jam dalam sehari dan dapat diakses oleh seluruh pengguna	(LK7) Administrator server database (LK8) Administrator situs web
A2.2	Ketersediaan *database*	Database layanan akademik harus tersedia dan dapat melayani permintaan data selama 24 jam dalam sehari	(LK7) Administrator server database (LK8) Administrator situs web
A2.3	Eksekusi kode pemograman web	Kemampuan untuk menjalankan kode pemrograman di *web server*	(LK8) Administrator situs web (LK9) Proses server web
A2.4	Eksekusi perintah *SQL read database*	Kemampuan untuk menjalankan *SQL query select* pada *database*, bagi pengguna yang telah *login* ke sistem, sehingga dapat menerima informasi yang tersimpan pada *database*	(LK5) Admin akademik (LK6) Admin prodi (LK7) Administrator server database (LK10) Database read user (LK11) Database read/write user
2.5	Eksekusi perintah *SQL read/write database*	Kemampuan untuk menjalankan *SQL query select*, *insert*, dan *update* pada *database*, bagi pengguna yang telah *login* ke sistem, sehingga memiliki akses baca tulis pada *database*	(LK7) Administrator server database (LK11) Database read/write user

Aset			
ID	Nama	Deskripsi	Level Kepercayaan
2.6	Manajemen data	Kemampuan *Administrator* untuk mengelola data pada sistem	(LK5) Admin akademik (LK6) Admin prodi (LK7) Administrator server database (LK11) Database read/write user
2.7	Melihat log	Kemampunan *Administrator* sistem untuk melihat *log* terkait web dan *database*	(LK7) Administrator server database
3	Situs web	Aset yang berkaitan dengan situs web layanan akademik	
3.1	Sesi login	Sesi *login* pengguna ke situs web layanan akademik	(LK2) Pengguna dengan kredensial login yang valid
3.2	Layanan akademik	Pengguna yang telah *login* dapat mengakses segala layanan yang tersedia pada aplikasi SIA	(LK2) Pengguna dengan kredensial login yang valid (LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi (LK9) Proses server web (LK10) Database read user (LK11) Database read/write user
3.2	Akses ke *database server*	Akses ke *database server* memungkinkan seorang administrator untuk mengelola database, memberi akses penuh ke database pengguna dan semua data yang ada di dalam database.	(LK7) Administrator server database

5. Level Kepercayaan

Level kepercayaan mewakili hak akses yang akan diberikan aplikasi kepada entitas eksternal. Level kepercayaan yang diidentifikasi pada sistem informasi akademik didokumentasikan dengan memberikan nomor unik, nama entitas eksternal, dan deskripsi entitas eksternal, seperti ditunjukkan pada Tabel 4.5.

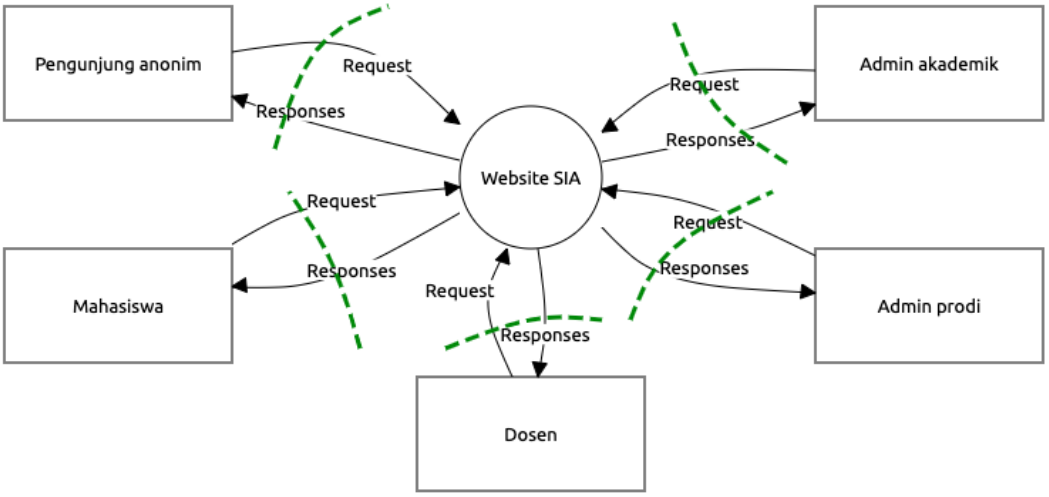
Tabel 4.5. Identifikasi Level Kepercayaan pada Aplikasi

Level Kepercayaan		
ID	Nama	Deskripsi
LK1	Pengguna web anonim	Seseorang yang mengakses situs web sistem informasi akademik perguruan tinggi tetapi tidak mempunyai kredensial *login*
LK2	Pengguna dengan kredensial *login* yang valid	Seseorang yang mengakses situs web sistem informasi akademik perguruan tinggi dan telah login menggunakan kredensial *login* yang valid
LK3	Pengguna dengan kredensial *login* tidak valid	Seseorang yang mengakses situs web sistem informasi akademik perguruan tinggi dan mencoba untuk login menggunakan kredensial *login* yang tidak valid
LK4	Dosen	Seseorang tenaga pendidik perguruan tinggi
LK5	Admin akademik	Seseorang tenaga kependidikan pada bagian akademik perguruan tinggi yang memiliki kewenangan tertentu
LK6	Admin prodi	Seseorang dari pihak program studi perguruan tinggi yang memiliki kewenangan tertentu
LK7	Administrator *database server*	Seseorang administrator yang memiliki akses penuh ke *database server* situs sistem informasi akademik perguruan tinggi
LK8	Administrator situs web	Seseorang administrator yang memiliki akses penuh untuk mengkonfigurasi situs web sistem informasi akademik perguruan tinggi
LK9	Proses *web server*	Merupakan entitas yang dijalankan oleh *web server* sebagai kode tertentu dan mampu melakukan proses otentitikasi dirinya sendiri terhadap *database server*
LK10	*Database read user*	Akun pengguna *database* yang memiliki hak akses hanya dapat membaca *database*
LK11	*Database read/write user*	Akun pengguna *database* yang memiliki hak akses dapat membaca dan menulis pada *database*

