

DESAIN SISTEM E-LEARNING KAMPUS BERBASIS WEB DENGAN PENERAPAN HASHING, ENKRIPSI SIMETRIS, DAN TOKEN KEAMANAN

Hendra Finur¹, Muhammad Furqan Hakim², Riska³, Sahril Saputra⁴

^{1,2,3}Program Studi Sistem Informasi, Fakultas Pertanian dan Sains Teknologi,
Universitas Graha Karya Muara Bulian, Jambi, Indonesia

⁴Program Studi Sistem Informasi, Institut Teknologi dan Sains Nahdatul Ulama Jambi,
Jambi, Indonesia

e-mail: ¹hendra0finur@gmail.com, ²mfurqanhakim139@ugkmb.ac.id,
³Riskaikka10@gmail.com, ⁴sahril.saputra198@gmail.com

ABSTRAK

Pemanfaatan teknologi informasi dalam pembelajaran daring menuntut perguruan tinggi untuk memiliki sistem e-learning yang tidak hanya fungsional, tetapi juga aman dalam mengelola data akademik dan data pengguna. Sistem e-learning umumnya menyimpan informasi sensitif seperti identitas pengguna, nilai akademik, serta aktivitas pembelajaran, sehingga aspek keamanan menjadi faktor yang sangat penting. Namun, banyak sistem e-learning yang dikembangkan tanpa perancangan keamanan yang memadai sejak tahap awal. Penelitian ini bertujuan untuk merancang aplikasi web e-learning kampus berbasis PHP dengan menerapkan mekanisme keamanan data berbasis kriptografi. Metode penelitian yang digunakan adalah metode Research and Development (R&D) dengan pendekatan perancangan sistem. Aspek kriptografi yang diterapkan dalam perancangan sistem ini meliputi kriptografi hashing untuk pengamanan autentikasi pengguna, enkripsi simetris untuk perlindungan data sensitif, serta mekanisme token keamanan untuk menjaga integritas sesi dan permintaan sistem. Perancangan sistem dilakukan menggunakan Unified Modeling Language (UML) untuk memodelkan kebutuhan fungsional serta Entity Relationship Diagram (ERD) untuk merancang struktur basis data. Hasil penelitian ini berupa rancangan sistem e-learning yang mencakup use case diagram, rancangan basis data, dan perancangan mekanisme keamanan berbasis kriptografi. Rancangan ini diharapkan dapat menjadi acuan dalam pengembangan aplikasi e-learning kampus yang aman, terstruktur, dan sesuai dengan kebutuhan akademik.

Keywords: *E-Learning, Learning Management System, Kriptografi, Hashing, Enkripsi Simetris, Keamanan Sistem.*

ABSTRACT

Information technology adoption in online learning requires higher education institutions to provide an e-learning system that is not only functional but also secure in managing academic and user data. E-learning platforms commonly store sensitive information such as user identities, academic grades, and learning activities, making security a critical factor. However, many e-learning systems are developed without adequate security design from the early stages. This study aims to design a campus e-learning web application using pure PHP by applying cryptography-based data security mechanisms. The research method employs a Research and Development (R&D) approach with a system design orientation. The cryptographic aspects incorporated in the proposed design include cryptographic hashing for securing user authentication, symmetric encryption for protecting sensitive data, and security token mechanisms to ensure the integrity of sessions and system requests. The system design is modeled using Unified Modeling Language (UML) to represent functional requirements and an Entity Relationship Diagram (ERD) to design the database structure. The results of this study are an e-learning system design that includes use case diagrams, a database design, and a cryptography-based security mechanism design. This design is expected to serve as a reference for developing a secure, well-structured campus e-learning application aligned with academic needs.

Keywords: *E-Learning, Learning Management System, Cryptography, Hashing, Symmetric Encryption, Security Tokens.*

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi digital dalam berbagai sektor, termasuk sektor pendidikan tinggi. Pemanfaatan sistem informasi berbasis web dalam proses pembelajaran dinilai mampu meningkatkan efisiensi, fleksibilitas, serta aksesibilitas layanan akademik

bagi dosen dan mahasiswa [1], [2]. Transformasi digital dalam pendidikan juga berperan penting dalam meningkatkan kualitas pembelajaran dan layanan akademik di perguruan tinggi [3].

Salah satu bentuk penerapan teknologi informasi dalam pendidikan adalah pembelajaran daring atau e-learning. E-learning memungkinkan proses pembelajaran dilakukan secara fleksibel tanpa batasan ruang dan waktu, serta mendukung aktivitas akademik seperti distribusi materi, diskusi, penugasan, dan evaluasi pembelajaran [4], [5]. Untuk mendukung pembelajaran daring secara terstruktur, banyak institusi pendidikan mengadopsi Learning Management System (LMS) sebagai platform utama pembelajaran [6].

LMS berfungsi sebagai sistem yang mengelola pengguna, materi pembelajaran, aktivitas akademik, serta penilaian hasil belajar [7]. Penelitian sebelumnya menunjukkan bahwa penggunaan LMS dapat meningkatkan efektivitas pembelajaran apabila sistem tersebut dirancang sesuai dengan kebutuhan pengguna dan konteks institusi pendidikan [8], [9]. Namun, beberapa penelitian juga melaporkan bahwa LMS yang bersifat umum sering memiliki keterbatasan dalam fleksibilitas, kompleksitas penggunaan, serta penyesuaian terhadap kebijakan akademik internal kampus [10].

Selain aspek fungsional, sistem e-learning juga mengelola data yang bersifat sensitif, seperti data identitas pengguna, nilai akademik, serta rekam aktivitas pembelajaran. Data tersebut memiliki tingkat kerahasiaan yang tinggi dan memerlukan perlindungan yang memadai [11]. Lemahnya mekanisme keamanan pada sistem informasi pendidikan dapat menyebabkan berbagai risiko, seperti kebocoran data, manipulasi nilai akademik, serta penyalahgunaan akun pengguna [12].

Keamanan sistem informasi bertujuan untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data [13]. Salah satu pendekatan utama dalam menjaga keamanan sistem informasi adalah penerapan kriptografi. Kriptografi digunakan untuk melindungi data dan komunikasi dalam sistem berbasis web melalui mekanisme matematis dan algoritmik yang terstandarisasi [14], [15].

