



MEMOIRE

Présenté par

Cheikh Essouvi Elmoustapha Ahmed Elhadj

Pour l'obtention de diplôme de

MASTER

Filière : Informatique

Spécialité : Systèmes Informatiques Intelligents

Thème

La sécurité dans les plateformes d'apprentissage

Soutenu le : 20 / 05 / 2024

Devant le Jury composé de :

Qualité	Nom et Prénom	Grade	Université
Président	Mr. Djedjai	MCB	Chadli Bendjedid El-Tarf
Rapporteur	Mr. Chaouki Chemam	MCB	Chadli Bendjedid El-Tarf
Examineur	Mr. Touahri	MCB	Chadli Bendjedid El-Tarf

Année Universitaire : 2023/2024

Remerciements

Louange à Dieu et gratitude envers Lui, le Tout-Puissant et le Grand, car c'est Lui seul qui mérite les louanges et l'exaltation pour nous avoir aidés et nous avoir donné patience et persévérance tout au long de ces années. Nous exprimons notre sincère reconnaissance et notre profonde gratitude du fond de nos cœurs à nos parents, qui sont la raison de tout le bien dans lequel nous sommes, et nous espérons être toujours à la hauteur de leur confiance.

Nous remercions également le Dr Chaouki Chemmam, qui nous a encadrés tout au long de ce projet. Nous le remercions pour tout ce qu'il nous a donné et pour ses conseils qui nous ont toujours guidés sur le bon chemin. Nous le remercions pour son style de traitement, empreint de gentillesse et de politesse, malgré sa grandeur, sa valeur et son respect. Bien qu'il soit docteur et notre professeur, nous n'avons pas ressenti cette grande différence entre lui et nous, car il nous a traités avec toute la bienveillance et l'humilité, nous considérant comme ses frères.

Nous remercions également les membres distingués du comité de discussion, et nous espérons que notre présentation sera à la hauteur des attentes.

Louanges à Dieu, Seigneur des mondes, et prières et paix soient sur le plus noble des prophètes et messagers, notre maître Mohammed.

Avec fierté, gratitude et reconnaissance, je tiens à dédier ce travail à mes parents, ces deux personnes qui ont consacré leur vie et leurs efforts pour nous rendre heureux, mes frères et moi. Ils ont cherché avec amour et détermination à faire de nous des individus prospères, en nous offrant amour, conseils, prières et soutien financier, nous donnant tout ce dont nous avons besoin.

À mes frères, dont j'ai énormément bénéficié et qui m'ont encouragé à avancer, je dédie ce travail. Et bien sûr, à tous les enseignants, amis et collègues qui m'ont aidé durant cette période, en particulier notre superviseur, le Dr. Chaouki Chemmam.

Table des matières

Contents

Remerciements	2
Dédicace	3
Table des matières	4
Contents.....	4
Liste des figures	6
Liste des listings	7
Liste des acronymes	8
Introduction Générale.....	10
1. Contexte du projet et problématique	10
2. Motivations.....	10
3. Objectifs	10
4. Contenu du mémoire	11
Chapitre 1 : Généralité sur L’usage de IA dans E-Learning	12
1. Introduction	12
2. Application de l’intelligence artificiel dans l’apprentissage en ligne	14
2.1 Avis general	14
2.2 Système de gestion de l'apprentissage (LMS)	15
3. MODÈLE D'APPRENTISSAGE PERSONNALISÉ : EXIGENCES ET DÉFIS	17
3.1 EXIGENCES	17
3.2 DEFITS	18
Chapitre 2 : Généralité sur la sécurité	20
1. Introduction.....	20
2. Revue sur les politiques et stratégies de sécurité	21
2.1. Prévention (PREV)	22
2.2.	22
Dissuasion (DETER)	23

2.3. Détection (DETECT)	23
3. SECURISE LES PLATEFORMES D'APPRENTISSAGE EN LIGNE	25
3.1 Aprecu general	25
3.2 Exigences de sécurité de base et problèmes de sécurité les plus importants.....	25
3.2.1 Exigences de sécurité de base	25
3.2.2 Les problèmes de sécurité les plus importants pour l'e-learning	25
3.3 Sécurité de la plateforme e-learning	29
Chapitre 3 : Réalisation	33
1. Introduction	33
2. Approche Proposée	34
2.1 Sécurisation de la plateforme contre les attaques externes	34
2.2 Assurer la confidentialité pour sécuriser la plateforme contre les attaques internes .	34
2.3 Modèle d'IA pour la Détection des Intrusions sur une Plateforme d'Apprentissage	
35	
3. Conception et Architecture.....	37
3.1 Diagramme de cas d'utilisation	37
.....	37
3.2 Schemas Diagramme	38
4. Implémentation.....	39
4.1 Technologies utilisées : outils et environnement de développement	39
4.1.1 Outils	39
4.1.2 Environnement	45
4.2 Implémentation de l'application	46
4.2.1 Création u projet en utilisant reactjs.....	46
4.2.2 Création du model IA	48
5.Présentation du système	52
5.1 Capture des pages.....	52
6. Conclusion.....	64
Conclusion et Perspectives.....	65
Références	66

Liste des figures

Figure 1 : Test de turing	12
Figure 2 : Reseau de Neuron Artificiel	13
Figure 3 : Learning Management System	16
Figure 4 : Prevention	22
Figure 5 : Detection.....	24
Figure 6 : Cross-Site Scripting	26
Figure 7 : SQL injection.....	28
Figure 8 : Diagramme de cas d'utilisation.....	37
Figure 9 : Diagramme de schemas	39
Figure 10 : Login.....	53
Figure 11 : Inscription	54
Figure 12 : page admin.....	55
Figure 13 : Page d'ajout department.....	56
Figure 14 : Page de modules	57
Figure 15 : Page de prof	57
Figure 16 : Page d'ajouter cour.....	58
Figure 17 : Page de cour etudiants	58
Figure 18 : Page cour	59
Figure 19 : Blog.....	59
Figure 20 : Add blog	60
Figure 21 : Profile	60
Figure 22 : page de home	61

Liste des listings

Code 1 : create-react-app.....	46
Code 2 : Install-firebase-Sdk.....	46
Code 3 : Configuration-firebase	46
Code 4 : Install firebase- CLI.....	47
Code 5 : Connecter au firebase	47
Code 6 : Intialisation de projet	47
Code 7 : Construction app.....	47
Code 8 : Deploy app.....	47
Code 9: Intialisation firebase.....	48
Code 10 : Coollection de donnees.....	49
Code 11: Incluez TensorFlow.js dans le code HTML	49
Code 12 : Entraîner le modèle-1	50
Code 13 : Entraîner le modèle-2	50
Code 14 : Firebase-function	51
Code 15 : Implement-function-1	51
Code 16 : Implement-function-2	51
Code 17 : déployer la fonction	52
Code 18 : Integrate-model.....	52

Liste des acronymes

IA: Intelligence Artificielle

RNA : Réseaux de Neurones Artificiels (Artificial Neural Networks)

IDS : Intrusion Detection System (Système de Détection d'Intrusion)

FIS : Fuzzy Inference System (Système d'Inférence Floue)

SNORT : Snort (Outil de détection d'intrusion en réseau)

IP : Internet Protocol (Protocole Internet)

DARPA : Defense Advanced Research Projects Agency (Agence pour les Projets de Recherche Avancée de Défense)

TCPdump : TCPdump (Outil d'analyse de trafic réseau)

DOS : Denial of Service (Attaque par Déni de Service)

R2L : Remote to Local (Intrusions distantes vers locales)

U2R : User to Root (Intrusions utilisateur vers root)

CDSS : Clinical Decision Support System (Système d'Aide à la Décision Clinique)

IRM : Information Rights Management (Gestion des Droits de l'Information)

GRNN : General Regression Neural Network (Réseau de Neurones à Régression Générale)

LS-SVM : Least Squares Support Vector Machine (Machine à Vecteurs de Support aux Moindres Carrés)

LMS : Learning Management System (Système de Gestion de l'Apprentissage)

CD-ROM : Compact Disc Read-Only Memory (Disque Compact à Mémoire en Lecture Seule)