4.1.2 Data Flow Diagram

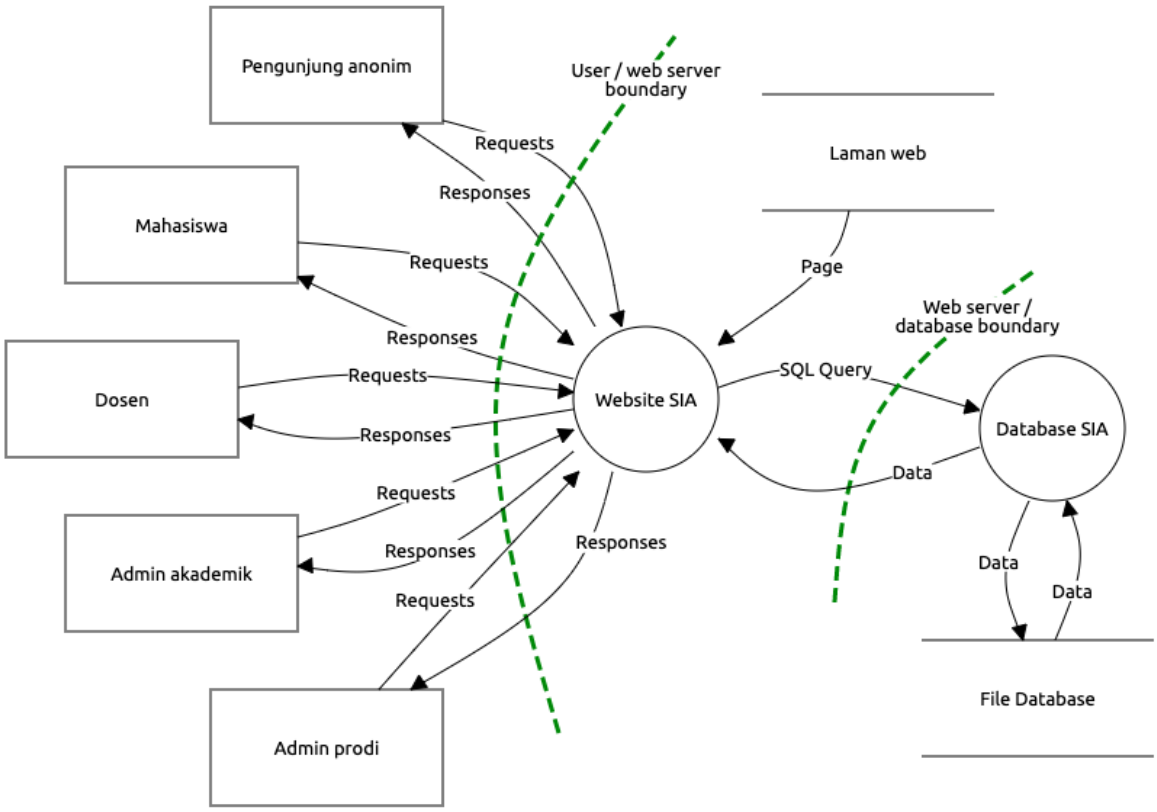
Setelah menyusun dokumen *Threat Model*, langkah selanjutnya adalah menyusun *Data Flow Diagram*. Representasi visual *Data Flow Diagram* memungkinkan untuk memperoleh pemahaman yang lebih baik mengenai aplikasi ketika memproses data. Berikut adalah hasil penyusunan *Data Flow Diagram* sistem informasi akademik pada Universitas XYZ.

1. *Context diagram* sistem informasi akademik



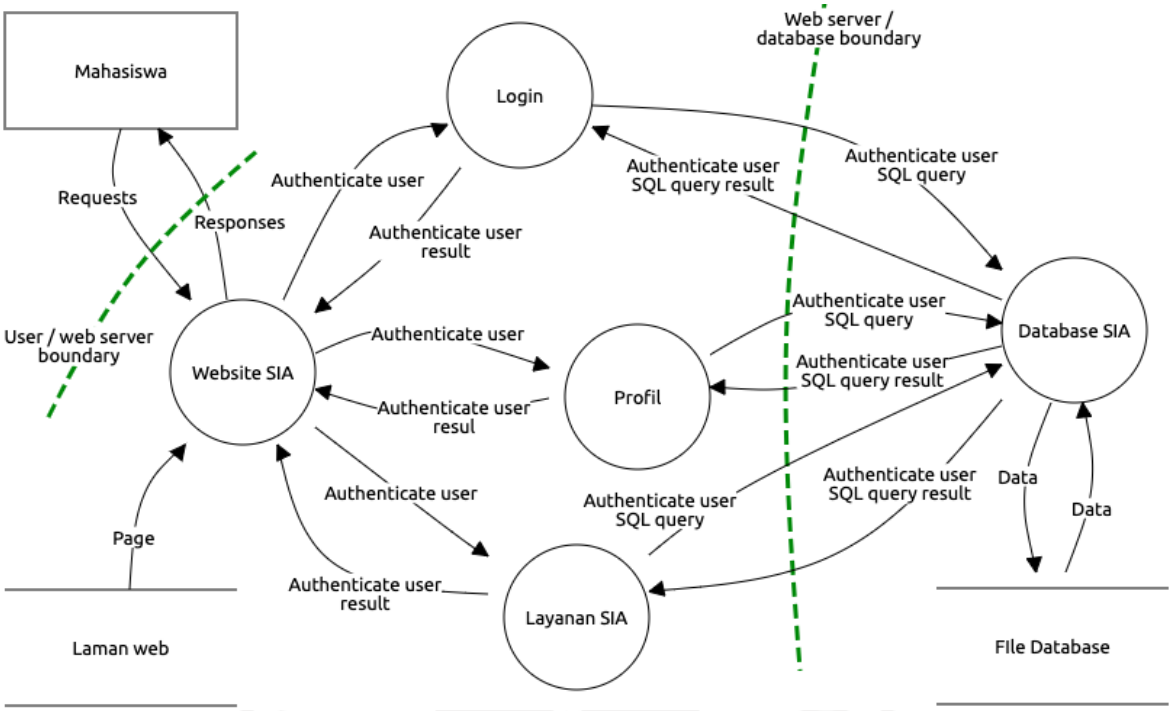
Gambar 4.1. *Context diagram* sistem informasi akademik