Dalam pengembangan aplikasi web modern, kriptografi umumnya diterapkan melalui beberapa mekanisme utama. Kriptografi hashing digunakan untuk mengamankan autentikasi pengguna dengan cara menyimpan representasi hash dari kata sandi [16]. Enkripsi simetris digunakan untuk melindungi data sensitif agar tidak dapat dibaca oleh pihak yang tidak berwenang [17]. Selain itu, mekanisme token keamanan digunakan untuk menjaga integritas sesi dan permintaan sistem pada aplikasi web [18].

Beberapa penelitian di bidang keamanan aplikasi web menunjukkan bahwa penerapan mekanisme kriptografi yang tepat dapat meningkatkan ketahanan sistem terhadap berbagai serangan keamanan, seperti pencurian kredensial dan manipulasi data [19]. Namun, pada praktiknya masih banyak aplikasi e-learning yang dikembangkan dengan fokus utama pada penyediaan fitur pembelajaran, sementara aspek keamanan belum dirancang secara terintegrasi sejak tahap awal pengembangan [20].

Berdasarkan permasalahan tersebut, penelitian ini difokuskan pada perancangan aplikasi web e-learning kampus berbasis PHP dengan penerapan kriptografi hashing, enkripsi simetris, dan token keamanan. Perancangan sistem dilakukan dengan mengintegrasikan aspek keamanan berbasis kriptografi ke dalam tahap awal perancangan sistem, sehingga aplikasi e-learning yang dihasilkan tidak hanya mendukung proses pembelajaran daring, tetapi juga memiliki mekanisme perlindungan data yang memadai dan terstruktur.

2. TINJAUAN PUSTAKA

2.1 E-Learning dan Learning Management System (LMS)

E-learning merupakan pendekatan pembelajaran yang memanfaatkan teknologi informasi untuk mendukung penyampaian materi, aktivitas pembelajaran, serta evaluasi secara daring. Penerapan e-learning pada pendidikan tinggi dapat meningkatkan fleksibilitas akses, memperluas jangkauan layanan akademik, dan mendukung kontinuitas pembelajaran. Berbagai penelitian menegaskan bahwa efektivitas e-learning dipengaruhi oleh desain sistem, kesiapan pengguna, serta kesesuaian platform dengan kebutuhan institusi. [4], [6], [8], [10]

Learning Management System (LMS) menjadi platform utama dalam implementasi e-learning karena menyediakan fasilitas pengelolaan pengguna, distribusi materi, tugas, kuis/ujian, hingga pelaporan hasil belajar. Studi empiris menunjukkan bahwa LMS yang dirancang sesuai konteks kampus dapat meningkatkan keterlibatan dan kepuasan pengguna. Namun, terdapat pula tantangan implementasi seperti kompleksitas penggunaan, hambatan adopsi, serta kebutuhan kustomisasi berdasarkan kebijakan akademik internal. [2], [7], [9], [25], [26]

2.2 Adopsi dan Keberhasilan Sistem E-Learning

Keberhasilan sistem e-learning di perguruan tinggi tidak hanya ditentukan oleh kelengkapan fitur, tetapi juga oleh penerimaan pengguna (dosen dan mahasiswa) serta faktor pendukung organisasi. Penelitian-penelitian terdahulu menekankan pentingnya faktor kemudahan penggunaan, persepsi manfaat, dukungan institusi, dan kualitas layanan sistem untuk mencapai adopsi yang optimal. [1], [3], [5], [21]

Selain itu, keterlibatan mahasiswa dalam aktivitas pembelajaran daring juga dipengaruhi oleh desain aktivitas pembelajaran dan kualitas konten. Beberapa studi menyoroti bahwa perancangan aktivitas yang terstruktur, dukungan penilaian yang transparan, serta manajemen konten yang baik menjadi determinan penting terhadap keberhasilan pembelajaran berbasis LMS. [24], [27], [28], [29]

2.3 Perancangan Sistem Informasi untuk E-Learning

Perancangan sistem informasi bertujuan memodelkan kebutuhan pengguna dan proses bisnis sebelum implementasi dilakukan. Dalam konteks sistem e-learning, pemodelan kebutuhan penting untuk memastikan fitur inti (materi, penugasan, kuis, penilaian) sesuai dengan alur akademik kampus. Pendekatan perancangan berbasis model (model-driven) juga membantu mengurangi risiko salah tafsir kebutuhan dan memudahkan validasi oleh stakeholder. [22], [23], [27], [28]

Unified Modeling Language (UML) sering digunakan untuk memodelkan sistem melalui use case, activity, dan diagram lainnya. Use case diagram khususnya digunakan untuk mengidentifikasi aktor dan interaksi mereka dengan sistem sehingga ruang lingkup fungsional sistem dapat didefinisikan dengan jelas. Konsistensi antara pemodelan kebutuhan dan rancangan data menjadi faktor penting agar implementasi sistem tidak menyimpang dari tujuan awal. [29], [31], [32]

2.4 Perancangan Basis Data (ERD) pada Sistem E-Learning

Basis data merupakan komponen inti yang menyimpan data akademik dan aktivitas pembelajaran. Perancangan basis data pada LMS perlu mengakomodasi entitas seperti pengguna, mata kuliah, kelas, materi, tugas, kuis, dan nilai. ERD (Entity Relationship Diagram) digunakan untuk memodelkan entitas, atribut, serta relasi antar entitas sehingga integritas data dapat dipertahankan. [36], [37], [38]

Beberapa penelitian menegaskan pentingnya normalisasi, penerapan constraint relasional, serta strategi indexing untuk meningkatkan konsistensi dan kinerja akses data pada sistem akademik. Rancangan gradebook dan struktur nilai juga memerlukan perhatian karena berdampak pada proses rekapitulasi nilai dan pelaporan. [39], [40]

2.5 Keamanan Sistem Informasi pada Platform E-Learning

Sistem e-learning mengelola data sensitif, seperti identitas pengguna, nilai akademik, dan rekam aktivitas pembelajaran. Oleh karena itu, keamanan sistem menjadi faktor krusial untuk menjaga kerahasiaan, integritas, dan ketersediaan data. Berbagai studi menyebutkan bahwa sistem pendidikan berbasis web rentan terhadap ancaman seperti kebocoran data, pencurian kredensial, manipulasi nilai, dan serangan pada sesi pengguna. [11], [12], [20]