VPN : Virtual Private Network (Réseau Privé Virtuel)

NEEF : Network Enabled Electronic Funds Transfer (Transfert Électronique de Fonds via Réseau)

XSS : Cross-Site Scripting (Scripts Inter-Sites)

SQL : Structured Query Language (Langage de Requête Structuré)

URL : Uniform Resource Locator (Localisateur Uniforme de Ressource)

HTML : HyperText Markup Language (Langage de Balises Hypertexte)

HTTPS : HyperText Transfer Protocol Secure (Protocole de Transfert Hypertexte Sécurisé)

MFA : Multi-Factor Authentication (Authentification Multi-Facteurs)

CMS: Content Management System (Système de Gestion de Contenu)

BYOD : Bring Your Own Device (Apportez Votre Propre Appareil)

DRM : Digital Rights Management (Gestion des Droits Numériques)

NOSQL : Not Only SQL (Pas Seulement SQL, base de données non relationnelle)

SSL : Secure Sockets Layer (Couche de Socket Sécurisée)

REACTJS : React JavaScript (Bibliothèque JavaScript pour la création d'interfaces utilisateur)

CDN : Content Delivery Network (Réseau de Distribution de Contenu)

CLI : Command Line Interface (Interface en Ligne de Commande)

SPA : Single-Page Applications (Applications à Page Unique)

PWA : Progressive Web Apps (Applications Web Progressives)

SDK : Software Development Kit (Kit de Développement Logiciel)

DOM : Document Object Model (Modèle Objet de Document)

API : Application Programming Interface (Interface de Programmation d'Applications)

JSON : JavaScript Object Notation (Notation Objet JavaScript)

JSX : JavaScript XML (Extension de syntaxe pour JavaScript, utilisée avec React)

XML : eXtensible Markup Language (Langage de Balises Extensible)

UML : Unified Modeling Language (Langage de Modélisation Unifié)

Introduction Générale

Aujourd'hui, le domaine de l'intelligence artificielle est devenu l'un des domaines les plus importants de la technologie de l'information et des sciences des données, car il entre dans la fabrication et le développement de plusieurs domaines, tout en touchant directement la vie individuelle. Il n'y a plus de place pour l'ignorer ou ne pas suivre son évolution et en tirer parti pour les nombreuses fonctionnalités précieuses et rapides qu'il offre, ainsi que pour le temps et l'effort qu'il économise. Par conséquent, l'intelligence artificielle a envahi tous les domaines avec force et est devenue un outil important pour suivre le développement des technologies de l'information, rivalisant presque avec l'humain en termes de réflexion, d'apprentissage et de prise de décision, et le surpassant dans le domaine du calcul et de l'accomplissement rapide des tâches complexes.

1. Contexte du projet et problématique

Nous visons à travers ce projet de développer une plateforme d'apprentissage en ligne en utilisant des technologies nouvelles et avancées qui suivent les mises à jour de sécurité afin de réduire les risques de piratage et d'augmenter le niveau de sécurité, sachant qu'aucun système n'est totalement sécurisé à 100%. La plateforme offrira aux étudiants la possibilité de suivre leurs recherches et leurs études académiques.

2. Motivations

Les principales motivations derrière la réalisation de ce projet sont d'appliquer les connaissances scientifiques que nous avons acquises au cours des deux dernières années, de présenter un projet de fin d'études utile pour l'université et pour nous en tant qu'étudiants, et de commencer à entrer dans le domaine et à acquérir une expérience qui nous permettra de nous préparer à intégrer le marché du travail.

3. Objectifs

Nos buts pour le développement de cette plateforme incluent la contribution positive au développement de la recherche scientifique dans notre université et la promotion de sa reconnaissance à travers une interface d'application qui présente des informations et des installations universitaires. De plus, nous visons à permettre aux étudiants d'accéder à leurs cours de manière fluide et sécurisée, ainsi qu'à rassembler toutes les références et les articles des

enseignants et des étudiants en un seul endroit, tout en leur accordant le droit de publier des articles sur la plateforme.

4. Contenu du mémoire

En plus des pages d'accueil, de table des matières, de dédicace, de remerciements et autres, ce rapport est divisé en trois chapitres, à savoir :

- Chapitre 1 : Introduction sur l'IA
- Chapitre 2 : Introduction sur la sécurité
- Chapitre 3 : Réalisation

Chapitre 1 : Généralité sur L'usage de IA dans E-Learning

1. Introduction

L'intelligence est la capacité de penser rapidement et de trouver des solutions aux problèmes en se basant sur les informations disponibles et les moyens à disposition, tout en développant des capacités liées à l'analyse, à la déduction, à la planification, et à la collecte et la coordination des idées en général. Jusqu'à récemment, l'être humain était considéré comme l'être le plus intelligent sans rival. Cependant, avec l'apparition de l'intelligence artificielle (IA) et ses capacités énormes, une comparaison s'impose entre l'intelligence humaine et l'intelligence artificielle. Il est vrai que l'homme a développé l'IA, mais cette dernière l'a surpassé dans plusieurs domaines, notamment en ce qui concerne la rapidité de traitement, l'accomplissement de tâches complexes, et la capacité à résoudre facilement des opérations mathématiques compliquées.

Nous connaissons l'intelligence humaine, mais qu'est-ce que l'intelligence artificielle ?

L'intelligence artificielle est le développement de machines et de logiciels intelligents leur permettant de penser, d'apprendre, de rassembler des connaissances, de communiquer, d'analyser, de stocker et de percevoir des choses en se basant sur une simulation humaine. John McCarthy a inventé ce terme en 1956 comme une branche de l'informatique. L'intelligence artificielle est l'étude de l'informatique qui rend possible la perception, la pensée, l'action, l'apprentissage et la prédiction.

L'intelligence artificielle diffère de l'informatique en raison de son accent sur la perception, la pensée, l'action, l'interaction, la prise de décisions, et le traitement d'une manière imitant l'humain. Elle a été testée pour la première fois en utilisant le test de Turing, proposé par Alan Turing en 1950 (voir figure1).

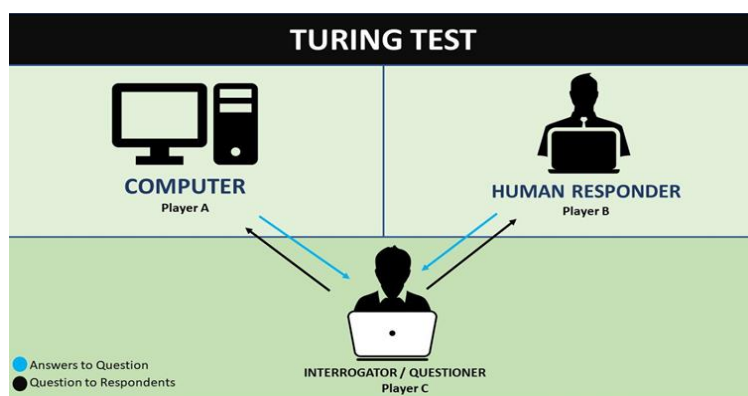


Figure 1 : Test de turing

Ce test est conçu pour évaluer si une machine peut penser ou non. Le test implique un enquêteur humain interagissant avec un humain et une machine, et il doit déterminer qui est l'humain et qui est la machine. L'ordinateur passe le test si l'enquêteur ne peut pas distinguer les réponses de l'humain et de la machine après avoir posé quelques questions écrites.

L'intelligence artificielle rend les machines plus intelligentes et utiles. Elle fonctionne grâce aux neurones artificiels (réseau neuronal artificiel) et aux théories scientifiques basées sur les données et la logique qui lui permettent d'apprendre et de tester (voir Figure2).

Les techniques de l'intelligence artificielle ont mûri au point d'offrir de véritables avantages pratiques dans de nombreuses applications. Les principaux domaines de l'intelligence artificielle comprennent :

- Les systèmes experts,
- Le traitement du langage naturel,
- La compréhension de la parole,
- La robotique et les systèmes sensoriels,
- La vision par ordinateur et la reconnaissance des scènes,
- L'enseignement informatique intelligent,
- La computation neuronale.

