

RANCANGAN APLIKASI PELAPORAN PELECEHAN KAMPUS TERINTEGRASI PROTOKOL KEAMANAN DATA DAN *PUSH NOTIFICATION COMMAND CENTER*

Widi Linggih Jaelani¹, Wina Witanti², Titania Sari³, Ira Monellia⁴, Ahsani Takwim⁵

Teknik Informatika^{1, 2, 3, 5}

Bidang Perencanaan TIK⁴

Universitas Teknologi Bandung^{1, 3, 5}

Universitas Jenderal Achmad Yani²

Dinas Komunikasi dan Informatika⁴

jaelaniwidi@gmail.com¹, witanti@gmail.com², titaniasari@utb-univ.ac.id³, iramonellia@gmail.com⁴, ahsanitakwim@sttbandung.ac.id⁵

Abstrak

Kasus pelecehan seksual di lingkungan perguruan tinggi merupakan permasalahan serius yang membutuhkan mekanisme pelaporan yang aman, mudah diakses, menjaga kerahasiaan identitas pelapor, serta mendukung proses tindak lanjut secara cepat dan terstruktur. Rendahnya tingkat pelaporan dapat dipengaruhi oleh rasa takut terhadap pelaku, tekanan psikologis, stigma sosial, relasi kuasa, serta kekhawatiran terhadap kemungkinan terbukanya identitas dan data pribadi pelapor. Selain itu, mekanisme pelaporan yang masih dilakukan secara manual dapat menyebabkan proses pencatatan, pengelolaan, pemantauan, dan tindak lanjut laporan menjadi kurang optimal. Kondisi tersebut menunjukkan perlunya suatu rancangan sistem pelaporan digital yang tidak hanya menyediakan fungsi pelaporan, tetapi juga mempertimbangkan aspek keamanan data dan mekanisme penyampaian informasi secara *real-time*. Penelitian ini bertujuan untuk merancang aplikasi pelaporan pelecehan kampus yang mengintegrasikan mekanisme keamanan data dan *push notification* berbasis *command center*. Metode penelitian menggunakan pendekatan perancangan sistem berdasarkan analisis kebutuhan fungsional dan non-fungsional dengan menerapkan konsep *multi-layer security*. Rancangan sistem mencakup pelaporan digital berbasis web dan *mobile*, mekanisme anonimitas pelapor menggunakan algoritma RSA, enkripsi data menggunakan *Advanced Encryption Standard* (AES) untuk perlindungan *data at rest*, serta HTTPS/TLS untuk perlindungan *data in transit*. Selain itu, rancangan mencakup autentikasi berlapis menggunakan *Multi-factor authentication* (MFA), pengendalian hak akses menggunakan *Role-Based Access control* (RBAC), pencatatan aktivitas melalui audit log, monitoring aktivitas sistem, dan *tracking* status laporan. Mekanisme *push notification* dirancang untuk memberikan informasi secara *real-time* ketika terdapat laporan baru maupun perubahan status laporan, sedangkan *command center* dirancang sebagai pusat monitoring dan pengelolaan laporan bagi pihak yang memiliki kewenangan. Luaran penelitian berupa rancangan arsitektur sistem, kebutuhan fungsional dan non-fungsional, alur proses pelaporan, rancangan mekanisme keamanan, rancangan kontrol akses, serta rancangan mekanisme notifikasi dan monitoring yang dapat menjadi dasar pengembangan sistem pada tahap berikutnya. Kebaruan penelitian terletak pada rancangan integrasi beberapa mekanisme keamanan, yaitu RSA, AES, HTTPS/TLS, MFA, dan RBAC, dengan *push notification* serta *command center* dalam satu rancangan sistem pelaporan pelecehan kampus. Rancangan ini diharapkan dapat menjadi dasar pengembangan sistem pelaporan yang lebih aman, responsif, terstruktur, dan mendukung kerahasiaan data pelapor.

Kata kunci : Sistem pelaporan, keamanan data, RSA, *push notification*, *command center*

Abstract

Sexual harassment in higher education institutions is a serious issue that requires a reporting mechanism that is secure, accessible, capable of maintaining the confidentiality of reporters' identities, and able to support timely and structured follow-up processes. Low reporting rates may be influenced by fear of perpetrators, psychological pressure, social stigma, power relations, and concerns about the disclosure of reporters' identities and personal data. In addition, manual reporting mechanisms may result in suboptimal processes for recording, managing, monitoring, and following up on reports. These conditions indicate the need for a digital reporting system design that not only provides reporting functions but also incorporates data security mechanisms and real-time information delivery. This study aims to design a campus harassment reporting application that integrates data security mechanisms and command center-based push notifications. The research method employs a system design approach based on functional and non-functional requirements analysis by applying the multi-layer security concept. The proposed system design includes web- and mobile-based digital reporting, a reporter anonymity mechanism using the RSA algorithm, data encryption using the *Advanced Encryption Standard* (AES) to protect data at rest, and HTTPS/TLS to protect data in transit. In addition, the design incorporates layered authentication using *Multi-factor authentication* (MFA), *Role-Based Access control* using *Role-Based Access control* (RBAC), activity recording through audit logs, system activity monitoring, and report status tracking. The push notification mechanism is designed to provide real-time information when a new report is submitted or when the status of a report changes, while the command center is designed as a centralized monitoring and report management facility for authorized parties. The research outputs consist of the proposed system architecture, functional and non-functional requirements, reporting process flows, security mechanism design, access control design, and notification and monitoring mechanism design, which can serve as a basis for system development in the subsequent stage. The novelty of this study lies in the proposed integration of multiple security mechanisms, including RSA, AES, HTTPS/TLS, MFA, and RBAC, with push notifications and a command center within a single campus harassment reporting system design. The proposed design is expected to provide a foundation for developing a more secure, responsive, structured, and confidentiality-oriented reporting system.

Keywords : Reporting system, data security, RSA, *push notification*, *command center*.

I. PENDAHULUAN

Saat ini kasus pelecehan seksual di lingkungan pendidikan khususnya perguruan tinggi merupakan permasalahan serius, dimana terdapat peningkatan kasus. Berdasarkan data Federasi Serikat Guru Indonesia (FSGI), sepanjang Januari–Maret 2026 tercatat 22 kasus kekerasan di satuan pendidikan dan 91% di antaranya merupakan kekerasan seksual. FSGI menyatakan bahwa angka tersebut menunjukkan tren peningkatan signifikan dibanding tahun sebelumnya. Hal menjadi bisa menjadi perhatian berbagai pihak, baik institusi pendidikan maupun pemerintah. Pelecehan di kampus dapat terjadi dalam berbagai bentuk seperti pelecehan verbal, non-verbal, fisik, hingga pelecehan berbasis relasi kuasa antara dosen dan mahasiswa [1,17]. Fenomena ini sering kali tidak dilaporkan secara optimal karena korban mengalami ketakutan, tekanan psikologis, serta kekhawatiran terhadap stigma sosial dan akademik [2]. Rendahnya tingkat pelaporan juga dipengaruhi oleh tidak tersedianya sistem pelaporan yang aman, anonim, dan mudah diakses oleh mahasiswa [3]. Urgensi penelitian ini semakin penting seiring berkembangnya transformasi digital di lingkungan perguruan tinggi dan meningkatnya kebutuhan terhadap sistem pelaporan yang aman, cepat, serta dapat melindungi pelapor. Banyak korban maupun saksi pelecehan memilih untuk tidak melaporkan kejadian yang dialami karena khawatir identitas mereka diketahui oleh pihak tertentu atau data pribadi mengalami kebocoran. Selain itu, mekanisme pelaporan yang masih dilakukan secara manual menyebabkan proses penanganan menjadi lambat dan monitoring kasus kurang optimal. Kondisi tersebut menunjukkan bahwa perguruan tinggi membutuhkan sistem pelaporan berbasis digital yang mampu menjamin keamanan data sekaligus memberikan respons cepat terhadap laporan yang diterima.