2. *Data flow diagram* sistem informasi akademik level 1



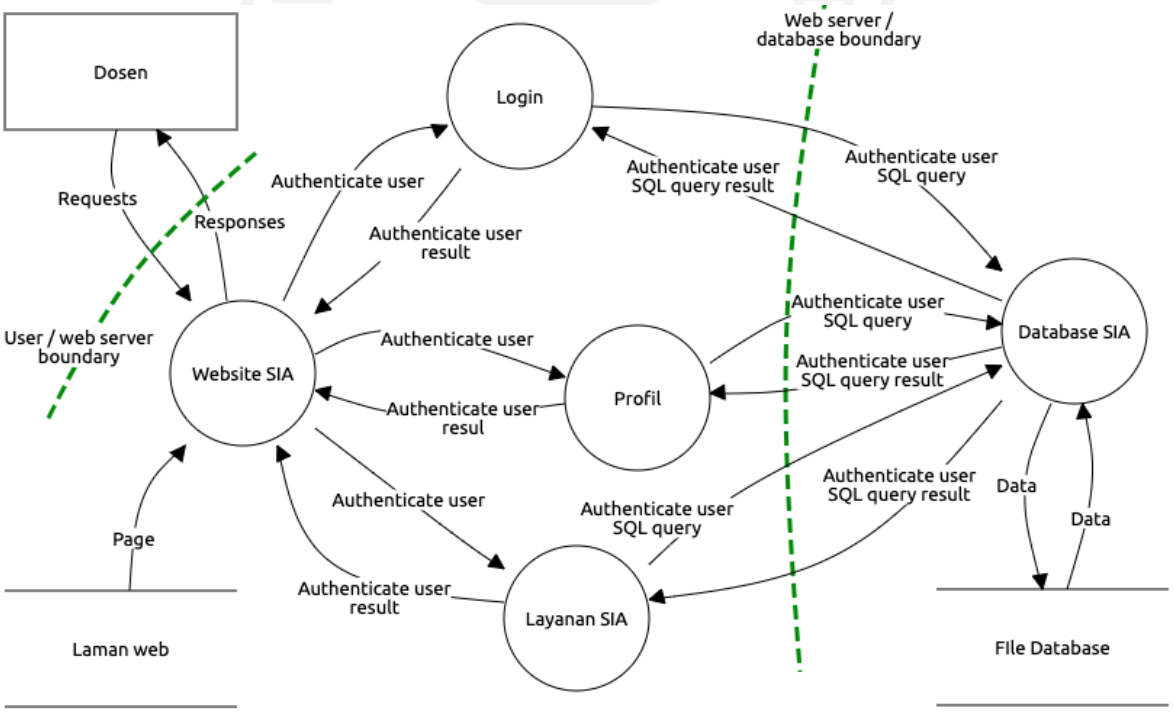
Gambar 4.2. DFD sistem informasi akademik level 1

3. *Data flow diagram* sistem informasi akademik level-2 pengguna mahasiswa



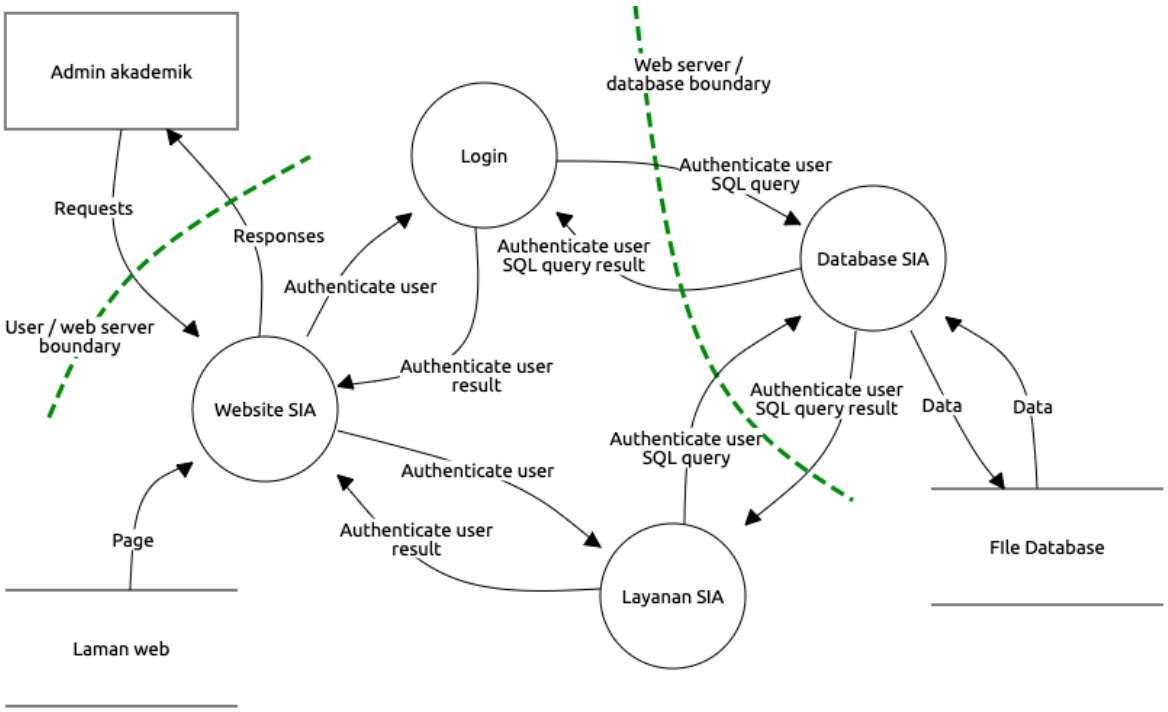
Gambar 4.3. DFD sistem informasi akademik level-2 pengguna mahasiswa