Parmi ces technologies, le système expert est une technologie en croissance rapide ayant un impact significatif sur divers aspects de la vie. Les différentes technologies appliquées dans l'intelligence artificielle incluent le réseau neuronal, la logique floue, le calcul évolutif, et l'intelligence artificielle hybride.

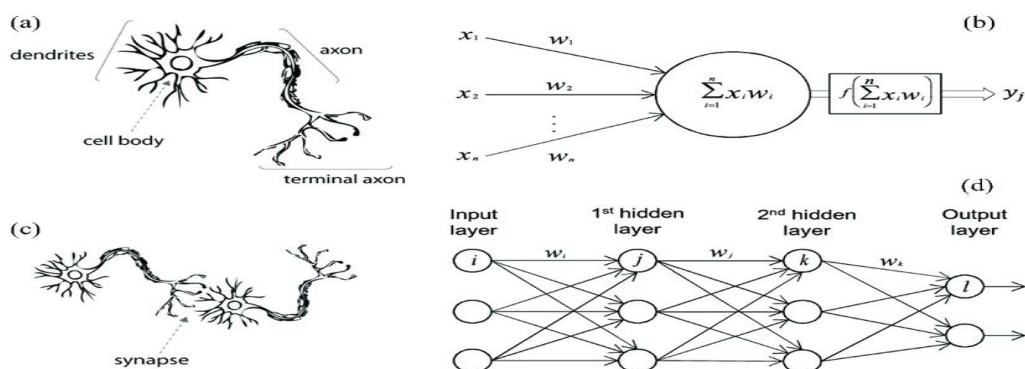


Figure 2 : Réseau de Neuron Artificiel

2. Application de l'intelligence artificiel dans l'apprentissage en ligne

2.1 Avis general

L'ère de l'intelligence artificielle et des mégadonnées arrive rapidement avec l'augmentation rapide des technologies de l'informatique et des communications, apportant avec elle une nouvelle ère éducative. L'enseignement mobile et le fractionnement de l'enseignement deviennent de nouvelles tendances. De plus, l'intelligence artificielle et les technologies de réseaux mobiles en éducation sont un domaine de recherche brûlant. Cependant, de nombreux problèmes scientifiques et techniques restent à résoudre. La question de la technologie de l'information basée sur l'éducation avec les réseaux mobiles est une question majeure à résoudre. De plus, la nouvelle génération de réseaux mobiles et de technologies de l'information en éducation est désormais un domaine de recherche important.

Avec les coûts de l'enseignement supérieur qui continuent d'augmenter, les étudiants sont de plus en plus confrontés au défi de choisir une spécialité et une institution accréditée qui offrent une éducation de qualité et un succès futur. Les individus de la génération Y et les adultes recherchent des programmes sur le campus et des cours à temps plein, tandis que les universités cherchent des méthodes d'apprentissage non traditionnelles. Les programmes traditionnels à temps plein sur le campus sont exigeants, et les moments économiques difficiles nécessitent des individus actifs

travaillant dans diverses institutions pour continuer à gagner leur vie. Les programmes à distance ont commencé dans les années 1980, mais l'innovation et l'expansion du contenu ont rendu les programmes éducatifs en ligne plus compétitifs pour les étudiants. Actuellement, les étudiants peuvent s'inscrire à des programmes de licence ou de master dans diverses institutions éducatives et compléter le programme depuis chez eux. Plus important encore, les programmes virtuels ou l'apprentissage en ligne offrent une réduction des frais de scolarité de 25 à 50 pour cent.

Georgia Tech est une université publique qui a contribué à la démocratisation de l'éducation en étendant divers cours au-delà des salles de classe physiques. Le nombre d'étudiants inscrits aux cours en ligne augmente chaque année. Il est prévu que dans 20 ans, 25 pour cent des universités pourraient échouer à maintenir les salles de classe traditionnelles en raison des coûts élevés et du faible nombre d'inscriptions. L'intelligence artificielle va complètement transformer l'apprentissage en ligne car elle améliorera ou modifiera les techniques d'enseignement actuelles. Par exemple, l'utilisation de Seeing AI pour enseigner aux étudiants aveugles. Actuellement, le modèle d'enseignement suppose que les enseignants/professeurs sont "la source du savoir et l'étudiant est le récepteur". L'utilisation de l'intelligence artificielle aidera l'enseignant à éliminer

les tâches chronophages comme donner des conférences, une activité répétitive, leur permettant ainsi de se concentrer sur des tâches de plus grande valeur. Un exemple concret d'intelligence artificielle dans l'apprentissage en ligne est l'utilisation d'un système de gestion de l'apprentissage qui fournit une réponse immédiate lorsque l'étudiant pose une question.

Pour l'étudiant qui n'apprécie pas les sessions de classe normales, l'intelligence artificielle peut être utilisée dans les systèmes de gestion de l'apprentissage (LMS) pour répondre aux différents aspects de l'apprentissage, qu'ils soient visuels, auditifs ou textuels, en fournissant un contenu efficace selon la méthode d'apprentissage préférée. La plateforme peut diviser les conférences ou les tâches de lecture en composants plus petits que les apprenants peuvent comprendre. Il convient de noter que les étudiants internationaux cherchant à obtenir une éducation dans différentes institutions à travers le monde peuvent rencontrer une barrière linguistique, compliquant leur progression éducative. L'intelligence artificielle aidera ces étudiants en traduisant les textes pour qu'ils puissent les comprendre ou les traduire dans leur langue maternelle. Le graphique ci-dessus montre les systèmes de gestion de l'apprentissage basés sur l'intelligence artificielle.

2.2 Système de gestion de l'apprentissage (LMS)

Le système de gestion de l'apprentissage à distance est une forme tangible de l'utilisation de l'Internet, qui utilise des médias électroniques et est connu sous le nom d'apprentissage en ligne. L'apprentissage en ligne fait partie du domaine de la vie électronique, qui est une technologie liée au cycle de vie. Basé sur l'électronique, la vie électronique permet aux humains de mener des activités quotidiennes grâce à l'aide de la technologie. Parmi les options médiatiques électroniques disponibles figurent l'Internet, les satellites ou les CD-ROM. Grâce à l'apprentissage en ligne, l'éducation peut être offerte simultanément ou à des moments différents.

Elliot Masie, Cisco Systems et Cornelia (2000) affirment que l'apprentissage en ligne est un type d'apprentissage qui peut transmettre des matériaux via des médias électroniques : Internet, intranet, satellites, télévision. Martin Jenkins et Janet Hanson (2003) considèrent que l'apprentissage en ligne est un processus d'apprentissage facilité par l'utilisation des technologies de l'information et des communications pour créer des compétences qui ne sont pas obtenues grâce aux modèles d'apprentissage traditionnels .

Le système de gestion de l'apprentissage (LMS) aidera à suivre les performances des individus, à s'inscrire à un cours en ligne et à communiquer avec le système en cas de besoin d'aide. Le problème étudié est de savoir si l'intelligence artificielle dans l'apprentissage en ligne améliorera la qualité de l'éducation offerte dans diverses universités. Une éducation de qualité dans des institutions de haut niveau signifie que les apprenants seront innovants et créatifs. Lorsque l'étudiant ne comprend pas le contenu du cours et son impact dans l'environnement de travail, cela signifie que l'innovation et la créativité ne sont pas réalisées. Les institutions resteront dans le statu quo tandis que d'autres pays progresseront technologiquement. Par conséquent, l'intelligence artificielle doit être intégrée dans les cours d'enseignement supérieur pour pouvoir traduire les informations et garantir que l'étudiant comprend le résultat du cours. Les apprenants échouent parce qu'ils ne savent pas ce qui est testé ; il est donc nécessaire d'introduire