Dalam konteks transformasi digital, pemanfaatan teknologi informasi menjadi solusi yang relevan untuk meningkatkan efektivitas sistem pelaporan pelecehan di lingkungan kampus. Aplikasi pelaporan berbasis digital memungkinkan korban atau saksi untuk melaporkan kejadian secara cepat, terdokumentasi, serta dapat dilakukan secara anonim untuk menjaga keamanan pelapor [3]. Namun demikian, sistem pelaporan tersebut harus dirancang dengan mempertimbangkan aspek keamanan data karena informasi yang dilaporkan bersifat sangat sensitif dan berisiko tinggi jika terjadi kebocoran [4]. Keamanan data dalam sistem pelaporan menjadi aspek kritis karena menyangkut perlindungan identitas korban, kronologi kejadian, serta bukti pendukung lainnya [5]. Ancaman seperti serangan siber, kebocoran *Database*, serta penyalahgunaan akses internal menjadi tantangan utama dalam pengembangan sistem informasi kampus [4]. Oleh karena itu, diperlukan penerapan protokol keamanan seperti *enkripsi* data, autentikasi berlapis, serta pengujian keamanan sistem secara berkala. Penelitian oleh W. L. Jaelani menunjukkan bahwa penerapan keamanan berlapis pada sistem informasi mampu meningkatkan perlindungan data dan meminimalisir risiko serangan siber [6]. Selain aspek keamanan, kecepatan respons terhadap laporan juga menjadi faktor penting dalam penanganan kasus pelecehan di kampus. Integrasi fitur *push notification* memungkinkan sistem memberikan notifikasi secara *real-time* kepada pihak terkait seperti satgas kampus atau unit layanan mahasiswa [7]. Dengan adanya *command center* yang terintegrasi, laporan yang masuk dapat segera ditindaklanjuti sehingga meningkatkan efektivitas penanganan kasus [8].

Penelitian ini bertujuan untuk merancang aplikasi pelaporan pelecehan kampus yang terintegrasi dengan protokol keamanan data dan *push notification* berbasis *command center* guna meningkatkan keamanan data, kecepatan respons, transparansi proses pelaporan, serta kepercayaan pengguna terhadap sistem. Adapun manfaat praktis dari penelitian ini adalah memberikan solusi sistem pelaporan yang aman, responsif, dan mudah digunakan oleh mahasiswa maupun pihak kampus dalam menangani kasus pelecehan. Sementara itu, manfaat teoritis penelitian ini adalah memberikan *kontribusi* terhadap pengembangan keilmuan di bidang keamanan sistem informasi, khususnya penerapan *multi-layer security* pada sistem pelaporan berbasis digital. Kebaruan penelitian ini terletak pada integrasi beberapa teknologi keamanan dan monitoring dalam satu platform terpusat. Penelitian ini tidak hanya berfokus pada sistem pelaporan digital, tetapi juga mengintegrasikan fitur anonimitas berbasis algoritma RSA, *enkripsi* data menggunakan AES dan HTTPS, autentikasi berlapis (*MFA*), kontrol akses berbasis *RBAC*, serta *push notification real-time* yang terhubung dengan *command center*. Algoritma RSA dipilih karena dalam implementasinya RSA dapat membantu proses pendistribusian kunci yang dipakai oleh *User* tujuan untuk melakukan *dekripsi* *chipper text* menjadi *plain text* yang dikirimkan. *Enkripsi* data menggunakan AES dan HTTPS dipakai untuk memecahkan permasalahan dalam proses *pengenkripsian* data aduan yang dilaporkan oleh pelapor, dimana kedua Teknik ini dipakai secara bersamaan dengan tujuan supaya pada saat melakukan tahapan *enkripsi* didalam sistem, tahapannya bisa dilakukan dari end to end sehingga menghasilkan data yang aman. Autentikasi berlapis (*MFA*) dipilih dengan tujuan untuk membantu memfilter *User* yang masuk kedalam sistem dan untuk *push notification real-time* dipakai dengan tujuan supaya proses penindakan setiap pelaporan bisa dilakukan sesegera mungkin dimana Teknik ini akan memberikan informasi atau aduan yang sifatnya mendesak. Pendekatan ini memberikan nilai tambah dibandingkan penelitian sebelumnya yang umumnya hanya berfokus pada sistem pelaporan atau keamanan data secara terpisah.

II. TINJAUAN PUSTAKA

1. Sistem Informasi Pelaporan

Sistem informasi pelaporan merupakan sistem yang dirancang untuk mengumpulkan, mengelola, dan menyampaikan informasi terkait suatu kejadian atau insiden secara terstruktur. Sistem ini berperan penting dalam meningkatkan partisipasi pengguna dalam melaporkan kejadian karena memberikan kemudahan akses dan efisiensi waktu [3]. Dalam konteks pelecehan kampus, sistem pelaporan digital memungkinkan korban untuk melaporkan kejadian tanpa harus bertatap muka langsung, sehingga dapat mengurangi tekanan psikologis [2].

Selain itu, sistem pelaporan juga dapat menyimpan data secara terpusat sehingga memudahkan proses monitoring dan evaluasi oleh pihak kampus [3].

2. Keamanan Data dalam Sistem Informasi

Keamanan data merupakan aspek fundamental dalam sistem informasi yang bertujuan untuk melindungi data dari akses yang tidak sah. Prinsip utama keamanan data meliputi kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) [5]. Ancaman keamanan seperti SQL Injection, *Cross-Site Scripting* (XSS), dan kebocoran data menjadi risiko utama dalam sistem berbasis web [4]. Penerapan *enkripsi* data, *firewall*, serta kontrol akses berbasis peran menjadi solusi dalam meningkatkan keamanan sistem [5]. Pendekatan keamanan berbasis sistem terdistribusi juga dapat meningkatkan ketahanan sistem terhadap serangan [9]. Selain itu, penggunaan teknologi *cloud computing* memberikan fleksibilitas sekaligus tantangan baru dalam menjaga keamanan data [10]. Penelitian oleh W. L. Jaelani menekankan bahwa integrasi protokol keamanan dan audit sistem secara berkala sangat penting dalam menjaga keandalan sistem informasi [6].

3. *Push Notification* dalam Sistem Informasi

Push notification merupakan teknologi yang memungkinkan sistem mengirimkan informasi secara otomatis kepada pengguna tanpa permintaan langsung. Teknologi ini banyak digunakan untuk meningkatkan interaksi pengguna serta mempercepat penyampaian informasi. Dalam sistem informasi kampus, *push notification* digunakan untuk menyampaikan informasi akademik, pengumuman, dan notifikasi penting lainnya [7]. Implementasi *push notification* berbasis *REST API* memungkinkan integrasi sistem yang fleksibel dan scalable. Dalam sistem pelaporan pelecehan, fitur ini sangat penting untuk memberikan update status laporan dan notifikasi kepada pihak terkait secara *real-time* [8].

4. Protokol Keamanan Data

Protokol keamanan data merupakan sekumpulan aturan dan mekanisme yang dirancang untuk melindungi data selama proses penyimpanan, transmisi, dan pengolahan dalam suatu sistem informasi. Penerapan protokol keamanan menjadi sangat penting dalam sistem pelaporan pelecehan kampus karena data yang dikelola bersifat sensitif dan berkaitan dengan privasi pengguna [11]. Salah satu komponen utama dalam protokol keamanan data adalah *enkripsi*, yaitu proses mengubah data menjadi bentuk yang tidak dapat dibaca tanpa kunci *dekripsi* yang sesuai. Penggunaan algoritma *enkripsi* seperti *Advanced Encryption Standard* (AES) dan RSA banyak diterapkan dalam sistem informasi modern untuk menjaga kerahasiaan data [12]. *Enkripsi* tidak hanya diterapkan pada data yang disimpan (*data at rest*), tetapi juga pada data yang dikirim melalui jaringan (*data in transit*) menggunakan protokol seperti HTTPS dan TLS [13].