4. *Data flow diagram* sistem informasi akademik level-2 pengguna dosen



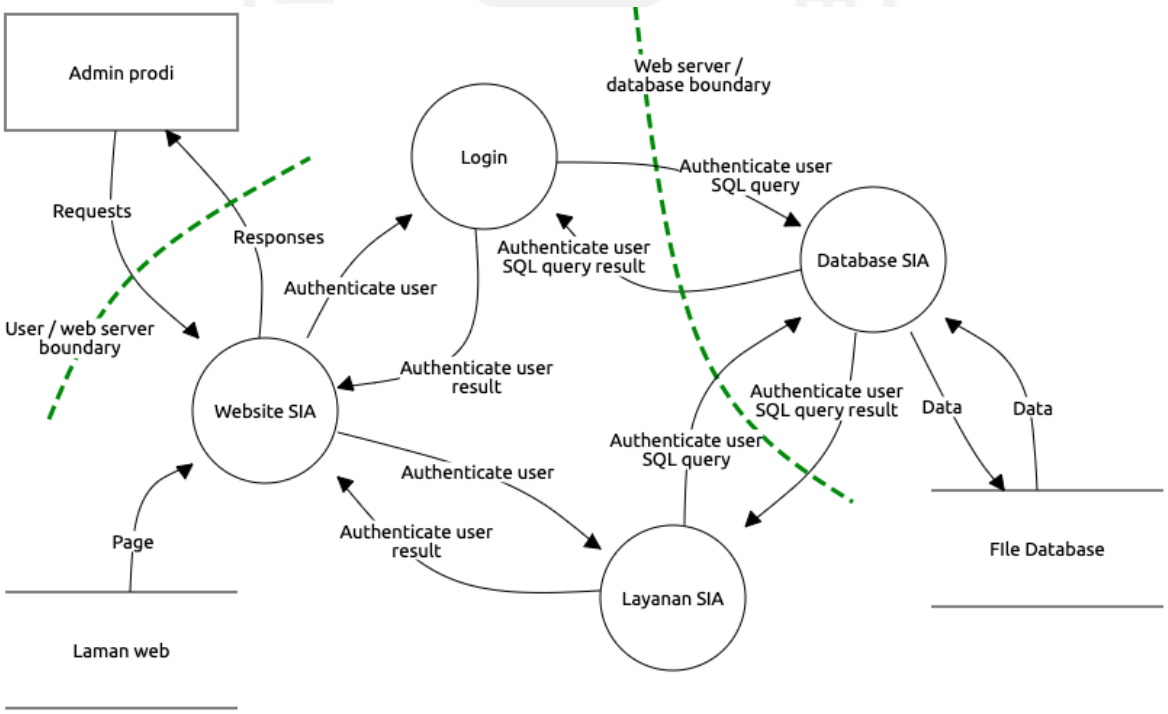
Gambar 4.4. DFD sistem informasi akademik level-2 pengguna dosen

5. *Data flow diagram* sistem informasi akademik level-2 pengguna admin akademik



Gambar 4.5. DFD sistem informasi akademik level-2 pengguna admin akademik

6. *Data Flow Diagram* Admin Program Studi



Gambar 4.6. DFD sistem informasi akademik level-2 pengguna admin prodi

4.2 Klasifikasi Ancaman

Proses klasifikasi ancaman digunakan untuk mengelompokkan jenis ancaman dari hasil identifikasi berbagai ancaman yang mungkin akan terjadi pada sistem. Ancaman pada sistem informasi akademik akan diidentifikasi dengan mengacu pada kategori *STRIDE* sebagai standarisasi penentuan jenis ancaman. Ketika mengidentifikasi sebuah ancaman, maka motif ancaman akan diklasifikasikan pada jenis ancaman yang sesuai dengan karakteristik STRIDE. Struktur klasifikasi setiap kategori ancaman STRIDE yaitu *spoofing*, *tampering*, *repudiation*, *information disclosure*, *denial of service*, dan *elevation of priviledge* telah diuraikan pada Tabel 3.1.

Setiap tindak ancaman yang teridentifikasi akan memiliki keterkaitan dengan entitas luar yang direpresentasikan sebagai level kepercayaan. Suatu ancaman tentu tidak akan terwujud menjadi sebuah ancaman apabila tidak ada pihak yang menjalankan tindakan ancaman ini. Adanya keterkaitan yang erat antara tindak ancaman dengan entitas luar maka setiap ancaman akan dicari keterkaitannya dengan level kepercayaan sebagai representasi dari entitas luar. Mengingat pola hubungan ini maka setiap ancaman yang diidentifikasi akan dicari keterkaitannya dengan level kepercayaan yang telah ditentukan pada pada Tabel 4.5.

Sebagai contoh proses mengklasifikasian ancaman, identifikasi ancaman yang pertama adalah keteledoran seorang pengguna terhadap informasi *login* miliknya berupa nama dan kata sandi yang biasa dipakai untuk mengakses layanan sistem informasi akademik. Ancaman pertama ini ditandai dengan nomor identitas T1 (*Threat* 1) dan dicari keterkaitannya dengan level kepercayaan pada Tabel 4.5. Ancaman kemudian diidentifikasi berdasarkan kategori *STRIDE* pada Tabel 3.1. Selanjutnya diketahui bahwa motif ancaman T1 merupakan ancaman dengan kategori *spoofing*, yaitu tindak ancaman yang ditujukan untuk mengakses dan menggunakan kredensial pengguna lain secara ilegal. Ancaman T1 kemudian diidentifikasi keterkaitannya dengan level kepercayaan, dan diketahui bahwa T1 memiliki keterkaitan dengan LK2, LK4, LK5, dan LK6.

Hasil identifikasi ancaman selengkapnya disajikan pada Tabel 4.6.

Tabel 4.6. Klasifikasi Ancaman

ID	Deskripsi	Level Kepercayaan	STRIDE
T1	Pengguna meninggalkan kredensial login di tempat umum, atau secara tidak sengaja menyimpan informasi login di browser komputer publik, atau membagikan informasi login ke teman atau kerabatnya	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi	S

ID	Deskripsi	Level Kepercayaan	STRIDE
T2	Pengguna memberikan kredensial login kepada orang lain secara tidak sengaja, misal melalui serangan social engineering	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi	S
T3	Seseorang yang telah diberitahu kredensial login pengguna (misal teman atau kerabat) menyalahgunakan akun/identitas pengguna untuk tindak kejahatan	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen	S
T4	Seorang admin menyalahgunakan akun/identitas pengguna untuk tindak kejahatan	(LK5) Admin akademik (LK6) Admin prodi (LK7) Admin server database	S
T5	Penyerang memalsukan laman login web untuk mendapatkan informasi kredensial login dari pengguna	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi	S
T6	Admin secara sengaja atau tidak sengaja menambah, memodifikasi, atau menghapus data pengguna pada sistem database di luar ketentuan	(LK5) Admin akademik (LK7) Admin server database	T
T7	Penyerang dengan sengaja menambah, memodifikasi, atau menghapus data yang tersimpan pada sistem database	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi (LK7) Admin server database	T
T8	Seseorang menggunakan identitas pengguna yang sah untuk melakukan tindak kejahatan	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi (LK7) Admin server database	R
T9	Penyangkalan pihak pengguna yang sah bahwa tidak melakukan tindakan menambah, mengubah, atau menghapus data	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen	R