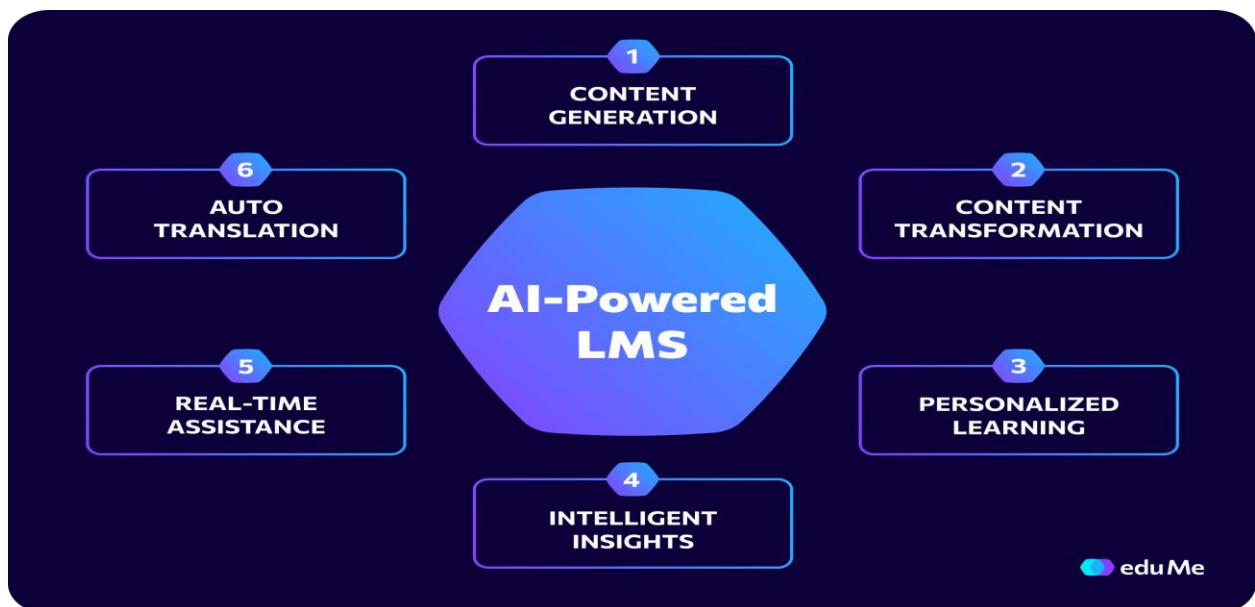


Figure 3 : Learning Management System

3. MODÈLE D'APPRENTISSAGE PERSONNALISÉ : EXIGENCES ET DÉFIS

3.1 EXIGENCES

Un système d'apprentissage personnalisé a les exigences fondamentales suivantes :

- **Adaptabilité** : L'adaptabilité se réfère à la capacité d'enseigner en fonction du niveau de chaque apprenant. Un système d'apprentissage personnalisé doit être adaptatif pour fournir un contenu personnalisé en fonction du niveau de chaque apprenant .
- **Flexibilité** : La flexibilité implique de fournir des contenus selon le mode préféré de l'apprenant. Cela nécessite que le contenu éducatif soit développé en utilisant différents modes d'apprentissage. Par exemple, les apprenants peuvent être enseignés en utilisant des jeux, des vidéos et des lectures à haute voix. Ils peuvent avoir des préférences et des goûts différents pour chaque mode . L'étendue de la modalité peut être encore divisée en environnements, arrière-plans, couleurs et objets utilisés dans le mode d'apprentissage. Par exemple, un environnement d'apprentissage spécifique au genre peut être utile pour améliorer l'apprentissage .
- **Évaluations continues** : Les évaluations périodiques sont une partie intégrante d'un système d'apprentissage personnalisé. Cela permet au système d'évaluer les attributs d'adaptabilité et de flexibilité. Un système d'apprentissage personnalisé doit disposer d'un large corpus d'évaluations, capable de répondre aux besoins d'adaptabilité et de flexibilité .
- **Collecte et récupération de données robustes et continues** : Les caractéristiques intrinsèques d'adaptabilité et de flexibilité nécessitent une collecte de données robuste et continue. En plus des résultats des évaluations des apprenants, d'autres attributs tels que les modèles d'utilisation et les tendances d'apprentissage peuvent également être importants pour déterminer les similitudes entre les apprenants .
- **Recommandation utilisant l'adaptabilité et la flexibilité** : Recommander des contenus efficaces est intrinsèque à l'apprentissage personnalisé. Cela est réalisé à l'aide d'un moteur basé sur l'IA, qui calcule des recommandations personnalisées en fonction des évaluations

et des données d'utilisation de l'apprenant. Ces recommandations doivent être continuellement mises à jour afin d'améliorer l'expérience de l'apprenant .

- Évaluation des recommandations utilisant le traçage des connaissances : Un système d'apprentissage personnalisé recommande un contenu personnalisé à chaque apprenant. Cependant, cette recommandation doit également être testée et évaluée afin d'évaluer la performance du système et d'identifier les mesures d'amélioration .

3.2 DEFITS

Les exigences mentionnées ci-dessus ont identifié divers défis liés au développement d'un cadre d'apprentissage électronique personnalisé et adaptable :

- Identification et collecte des caractéristiques : Un système d'apprentissage personnalisé recommande du contenu sur la base de caractéristiques. Cependant, l'identification du bon ensemble de caractéristiques est un défi. Par exemple, des questions telles que quels objets, thèmes ou couleurs dans un jeu sont utiles pour enseigner un concept spécifique à des apprenants d'un groupe d'âge et de sexe spécifiques . Cette question nécessite l'identification du bon ensemble de caractéristiques ainsi qu'un processus étendu pour collecter les attributs corrects afin d'identifier la relation appropriée .
- Contenus adaptables : Le système d'apprentissage en ligne doit contenir du contenu pédagogique sur un sujet particulier dans plusieurs modalités. La fourniture de contenu dans plusieurs modalités répondra aux besoins des apprenants . Un système d'apprentissage personnalisé exige que des contenus adaptables soient fournis à chaque apprenant. La génération et la fourniture de contenus adaptables est un défi . Cela nécessite que du contenu personnalisé soit généré sur la base d'un ensemble approprié de caractéristiques afin que l'apprentissage puisse être amélioré. Un mécanisme efficace est nécessaire à cet égard, capable d'incorporer le bon ensemble de caractéristiques pour générer des contenus en utilisant plusieurs modalités.
- Suivi des connaissances : Un système éducatif personnalisé exige que le niveau de compréhension de l'apprenant soit suivi de manière à ce que les concepts non compris par l'apprenant soient clairement identifiés. Il existe des défis dans l'identification et le suivi du niveau de l'apprenant. Cela se fait par le biais d'évaluations. Cependant, concevoir des évaluations et les mapper à des concepts est une tâche étendue. En ce sens, une réponse incorrecte à une évaluation peut être liée à un manque de connaissances dans plusieurs concepts. De même, une réponse correcte à un élément

d'évaluation ne signifie pas nécessairement que tous les concepts de connaissance ont été complètement compris.

- Évaluations continues et collecte de données : Un système éducatif personnalisé repose sur les résultats des évaluations, les journaux des utilisateurs et les ensembles de données de modalités pour répondre aux exigences de l'apprentissage adaptatif et adaptable. Cependant, comme ces résultats changent continuellement, identifier et utiliser le bon intervalle pour le calcul des résultats n'est pas trivial. Cela peut également varier selon les apprenants.
- Élicitation des préférences des apprenants : L'élicitation des préférences d'un apprenant pour un certain mode de contenu pédagogique est une tâche difficile. Nous recommandons d'élucider les préférences des apprenants en utilisant des techniques de collecte de données explicites et implicites. De préférence, un test diagnostique devrait être présenté à un apprenant. Ce test peut consister en un contenu de différentes modalités et une évaluation pour chaque modalité. Par exemple, nous pouvons concevoir le test pour présenter d'abord un texte sur le théorème de Pythagore puis effectuer une évaluation par la suite. Nous pratiquons la même chose avec la vidéo et d'autres modalités de contenu disponibles. L'évaluation fournira une mesure explicite de la performance de l'apprenant sur une modalité. Nous analysons ensuite le comportement de l'apprenant lorsqu'il interagit avec le contenu pédagogique d'une modalité spécifique. Cette analyse peut inclure le temps d'engagement, l'activité des apprenants et d'autres mesures connexes. Ces mesures sont des caractéristiques de données implicites pour identifier les préférences des apprenants.
- Mise à jour des préférences des apprenants : Avec l'acquisition des connaissances, les préférences des apprenants peuvent également changer. Au début, un apprenant peut préférer des leçons vidéo et animées pour les concepts introductifs de base, puis vouloir des explications textuelles plus détaillées pour les concepts avancés. Pour résoudre ce problème, le modèle d'apprenant doit être mis à jour avec un nouvel ensemble de données d'entraînement extraites en utilisant des techniques de collecte de données explicites et implicites.
- Ingénierie des caractéristiques des interactions apprenant-**contenu** : Les données des interactions apprenant-contenu sous leur forme de base ne révèlent pas de modèles. Nous devons effectuer une ingénierie des caractéristiques sur les données d'interactions brutes pour trouver des modèles significatifs . Pour modéliser la détection de la modalité préférée comme un problème d'apprentissage automatique, il est nécessaire d'extraire des signaux comportementaux de l'apprenant à partir des données. Ces signaux serviront de proxy pour les paramètres psychologiques nécessaires à la modélisation de la modalité préférée d'un apprenant. Par exemple, un apprenant qui parcourt rapidement une leçon ne se concentre pas correctement sur le matériel pédagogique. En extrayant des caractéristiques telles que les mouvements de défilement et de curseur, nous pouvons identifier l'attention de l'apprenant dans