Kerentanan aplikasi web sering kali terjadi akibat lemahnya validasi input, manajemen sesi, dan kontrol akses. Rekomendasi keamanan aplikasi web menekankan penerapan praktik keamanan yang sistematis, termasuk mitigasi risiko yang terdokumentasi dan diuji. Pendekatan keamanan yang baik perlu dirancang sejak awal agar tidak menjadi tambahan di akhir pengembangan. [18], [19], [49], [50]

2.6 Kriptografi untuk Keamanan Autentikasi (Hashing)

Kriptografi berperan dalam melindungi informasi penting dalam sistem informasi, terutama pada proses autentikasi dan perlindungan data. Untuk autentikasi, penyimpanan kata sandi dalam bentuk plaintext sangat berisiko, sehingga fungsi hash kriptografis digunakan untuk menyimpan representasi aman dari kata sandi pengguna. Pendekatan ini menjadi praktik standar untuk mengurangi dampak kebocoran database. [13], [14], [16], [30]

Selain hashing, keamanan autentikasi juga sering didukung oleh mekanisme threat modeling dan pola autentikasi aman. Hal ini diperlukan agar rancangan autentikasi tidak hanya aman secara penyimpanan, tetapi juga tahan terhadap serangan seperti brute force dan credential stuffing. [31], [32]

2.7 Enkripsi Simetris untuk Perlindungan Data Sensitif

Selain autentikasi, data akademik tertentu (misalnya nilai atau data sensitif lain yang ditentukan oleh kebijakan kampus) perlu dilindungi melalui enkripsi. Enkripsi simetris menjadi pilihan umum untuk perlindungan data karena efisiensinya pada aplikasi web dan kemampuannya melindungi data-at-rest.

Efektivitas enkripsi simetris bergantung pada manajemen kunci yang baik, termasuk penyimpanan, kontrol akses, dan rotasi kunci. [17], [41], [42], [43]

Beberapa penelitian juga menekankan perlunya mempertimbangkan overhead kinerja dalam penerapan enkripsi pada server aplikasi, agar perlindungan data tidak menurunkan pengalaman pengguna secara signifikan. Strategi desain keamanan yang memadukan enkripsi dan kontrol akses sering direkomendasikan untuk sistem yang menangani data sensitif. [44], [45]

2.8 Token Keamanan untuk Integritas Sesi dan Permintaan Sistem

Pada sistem web, keamanan sesi dan permintaan (request) merupakan aspek penting karena banyak serangan memanfaatkan kelemahan session management atau manipulasi request. Token keamanan umum digunakan untuk memastikan permintaan berasal dari sesi yang valid serta untuk mitigasi serangan seperti CSRF dan replay attack. [33], [34], [47]

Pembentukan token yang aman memerlukan sumber random dengan entropi yang cukup dan mekanisme validasi yang tepat. Penerapan token pada operasi sensitif (akses nilai, pengumpulan tugas, aktivitas kuis) dapat meningkatkan ketahanan sistem terhadap penyalahgunaan sesi dan serangan berbasis permintaan. [35], [46], [48]

2.9 Sintesis Literatur dan Posisi Penelitian

Berdasarkan kajian pustaka, dapat disimpulkan bahwa sistem e-learning yang baik perlu memenuhi dua dimensi utama: (1) dukungan fungsional pembelajaran yang terstruktur dan sesuai konteks institusi serta (2) keamanan sistem yang dirancang sejak awal. Banyak penelitian membahas e-learning dan keberhasilan LMS, sementara isu keamanan sering kali diperlakukan sebagai aspek tambahan. Oleh sebab itu, penelitian ini memposisikan kontribusinya pada perancangan sistem e-learning kampus berbasis PHP yang mengintegrasikan keamanan berbasis kriptografi melalui hashing, enkripsi simetris, dan token keamanan sejak tahap perancangan, sehingga menghasilkan rancangan yang terstruktur sekaligus lebih siap menghadapi risiko keamanan. [15], [22], [24], [50]

3. METODE PENELITIAN

Metodologi penelitian yang digunakan dalam penelitian ini adalah metode Research and Development (R&D) dengan pendekatan perancangan sistem informasi. Metode ini dipilih karena penelitian berfokus pada perancangan aplikasi web e-learning kampus yang dilengkapi dengan mekanisme keamanan berbasis kriptografi, bukan pada pengujian algoritma kriptografi secara eksperimental.

Pendekatan R&D memungkinkan peneliti untuk merancang model sistem secara sistematis mulai dari identifikasi permasalahan hingga evaluasi rancangan sistem. Dalam penelitian ini, aspek keamanan berbasis kriptografi dirancang sejak tahap awal perancangan agar menjadi bagian integral dari sistem e-learning yang dikembangkan.

3.1 Alur Penelitian

Alur penelitian menggambarkan tahapan-tahapan yang dilakukan secara berurutan dalam proses perancangan aplikasi web e-learning kampus. Tahapan penelitian dimulai dari identifikasi masalah hingga evaluasi rancangan sistem yang dihasilkan.



Gambar 1. Alur Penelitian

Berdasarkan Gambar 1, alur penelitian dalam perancangan sistem ini terdiri dari beberapa tahapan sebagai berikut:

3.1.1 Identifikasi Masalah

Tahap awal penelitian dilakukan untuk memetakan kondisi penerapan e-learning di perguruan tinggi dan mengidentifikasi gap antara kebutuhan pengguna dengan sistem yang tersedia. Identifikasi masalah difokuskan pada dua aspek utama: kebutuhan pembelajaran daring dan risiko keamanan data akademik (misalnya nilai, identitas, aktivitas pembelajaran). Pada tahap ini juga ditentukan ruang lingkup penelitian, sasaran pengguna (administrator kampus, dosen, mahasiswa), serta batasan penelitian agar desain sistem tetap terukur dan relevan terhadap konteks institusi pendidikan [12]. Output tahap ini: rumusan masalah, ruang lingkup, dan daftar isu prioritas (fungsi inti + keamanan).