ID	Deskripsi	Level Kepercayaan	STRIDE
T10	Penyangkalan pihak admin bahwa tidak melakukan tindakan menambah, mengubah, atau menghapus data	(LK5) Admin akademik (LK6) Admin prodi (LK7) Admin server database (LK8) Admin situs web	R
T11	Pencatatan log yang minim sebagai bukti penanganan klaim penyangkalan	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi (LK7) Admin server database (LK8) Admin situs web (LK9) Proses server web (LK11) Database read/write user	R
T12	Penyerang membaca informasi pribadi pengguna yang tersimpan pada sistem database	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen	I
T13	Penyerang menyebarluaskan informasi tentang data pribadi pengguna	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen	I
T14	Penyerang mengumpulkan data pengguna sebagai target tindak kejahatan	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen	I
T15	Penyerang membanjiri bandwidth melalui banyak request dengan maksud untuk memperlambat atau bahkan menumbangkan sistem	(LK9) Proses server web (LK11) Database read/write user	D
T16	Penyerang mengupload banyak file dengan maksud untuk memenuhi media penyimpanan database	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen (LK9) Proses server web (LK11) Database read/write user	D
T17	Seseorang bukan pengguna yang sah mengakses sistem menggunakan kredensial login pengguna yang memiliki akses lebih tinggi	(LK2) Pengguna dengan kredensial login valid (LK4) Dosen (LK5) Admin akademik (LK6) Admin prodi (LK7) Admin server database	E

4.3 Penilaian Ancaman

Tahap penilaian ancaman bertujuan untuk memperoleh informasi tentang ranking risiko dari ancaman yang sebelumnya telah diklasifikasikan pada Tabel 4.6. Proses penilaian ancaman dilakukan menggunakan pendekatan *DREAD* dengan uraian penilaian sebagai berikut.

1. Berdasarkan klasifikasi ancaman Tabel 4.6, sebagai contoh penilaian adalah ancaman pertama (T1) yaitu "pengguna meninggalkan kredensial login di tempat umum, atau secara tidak sengaja menyimpan informasi *login* di *browser* komputer publik, atau membagikan informasi *login* ke teman atau kerabatnya".
2. Ancaman T1 memiliki 4 level kepercayaan yaitu LK2, LK4, LK5, dan LK6. Proses penilaian dilakukan secara bertahap pada setiap level kepercayaan di setiap ancaman. Karena ancaman T1 memiliki 4 level kepercayaan, maka sebagai contoh uraian proses penilaian ini akan diambil level kepercayaan yaitu LK2 "Pengguna dengan kredensial login valid".
3. Langkah berikutnya adalah menilai ancaman T1 untuk kelima kategori *DREAD* dengan aturan penilaian pendekatan *DREAD*, yaitu ancaman yang memiliki peringkat tinggi dinilai sama dengan 3, peringkat sedang dinilai sama dengan 2, dan ancaman dengan peringkat rendah dinilai sama dengan 1 (Fruhlinger, 2020). Adapun skema pendekatan penilaian setiap kategori *DREAD* telah diuraikan pada Tabel 3.2. Proses pendekatan penilaian kelima kategori *DREAD* untuk ancaman T1 dengan level kepercayaan LK2 sebagai berikut.
    a. (D) *Damage potential*, yaitu seberapa besar potensi kerusakan yang terjadi jika serangan berhasil dilakukan. Ancaman T1 dengan level kepercayaan LK2 (Pengguna dengan kredensial login valid), dalam hal ini adalah mahasiswa, diberikan nilai potensi kerusakan sama dengan 1 karena apabila seorang penyerang berhasil mengakses kredensial milik seorang mahasiswa, maka potensi kerusakan masih dalam peringkat rendah karena hanya sebatas pada satu pengguna yang akan melakukan tindak ancaman berikutnya.
    b. (R) *Reproducibility* yaitu seberapa mudah untuk mereproduksi serangan. Ancaman T1 dengan level kepercayaan LK2 (pengguna dengan kredensial login valid), dalam hal ini adalah mahasiswa, diberikan nilai reproduksi serangan sama dengan 3 karena apabila penyerang telah memperoleh kredensial login mahasiswa, penyerang dengan mudah untuk memproduksi serangan-serangan tertentu secara berulang. Kemudahan untuk melakukan serangan ini dinilai berisiko tinggi sehingga diberikan nilai 3.

c. (E) *Exploitability* yaitu berapa banyak waktu, tenaga, dan keahlian yang dibutuhkan untuk mengeksploitasi ancaman. Ancaman T1 merupakan bentuk keteledoran pengguna, sehingga usaha untuk mendapatkan kredensial tersebut sangat mudah, maka ancaman T1 pada kategori *exploitability* diberi nilai 3.

d. (A) *Affected user* yaitu seberapa banyak pengguna yang terpengaruh jika ancaman dieksploitasi. Ancaman T1 dengan level kepercayaan LK2 (pengguna dengan kredensial login valid), dalam hal ini adalah mahasiswa, diberikan nilai sama dengan 1 karena jumlah pengguna yang terpengaruh oleh ancaman T1 ini sangat minim, yaitu hanya satu akun pengguna yang terkena dampaknya.

e. (D) *Discoverability* yaitu seberapa mudah bagi penyerang untuk menemukan ancaman pada sistem. Ancaman T1 merupakan bentuk keteledoran pengguna, sehingga usaha untuk menemukan ancaman berupa informasi kredensial *login* tersebut terbilang sangat mudah, maka ancaman T1 untuk level kepercayaan LK2 pada kategori *discoverability* diberi nilai 3.

4. Berdasarkan proses penilaian ancaman setiap kategori *DREAD* pada langkah ketiga, diperoleh nilai setiap kategori yaitu D = 1, R = 3, E = 3, A = 1, dan D = 3, sehingga dihasilkan perhitungan 1 + 3 + 3 + 1 + 3 = 11.
5. Hasil perhitungan total nilai ancaman kemudian diranking sesuai aturan peringkat ancaman seperti pada Tabel 3.3, yaitu rentang nilai antara 5–7 adalah risiko rendah, rentang nilai antara 8–11 adalah risiko sedang, dan rentang nilai antara 12–15 adalah risiko tinggi (Logixconsulting, 2019). Perhitungan pada langkah ketiga menghasilkan total nilai 11, sehingga dapat dikatakan bahwa ancaman T1 dengan level kepercayaan LK2 merupakan ancaman dengan risiko sedang.
6. Seluruh ancaman dengan level kepercayaan yang menyertainya akan dinilai dengan langkah-langkah tersebut.