l'activité d'apprentissage. Concevoir de telles caractéristiques aide grandement à modéliser le comportement et les préférences des apprenants .

- Évaluation de la modalité préférée détectée : L'évaluation de la modalité préférée détectée est un composant important du modèle d'apprentissage adaptable global. La précision de ce modèle définira l'expérience et la performance de l'apprenant. Une modalité détectée incorrectement et une recommandation de contenu ultérieure entraveront la performance de l'apprenant et celui-ci pourrait avoir des difficultés à comprendre les leçons .

Chapitre 2 : Généralité sur la sécurité

1. Introduction

Les organisations prennent de plus en plus conscience de l'importance des informations et des technologies associées dans la plupart des fonctions, en particulier pour stimuler l'innovation et générer un avantage concurrentiel. Les services d'information et de technologie des entreprises sont vulnérables à divers risques de sécurité dans l'environnement informationnel actuel, notamment la fuite de données sensibles et les interruptions prolongées de l'accès aux courriels et à Internet, ce qui affecte considérablement la continuité des activités. Une organisation doit mettre en œuvre une stratégie de sécurité de l'information en établissant un cadre complet permettant de développer, d'institutionnaliser, d'évaluer et d'améliorer un programme de sécurité de l'information pour faire face à ces risques de sécurité. En particulier, la stratégie de sécurité de l'information doit soutenir les plans stratégiques globaux de l'organisation, avec un contenu traçable jusqu'à ces sources de haut niveau.

Bien que la plupart des organisations utilisent des mesures de sécurité "de base", le nombre d'incidents de sécurité augmente. Selon des recherches, plus de 60 % des entreprises utilisent des contre-mesures techniques de sécurité de l'information telles que les logiciels antivirus, les pare-

feux, les logiciels anti-espions, les réseaux privés virtuels (VPN), la gestion des vulnérabilités/patchs, le cryptage des données en transit et les systèmes de détection d'intrusion. Les rapports indiquent également que les organisations sont continuellement soumises à des attaques ciblées. Ces mêmes études montrent également que le risque de sécurité augmente en raison de la montée des menaces internes et externes. En conséquence, la gestion de la sécurité devient de plus en plus difficile. Les entreprises doivent utiliser des stratégies pour orienter leurs efforts de sécurité et tirer le meilleur parti de leurs ressources limitées dans cet environnement. Cependant, un seul système peut ne pas être suffisant.

Certains affirment que pour garantir l'efficacité des mesures de sécurité et maintenir les politiques de sécurité, les entreprises devraient employer plusieurs stratégies de sécurité de l'information. Une grande partie de la littérature se concentre sur les aspects opérationnels de la sécurité de l'information, en particulier les contrôles de sécurité et leur mise en œuvre pour "prévenir" les attaques de sécurité contre les entreprises. Cependant, en plus de la prévention, plusieurs stratégies de sécurité ont été conceptualisées dans la littérature, notamment la détection, la dissuasion et la déception. Il y a eu peu de recherches sur le terrain pour déterminer quelles stratégies de sécurité les organisations utilisent pour faire face à divers risques de sécurité et comment elles sont mises en œuvre. Les risques de sécurité des entreprises ont été principalement ignorés par les gestionnaires de sécurité. En général, les plans ont été mis en œuvre de manière ad hoc plutôt que dans le cadre d'une approche planifiée et systématique de gestion des risques.

2. Revue sur les politiques et stratégies de sécurité

La stratégie est généralement définie comme la détermination des moyens à utiliser, comment les utiliser et comment les appliquer. Beckman et Rosenfield (2008) décrivent la stratégie comme "déterminer où votre entreprise veut aller et découvrir comment y parvenir". Ces définitions peuvent être utilisées pour élaborer une stratégie de sécurité de l'information. Selon ces points de vue, la stratégie de sécurité de l'information, selon Perk et al., est "l'art de décider comment utiliser au mieux les technologies et mesures de sécurité de l'information appropriées, et de les déployer et les appliquer de manière coordonnée pour défendre les infrastructures d'information de l'organisation contre les menaces internes et externes en offrant la confidentialité, l'intégrité et la disponibilité au moindre effort et coût tout en restant efficace." Des méthodes telles que la dissuasion, la prévention, la surveillance, la détection, la réponse, la déception, la défense périmétrique, la compartimentation et la stratification ont été découvertes par la recherche. Deux éléments clés des stratégies ont émergé de la revue de la littérature : le temps et l'espace. Les stratégies peuvent être mises en œuvre avant une attaque ou après qu'elle ait eu lieu. Du point de

vue spatial, la conception de l'environnement "de bataille" est essentielle. Diviser le champ de bataille en zones pour séparer les systèmes informatiques de confiance et non fiables, par exemple, peut empêcher un système informatique non fiable d'infiltrer une zone de confiance. Enfin, le choix de stratégies d'attaque et de réponse spécifiques influence la stratégie du point de vue de la prise de décision. Les sections suivantes définissent et décrivent l'approche basée sur la politique de sécurité.

2.1. Prévention (PREV)

La prévention vise à empêcher l'accès illégal, la modification, la destruction ou la divulgation des actifs informationnels. Lorsqu'on aborde les politiques de sécurité de l'information d'un point de vue purement préventif, cela implique que l'entreprise a une tolérance minimale envers tout impact ; par conséquent, des mesures doivent être déployées pour prévenir toutes les attaques contre l'organisation. Les fuites d'informations peuvent être évitées grâce à des techniques de prévention. Par exemple, une politique de bureau propre, imposée par des inspections régulières des documents manquants ou confidentiels, peut être utile. Des barrières peuvent être érigées autour des actifs importants avant une attaque sur le plan technologique. La documentation est une mesure préventive courante visant à restreindre l'accès aux utilisateurs autorisés. Utilisez des logiciels qui régulent l'interaction des utilisateurs avec les actifs informationnels, et cryptez les informations qui circulent sur les réseaux pour éviter les fuites - même si le réseau est compromis. Utilisez des pare-feu pour filtrer le trafic réseau, et des systèmes de détection d'intrusion qui utilisent des modèles de détection des anomalies et des signatures pour identifier les données suspectes sont également des techniques préventives. L'importance des systèmes de balayage des vulnérabilités et de leur correction est également à noter.



2.2.