Selain *enkripsi*, autentikasi merupakan bagian penting dari protokol keamanan yang bertujuan untuk memastikan bahwa hanya pengguna yang berhak yang dapat mengakses sistem. Metode autentikasi yang umum digunakan meliputi *User name* dan *password*, *Multi-factor authentication* (MFA), serta biometrik. Penerapan autentikasi berlapis dapat meningkatkan keamanan sistem dan mengurangi risiko akses tidak sah [14]. Selanjutnya, kontrol akses (*access control*) digunakan untuk mengatur hak akses pengguna terhadap data dan fitur dalam sistem. Model kontrol akses seperti *Role-Based Access control* (RBAC) memungkinkan pengelolaan hak akses berdasarkan peran pengguna dalam sistem. Dalam sistem pelaporan pelecehan kampus, kontrol akses sangat penting untuk memastikan bahwa hanya pihak tertentu seperti admin atau satgas yang dapat mengakses laporan secara penuh [15].

Protokol keamanan data juga mencakup mekanisme audit dan *log ging* yang digunakan untuk mencatat aktivitas pengguna dalam sistem. Audit *log* memungkinkan pelacakan terhadap aktivitas yang mencurigakan serta membantu dalam proses investigasi jika terjadi pelanggaran keamanan. Penerapan monitoring secara *real-time* juga dapat meningkatkan kemampuan sistem dalam mendeteksi dan merespons ancaman keamanan [16]. Selain itu, penggunaan teknologi keamanan jaringan seperti *firewall* dan *intrusion detection system* (IDS) dapat membantu melindungi sistem dari serangan eksternal. *Firewall* berfungsi untuk menyaring lalu lintas jaringan yang masuk dan keluar dari sistem, sedangkan IDS digunakan untuk mendeteksi aktivitas yang mencurigakan [13].

Penelitian oleh W. L. Jaelani menunjukkan bahwa integrasi berbagai protokol keamanan seperti *enkripsi*, autentikasi berlapis, dan monitoring sistem dapat meningkatkan tingkat keamanan secara signifikan pada sistem informasi. Pendekatan keamanan yang terintegrasi ini sangat relevan untuk diterapkan dalam sistem pelaporan pelecehan kampus guna menjamin kerahasiaan dan keamanan data pengguna [6].

5. Algoritma RSA

Algoritma RSA (*Rivest-Shamir-Adleman*) merupakan salah satu algoritma kriptografi asimetris yang menggunakan pasangan kunci, yaitu *public key* dan *private key*. Kriptografi asimetris memungkinkan proses *enkripsi* dan *dekripsi* dilakukan menggunakan kunci yang berbeda. *Public key* dapat didistribusikan kepada pihak lain untuk melakukan *enkripsi*, sedangkan *private key* harus dijaga kerahasiaannya dan digunakan untuk melakukan *dekripsi* [11], [12]. RSA bekerja berdasarkan prinsip matematika yang berkaitan dengan faktorisasi bilangan bulat besar. Secara umum, proses RSA melibatkan pembentukan modulus n yang diperoleh dari perkalian dua bilangan prima besar p dan q . Kunci publik terdiri atas pasangan (e, n) , sedangkan kunci privat menggunakan pasangan (d, n) . Proses *enkripsi* dapat dinyatakan dengan persamaan:

$$C = M^e \bmod n$$

sedangkan proses *dekripsi* dinyatakan sebagai:

$$M = C^d \bmod n$$

Dengan M merupakan *plaintext*, C merupakan *ciphertext*, e merupakan eksponen publik, d merupakan eksponen privat, dan n merupakan modulus [11], [12]. Dalam penelitian ini, RSA digunakan sebagai salah satu mekanisme untuk melindungi identitas pelapor. Data identitas seperti nama, alamat surat elektronik, atau identitas pengguna dapat diproses menggunakan mekanisme kriptografi sebelum disimpan atau dipertukarkan. Pendekatan tersebut mendukung tujuan anonimitas pelapor karena data identitas tidak disimpan dalam bentuk terbuka. Dokumen penelitian sebelumnya juga menetapkan RSA sebagai komponen anonimitas pelapor dan menjelaskan penggunaan *public key* serta *private key* untuk proses *enkripsi* dan *dekripsi*. Namun, secara implementasi, RSA lebih tepat digunakan untuk *enkripsi* data berukuran kecil atau kunci, bukan seluruh data laporan yang berukuran besar. Oleh karena itu, RSA dapat dikombinasikan dengan AES melalui pendekatan *hybrid encryption*. AES digunakan untuk *enkripsi* data laporan, sedangkan RSA digunakan untuk melindungi kunci AES. Pendekatan ini memberikan kombinasi antara efisiensi kriptografi simetris dan keamanan pertukaran kunci kriptografi asimetris [11], [12].

6. *Enkripsi Data Menggunakan AES dan HTTPS*

Advanced Encryption Standard (AES) merupakan bagian dari algoritma kriptografi simetris yang menggunakan kunci yang sama pada proses *enkripsi* dan *dekripsi*. AES dirancang untuk memberikan perlindungan terhadap kerahasiaan data dengan efisiensi yang tinggi sehingga sesuai digunakan untuk melindungi data dalam jumlah besar [12]. Secara konseptual, proses AES dapat dinyatakan sebagai:

$$C = E_k(P)$$

$$P = D_k(C)$$

Dengan P merupakan *plaintext*, C merupakan *ciphertext*, K merupakan kunci rahasia, E_k merupakan fungsi *enkripsi*, dan D_k merupakan fungsi *dekripsi*. Dokumen penelitian sebelumnya menggunakan formulasi yang sama untuk menjelaskan penerapan AES pada data yang disimpan dalam *Database*. Dalam sistem pelaporan pelecehan kampus, AES digunakan untuk melindungi *data at rest*, yaitu data yang tersimpan pada *Database* atau media penyimpanan. Data yang dapat dilindungi meliputi kronologi kejadian, informasi pendukung laporan, dokumen bukti, maupun data sensitif lainnya. Dengan demikian, apabila *Database* berhasil diakses tanpa otorisasi, informasi yang diperoleh tetap berada dalam bentuk *ciphertext* sehingga tidak dapat langsung dibaca. Selain perlindungan data saat tersimpan, sistem juga membutuhkan perlindungan ketika data dikirim melalui jaringan. Untuk kebutuhan tersebut digunakan HTTPS (*Hypertext Transfer Protocol Secure*) yang memanfaatkan TLS (*Transport Layer Security*) untuk mengamankan komunikasi antara *client* dan *server* [13].

7. *Autentikasi Berlapis menggunakan Multi-factor authentication (MFA)*

Multi-factor authentication (MFA) merupakan mekanisme autentikasi yang menggunakan dua atau lebih faktor autentikasi untuk memverifikasi identitas pengguna sebelum pengguna memperoleh akses terhadap sistem. Secara umum, faktor autentikasi MFA dapat dikelompokkan menjadi tiga kategori utama:

- Something you know*, seperti *password* atau PIN.
- Something you have*, seperti perangkat seluler, token, atau kode OTP.
- Something you are*, seperti sidik jari atau pengenalan wajah.

Penerapan MFA memberikan lapisan keamanan tambahan dibandingkan autentikasi yang hanya menggunakan *User name* dan *password*. Apabila kredensial pengguna berhasil diketahui oleh pihak yang tidak berwenang, faktor autentikasi kedua masih diperlukan untuk memperoleh akses ke sistem [14].