Penilaian setiap kategori *DREAD* untuk setiap ancaman yang teridentifikasi disajikan pada Tabel 4.7, secara lengkap dapat dilihat pada lampiran A.

Tabel 4.7. Penilaian Ancaman

Threat	Level Kepercayaan	D	R	E	A	D	TOTAL	RISIKO
T1	LK2	1	3	3	1	3	11	Sedang
T1	LK4	2	3	3	2	3	13	Tinggi
T1	LK5	3	3	3	3	3	15	Tinggi
T1	LK6	3	3	3	3	3	15	Tinggi

Threat	Level Kepercayaan	D	R	E	A	D	TOTAL	RISIKO
T2	LK2	1	3	2	1	2	9	Sedang
T2	LK4	2	3	2	2	2	11	Sedang
T2	LK5	3	3	2	3	2	13	Tinggi
T2	LK6	3	3	2	3	2	13	Tinggi
T3	LK2	2	3	3	1	3	12	Tinggi
T3	LK4	2	3	3	2	3	13	Tinggi
T4	LK5	2	3	3	2	3	13	Tinggi
T4	LK6	2	3	3	2	3	13	Tinggi
T4	LK7	3	3	3	3	3	15	Tinggi
T5	LK2	1	2	2	1	2	8	Sedang
T5	LK4	2	2	2	2	2	10	Sedang
T5	LK5	3	2	2	3	2	12	Tinggi
T5	LK6	3	2	2	3	2	12	Tinggi
…	…	…	…	…	…	…	…	…
T17	LK7	3	1	1	3	1	9	Sedang

4.4 Mitigasi

Penyusunan kontrol mitigasi sebagai langkah untuk mengurangi risiko dapat dilakukan setelah mengetahui hasil perankingan setiap ancaman. Adanya peringkat setiap ancaman ini juga digunakan sebagai dasar untuk menyusun daftar mitigasi terhadap ancaman sesuai prioritas risiko tertinggi.

Berdasarkan data penilaian ancaman pada Tabel 4.7 dapat disusun langkah mitigasi sesuai dengan klasifikasi ancaman. Daftar penilaian ancaman ini dapat dikelompokkan terlebih dahulu sesuai tingkat risikonya untuk mempermudah melihat daftar ancaman yang memiliki risiko tinggi.

Ancaman T1 dengan level kepercayaan LK4 memiliki peringkat risiko tinggi. Ancaman T1 ini merupakan klasifikasi ancaman *spoofing*, sehingga langkah pencegahan yang dapat dilakukan sesuai teknik mitigasi pada bidang *authentication* yang disarankan dapat berupa proses otentikasi yang lebih aman, perlindungan data rahasia pengguna, tidak menuliskan *password* di media apapun, sosialisasi kepada pengguna layanan sistem informasi akademik tentang pentingnya keamanan dan kewaspadaan terhadap kredensial login miliknya.

Ancaman kategori lain yang berisiko tinggi adalah *tampering* dengan contoh ancaman T6 pada level kepercayaan LK5. *Tampering* merupakan ancaman dengan kontrol keamanan bidang *integrity*. Langkah pencegahan yang disarankan pada bidang *integrity* ini adalah proses otentikasi yang lebih aman, penerapan *digital signature* yang akan tercatat secara otomatis pada *log* di setiap perubahan data, penerapan kode *hash* untuk memvalidasi data. Berdasarkan pada kasus perubahan nilai yang pernah terjadi oleh pihak yang tidak berwenang, maka mitigasi yang dapat dilakukan adalah penerapan kode *hash* pada file yang dipakai untuk mengirimkan data nilai akhir mahasiswa. Ketika dosen mengunggah file yang memuat data nilai, sistem secara otomatis akan menghitung dan mencatat kode hash file tersebut. Kode *hash* ini akan berfungsi sebagai kode validasi oleh pihak akademik dalam memproses nilai akhir mahasiswa. Jika terdapat perubahan isi pada file, maka kode *hash* file tersebut akan ikut berubah, sehingga proses penilaian akhir mahasiswa dapat dikroscek terlebih dahulu ke pihak dosen karena adanya ketidakcocokan kode *hash* file yang diunggah dosen.

Ancaman berikutnya yang memiliki peringkat risiko tinggi adalah ancaman kategori *repudiation* yang masuk dalam kontrol keamanan *confirmation*. Langkah pencegahan yang disarankan pada bidang keamanan *confirmation* adalah penerapan *digital signature* dan penerapan *timestamp* di setiap perubahan data, pencatatan segala sesuatu tindakan pada sistem pada *log* sebagai bahan pembuktian atas terjadinya perubahan pada sistem.

Usulan mitigasi selengkapnya ditunjukkan pada Tabel 4.8.

Tabel 4.8. Usulan Mitigasi

1.	**Ancaman**	T1, T2, T3, T5
	Level Kepercayaan	LK4, LK5, LK6
	Kategori	*Spoofing*
	Bidang Keamanan	*Authentication*
	Mitigasi	- Abaikan fitur penyimpanan *username* dan *password* yang ditawarkan pada *browser* - Penggunaan mode *browser incognito/private* ketika memakai komputer publik untuk mengakses sistem - Menghindari pencatatan *password* di media apapun - Tidak memberitahukan kredensial login miliknya ke orang lain tanpa terkecuali - Abaikan segala jenis permintaan informasi kredensial *login* melalui tautan yang tidak terpercaya

		- Sosialisasi kepada pengguna tentang pentingnya keamanan dan kewaspadaan terhadap kredensial login miliknya
2.	**Ancaman**	T6, T7
	Level Kepercayaan	LK4, LK5, LK6, LK7
	Kategori	*Tampering*
	Bidang Keamanan	*Integrity*
	Mitigasi	- Penerapan *digital signature* yang akan tercatat secara otomatis pada *log* perubahan data - Penerapan kode *hash* untuk validasi - Pencatatan *log* tentang segala perubahan data
3.	**Ancaman**	T8, T11
	Level Kepercayaan	LK7, LK8
	Kategori	*Repudiaction*
	Bidang Keamanan	*Confirmation*
	Mitigasi	- Segala sesuatu tindakan pada sistem harus dicatat pada *log* untuk bahan pembuktian atas terjadinya suatu tindakan pada sistem - Penerapan *digital signature* yang akan tercatat secara otomatis pada *log* perubahan data

BAB 5
Penutup

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dapat diambil kesimpulan sebagai berikut.