Figure 4 : Prevention

Dissuasion (DETER)

La dissuasion est utilisée pour influencer le comportement et les attitudes des personnes. L'efficacité de la dissuasion dans les organisations est déterminée par deux facteurs critiques : la confiance dans les sanctions et leur sévérité, influencés par plusieurs facteurs secondaires critiques. La confiance dans les sanctions (c'est-à-dire la probabilité d'attraper les contrevenants) est déterminée par le degré de connaissance du type de sanction et l'efficacité des organismes chargés de l'application à identifier les comportements contraires. L'étendue des sanctions pouvant être appliquées affecte la sévérité des sanctions. La dissuasion a été utilisée pour décrire la discipline des travailleurs qui ne respectent pas les politiques de sécurité dans les politiques de sécurité, étant l'un des points focaux critiques de la dissuasion. Les organisations devraient mettre en place un programme d'éducation et de formation pour informer les employés sur les politiques et les normes organisationnelles, selon Straub et Welke (1998), pour rendre les activités de sécurité de l'information plus réussies. Les tactiques de dissuasion, telles que la sévérité des sanctions, la connaissance des activités de dissuasion et le nombre de personnes impliquées dans la sécurité, ont prouvé leur efficacité à réduire les abus informatiques, selon Straub (1990). D'autres ont découvert que les tactiques de dissuasion améliorent la sécurité de l'information, bien que la sévérité des sanctions n'affecte pas beaucoup l'efficacité (Kankanhalli et al., 2003). D'autres recherches récentes ont montré que la sévérité des sanctions a un impact significatif sur la quantité d'abus, contrairement aux résultats de Kankanhalli et al. (2003). Les organisations doivent renforcer la formation à la conformité aux politiques de sécurité et resserrer la surveillance des violations de politiques.

2.3. Détection (DETECT)

La détection est une méthode opérationnelle de bas niveau pour détecter des activités de sécurité spécifiques. L'objectif de la détection est de permettre à l'organisation de réagir de manière ciblée. En revanche, la surveillance cherche à obtenir une compréhension globale de la situation. Ainsi, la détection se concentre sur un seul incident, tandis que la surveillance surveille la situation dans son ensemble. Identifier les comportements nuisibles ou étranges, les intrusions ou les usages abusifs, et les attaques spécifiques contre les serveurs web sont tous des exemples de détection. La détection peut également être utilisée pour recueillir des preuves d'abus et d'activités suspectes, ainsi que pour identifier les coupables. Les dispositifs spécialisés de détection des intrusions informatiques et réseau, les scanners de réseau, les scanners de système, les détecteurs d'abus et d'anomalies, les logiciels de filtrage de contenu et antivirus, ainsi que les programmes d'audit sont les technologies de sécurité utilisées dans l'approche de détection.

Depuis ses débuts, la technologie de l'information et des communications a transformé la création de valeur économique en permettant aux entreprises de transférer leur dépendance aux actifs tangibles et à l'argent vers le capital intellectuel. En conséquence, la plupart des marchés dépendent désormais de ce que Kuehl (2009) appelle le "premier domaine fabriqué par l'homme". Parmi les avantages de l'exploitation du domaine cybernétique figure la capacité unique des entreprises à tirer parti de l'absence relative de restrictions temporelles et géographiques comme facilitateur de modèles commerciaux uniques. Cependant, l'ampleur de la vulnérabilité impliquée par cette dépendance devient une conséquence secondaire de plus en plus importante. Les risques cybernétiques peuvent compromettre la sécurité, la stabilité et la viabilité à long terme d'une organisation en compromettant la confidentialité, l'intégrité et la disponibilité du capital informationnel et structurel. Des exemples de cette perturbation potentielle et de ses externalités vont de l'effondrement organisationnel à l'incapacité des infrastructures des États-nations. En raison de leur double fonction de créateurs de technologie et de facilitateurs de son utilisation, les organisations continuent de se présenter comme des vecteurs d'action critiques même lorsqu'elles discutent des impacts sociétaux de la sécurité de l'information. De manière surprenante, la plupart des modèles commerciaux considèrent la sécurité de l'information comme une responsabilité secondaire car elle offre peu de possibilités de monétisation et de création de valeur - la raison d'être de l'organisation. La stratégie de sécurité de l'information repose sur un scénario de "guerre" symbolique auto-perpétuelle qui, contrairement aux "batailles" individuelles, ne peut être gagnée de manière concluante. En d'autres termes, la sécurité de l'information n'est pas une question qui peut être "résolue". De plus, la gestion de la sécurité de l'information révèle un noyau épistémique similaire à d'autres efforts stratégiques. La sécurité de l'information, l'expertise et le capital intellectuel sont des éléments essentiels du succès commercial. De différentes manières, le concept de "connaissance" imprègne la sécurité de l'information et les récits de risques

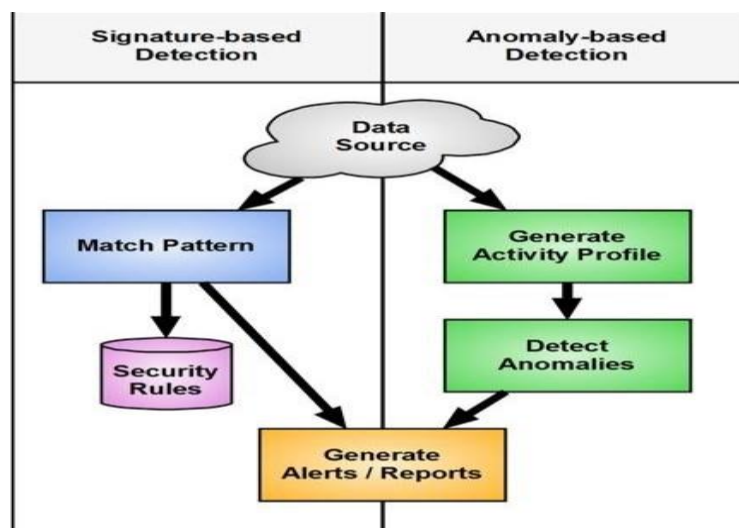


Figure 5 : Detection

organisationnels. Neef (2005) affirme que la capacité d'une organisation à gérer les risques avec succès repose sur sa capacité à gérer les connaissances pertinentes.

3. SECURISE LES PLATEFORMES D'APPRENTISSAGE EN LIGNE

3.1 Aperçu général

Les plateformes d'apprentissage en ligne sont devenues des outils essentiels pour l'enseignement supérieur, notamment dans le contexte de la pandémie de COVID 19. Nous savons tous à quel point le domaine du e-learning est immense. Statista prédit que le marché mondial de l'apprentissage en ligne atteindra près de 400 milliards de dollars d'ici 2026. Cette croissance et cette popularité ouvrent la voie à une nouvelle vague de défis en matière de cybersécurité. Les établissements d'enseignement doivent savoir que même s'il est nécessaire de dépenser beaucoup d'argent pour créer un portail fiable et convivial pour les apprenants, il est tout aussi important de prendre des mesures appropriées pour protéger leurs plateformes éducatives en ligne, faute de quoi elles pourraient présenter des risques de sécurité importants pour les apprenants et les apprenants. enseignants, tels que les failles de sécurité, les données, le vol d'identité, les cyberattaques et la fraude académique. La gestion de la sécurité des systèmes d'apprentissage en ligne et le contrôle d'accès attirent de plus en plus l'attention des chercheurs et des développeurs d'applications Web. Répondre aux exigences de sécurité dans un système d'apprentissage en ligne est une question très complexe car il est nécessaire de protéger le contenu, les services et les données personnelles non seulement des utilisateurs externes, mais également des utilisateurs internes, y compris les administrateurs système.

3.2 Exigences de sécurité de base et problèmes de sécurité les plus importants

3.2.1 Exigences de sécurité de base

Les aspects de sécurité de base suivants des plateformes d'apprentissage en ligne doivent être respectés : authentification, contrôle d'accès, confidentialité, intégrité, disponibilité et non-répudiation.

3.2.2 Les problèmes de sécurité les plus importants pour l'e-learning

Voici les problèmes de sécurité les plus courants sur les plateformes d'apprentissage en ligne :

- Scripts intersites (ou XSS)
- Injection directe de code SQL dans la page Web.
- Injection à distance à l'aide d'un fichier de virus/cheval de Troie ;
- Injection SQL dans l'URL (SQL URL injection) ;
- Effectuer diverses recherches à l'aide des moteurs de recherche pour récupérer des informations personnelles sur le site : mot de passe, nom d'utilisateur.
- Crackage de mots de passe à l'aide de systèmes de décryptage.
- L'indexation d'un site Web ne doit pas révéler de fonctionnalités de sécurité telles que des scripts, une connexion à l'adresse d'une base de données, etc.