8. *Role-Based Access control (RBAC)*

Role-Based Access control (RBAC) merupakan model pengendalian akses yang memberikan hak akses kepada pengguna berdasarkan *role* atau peran yang dimilikinya dalam sistem. Berbeda dengan pemberian hak akses secara individual, RBAC memungkinkan administrator mengelompokkan hak akses berdasarkan tanggung jawab pengguna. Implementasi RBAC harus mengikuti prinsip *least privilege*, yaitu setiap pengguna hanya memperoleh hak akses minimum yang diperlukan untuk melaksanakan tugasnya [15]. Prinsip tersebut penting karena data laporan pelecehan termasuk data sensitif sehingga tidak semua pengguna diperbolehkan melihat informasi secara penuh.

9. *Push Notification Real-time*

Push notification merupakan mekanisme komunikasi yang memungkinkan *server* mengirimkan informasi atau pemberitahuan kepada perangkat pengguna tanpa pengguna harus melakukan permintaan secara manual. Teknologi ini banyak digunakan untuk menyampaikan informasi yang membutuhkan respons cepat [7], [8]. Pada sistem pelaporan pelecehan kampus, *push notification* digunakan untuk menginformasikan perubahan

status laporan dan laporan baru kepada pihak yang berkepentingan. Misalnya, ketika mahasiswa mengirimkan laporan baru, sistem dapat mengirimkan notifikasi kepada satgas. Sebaliknya, ketika satgas mengubah status laporan menjadi diproses, diverifikasi, atau selesai, sistem dapat mengirimkan notifikasi kepada pelapor.

10. Penelitian Terkait

TABEL I
PENELITIAN TERKAIT

No	Peneliti	Judul Penelitian	Fokus Penelitian	Hasil Penelitian	Perbedaan dengan Penelitian Ini
1	Jurnal Informatika <i>Teknologi dan Sains</i> [3]	Rancang Bangun Sistem Pelaporan Insiden Kejahatan Siber	Sistem pelaporan digital untuk pelaporan insiden	Sistem digital meningkatkan partisipasi pelaporan dan efisiensi pengelolaan data	Penelitian sebelumnya berfokus pada fungsi pelaporan digital tanpa mekanisme keamanan kriptografi yang terintegrasi. Penelitian ini menggunakan pendekatan <i>multi-layer security</i> dengan RSA untuk proteksi identitas pelapor, AES untuk <i>enkripsi</i> data laporan, HTTPS/TLS untuk keamanan transmisi, MFA untuk autentikasi, serta RBAC untuk pembatasan akses berdasarkan peran. Selain itu, laporan diintegrasikan dengan <i>push notification</i> dan <i>command center</i> untuk mendukung respons <i>real-time</i> .
2	V. D. Cahya, T. Ariyadi, dan D. Kurniawan [4]	Analisa Keamanan Data Pada Sistem Informasi Kampus Menggunakan Metode Burp Suite	Pengujian keamanan sistem informasi kampus	Ditemukan berbagai kerentanan keamanan pada sistem berbasis web	Penelitian sebelumnya menggunakan Burp Suite sebagai metode pengujian untuk mengidentifikasi kerentanan, sedangkan penelitian ini menggunakan pendekatan perancangan sistem dengan menerapkan keamanan pada beberapa layer. Proteksi dirancang menggunakan RSA, AES, HTTPS/TLS, MFA, dan RBAC, kemudian aktivitas sistem dicatat melalui audit <i>log</i> . Dengan demikian, penelitian ini tidak hanya mengidentifikasi kerentanan, tetapi merancang mekanisme pencegahan dan pengendalian akses sejak tingkat aplikasi, data, autentikasi, hingga komunikasi jaringan.
3	A. M. Ujung dan M. I. P. Nasution [5]	Sistem Keamanan <i>Database</i>	Perlindungan keamanan <i>Database</i>	<i>Enkripsi</i> dan kontrol akses dapat meningkatkan keamanan data	Penelitian sebelumnya berfokus pada proteksi <i>Database</i> , sedangkan penelitian ini menerapkan keamanan secara <i>end-to-end</i> . AES digunakan untuk <i>enkripsi</i> data sensitif pada <i>Database (data at rest)</i> , RSA digunakan untuk melindungi identitas pelapor dan/atau kunci AES melalui pendekatan <i>hybrid encryption</i> , HTTPS/TLS digunakan untuk melindungi <i>data in transit</i> , MFA

					digunakan untuk memperkuat autentikasi, dan RBAC digunakan untuk membatasi akses berdasarkan <i>role</i> .
4	S. Mutrofin, E. C. Dinata, dan E. N. Jannah [7]	Implementasi <i>Push Notification</i> dalam Sistem Informasi Manajemen Evaluasi Pembelajaran	<i>Push notification</i> pada sistem informasi kampus	<i>Push notification</i> meningkatkan efektivitas komunikasi dan penyampaian informasi	Penelitian sebelumnya menerapkan <i>push notification</i> pada konteks informasi pembelajaran, sedangkan penelitian ini menggunakan <i>push notification</i> sebagai mekanisme <i>event-driven notification</i> pada alur penanganan laporan pecehan. Notifikasi dipicu ketika laporan baru diterima atau terjadi perubahan status laporan dan diteruskan kepada aktor yang memiliki hak akses melalui <i>command center</i> . Dengan demikian, <i>push notification</i> menjadi bagian dari mekanisme respons insiden, bukan hanya media penyampaian informasi.
5	A. B. Pratama dan A. Triawan [8]	Penerapan <i>Push Notification</i> Menggunakan REST untuk Informasi Sistem	Implementasi <i>REST API</i> dan <i>push notification</i>	Sistem mampu mengirim notifikasi secara <i>real-time</i>	Penelitian sebelumnya berfokus pada implementasi komunikasi <i>REST API</i> dan <i>push notification</i> , sedangkan penelitian ini mengintegrasikan mekanisme notifikasi dengan <i>workflow</i> pelaporan. Perubahan status laporan menjadi trigger pengiriman notifikasi kepada pelapor maupun satgas. Mekanisme tersebut diintegrasikan dengan <i>command center</i> , RBAC, audit log, dan sistem <i>tracking</i> sehingga setiap notifikasi memiliki konteks terhadap proses penanganan laporan dan dapat dipantau secara terstruktur.
6	N. Umah et al. [9]	Pengembangan Sistem Terdistribusi untuk Peningkatan Keamanan Data dan Komunikasi	Sistem terdistribusi dan keamanan data	Sistem terdistribusi meningkatkan keamanan dan keandalan sistem	Penelitian sebelumnya menitikberatkan pada arsitektur sistem terdistribusi untuk keamanan dan komunikasi, sedangkan penelitian ini berfokus pada keamanan data sensitif dalam sistem pelaporan pecehan. Pendekatan yang digunakan berupa <i>multi-layer security</i> dengan kombinasi RSA, AES, HTTPS/TLS, MFA, RBAC, dan audit log. Selain itu, penelitian ini memiliki mekanisme anonimitas/ <i>pseudonymization</i> pelapor serta integrasi <i>command center</i> dan <i>push notification</i> untuk

					mempercepat respons terhadap laporan.
7	W. L. Jaelani [6]	Analisis dan Implementasi Keamanan Sistem Informasi Berbasis <i>Multi-layer security</i>	Implementasi keamanan berlapis pada sistem informasi	<i>Multi-layer security</i> meningkatkan perlindungan data dan monitoring sistem	Penelitian sebelumnya menjadi dasar konsep <i>multi-layer security</i> , sedangkan penelitian ini mengadaptasi dan mengimplementasikan konsep tersebut secara spesifik pada sistem pelaporan pelecehan kampus. Layer keamanan dirancang lebih spesifik melalui RSA untuk anonimitas identitas, AES untuk <i>data at rest</i> , HTTPS/TLS untuk <i>data in transit</i> , MFA untuk autentikasi, RBAC untuk otorisasi, serta audit log untuk pelacakan aktivitas. Seluruh mekanisme tersebut diintegrasikan dengan <i>push notification</i> dan <i>command center</i> sehingga keamanan data dan respons penanganan laporan berada dalam satu arsitektur sistem.