3.1.2 Studi Literatur

Studi literatur dilakukan untuk memperoleh dasar teori dan referensi ilmiah yang relevan dengan perancangan sistem e-learning dan keamanan berbasis kriptografi. Literatur yang ditinjau mencakup:

1. Konsep e-learning dan Learning Management System (LMS) serta faktor adopsinya di pendidikan tinggi [3]
2. Pendekatan perancangan sistem informasi dan pemodelan kebutuhan (engineering requirement) [7]
3. Keamanan sistem informasi pada aplikasi web, termasuk kerentanan umum dan praktik mitigasinya [18]
4. Kriptografi untuk kebutuhan autentikasi, perlindungan data sensitif, serta integritas sesi/permintaan pada aplikasi web [16]

Studi literatur digunakan untuk menyusun kerangka konseptual bahwa keamanan perlu masuk sejak tahap desain (security-by-design), bukan ditambahkan di akhir. Output tahap ini: ringkasan teori, pemetaan konsep-kebutuhan sistem, dan landasan pemilihan mekanisme keamanan.

3.1.3. Analisis Kebutuhan Sistem

Analisis kebutuhan dilakukan untuk merumuskan kebutuhan sistem secara terstruktur berdasarkan hasil identifikasi masalah dan studi literatur. Analisis dibagi menjadi:

a. Kebutuhan Fungsional

Kebutuhan fungsional memuat fitur inti sistem e-learning, misalnya:

1. manajemen pengguna dan peran (admin/dosen/mahasiswa)
2. manajemen mata kuliah dan kelas
3. pengelolaan materi pembelajaran
4. penugasan (pembuatan, pengumpulan, penilaian)
5. kuis/ujian (pelaksanaan, attempt, hasil)
6. gradebook dan pelaporan akademik

b. Kebutuhan Non-Fungsional

Kebutuhan non-fungsional difokuskan pada aspek kualitas sistem, mencakup:

1. keamanan (otentikasi aman, integritas sesi, perlindungan data sensitif)
2. kinerja dan skalabilitas (mendukung ± 1000 mahasiswa)
3. keandalan, auditabilitas, dan kemudahan pemeliharaan

Dalam tahap ini juga ditetapkan prioritas kebutuhan (must-have vs nice-to-have) agar desain tetap realistis. Output tahap ini: dokumen kebutuhan (SRS ringkas) + prioritas kebutuhan.

3.1.4 Perancangan Sistem

Tahap perancangan sistem dilakukan untuk menghasilkan model sistem yang siap dijadikan acuan implementasi.

a. Perancangan Use Case (UML)

Use case diagram dirancang untuk menggambarkan aktor, batas sistem, fungsi utama, serta relasi antar use case (include/extend). Model ini digunakan untuk memastikan kebutuhan fungsional sudah lengkap dan tidak tumpang tindih. [24]

b. Perancangan Basis Data (ERD)

ERD dirancang untuk memodelkan entitas, atribut, relasi, dan kardinalitas (misalnya user–kelas–materi–nilai). Perancangan data juga mempertimbangkan konsistensi relasi dan keterlacakan aktivitas akademik. [30]

c. Perancangan Arsitektur Sistem

Arsitektur sistem menggambarkan hubungan antar komponen (client–server–database) serta titik integrasi mekanisme keamanan. Pada tahap ini disusun pula aturan alur data penting (misalnya alur pengumpulan tugas dan nilai) agar dapat dikontrol dengan baik. Output tahap ini: Use Case Diagram, ERD, dan rancangan arsitektur sistem.

3.1.5. Perancangan Keamanan Berbasis Kriptografi

Tahap ini merancang mekanisme keamanan sebagai bagian integral dari rancangan sistem, dengan mengacu pada prinsip kerahasiaan, integritas, dan autentikasi.

a. Kriptografi Hashing untuk Autentikasi

Rancangan hashing digunakan untuk menyimpan kredensial pengguna secara aman sehingga password tidak tersimpan dalam bentuk plaintext. Hashing juga menjadi dasar verifikasi login. [16]

b. Enkripsi Simetris untuk Data Sensitif

Enkripsi simetris dirancang untuk melindungi data sensitif tertentu (contoh: nilai, informasi tertentu yang berisiko) sebelum disimpan/diolah, sehingga data tidak terbaca bila terjadi akses tidak sah pada storage. [41]

c. Token Keamanan untuk Integritas Sesi dan Permintaan

Token keamanan dirancang untuk memastikan request berasal dari sesi yang sah (mitigasi penyalahgunaan sesi dan manipulasi request). Token dapat digunakan pada operasi sensitif seperti akses nilai, submit tugas, dan aktivitas kuis. [34]

Selain itu, rancangan keamanan juga menegaskan kontrol akses berbasis peran dan penempatan keamanan pada arsitektur secara berlapis (defense-in-depth) [49]. Output tahap ini: rancangan keamanan (hashing + enkripsi simetris + token) dan titik penerapan pada arsitektur.

3.1.6 Evaluasi Rancangan Sistem

Tahap evaluasi dilakukan untuk menilai kesesuaian rancangan terhadap kebutuhan dan memastikan rancangan dapat diimplementasikan secara logis.

Evaluasi dilakukan melalui:

1. Validasi kebutuhan vs desain: memastikan seluruh kebutuhan fungsional & non-fungsional terakomodasi.
2. Konsistensi UML–ERD: memastikan use case memiliki dukungan struktur data yang memadai (tidak ada use case tanpa data pendukung dan sebaliknya).
3. Evaluasi rancangan keamanan: memastikan hashing, enkripsi simetris, dan token berada pada proses yang tepat dan tidak saling bertentangan dengan proses bisnis utama.[18]

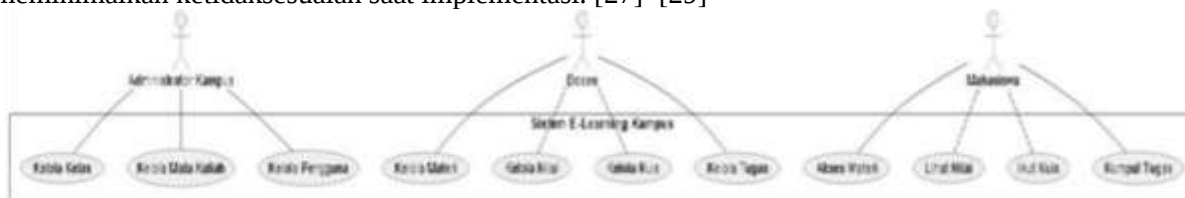
Output tahap ini: catatan evaluasi, daftar revisi rancangan (bila ada), dan rancangan final.