Les plus courantes, que nous détaillerons un peu plus, sont :

3.2.2.1 Scripts intersites (xss)

Devinez l'ID de session du site (prédiction de session). Le cross-site scripting (ou XSS) est l'une des attaques Web les plus courantes au niveau des applications. XSS cible généralement les scripts sur la page qui s'exécutent côté client (dans le navigateur Web de l'utilisateur) plutôt que côté serveur (voir Figure 6).



Figure 6 : Cross-Site Scripting

XSS lui-même est une menace résultant de vulnérabilités de sécurité Internet côté client. Les langages de script, HTML et JavaScript sont les principales raisons de cette prouesse. Le concept de XSS est de manipuler les scripts côté client d'une application Web pour les exécuter comme le souhaite un utilisateur malveillant. Comme la gamification, un script peut être intégré dans une page qui peut ensuite être exécuté à chaque fois que la page est chargée, ou à chaque fois qu'un événement associé est exécuté. Une attaque XSS peut être utilisée pour obtenir les résultats malveillants suivants :

- Accès à des informations sensibles.

- Vol d'identité; •

Modifier les fonctions du navigateur.

- Dégradation des applications Web.

• Attaques par déni de service. Pour prévenir une telle attaque, le concepteur de la plateforme e-learning peut prendre les mesures suivantes :

- Assurez-vous que les pages du site Web n'affichent les entrées de l'utilisateur qu'après avoir été validées pour tout code malveillant.

- Ne faites pas entièrement confiance aux sites Web qui utilisent HTTPS (Secure Sockets Layer) en ce qui concerne XSS ; HTTPS garantit des connexions sécurisées, mais le traitement des données saisies par l'utilisateur est interne à l'application. Si une application contient des vulnérabilités XSS, un attaquant peut envoyer un script malveillant qui peut toujours être exécuté par l'application et conduire à des intrusions XSS ;

- Convertissez tous les caractères non alphanumériques en entités de caractères HTML avant d'afficher les entrées utilisateur dans les moteurs de recherche et les forums.

- Utilisez largement les outils de test pendant la phase de conception pour éliminer ces vulnérabilités XSS dans votre application eLearning avant sa mise en ligne.

3.2.2.2 Injection SQL

L'injection SQL est un type d'attaque relativement simple et peut être évitée en respectant strictement certains codes de base. Applications. Grâce à cette méthode, un pirate informatique peut transmettre une chaîne d'entrée à une application dans l'espoir d'obtenir un accès non autorisé à la base de données. Les pirates injectent des requêtes ou des caractères SQL dans l'application Web pour effectuer une action inattendue qui peut alors agir de manière malveillante (voir Figure 7).



Figure 7 : SQL injection

De telles demandes peuvent conduire à un accès non autorisé aux données, à un contournement de l'authentification ou à l'arrêt de la base de données, même si elles se trouvent sur le même serveur Web ou sur un serveur distinct. Les moyens les plus courants d'éviter ce type de vulnérabilités sont :

- Vérifiez les saisies utilisateur pour détecter les caractères dangereux tels que les guillemets simples.
- Utilisez des instructions préparées, qui indiquent exactement à la base de données à quoi s'attendre avant de lui transmettre les données fournies par l'utilisateur.
- Chiffrez les données sensibles.
- Assurez-vous que les messages d'erreur ne révèlent rien sur la structure interne de l'application ou de la base de données. L'injection SQL peut également être appliquée aux URL, qu'un attaquant peut modifier pour accéder à des informations importantes. Pour éviter cela, il est recommandé d'éviter d'envoyer des informations importantes dans l'URL. Les sessions permettent d'enregistrer l'état et les variables spécifiques à l'utilisateur dans les requêtes de page ultérieures. Ceci est réalisé en transmettant une valeur d'identité unique et difficile à deviner (ID de session) au navigateur (soit dans un cookie, soit dans un cookie). URL) que le navigateur envoie à chaque nouvelle 6 requête (Przemek, 2007). La session reste active tant que le navigateur continue d'envoyer l'identifiant à chaque nouvelle requête. La prédiction de session consiste à deviner un identifiant de session valide à l'aide de divers outils et méthodes (par exemple, la technique de la force brute). L'attaque est possible lorsque l'ID de session est faiblement codé, trop court ou défini de manière séquentielle. Les sessions non expirantes sur un serveur HTTP peuvent permettre à un attaquant d'accéder à des données illimitées. Pour éviter les problèmes liés à la sécurité des sessions, vous devez suivre ces bonnes pratiques :
 - L'ID de session doit être suffisamment long et imprévisible.
 - Vérifiez si l'ID de session est valide ou non.
 - Vérifiez si l'ID de session a été généré par l'application (et non saisi manuellement par l'utilisateur) ;
 - Régénérez l'ID de session après une certaine période de temps ou lorsque le niveau de privilège de l'utilisateur change.
 - Utilisez des cookies uniquement pour publier l'identifiant de session.
 - Évitez l'option « se souvenir de moi » (contacts permanents) ;

- La session se termine en raison d'une erreur de sécurité.
- La session se termine après une période d'inactivité. Supprimer le cookie de session lorsque la session est détruite

3.3 Sécurité de la plateforme e-learning

Pour protéger la plateforme éducative, des politiques de sécurité doivent être mises en œuvre en fonction de :

Utilisez des méthodes d'authentification fortes

L'une des étapes les plus fondamentales et les plus importantes pour sécuriser votre plateforme d'apprentissage en ligne consiste à utiliser des méthodes d'authentification fortes pour les apprenants et les enseignants. Cela signifie avoir besoin de mots de passe forts, les changer régulièrement et utiliser l'authentification multifacteur (MFA) autant que possible. MFA ajoute une couche de sécurité supplémentaire en obligeant les utilisateurs à vérifier leur identité à l'aide d'un appareil ou d'un autre code, ainsi que leur mot de passe. De cette façon, même si quelqu'un vole ou devine votre mot de passe, il ne pourra pas accéder à votre plateforme d'apprentissage en ligne sans le deuxième facteur.

Installer un certificat SSL

Pour une sécurité optimale, il serait préférable de crypter toutes les communications effectuées sur votre portail e-learning. Vous devez acheter et installer SSL sur votre portail pour ce rôle. Un certificat SSL est un protocole de cryptage qui sécurise les communications entre les serveurs Web et les utilisateurs. Toutes les données transmises entre les navigateurs des étudiants (ou d'autres employés) et les serveurs du système scolaire seront cryptées. Le cryptage signifie que même si des pirates informatiques accèdent aux fichiers, ils ne pourront pas lire la connexion. La seule personne capable de lire et de décrypter les données collectées dans le tunnel de chiffrement de bout en bout est le détenteur des clés de décryptage. Tout ce dont vous avez besoin pour obtenir ces niveaux de cryptage est un certificat SSL. Vous pouvez choisir différents types de certificats SSL pour sécuriser votre plateforme en ligne. La certification que vous choisissez dépend entièrement des besoins de votre site Web.

Cryptez et sauvegardez vos données

Une autre étape clé pour sécuriser votre plateforme eLearning consiste à chiffrer et à sauvegarder vos données. Le cryptage est le processus de conversion de vos données en un code qui ne peut être déchiffré que par des personnes autorisées. Cela empêche les pirates d'accéder à vos données ou de les altérer, même s'ils parviennent à compromettre votre réseau ou votre appareil. La sauvegarde est le processus de création de copies de vos données et de leur stockage dans un emplacement distinct, tel qu'un service cloud ou un disque dur externe. Cela garantit que vous pouvez récupérer vos données en cas de sinistre, tel qu'une attaque de ransomware, une panne matérielle ou une erreur humaine.