III. ANALISIS DAN PERANCANGAN

1. Identifikasi Permasalahan

Permasalahan utama dalam penanganan kasus pelecehan di lingkungan kampus terletak pada:

- a. Rendahnya tingkat pelaporan oleh korban maupun saksi. Hal ini disebabkan oleh berbagai faktor, antara lain munculnya rasa takut terhadap pelaku, kekhawatiran akan stigma sosial, serta adanya relasi kuasa yang membuat korban enggan melaporkan kejadian yang dialaminya.
- b. Sistem pelaporan yang tersedia di sebagian besar perguruan tinggi dirasa masih kurang efektif, seperti pelaporan langsung kepada pihak kampus atau melalui dokumen tertulis. Pendekatan ini dinilai kurang efektif karena membutuhkan keberanian tinggi dari korban dan tidak menjamin kerahasiaan identitas pelapor.
- c. Belum adanya sistem yang mampu menjamin keamanan data pelaporan. Data yang berkaitan dengan kasus pelecehan termasuk kategori data sensitif yang memerlukan perlindungan khusus. Risiko kebocoran data, akses tidak sah, serta penyalahgunaan informasi menjadi ancaman serius yang dapat memperburuk kondisi korban.
- d. Dimungkinkan terjadi keterlambatan respons dari pihak kampus terhadap laporan yang masuk. Keterlambatan ini bisa terjadi karena proses pelaporan masih memakan waktu sehingga tidak bisa menangani kasus secara langsung dimana tidak adanya sistem notifikasi *real-time* menyebabkan laporan sering terlambat ditindaklanjuti, sehingga penanganan kasus menjadi tidak optimal.

2. Analisis Kebutuhan Sistem

Berdasarkan identifikasi permasalahan, sistem yang akan dirancang harus mampu memenuhi kebutuhan sebagai berikut:

a. Analisis Permasalahan Inti

Permasalahan dalam penelitian ini dapat dianalisis menjadi tiga aspek utama:

- 1) Aspek Sosial : Korban cenderung tidak melaporkan kejadian karena faktor psikologis dan sosial. Sistem manual tidak mampu mengatasi hambatan ini karena tidak memberikan rasa aman bagi pelapor.
- 2) Aspek Teknologi : Belum adanya sistem digital yang terintegrasi menyebabkan proses pelaporan tidak efisien dan sulit dipantau. Selain itu, sistem yang ada belum dilengkapi dengan fitur keamanan yang memadai.
- 3) Aspek Keamanan Informasi : Data pelaporan rentan terhadap kebocoran karena belum adanya penerapan protokol keamanan yang kuat seperti *enkripsi*, autentikasi berlapis, dan monitoring sistem.

b. Kebutuhan Fungsional

TABEL II
KEBUTUHAN FUNGSIONAL

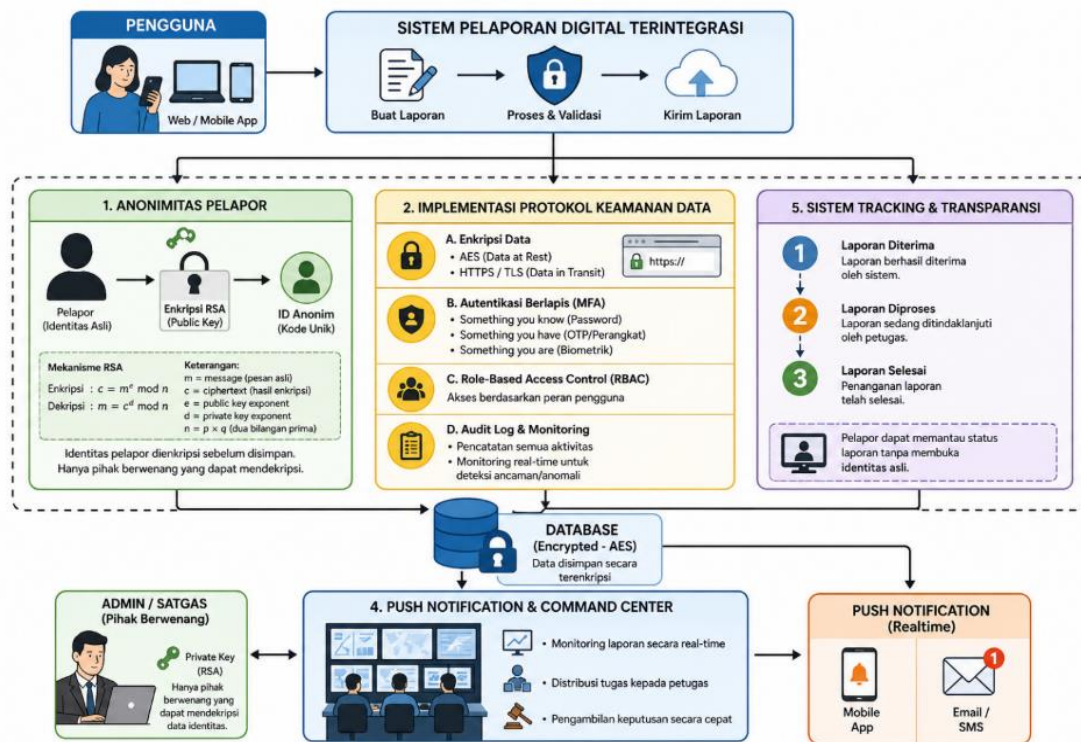
Kebutuhan Pengguna	Functional Requirement & Priority			
	High t Priority	Medium Priority	Low Priority	No Priority
Saya ingin (admin, satgas, mahasiswa dan dosen) Sistem menyediakan fitur <i>log in</i> bagi pengguna	F01 Fitur utama untuk memberikan akses ke dalam sistem dengan memasukkan kredensial berupa <i>User name</i> /email dan <i>password</i> .	F05 Memberikan informasi kepada pengguna jika terjadi kesalahan seperti <i>User name</i> atau <i>password</i> tidak sesuai.	F09 Fitur tambahan untuk membantu pengguna yang lupa <i>password</i> dengan mekanisme verifikasi melalui email atau metode lain.	F10 <i>User name</i> dan <i>password</i> disediakan oleh admin
Saya ingin (mahasiswa dan dosen) Sistem membuat pelaporan pecehan.	F02 Fitur utama sistem yang memungkinkan pengguna mengirimkan laporan kejadian pecehan secara langsung melalui aplikasi sebagai bentuk pelaporan resmi. F03 Penting untuk melindungi keamanan dan privasi pelapor agar tidak terjadi intimidasi atau dampak negatif terhadap pelapor.	F06 Sistem mampu menyimpan data laporan secara terstruktur dan aman.		
Saya ingin (mahasiswa dan dosen) Sistem menyediakan fitur <i>tracking</i> status laporan.	F04 Fungsi utama bagi pihak berwenang untuk memproses laporan, melakukan verifikasi, serta menentukan tindakan lanjutan terhadap kasus yang dilaporkan.			
Saya ingin (admin dan satgas) Sistem mengirimkan notifikasi secara <i>real-time</i> kepada pihak pelapor		F07 Digunakan agar pelapor dapat memantau perkembangan laporan yang telah dikirim (misalnya: diproses, diverifikasi, selesai).		
Saya ingin Sistem memungkinkan admin atau satgas untuk mengelola dan menindaklanjuti laporan.		F08 Mendukung respon cepat dari tim penanganan dengan memberikan pemberitahuan langsung ketika ada laporan baru atau perubahan status laporan.		