4. PEMBAHASAN

Bagian ini memaparkan hasil perancangan sistem e-learning kampus beserta pembahasannya, mencakup perancangan fungsional, rancangan basis data, serta rancangan keamanan berbasis kriptografi. Fokus hasil penelitian adalah keluaran desain berupa UML (use case dan activity), ERD, serta rancangan arsitektur keamanan. Pendekatan perancangan ini sejalan dengan praktik rekayasa perangkat lunak dan perancangan sistem informasi untuk domain pendidikan yang menekankan konsistensi kebutuhan–model–data. [21]–[23]

3.1 Hasil Perancangan Fungsional Sistem

Hasil perancangan fungsional menunjukkan bahwa sistem e-learning kampus dirancang untuk mendukung aktivitas pembelajaran daring secara terstruktur: pengelolaan pengguna, mata kuliah, kelas, materi, tugas, kuis/ujian, dan penilaian. Pembagian peran (administrator kampus, dosen, mahasiswa) diterapkan untuk memastikan kontrol akses sesuai kewenangan, yang merupakan praktik umum dalam sistem pembelajaran daring untuk meningkatkan keteraturan operasional dan akuntabilitas. [24]–[26] Untuk memodelkan fungsi utama per aktor, digunakan use case diagram sebagai acuan kebutuhan fungsional. Model ini juga memudahkan validasi rancangan terhadap kebutuhan pengguna dan meminimalkan ketidaksesuaian saat implementasi. [27]–[29]

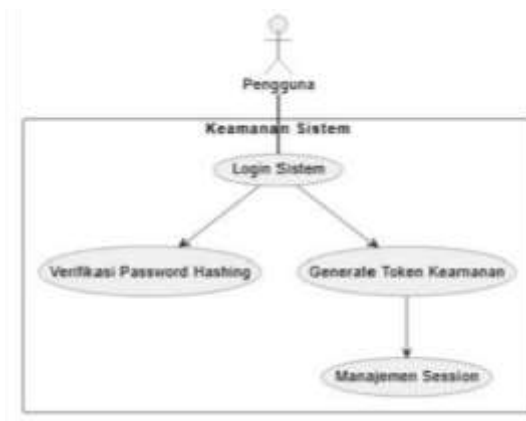


Gambar 2. Use Case Diagram Sistem E-Learning Kampus

3.2 Hasil Perancangan Keamanan pada Autentikasi (Hashing & Token)

Perancangan keamanan autentikasi menekankan dua hal utama: (1) pengamanan kredensial melalui hashing dan (2) penguatan validasi akses melalui token keamanan. Hashing digunakan agar kata sandi tidak tersimpan dalam bentuk asli pada basis data, sehingga mengurangi risiko kompromi kredensial ketika terjadi kebocoran data. [30]–[32]

Token keamanan digunakan untuk menjaga integritas sesi dan permintaan (request) agar sistem dapat memverifikasi bahwa permintaan yang masuk berasal dari pengguna yang sah serta sesi yang valid. Pendekatan token juga lazim digunakan untuk mitigasi serangan berbasis sesi dan permintaan berbahaya pada aplikasi web. [33]–[35]



Gambar 3. Use Case Keamanan Autentikasi Pengguna

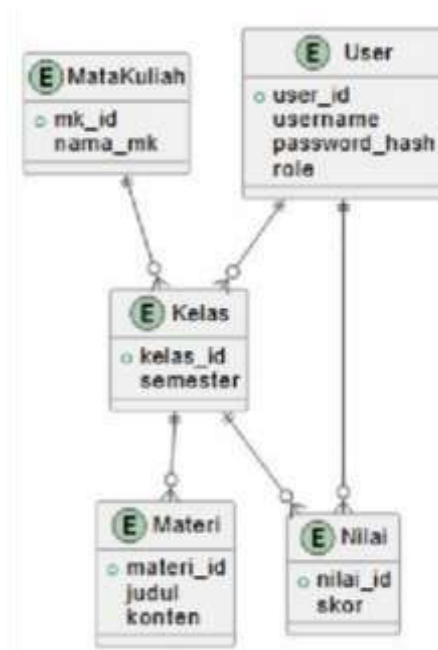


Gambar 4. Diagram Aktivitas Proses Login Aman

3.3 Hasil Perancangan Basis Data (ERD)

Perancangan basis data dilakukan untuk memastikan sistem mampu menyimpan data akademik dan aktivitas pembelajaran secara konsisten. Entitas utama yang dibutuhkan pada sistem e-learning umumnya mencakup pengguna, mata kuliah, kelas, materi, dan nilai. Relasi antar entitas dirancang untuk mendukung integritas data (misal: keterkaitan kelas–materi–nilai) dan kebutuhan pelaporan akademik. [36]–[38]

ERD digunakan agar struktur data dapat dipahami secara konseptual sebelum diimplementasikan ke skema relasional. Hal ini membantu mengurangi redundansi, memudahkan normalisasi, dan memperjelas aturan relasi antar data. [39], [40]

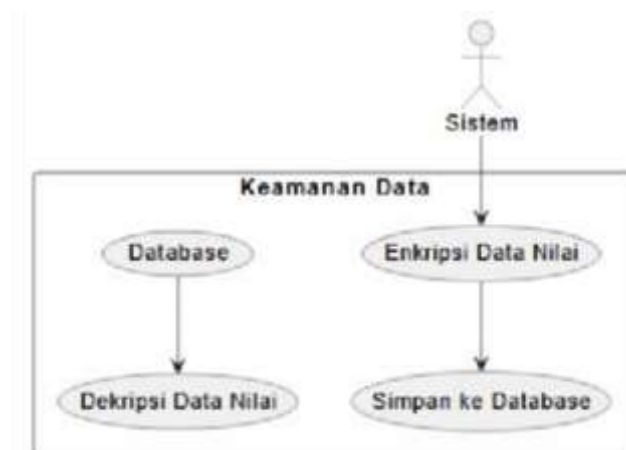


Gambar 5. Entity Relationship Diagram (ERD) Sistem E-Learning

3.4 Perancangan Keamanan Data Sensitif (Enkripsi Simetris)

Selain autentikasi, rancangan keamanan difokuskan pada perlindungan data sensitif, khususnya data akademik seperti nilai dan informasi identitas tertentu. Enkripsi simetris dirancang sebagai mekanisme perlindungan data pada kondisi data tersimpan (data-at-rest) maupun saat proses pertukaran data (data-in-transit) pada komponen sistem tertentu. [41]–[43]