1. Penerapan *threat modeling* menggunakan pemodelan *STRIDE* pada Sistem Informasi Akademik Universitas XYZ dapat mengidentifikasi ancaman-ancaman yang dapat terjadi pada sistem, yaitu kategori *spoofing* sebanyak 5 ancaman, kategori *tampering* sebanyak 2 ancaman, kategori *repudiation* sebanyak 4 ancaman, kategori *information disclosure* sebanyak 3 ancaman, kategori *denial of service* sebanyak 2 ancaman, dan kategori *elevation of priviledge* sebanyak 1 ancaman.
2. Penerapan pemodelan *DREAD* dapat menghasilkan informasi tentang nilai setiap ancaman pada Sistem Informasi Akademik Universitas XYZ. Berdasarkan perhitungan pemodelan *DREAD* dapat diketahui bahwa ancaman yang memiliki risiko tinggi adalah ancaman pada kategori *spoofing*, *tampering*, dan *repudiaction*. Adapun ancaman dengan kategori *information disclosure* dan kategori *denial of service* pada Sistem Informasi Akademik Universitas XYZ memiliki peringkat risiko sedang.
3. Tahapan klasifikasi dan penilaian ancaman akan menghasilkan informasi peringkat risiko dari setiap ancaman. Selanjutnya hasil perankingan ini dapat digunakan sebagai dasar untuk menyusun kontrol mitigasi sesuai prioritas tingkat risiko ancaman. Adapun mitigasi yang dapat diterapkan pada Sistem Informasi Akademik Universitas XYZ terhadap ancaman *spoofing*, *tampering*, dan *repudiaction* disajikan pada Tabel 4.8.

5.2 Saran

Mengingat keterbatasan pada penelitian *threat modeling* ini maka perlu adanya saran untuk penelitian selanjutnya sebagai bentuk pengembangan atas keterbatasan penelitian ini. Saran untuk penelitian *threat modeling* pada sistem informasi berbasis website selanjutnya dapat mengkombinasikan perhitungan risiko menggunakan tool semisal *OWASP ZAP* sebagai bahan perbandingan atas hasil perhitungan peringkat risiko setiap ancaman.

Daftar Pustaka

Ahmad, L., & Munawir. (2018). *Sistem Informasi Manajemen: Buku Referensi*. Kota Banda Aceh: Go Print.

Alhassan, J. K., Abba, E., Olaniyi, O. M., & Waziri, V. O. (2016). Threat modeling of electronic health systems and mitigating countermeasures. *CEUR Workshop Proceedings*, *1830*(Icta), 82–89.

Budiarto, R. (2017). Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode FMEA dan ISO 27001 pada Organisasi XYZ. *Journal of Computer Engineering System and Science*, *2*(2), 48–58.

Chazar, C., & Ramdani, A. (2016). Model perencanaan keamanan sistem informasi menggunakan pendekatan metode octave dan iso 27001:2005. In *Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016)* (hal. 80–85).

Dehalwar, V., Kalam, A., Kolhe, M. L., & Zayegh, A. (2018). *Review of web-based information security threats in smart grid*. *2017 7th International Conference on Power Systems, ICPS 2017*. Creative Commons. https://doi.org/10.1109/ICPES.2017.8387407

EC-Council. (2020). What is Stride Methodology in Threat Modeling? Diambil dari https://blog.eccouncil.org/what-is-stride-methodology-in-threat-modeling/

Fruhlinger, J. (2020). Threat modeling explained: A process for anticipating cyber attacks. Diambil dari https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html

Habibi, R., Aditya, R., & Echa, D. (2020). *Sistem Informasi Peminjaman Ruangan*. Bandung: Kreatif Industri Nusantara.

Hamzah, R. F., Jaya, I. D., & Putri, U. M. (2020). Analisis Risiko Keamanan Sistem Informasi E-LKP Dengan Metode Octave Pada Perguruan Tinggi Negeri X. *Jusifo*, *6*(1), 55–65. https://doi.org/10.19109/jusifo.v6i1.5880

Hartono. (2020). *Transformasi Perpustakaan Dalam Ekosistem Digital: Konsep Dasar, Organisasi Informasi, dan Literasi Digital*. Jakarta: Prenada Media.

Homaidi, A. (2016). Sistem Informasi Akademik Amik Ibrahimy Berbasis Web. *Jurnal Ilmiah Informatika*, *1*(1), 17–23.

Ikhsan, H., & Jarti, N. (2018). Analisis Risiko Keamanan Teknologi Informasi Menggunakan Octave Allegro. *Jurnal Responsive*, *2*(1), 31–41.

Jouini, M., Rabai, L. B. A., & Aissa, A. Ben. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452

Klaić, A. (2010). Overview of the state and trends in the contemporary information security policy and information security management methodologies. *MIPRO 2010 - 33rd International Convention on Information and Communication Technology, Electronics and Microelectronics, Proceedings*, 1203–1208.

Kurniawan, E., & Riadi, I. (2018). Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM. *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, *2*(1), 12. https://doi.org/10.29407/intensif.v2i1.11830

Logixconsulting. (2019). What Is the DREAD Cybersecurity Model? Diambil dari https://www.logixconsulting.com/2019/12/18/what-is-the-dread-cybersecurity-model/

Mahmood, H. (2017). Application Threat Modeling using DREAD and STRIDE. Diambil dari https://haiderm.com/application-threat-modeling-using-dread-and-stride/

Meier, J. D., Mackman, A., Vasireddy, S., Dunner, M., Escamilla, R., Murukan, A., & Satyam. (2003). *Improving Web Application Security, Threats and Countermeasures*. Microsoft Corporation.

Mulyani, S., Suzan, L., Dagara, Y., Yuniarti K., E., Karya S., C. D., Azizah K., Z. N., & Alam M., M. (2018). *Sistem Informasi Akutansi: Aplikasi di Sektor Publik*. Bandung: Unpad Press.

Muslihudin, M., & Oktafianto. (2016). *Analisis dan Perancangan Sistem Informasi Menggunakan Model Terstruktur dan UML*. Yogyakarta: Andi.

Nugraha, U. (2016). Manajemen Risiko Sistem Informasi pada Perguruan Tinggi Menggunakan Kerangka Kerja NIST SP 800-300. In *Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016)* (hal. 121–126).