c. Kebutuhan Non-Fungsional

TABEL III
KEBUTUHAN NON-FUNGSIONAL

Atribut	Aspek Kebutuhan	Ruang Lingkup
Keamanan	Sistem harus memiliki tingkat keamanan tinggi dengan penerapan <i>enkripsi</i> data, autentikasi pengguna, dan kontrol hak akses berbasis <i>role</i> (admin, satgas, pelapor)	Modul autentikasi, <i>Database</i> , dan manajemen akses
Ketersediaan	Sistem harus memiliki ketersediaan tinggi (<i>high availability</i>) agar dapat diakses kapan saja tanpa <i>Downtime</i> yang signifikan	<i>Server hosting / cloud infrastructure</i>
Kegunaan (Usability)	Sistem harus mudah digunakan (<i>User -friendly</i>) dengan tampilan antarmuka yang sederhana, jelas, dan mudah dipahami oleh pengguna umum	<i>User Interface (UI/UX)</i>
Kinerja (Performance)	Sistem harus responsif dan cepat dalam memproses laporan serta mengirimkan notifikasi secara <i>real-time</i> kepada pihak terkait	<i>Backend system</i> dan layanan notifikasi
Kerahasiaan Data	Sistem harus mampu menjaga kerahasiaan data pengguna terutama identitas pelapor dengan mekanisme proteksi data sensitif	<i>Database</i> dan sistem keamanan data

3. Solusi yang Diusulkan



Gambar 1. Gambaran Usulan Sistem

Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan rancangan aplikasi pelaporan pelecehan kampus berbasis digital yang memiliki fitur utama sebagai berikut:

1) Sistem Pelaporan Digital Terintegrasi

Aplikasi memungkinkan pengguna untuk melaporkan kejadian secara langsung melalui perangkat *mobile* atau web. Sistem ini dirancang agar mudah digunakan dan dapat diakses kapan saja.

2) Fitur Anonimitas Pelapor

Fitur anonimitas pelapor merupakan salah satu komponen utama dalam sistem yang dirancang untuk memberikan perlindungan maksimal terhadap identitas pengguna yang melakukan pelaporan. Dalam konteks kasus pelecehan di lingkungan kampus, anonimitas menjadi faktor penting karena banyak korban atau saksi enggan melaporkan kejadian akibat adanya rasa takut, tekanan sosial, serta potensi dampak akademik maupun relasi kuasa [2]. Oleh karena itu, sistem harus mampu menjamin bahwa identitas pelapor tidak dapat diketahui oleh pihak yang tidak berwenang.

Pada rancangan sistem ini, mekanisme anonimitas tidak hanya bersifat konseptual, tetapi diimplementasikan secara teknis melalui penerapan algoritma kriptografi RSA (*Rivest-Shamir-Adleman*) sebagai bagian dari protokol keamanan data [11]. RSA merupakan algoritma kriptografi kunci publik (*asymmetric cryptography*) yang menggunakan dua kunci berbeda, yaitu kunci publik (*public key*) untuk proses *enkripsi* dan kunci privat (*private key*) untuk proses *dekripsi* [11]. Proses *enkripsi* dan *dekripsi* dalam algoritma RSA dinyatakan sebagai berikut:

$$c = m^e \bmod n$$

$$m = c^d \bmod n$$

Penjelasan

1. *m* (*message*): data atau pesan asli yang akan *dienkripsi*.
2. *c* (*ciphertext*): hasil *enkripsi* dari pesan.
3. *e* (*public key exponent*): kunci publik yang digunakan untuk *enkripsi*.
4. *d* (*private key exponent*): kunci privat yang digunakan untuk *dekripsi*.
5. *n*: hasil perkalian dua bilangan prima besar (*p* dan *q*).

Dalam implementasinya, data identitas pelapor seperti nama, email, atau nomor identitas akan *dienkripsi* menggunakan kunci publik sebelum dikirim dan disimpan ke dalam *Database* sistem [12]. Dengan demikian, informasi tersebut tidak dapat dibaca secara langsung oleh sistem maupun administrator tanpa melalui proses *dekripsi* menggunakan kunci privat yang hanya dimiliki oleh pihak tertentu yang berwenang, seperti ketua satgas atau sistem *command center* dengan otorisasi khusus [12].

Pendekatan ini memastikan bahwa identitas pelapor tetap terlindungi meskipun terjadi akses tidak sah terhadap *Database*, serta mencegah administrator sistem mengakses data sensitif tanpa izin yang sah [12]. Selain itu, risiko kebocoran data sensitif dapat diminimalisir secara signifikan melalui penerapan *enkripsi* dan kontrol akses berbasis peran (*Role-Based Access control*). Selain itu, sistem juga dapat menerapkan mekanisme *pseudonymization*, di mana setiap pelapor akan diberikan kode unik (ID anonim) yang digunakan untuk proses *tracking* laporan tanpa mengungkap identitas asli pengguna [5]. Dengan cara ini, pelapor tetap dapat memantau perkembangan laporan tanpa harus membuka identitasnya.

Mengacu pada penelitian yang dilakukan oleh W. L. Jaelani, penerapan keamanan berbasis *multi-layer security* yang mengintegrasikan *enkripsi* RSA, autentikasi berlapis, serta kontrol akses terbukti mampu meningkatkan tingkat perlindungan data dalam sistem informasi secara signifikan. Pendekatan ini sangat relevan untuk diterapkan dalam sistem pelaporan pelecehan kampus karena mampu menjamin kerahasiaan data sekaligus menjaga kepercayaan pengguna terhadap sistem [6]. Dengan adanya fitur anonimitas berbasis *enkripsi* RSA ini, diharapkan pengguna akan merasa lebih aman dan percaya untuk melaporkan kejadian pelecehan, sehingga dapat meningkatkan tingkat pelaporan serta mendukung terciptanya lingkungan kampus yang lebih aman dan responsif terhadap kasus-kasus sensitif [1].

3) Implementasi Protokol Keamanan Data

Implementasi protokol keamanan data dalam sistem pelaporan pelecehan kampus merupakan komponen krusial yang bertujuan untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi yang dikelola oleh sistem. Mengingat data yang diproses bersifat sensitif—seperti identitas pelapor, kronologi kejadian, dan bukti pendukung—maka diperlukan pendekatan keamanan berlapis (*multi-layer security*) untuk meminimalisir risiko kebocoran dan penyalahgunaan data [6]. Pendekatan ini juga sejalan dengan praktik terbaik dalam keamanan sistem informasi modern yang menekankan integrasi berbagai mekanisme proteksi [12].

4) *Enkripsi* data (AES/HTTPS)

Enkripsi data merupakan mekanisme utama dalam menjaga kerahasiaan informasi, baik saat data disimpan (*data at rest*) maupun saat ditransmisikan (*data in transit*). Dalam sistem ini, digunakan algoritma *Advanced Encryption Standard* (AES) untuk *enkripsi* data yang tersimpan di dalam *Database*, sehingga data tidak dapat dibaca tanpa kunci *dekripsi* yang sah [12].

$$C = EK(P) \text{ dan } P = DK(C)$$

Penjelasan:

1. *P* (*Plaintext*) Merupakan data asli atau pesan sebelum *dienkripsi*.
2. *C* (*Ciphertext*) Merupakan hasil dari proses *enkripsi*.
3. *K* (*Key / Kunci*) Kunci rahasia yang digunakan dalam proses *enkripsi* dan *dekripsi*.
4. *E_k* (*Encryption Function*) Fungsi untuk *enkripsi* data *plaintext* (*P*) menjadi *ciphertext* (*C*) menggunakan kunci *K*.
5. *D_k* (*Decryption Function*) Fungsi untuk mengembalikan *ciphertext* (*C*) menjadi *plaintext* (*P*) menggunakan kunci *K*.

Selain itu, untuk keamanan komunikasi data antara *client* dan *server*, digunakan protokol HTTPS (*Hypertext Transfer Protocol Secure*) yang berjalan di atas TLS (*Transport Layer Security*). Penggunaan HTTPS memastikan bahwa data yang dikirimkan melalui jaringan telah *dienkripsi* sehingga tidak dapat disadap oleh pihak ketiga (*man-in-the-middle attack*) [13]. Dengan kombinasi AES dan HTTPS, sistem mampu memberikan perlindungan menyeluruh terhadap data, baik saat disimpan maupun saat dikirimkan.