Pendekatan enkripsi simetris dipilih karena efisien untuk kebutuhan aplikasi skala kampus dan sesuai untuk perlindungan data yang sering diakses, selama manajemen kunci dilakukan dengan benar. [44], [45]



Gambar 6. Diagram Keamanan Data dengan Enkripsi Simetris

3.5 Perancangan Token Keamanan untuk Integritas Sesi & Request

Token keamanan dirancang untuk memastikan integritas sesi dan permintaan sistem, terutama pada operasi sensitif seperti akses nilai, pengumpulan tugas, dan aktivitas kuis. Validasi token sebelum eksekusi proses bisnis bertujuan mengurangi risiko manipulasi request, serangan replay, dan penyalahgunaan sesi. [46]–[48]

Gambar 7. Diagram Token Keamanan (*Session & Request*)

3.6 Arsitektur Keamanan Sistem (Integrasi Hashing, Enkripsi, Token)

Secara arsitektural, keamanan dirancang sebagai komponen yang terintegrasi pada lapisan aplikasi (web server) dan berinteraksi dengan basis data. Hashing ditempatkan pada proses autentikasi, enkripsi simetris pada pengolahan data sensitif, dan token keamanan pada validasi sesi serta permintaan sistem. Integrasi ini mendukung prinsip *defense-in-depth* pada aplikasi web. [49], [50]



Gambar 8. Arsitektur Keamanan Sistem E-Learning

3.7 Ringkasan Pembahasan

Berdasarkan hasil perancangan, sistem e-learning kampus telah dimodelkan secara fungsional melalui use case dan activity diagram, serta dimodelkan secara data melalui ERD. Pembeda utama rancangan ini adalah integrasi keamanan berbasis kriptografi (hashing, enkripsi simetris, token keamanan) sejak tahap desain, sehingga perancangan tidak hanya berorientasi pada fitur pembelajaran, tetapi juga pada perlindungan data akademik dan integritas akses sistem. [21], [24], [30], [41], [46]

5. KESIMPULAN

Berdasarkan hasil perancangan yang telah dilakukan, dapat disimpulkan bahwa rancangan sistem e-learning kampus berhasil memodelkan kebutuhan pembelajaran daring secara terstruktur melalui use case diagram yang memetakan aktor dan fungsi utama, seperti pengelolaan pengguna, kelas, materi, tugas, kuis/ujian, serta penilaian akademik. Rancangan basis data dalam bentuk Entity Relationship Diagram (ERD) mampu merepresentasikan struktur data akademik dan aktivitas pembelajaran secara konsisten sehingga mendukung integritas data dan kebutuhan pelaporan. Selain itu, aspek keamanan berbasis kriptografi telah diintegrasikan sejak tahap desain, meliputi penggunaan hashing untuk

pengamanan autentikasi pengguna, enkripsi simetris untuk perlindungan data sensitif, serta token keamanan untuk menjaga integritas sesi dan permintaan pada aplikasi web. Integrasi keamanan sejak tahap perancangan ini menjadikan sistem tidak hanya berorientasi pada fungsi pembelajaran, tetapi juga pada perlindungan data dan kontrol akses.

Meskipun demikian, penelitian ini masih terbatas pada tahap perancangan konseptual dan belum mencakup implementasi penuh serta pengujian keamanan dan performa secara eksperimental. Oleh karena itu, pengembangan selanjutnya disarankan untuk mengimplementasikan prototipe sistem dan melakukan uji coba terbatas, disertai pengujian keamanan seperti uji kerentanan dan pengujian mekanisme sesi serta performa sistem pada beban puncak. Selain itu, perlu dirancang kebijakan manajemen kunci enkripsi secara lebih rinci serta pengembangan modul lanjutan seperti integrasi dengan sistem akademik (SIKAD), audit log yang lebih komprehensif, dan penerapan role-based access control yang lebih granular agar sistem dapat diimplementasikan secara aman, stabil, dan sesuai kebutuhan institusi pendidikan.

DAFTAR PUSTAKA

- [1] N. Kumar and J. Jain, "Development of collaborative learning management systems for higher education in oncology using deep learning and blockchain," in 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Apr. 2024, pp. 1–5, doi: 10.1109/I2CT61223.2024.10543738.
- [2] M. D. Nguyen, T. Nguyen-Ngoc, C. H. Nguyen-Dinh, and A. P. Le, "A hybrid approach of blockchain and semantic web technologies to validating learning outcomes in accordance with legal constraints," *Int. j. inf. tecnol.*, vol. 14, no. 6, pp. 2893–2901, Oct. 2022, doi: 10.1007/s41870-022-01039-z.
- [3] S. Ouf, S. Ahmed, and Y. Helmy, "A blockchain based deep learning framework for a smart learning environment," *Sci. Rep.*, vol. 15, no. 1, p. 19519, Jun. 2025, doi: 10.1038/s41598-025-03688-z.
- [4] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and A. U. Hasanah, "Scheme iLearning DApps for Education using Blockchain-Based," in 2022 IEEE Creative Communication and Innovative Technology (ICCIT), Nov. 2022, pp. 1–7, doi: 10.1109/ICCIT55355.2022.10118979.
- [5] A. Y. Al-Zoubi, M. Dmour, and R. Aldmour, "Blockchain as a learning management system for laboratories 4.0," *Int. J. Onl. Eng.*, vol. 18, no. 12, pp. 16–34, Sep. 2022, doi: 10.3991/ijoe.v18i12.33515.
- [6] Blessing and Adeoye, "AI-Powered elearning for front-end development: Tailored entrepreneurship courses." <https://elibrary.ru/item.asp?id=80168574> (accessed Feb. 09, 2026).
- [7] M. Elkhodr, K. Wangsa, E. Gide, and S. Karim, "A systematic review and multifaceted analysis of the integration of artificial intelligence and blockchain: shaping the future of australian higher education," *Future Internet*, vol. 16, no. 10, p. 378, Oct. 2024, doi: 10.3390/fi16100378.
- [8] Paul, Aithal, and Saavedra, "Blockchain in Educational Development: Potentialities and Issues—Towards Sophisticated Digital Education Systems." <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4400249> (accessed Feb. 09, 2026).
- [9] L. K. Ramasamy and F. Khan, "Blockchain-Based E-Learning Platform: Transforming Education Through Decentralization," in *Blockchain for global education*, Cham: Springer Nature Switzerland, 2024, pp. 103–123.
- [10] A. A. Nassani, A. Grigorescu, Z. Yousaf, R. A. Trandafir, A. Javed, and M. Haffar, "Leading Role of E-Learning and Blockchain towards Privacy and Security Management: A Study of Electronics Manufacturing Firms," *Electronics*, vol. 12, no. 7, p. 1579, Mar. 2023, doi: 10.3390/electronics12071579.
- [11] S. Mondal, A. Panja, and S. Karforma, "An efficient e-certificate management system in e-learning using blockchain," *SC.*, vol. 89, no. March-April, Apr. 2023, doi: 10.36094/sc.v89.2023.An_Efficient_E-certificate_Management_System.Mondal.120.
- [12] A. Kumar, A. Shing, K. Saini, and A. Chabaque, "A Secure E-Learning Platform An Approach of Blockchain Technology," in 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Dec. 2022, pp. 1895–1900, doi: 10.1109/ICAC3N56670.2022.10074130.
- [13] S. Jin and L. Zhang, "Research on the Recommendation System of Music e-learning Resources with Blockchain based on Hybrid Deep Learning Model," *SCPE*, vol. 25, no. 3, pp. 1455–1465, Apr. 2024, doi: 10.12694/scpe.v25i3.2672.
- [14] Maalini, Gobinath, and Pravinkumar, "Eduverse: Integrating Blockchain Security, AI, and AR/VR for the Evolution of E-Learning Systems." <https://ieeexplore.ieee.org/abstract/document/11041452/> (accessed Feb. 09, 2026).