Owasp.org. (2020). CRV2 App Threat Modeling. Diambil dari https://owasp.org/www-community/CRV2_AppThreatModeling

Owasp. (2016). OWASP Cheat Sheet Series - OWASP. Diambil dari https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series

Prasetyowati, D. D., Gamayanto, I., Wibowo, S., & Suharnawi, S. (2019). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang. *JOINS (Journal of Information System)*, *4*(1), 65–75. https://doi.org/10.33633/joins.v4i1.2429

Prehanto, D. R. (2020). *Buku Ajar Konsep Sistem Informasi*. Surabaya: Scopindo Media Pustaka.

Rahmah, G. M. (2019). Analisis Manajemen Risiko Penerapan Sistem Informasi di Politeknik STMI Jakarta, *17*(2), 65–77.

Saputra, A., Nelmiawati, N., & Sitorus, M. A. R. (2017). Penilaian Ancaman pada Website Transkrip Aktifitas Mahasiswa Politeknik Negeri Batam Menggunakan Metode DREAD. *Jurnal Integrasi*, *9*(1), 53. https://doi.org/10.30871/ji.v9i1.281

Setyawan, M. Y. H., & Munari, A. S. (2020). *Panduan Lengkap Membangun Sistem Monitoring Kinerja Mahasiswa Internship Berbasis Web dan Globlal Positioning System*. Bandung: Kreatif Industri Nusantara.

Sevima.com. (2018). Manfaat Sistem Informasi Akademik Bagi Perguruan Tinggi & Mahasiswa. Diambil dari https://sevima.com/manfaat-sistem-informasi-akademik-bagi-perguruan-tinggi-mahasiswa/

Shevchenko, N. (2018). Threat Modeling: 12 Available Methods. Diambil dari https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html

Sutabri, T. (2012). *Konsep Sistem Informasi*. Yogyakarta: Andi.

Syafitri, W. (2016). Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ). *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer dan Teknologi Informasi*, *2*(2), 8. https://doi.org/10.24014/coreit.v2i2.2356

Techopedia. (2012). Information Systems Security (INFOSEC). Diambil dari https://www.techopedia.com/definition/24840/information-systems-security-infosec

Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI). *Jurnal Sistem Informasi Bisnis*, *9*(1), 47. https://doi.org/10.21456/vol9iss1pp47-54

Whitman, M. E., & Mattord, H. J. (2010). *Management of Information Security*. Boston: Course Technology.

LAMPIRAN A

Tabel 4.7. Penilaian Ancaman

Threat	Level Kepercayaan	D	R	E	A	D	JUMLAH	RISIKO
T1	LK2	1	3	3	1	3	11	Sedang
T1	LK4	2	3	3	2	3	13	Tinggi
T1	LK5	3	3	3	3	3	15	Tinggi
T1	LK6	3	3	3	3	3	15	Tinggi
T2	LK2	1	3	2	1	2	9	Sedang
T2	LK4	2	3	2	2	2	11	Sedang
T2	LK5	3	3	2	3	2	13	Tinggi
T2	LK6	3	3	2	3	2	13	Tinggi
T3	LK2	2	3	3	1	3	12	Tinggi
T3	LK4	2	3	3	2	3	13	Tinggi
T4	LK5	2	3	3	2	3	13	Tinggi
T4	LK6	2	3	3	2	3	13	Tinggi
T4	LK7	3	3	3	3	3	15	Tinggi
T5	LK2	1	2	2	1	2	8	Sedang
T5	LK4	2	2	2	2	2	10	Sedang
T5	LK5	3	2	2	3	2	12	Tinggi
T5	LK6	3	2	2	3	2	12	Tinggi
T6	LK5	2	3	3	3	3	14	Tinggi
T6	LK7	3	3	3	3	3	15	Tinggi
T7	LK2	1	3	3	1	2	10	Sedang
T7	LK4	2	3	3	2	2	12	Tinggi
T7	LK5	2	3	3	3	2	13	Tinggi
T7	LK6	2	3	3	3	2	13	Tinggi
T7	LK7	3	3	2	3	1	12	Tinggi
T8	LK2	1	2	2	1	2	8	Sedang
T8	LK4	2	2	2	2	2	10	Sedang
T8	LK5	2	2	2	3	2	11	Sedang
T8	LK6	2	2	2	3	2	11	Sedang
T8	LK7	3	2	2	3	2	12	Tinggi
T9	LK2	1	2	2	1	2	8	Sedang

Threat	Level Kepercayaan	D	R	E	A	D	JUMLAH	RISIKO
T9	LK4	2	2	2	2	2	10	Sedang
T10	LK5	2	2	2	2	2	10	Sedang
T10	LK6	2	2	2	2	2	10	Sedang
T10	LK7	3	2	2	2	2	11	Sedang
T10	LK8	3	2	2	2	2	11	Sedang
T11	LK2	1	2	2	1	2	8	Sedang
T11	LK4	2	2	2	2	2	10	Sedang
T11	LK5	2	2	2	2	2	10	Sedang
T11	LK6	2	2	2	2	2	10	Sedang
T11	LK7	3	2	2	3	2	12	Tinggi
T11	LK8	3	2	2	3	2	12	Tinggi
T11	LK9	3	2	2	3	1	11	Sedang
T11	LK11	3	2	2	3	1	11	Sedang
T12	LK2	1	2	2	1	2	8	Sedang
T12	LK4	2	2	2	2	2	10	Sedang
T13	LK2	1	2	2	1	2	8	Sedang
T13	LK4	2	2	2	2	2	10	Sedang
T14	LK2	1	2	2	1	1	7	Rendah
T14	LK4	1	2	2	1	1	7	Rendah
T15	LK9	3	1	1	3	1	9	Sedang
T15	LK11	3	1	1	3	1	9	Sedang
T16	LK2	1	2	2	3	2	10	Sedang
T16	LK4	2	2	2	3	2	11	Sedang
T16	LK9	3	1	1	3	3	11	Sedang
T16	LK11	3	1	1	3	3	11	Sedang
T17	LK2	1	2	2	1	2	8	Sedang
T17	LK4	2	2	2	2	2	10	Sedang
T17	LK5	2	1	1	3	1	8	Sedang
T17	LK6	2	1	1	3	1	8	Sedang
T17	LK7	3	1	1	3	1	9	Sedang