5) Autentikasi berlapis (*multi-factor authentication*)

Autentikasi berlapis (*multi-factor authentication*/MFA) merupakan mekanisme keamanan yang mengharuskan pengguna untuk melalui lebih dari satu tahap verifikasi sebelum mendapatkan akses ke sistem [14]. Metode ini umumnya menggabungkan beberapa faktor autentikasi, yaitu:

1. *Something you know* (*password* atau PIN)
2. *Something you have* (OTP atau perangkat)
3. *Something you are* (biometrik seperti sidik jari atau wajah)

Penerapan MFA dalam sistem ini bertujuan untuk mengurangi risiko akses tidak sah akibat pencurian kredensial pengguna [14]. Dengan adanya autentikasi berlapis, meskipun salah satu faktor keamanan berhasil ditembus, sistem tetap memiliki lapisan perlindungan tambahan untuk mencegah akses ilegal.

6) *Role-Based Access control* (RBAC)

Role-Based Access control (RBAC) merupakan metode pengendalian akses yang membatasi hak pengguna berdasarkan peran (*role*) yang dimiliki dalam sistem. Dalam sistem pelaporan pelecehan kampus, RBAC digunakan untuk mengatur akses terhadap data sensitif, sehingga hanya pihak tertentu yang dapat melihat atau mengelola informasi tertentu. Pendekatan ini memastikan bahwa prinsip *least privilege* diterapkan, yaitu setiap pengguna hanya memiliki akses sesuai kebutuhan tugasnya [5]. Dengan demikian, risiko penyalahgunaan data oleh pihak internal dapat diminimalisir.

7) Audit log dan monitoring sistem

Audit log merupakan mekanisme pencatatan seluruh aktivitas yang terjadi dalam sistem, seperti *log in* pengguna, pengiriman laporan, perubahan data, dan akses terhadap informasi sensitif. Setiap aktivitas yang dilakukan oleh pengguna akan direkam secara sistematis dan disimpan untuk keperluan analisis dan investigasi. Selain itu, sistem juga dilengkapi dengan fitur monitoring secara *real-time* yang memungkinkan deteksi dini terhadap aktivitas mencurigakan atau anomali dalam sistem [16]. Dengan adanya audit log dan monitoring, sistem tidak hanya bersifat reaktif tetapi juga proaktif dalam menghadapi ancaman keamanan. Pendekatan ini juga mendukung transparansi dan akuntabilitas dalam pengelolaan sistem pelaporan.

8) *Push Notification* dan *Command center*

Sistem dilengkapi dengan fitur *push notification* yang terintegrasi dengan *command center*. Setiap laporan yang masuk akan langsung diteruskan kepada pihak terkait secara *real-time*. *Command center* berfungsi sebagai pusat pengelolaan laporan yang memungkinkan:

1. Monitoring laporan secara *real-time*
2. Distribusi tugas kepada petugas
3. Pengambilan keputusan secara cepat

9) Sistem *Tracking* dan Transparansi

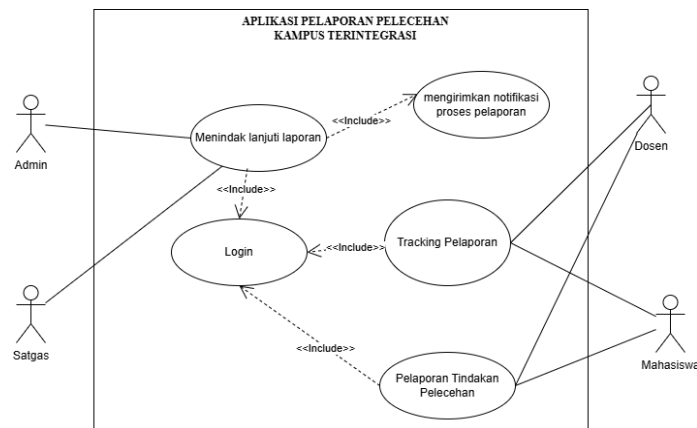
Pelapor dapat memantau status laporan yang telah dikirim, seperti:

1. Laporan diterima
2. Laporan diproses
3. Laporan selesai

Hal ini meningkatkan transparansi dan kepercayaan pengguna terhadap sistem.

4. UML Diagram

a. *Use Case Diagram*



Gambar 2. Use Case Diagram

b. Use Case Scenario

TABEL IV
USE CASE SCENARIO LOG IN

Use Case Name : Log in	ID : UC1	Important : High
Primary Actor : Mahasiswa Dosen Admin Satgas	Use Case type : Main Case	
Stakeholder & Interest : Pengguna ingin mengakses sistem dengan aman sesuai hak aksesnya, sistem harus mencegah akses tidak sah.		
Brief Description : Use case menggambarkan proses autentikasi pengguna menggunakan email/ <i>User name</i> dan <i>password</i> , serta MFA jika diterapkan.		
Triger : Pengguna membuka aplikasi sistem pelaporan Type : Detail		
Relationship: - Association: Mahasiswa, Dosen, Admin, Satgas Include:- Extend:- Generalization/Inheritance:-		
Normal Flow of Event : 1. Aktor membuka aplikasi sistem pelaporan 2. Sistem menampilkan halaman <i>log in</i> 3. Aktor memasukkan email/ <i>User name</i> dan <i>password</i> 4. Aktor menekan tombol “ <i>Log in</i> ” 5. Sistem memvalidasi data ke <i>Database</i> 6. Sistem meminta verifikasi tambahan (MFA jika aktif) 7. Sistem membuat session pengguna 8. Sistem menampilkan pesan “ <i>Log in</i> Berhasil” 9. Sistem mengarahkan ke <i>dashboard</i>		
Alternate flows: 5a. Data tidak valid Sistem mendeteksi kesalahan <i>log in</i> Sistem menampilkan pesan “ <i>User name</i> atau <i>Password</i> salah” Kembali ke form <i>log in</i>		
Exceptional Flows: <i>Database Down</i> Jika <i>Database</i> gagal diakses → tampil pesan “Koneksi gagal”		

TABEL V
USE CASE SCENARIO PELAPORAN TINDAKAN PELECEHAN

USE CASE SCENARIO PELAPORAN TINDAKAN PELECEHAN		
Use Case Name : Pelaporan Tindakan Pelecehan	ID : UC2	Important : High
Primary Actor : Mahasiswa Dosen		Use Case type : Main Case
Stakeholder & Interest : Pelapor ingin melaporkan kejadian secara aman dan anonim tanpa takut identitas terbongkar		

<i>Brief Description</i> : Pengguna membuat laporan peleccehan melalui sistem dengan opsi anonim.
<i>Triger</i> : Pengguna memilih menu “Buat Laporan”
<i>Relationship</i> : - <i>Association</i> : Mahasiswa, Dosen <i>Include</i> : Log in <i>Extend</i> :- <i>Generalization/Inheritance</i> :-
<i>Normal Flow of Event</i> : 1. Aktor memilih menu “Buat Laporan” 2. Sistem menampilkan form laporan 3. Aktor mengisi data kejadian (<i>kronolog i</i>, lokasi, bukti) 4. Aktor memilih opsi anonim 5. Sistem <i>enkripsi</i> data identitas (RSA/AES) 6. Aktor menekan tombol “Kirim Laporan” 7. Sistem memvalidasi data 8. Sistem menyimpan laporan ke <i>Database</i> 9. Sistem memberikan ID laporan 10. Sistem mengirim notifikasi ke satgas
<i>Alternate flows</i> : 7a. Data tidak lengkap Sistem menampilkan pesan “Lengkapi data” Kembali ke form
<i>Exceptional Flows</i> : <i>Database Down</i> Jika penyimpanan gagal → “Laporan gagal dikirim”