- [15] A. Bigiotti, M. P. F. Bottoni, and G. Nalli, "Blockchain in E-Learning Platform to Enhance Trustworthy and Sharing of Micro-credentials," in *Advanced information systems engineering workshops: caise 2024 international workshops, limassol, cyprus, june 3–7, 2024, proceedings*, vol. 521, J. P. A. Almeida, C. Di Ciccio, and C. Kalloniatis, Eds. Cham: Springer Nature Switzerland, 2024, pp. 5–17.
- [16] M. Poser, "Application Possibilities of Tokens on an E-Learning Platform," *Open Conf. Proc.*, vol. 2, pp. 105–109, Dec. 2022, doi: 10.52825/ocp.v2i.170.
- [17] Shadmanova, Karimov, and Taylanova, "Ensuring the security of an internetbased e-learning system through the use of integrated encryption methods." <https://jisis.org/wp-content/uploads/2024/12/2024.I4.024.pdf> (accessed Feb. 09, 2026).
- [18] Lu, "Construction of a Secure Sharing Model for Digital Educational Resources Using Blockchain and Cipher Policy Attribute Based Encryption in Smart Education." <https://search.proquest.com/openview/b27359366f82fd247a77b0659e1303dc/1?pq-origsite=gscholar&cbl=1616336> (accessed Feb. 09, 2026).
- [19] Ravi and Rajakaruna, "CRYPTOGRAPHY-BASED AI E-LEARNING PLATFORM: ENHANCING THE SUSTAINABILITY OF THE EDUCATION INDUSTRY." https://www.researchgate.net/profile/Jaymund-Floranza/publication/390551311_Social_media_usage_and_online_consumer_behavior_across_different_cultures_A_systematic_literature_review/links/67f3bfb9e8041142a16cc4e6/Social-media-usage-and-online-consumer-behavior-across-different-cultures-A-systematic-literature-review.pdf#page=180 (accessed Feb. 09, 2026).
- [20] Bidry, Ouaguid, and Hanine, "The Impact of Blockchain on E-Learning: Comparative Projects Analysis," in *Proceedings of the 7th International Conference on Networking, Intelligent Systems and Security*, New York, NY, USA, Apr. 2024, pp. 1–7, doi: 10.1145/3659677.3659732.
- [21] C.-L. Chen, K.-W. Zeng, W.-Y. Li, C.-F. Lee, L.-C. Liu, and Y.-Y. Deng, "Lightweight Post-Quantum Cryptography: Applications and Countermeasures in Internet of Things, Blockchain, and E-Learning," in *ECEI 2025*, Basel Switzerland, Aug. 2025, p. 14, doi: 10.3390/engproc2025103014.
- [22] O. A. Khashan, S. Alamri, W. Alomoush, M. K. Alsmadi, S. Atawneh, and U. Mir, "Blockchain-Based Decentralized Authentication Model for IoT-Based E-Learning and Educational Environments," *Comput. Mater. Contin.*, vol. 75, no. 2, pp. 3133–3158, 2023, doi: 10.32604/cmc.2023.036217.
- [23] T. Y. Lam and B. Dongol, "A blockchain-enabled e-learning platform," *Interactive Learning Environments*, vol. 30, no. 7, pp. 1229–1251, Aug. 2022, doi: 10.1080/10494820.2020.1716022.
- [24] L.-N. Degambur, S. Armoogum, and S. Pudaruth, "A Study of Security Impacts and Cryptographic Techniques in Cloud-based e-Learning Technologies," *ijacsa*, vol. 13, no. 1, 2022, doi: 10.14569/IJACSA.2022.0130108.
- [25] M. A. Haque et al., "Sustainable and efficient E-learning internet of things system through blockchain technology," *elea*, vol. 21, no. 3, pp. 216–235, May 2024, doi: 10.1177/20427530231156711.
- [26] A. Alam, "Platform Utilising Blockchain Technology for eLearning and Online Education for Open Sharing of Academic Proficiency and Progress Records," in *Smart data intelligence: proceedings of ICSMDI 2022*, R. Asokan, D. P. Ruiz, Z. A. Baig, and S. Piramuthu, Eds. Singapore: Springer Nature Singapore, 2022, pp. 307–320.
- [27] D. T. Naidoo, "Integrating TAM and IS success model: exploring the role of blockchain and AI in predicting learner engagement and performance in e-learning," *Front. Comput. Sci.*, vol. 5, Sep. 2023, doi: 10.3389/fcomp.2023.1227749.
- [28] M. Bidry, A. Ouaguid, and M. Hanine, "Enhancing E-Learning with Blockchain: Characteristics, Projects, and Emerging Trends," *Future Internet*, vol. 15, no. 9, p. 293, Aug. 2023, doi: 10.3390/fi15090293.
- [29] M. Nadini, L. Alessandretti, F. Di Giacinto, M. Martino, L. M. Aiello, and A. Baronchelli, "Mapping the NFT revolution: market trends, trade networks, and visual features.," *Sci. Rep.*, vol. 11, no. 1, p. 20902, Oct. 2021, doi: 10.1038/s41598-021-00053-8.
- [30] S. Chalim, F. Usman, M. Rokhman, I. Rusydi, Rahmat, and B. Zamawi, "Children's Education in the Metaverse Era: Between the Rapid Growth of Information Technology and Self-learning of Generation Z," *nzh*, vol. 7, no. 3, pp. 608–627, Nov. 2024, doi: 10.31538/nzh.v7i3.19.
- [31] K. Vikram, N. Sivaraman, and Dr. P. Balamurugan, "Crypto currency market price prediction using data science process," *IJRASET*, vol. 10, no. 2, pp. 1451–1454, Feb. 2022, doi: 10.22214/ijraset.2022.40521.
- [32] Sneha S, Monisha S, J. Jayashankari, and Dr. M. Preetha, "Crypto Currency Market Price Prediction using Data Science Technique," *IJARST*, pp. 16–20, Jun. 2022, doi: 10.48175/IJARST-4558.
- [33] N. Huda and K. Kasino, "Rancangan dan implementasi learning managements system berbasis web (studi kasus: SMA nahdhotul islam sri tiga)," *SMATIKA*, vol. 12, no. 02, pp. 245–254, Dec. 2022, doi: 10.32664/smatika.v12i02.707.
- [34] E. Nkhukhu-Orlando, "Blended learning dependability and perceived usefulness: the mediating role of organisational commitment," *ICER*, vol. 1, no. 1, pp. 246–253, Nov. 2024, doi: 10.34190/icer.1.1.3165.