TABEL VI
USE CASE SCENARIO TRACKING LAPORAN

USE CASE SCENARIO TRACKING LAPORAN		
Use Case Name : Tracking laporan	ID : UC3	Important : High
Primary Actor : Mahasiswa Dosen		Use Case type : Main Case
Stakeholder & Interest : Pelapor memantau status laporan (diproses, diverifikasi, selesai)		
Brief Description : Pengguna memantau status laporan (diproses, diverifikasi, selesai).		
Triger : Pengguna membuka menu “Tracking Laporan”		
Relationship: - Association: Mahasiswa, Dosen Include: Log in Extend:- Generalization/Inheritance:-		
Normal Flow of Event : 1. Aktor membuka menu <i>tracking</i> 2. Sistem meminta ID laporan / <i>log in</i> 3. Sistem mengambil data laporan 4. Sistem menampilkan status laporan 5. Aktor melihat perkembangan laporan		
Alternate flows: 3a. Data tidak ditemukan Sistem menampilkan “Laporan tidak ditemukan”		
Exceptional Flows: -		

TABEL VII
USE CASE SCENARIO

<i>Use Case Name</i> : Menindak Lanjuti Laporan	ID : UC4	<i>Important</i> : High
<i>Primary Actor</i> : Admin Satgas	<i>Use Case type</i> : Main Case	
<i>Stakeholder & Interest</i> : Admin ingin memproses laporan secara cepat dan aman		
<i>Brief Description</i> : menggambarkan proses admin dan satgas saat memproses setiap laporan yang masuk.		
<i>Triger</i> : Admin dan satgas membuka menu “Manajemen Laporan”		
<i>Relationship</i> : - <i>Association</i> : Satgas dan Admin <i>Include</i> : Log in <i>Extend</i> :- <i>Generalization/Inheritance</i> :-		

<i>Normal Flow of Event :</i> 1. Aktor <i>log in</i> ke sistem 2. Aktor membuka menu laporan 3. Sistem menampilkan daftar laporan 4. Aktor memilih salah satu laporan 5. Sistem menampilkan detail laporan 6. Aktor melakukan verifikasi 7. Aktor mengubah status (diproses/selesai) 8. Sistem menyimpan perubahan 9. Sistem mengirim notifikasi ke pelapor
<i>Alternate flows:</i> 6a. Data tidak valid Sistem menolak proses Menampilkan pesan error
<i>Exceptional Flows:</i> -

TABEL VIII
USE CASE SCENARIO MENGIRIMKAN NOTIFIKASI PROSES PELAPORAN

Use Case Scenario Mengirimkan Notifikasi Proses Pelaporan		
Use Case Name : Mengirimkan notifikasi proses pelaporan	ID : UC5	Important : Medium
Primary Actor : Admin Satgas		Use Case type : Internal proses
Stakeholder & Interest : Sistem mengirim <i>push notification</i> ke pelapor dan satgas secara <i>real-time</i>		
Brief Description : Menunjukkan progress pelaporan		
Trigger : Terjadi perubahan status laporan		
Relationship: - Association: Satgas dan Admin Include: Menindak lanjuti laporan Extend:- Generalization/Inheritance:-		
Normal Flow of Event : 1. Sistem mendeteksi perubahan data laporan 2. Sistem memproses notifikasi 3. Sistem mengirim notifikasi ke <i>User</i> terkait 4. Sistem mencatat <i>log</i> notifikasi		
Alternate flows: -		
Exceptional Flows: Jika <i>server</i> notifikasi gagal → dicatat di <i>log</i>		

IV. KESIMPULAN

Berdasarkan hasil perancangan sistem, dapat disimpulkan bahwa perancangan sistem pelaporan pelecehan kampus berbasis digital yang terintegrasi dengan protokol keamanan data dapat menjadi salah satu solusi dalam mengatasi rendahnya tingkat pelaporan. Hal ini dapat diyakini karena dalam proses analisis dan perancangan sistemnya dilakukan beberapa perencanaan penerapan teknik dan fitur yang dirasakan oleh pengguna diantaranya fitur anonimitas berbasis *enkripsi* RSA dapat memberikan perlindungan identitas pelapor, sementara implementasi keamanan berlapis seperti AES, HTTPS, MFA, dan RBAC dapat diimplementasikan guna untuk meningkatkan keamanan data secara menyeluruh. Ketika nantinya *system* ini akan dibuat. Integrasi *push notification* dan *command center* dalam rancangan implementasinya, dapat memungkinkan respons yang lebih cepat dalam pengelolaan setiap laporan yang diterima secara *real-time* nantinya. Selain itu, fitur *tracking* laporan nantinya bisa meningkatkan transparansi dan kepercayaan pengguna terhadap sistem karena didalam rancangannya pelapor bisa melakukan monitoring terhadap laporan yang diajukan, sudah sejauh mana penindakan dari laporan yang telah diajukan oleh pelapor. Dengan demikian, sistem ini berpotensi mendukung terciptanya lingkungan kampus yang lebih aman, responsif, dan terpercaya.

REFERENSI

- [1] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, "Panduan Pencegahan dan Penanganan Kekerasan Seksual di Perguruan Tinggi," 2023.
- [2] L. P. Sari dan D. H. Putra, "Analisis Faktor Rendahnya Pelaporan Kasus Pelecehan Seksual di Lingkungan Kampus," Jurnal Sosial Humaniora, vol. 5, no. 2, 2024.
- [3] "Rancang Bangun Sistem Pelaporan Insiden Kejahatan Siber," Jurnal Informatika Teknologi dan Sains, vol. 5, no. 1, 2023.
- [4] V. D. Cahya, T. Ariyadi, dan D. Kurniawan, "Analisa Keamanan Data Pada Sistem Informasi Kampus (SISKA) Menggunakan Metode Burp Suite," Jurnal Sains dan Terapan, vol. 4, no. 1, 2024.

- [5] A. M. Ujung dan M. I. P. Nasution, "Sistem Keamanan *Database* ," Jurnal Penelitian *Teknologi Informasi dan Sains*, vol. 1, no. 2, pp. 50–57, 2023.
- [6] W. L. Jaelani, "Analisis dan Implementasi Keamanan Sistem Informasi Berbasis *Multi-layer security*," Jurnal *Teknologi Informasi dan Keamanan Siber*, vol. 3, no. 1, pp. 15–25, 2025.
- [7] S. Mutofin, E. C. Dinata, dan E. N. Jannah, "Implementasi *push notification* dalam rancang bangun sistem informasi manajemen evaluasi pembelajaran di perguruan tinggi," *Teknologi: Jurnal Ilmiah Sistem Informasi*, vol. 12, no. 1, pp. 9–14, 2022.
- [8] A. B. Pratama dan A. Triawan, "Penerapan *Push Notification* Menggunakan REST untuk Informasi Sistem," Jurnal *Teknologi Informasi dan Sains*, vol. 14, no. 2, 2024.
- [9] N. Umah et al., "Sosialisasi Pengembangan Sistem Terdistribusi untuk Peningkatan Keamanan Data dan Komunikasi," Jurnal *Pengabdian Lentera*, vol. 1, no. 5, 2024.
- [10] D. F. Daulay dan R. Sayekti, "Strategi Menjamin Sistem Keamanan Data Berbasis Cloud Computing," Jurnal *Informatika Teknologi dan Sains*, vol. 7, no. 3, 2025.
- [11] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, New York: Wiley, 2015.
- [12] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson, 2017.
- [13] C. Kaufman, R. Perlman, dan M. Speciner, *Network Security: Private Communication in a Public World*, 2nd ed., Prentice Hall, 2016.
- [14] NIST, "Digital Identity Guidelines," National Institute of Standards and Technology, 2023.
- [15] R. Sandhu et al., "Role-Based Access control Models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.
- [16] S. Behl dan A. Behl, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2017.