- [35] P. W. Adi and R. Kusumaningrum, "Pengembangan Sistem Manajemen Naskah Soal dengan Keamanan Pre-Hash Coding," *tc*, vol. 20, no. 4, pp. 613–622, Nov. 2021, doi: 10.33633/tc.v20i4.5271.
- [36] R. J. Putra, D. M. Wiharta, and N. P. P. Sastra, "Pengembangan sistem notifikasi pada LMS moodle melalui penerapan multi channel access dengan pemanfaatan webhook," *JTE*, vol. 22, no. 2, p. 211, Dec. 2023, doi: 10.24843/MITE.2023.v22i02.P08.
- [37] K. Nur Saffanah and R. Andrian, "PERANCANGAN DESIGN UI/UX PADA APLIKASI LEARNING MANAGEMENT SYSTEM GUNA MENINGKATKAN EFEKTIVITAS DAN KEPUASAN PENGGUNA MENGGUNAKAN METODE DESIGN THINKING," *mnemonic*, vol. 7, no. 1, pp. 23–30, Feb. 2024, doi: 10.36040/mnemonic.v7i1.8474.
- [38] I. P. A. Purnawan, I. K. G. Darma Putra, and N. K. D. Rusjyanthi, "Evaluasi usability dan user experience LMS OASE universitas udayana menggunakan metode tuxel 2.0," *j. nas. pendidik. teknik. inform.*, vol. 10, no. 3, p. 177, Dec. 2021, doi: 10.23887/janapati.v10i3.40670.
- [39] V. Naumova and O. Bulvinska, "Managing student safety on the internet: open educational resources to help educators," *Osvitolohiya*, vol. 13, no. 13, pp. 78–90, 2024, doi: 10.28925/2412-124X.2024.13.8.
- [40] D. Kotsopoulos, "Developing an undergraduate business course using open educational resources," *cjsotl-rcacea*, vol. 13, no. 1, Feb. 2022, doi: 10.5206/cjsotlrcacea.2022.1.10992.
- [41] N. Shariff, . S., and K. Yadav, "Enhancing teaching and learning though digital data and learning analytics in education," *SRJIS*, vol. 9, no. 71, Jun. 2022, doi: 10.21922/srjis.v9i71.10217.
- [42] L. A. Phillips, S. J. Piechota, and C. D. Fogle, "Implementation and evaluation of open educational and free resources to replace textbook in program evaluation course.," *Scholarship of Teaching and Learning in Psychology*, vol. 7, no. 3, pp. 228–236, Sep. 2021, doi: 10.1037/stl0000253.
- [43] H. Farley, "Moocs in asia: promise unfulfilled or promise realized?," in *The Oxford Handbook of Higher Education in the Asia-Pacific Region*, D. Kapur, D. M. Malone, and L. Kong, Eds. Oxford University Press, 2023, pp. 356–376.
- [44] V. I. Marín and D. Villar-Onrubia, "Online infrastructures for open educational resources," in *Handbook of open, distance and digital education*, Singapore: Springer Singapore, 2022, pp. 1–20.
- [45] K. Jambrošić et al., "The Acoustics Knowledge Alliance project: the most recent addition to the Acoustic Courseware online educational platform," *inter noise*, vol. 268, no. 8, pp. 483–491, Nov. 2023, doi: 10.3397/IN_2023_0085.
- [46] F. Li, "An analysis of the construction methods of multimodal course knowledge graphs," *JERA*, vol. 9, no. 3, pp. 171–177, Jun. 2025, doi: 10.26689/jera.v9i3.10803.
- [47] "Study on online linguistics teaching courseware design and cognitive load," *FER*, vol. 6, no. 23, 2023, doi: 10.25236/FER.2023.062321.
- [48] A. Tella, O. P. Owoeye, and A. O. Dunmade, "Access to, use, and effect of open educational resources: the perspectives of LIS academics in selected nigerian universities," *IJIE*, vol. 8, no. 2, p. 65, Dec. 2024, doi: 10.20961/ijie.v8i2.85288.
- [49] L. Iroka and B. N. Amanze-Unagha, "Influence of open educational resources (OERs) on publication output of lecturers in public polytechnics in South-East, Nigeria," *JLST*, vol. 7, no. 3, 2025, doi: 10.47524/jlst.v7i3.191.
- [50] K. Najmani, E. H. Benlahmar, N. Sael, and A. Zellou, "A systematic literature review on recommender systems for moocs," *isi*, vol. 27, no. 6, pp. 895–902, Dec. 2022, doi: 10.18280/isi.270605.