Mettez à jour et corrigez votre logiciel

La quatrième étape essentielle pour sécuriser votre plateforme e-learning est de mettre à jour et de patcher régulièrement le logiciel. Les mises à jour et les correctifs sont des versions logicielles qui corrigent les bogues, améliorent les performances et ajoutent de nouvelles fonctionnalités. Il corrige également les vulnérabilités de sécurité que les pirates peuvent exploiter pour compromettre votre plateforme d'apprentissage en ligne. Par conséquent, vous devez toujours mettre à jour votre système d'exploitation, votre navigateur, votre logiciel antivirus, votre pare-feu et 8 votre logiciel d'apprentissage en ligne et appliquer les correctifs dès qu'ils sont disponibles. Vous devez également éviter d'utiliser des logiciels obsolètes ou non pris en charge et qui ne reçoivent plus de mises à jour de sécurité.

Utiliser un pare-feu

Vous devriez envisager d'acheter et d'installer un pare-feu pour votre portail d'apprentissage en ligne. Un pare-feu agit comme un véritable mur qui empêche le feu de se propager à certaines parties de votre site internet. Par exemple, un pare feu empêchera le trafic malveillant d'atteindre vos serveurs. De plus, lorsqu'il s'agit d'améliorer les fonctionnalités de votre plateforme en ligne, explorez les meilleures applications Shopify pour vous assurer que votre portail d'apprentissage en ligne est entièrement protégé.

Éduquez et formez vos utilisateurs

Une étape essentielle pour sécuriser votre plateforme d'apprentissage en ligne consiste à éduquer et former les utilisateurs aux meilleures pratiques en matière de cybersécurité. Les utilisateurs constituent souvent le maillon le plus faible de la chaîne de sécurité, car ils peuvent être victimes

de phishing, de logiciels malveillants, d'ingénierie sociale ou d'autres attaques susceptibles de compromettre leurs comptes ou leurs appareils.

Contrôler les rôles des utilisateurs du système de gestion de contenu

Définir les rôles des utilisateurs du CMS est un autre conseil essentiel pour une plateforme d'apprentissage en ligne sécurisée. Qui est autorisé à se connecter à la plateforme et de quel type d'accès aux systèmes informatiques les collaborateurs ont-ils besoin pour accomplir leurs tâches ? Si vous ne suivez pas cette tendance, vous devez vous préparer à des attaques internes. Saviez-vous que les menaces internes ont augmenté de 44 % ? Saviez-vous également que 55 % des organisations considèrent les utilisateurs expérimentés comme leur plus grande menace interne ? La balle est désormais dans votre camp. Soit vous définissez et limitez les privilèges des utilisateurs, soit vous êtes victime de menaces internes. C'est pourquoi la gestion des utilisateurs privilégiés est importante de nos jours.

Gestion des utilisateurs

Lorsqu'un employé quitte l'organisation ou part en congé, une procédure régulière doit être suivie pour révoquer ou restreindre ses privilèges d'accès. Une gestion efficace des utilisateurs est l'un des moyens les plus importants de sécuriser votre plateforme d'apprentissage en ligne. Outre l'attribution de rôles aux utilisateurs, il y aurait plutôt de maintenir un contrôle strict sur qui peut faire quoi. Cela contribuera à atténuer les risques posés par les anciens employés.

Contrôler l'accès aux cours

Contrôlez les appareils et les emplacements à partir desquels vos cours e-learning sont accessibles. Les cours sont automatiquement verrouillés sur les appareils des utilisateurs autorisés afin qu'ils ne puissent pas être partagés avec d'autres. Si le cours protégé est copié sur un autre appareil, il ne s'ouvrira pas. Vous pouvez éventuellement verrouiller l'utilisation à des emplacements (par exemple, un site d'entraînement physique) pour empêcher l'utilisation du BYOD en dehors des emplacements autorisés - si un cours protégé est accessible en dehors d'un emplacement autorisé, il ne sera pas ouvert et contrôlera le nombre d'appareils pouvant être utilisés. Utilisez les cours par vous-même : autorisez les utilisateurs à accéder aux cours protégés à partir d'un ou plusieurs appareils.

Contrôler la manière dont le contenu du cours est utilisé

Les contrôles de gestion des droits numériques (DRM) garantissent que le contenu de votre cours reste étroitement sous votre contrôle à tout moment. Arrêter la capture d'écran (même à partir de connexions distantes) Arrêter l'impression, autoriser l'impression ou spécifier le nombre d'impressions Faire expirer la formation après un certain nombre de jours d'utilisation, de visualisation ou d'impression, ou à une date précise Avec l'expiration, vous pouvez vous assurer que seul le contenu du cours le plus récent est accessible. Les cours peuvent expirer à des moments différents pour différents utilisateurs en modifiant les dates d'accès dans le système de gestion de la sécurité

1. Introduction

Le projet vise à améliorer l'expérience d'apprentissage en ligne des étudiants universitaires en fournissant un maximum de sécurité et de confidentialité aux utilisateurs.

L'objectif principal est de créer une plateforme d'apprentissage en ligne sécurisée qui offre aux étudiants un accès facile et privé à leur contenu éducatif. Cela facilitera le processus d'apprentissage et de recherche tout en garantissant la protection des données personnelles des utilisateurs.

L'accent est mis sur la mise en place de mécanismes de sécurité solides, tels que le cryptage avancé et des systèmes d'authentification robustes, pour prévenir tout accès non autorisé aux informations. De plus, un système de gestion des droits d'accès sophistiqué sera développé pour garantir que chaque étudiant et enseignant ne puisse accéder qu'aux ressources qui leur sont attribuées. Dans l'ensemble, ce projet vise à créer une expérience d'apprentissage en ligne sécurisée, privée et enrichissante pour les étudiants universitaires, en mettant la protection des données et la confidentialité des utilisateurs au cœur de ses préoccupations.

Voici quelques points saillants du projet :

- Plateforme d'apprentissage en ligne sécurisée : Cette plateforme offrira aux étudiants un accès sécurisé à leur contenu éducatif en ligne, ce qui augmentera l'accessibilité et la confidentialité.
- Accès aux cours et aux articles : Les étudiants auront un accès complet aux ressources éducatives disponibles, facilitant ainsi le processus d'apprentissage et de recherche.
- Protection de la confidentialité : L'accent est mis sur la garantie de la protection de la confidentialité, de sorte qu'aucun étudiant ou enseignant ne puisse accéder à ce qui ne leur est pas autorisé. Cela est très important pour établir la confiance des utilisateurs. La confidentialité peut être assurée par :

Cryptage avancé des données, Authentification à deux facteurs, Suivi de l'activité des utilisateurs.

2. Approche Proposée

Le rapport détaillé sur la méthodologie de notre projet de fin d'études vise à expliquer les méthodes de conception utilisées, à détailler le plan de travail et l'approche adoptée.

Dans ce projet, nous avons adopté un plan pour garantir la sécurité et la confidentialité des utilisateurs, basé sur deux axes principaux :

2.1 Sécurisation de la plateforme contre les attaques externes

Premièrement, nous avons utilisé des bases de données NoSQL pour éviter la vulnérabilité la plus courante des sites Web, à savoir les injections SQL. Nous avons opté pour des bases de données telles que Google Firestore, qui est une base de données NoSQL, offrant rapidité, flexibilité et facilité de développement. Elle est également robuste en termes de sécurité et offre des fonctionnalités avancées pour la gestion des données sensibles.

Deuxièmement, nous avons hébergé les fichiers du projet sur Firebase pour empêcher l'accès aux codes par des tiers non autorisés. Firebase offre également des certificats SSL gratuits pour sécuriser les connexions entre les utilisateurs et les serveurs, ainsi que des autorisations spécifiques pour chaque utilisateur.

Troisièmement, nous avons utilisé la bibliothèque JavaScript avancée React.js, connue pour sa capacité à renforcer la sécurité. React.js offre des fonctionnalités puissantes pour la sécurité et le cryptage, ce qui en fait un excellent choix pour le développement d'applications Web sécurisées et fiables.

Quatrièmement, nous avons développé un modèle d'intelligence artificielle pour détecter les intrusions et identifier les failles de sécurité.

Cinquièmement, nous avons utilisé des méthodes et des outils de sécurité bien connus tels que l'authentification et le cryptage.

2.2 Assurer la confidentialité pour sécuriser la plateforme contre les attaques internes

Premièrement, nous avons utilisé l'authentification d'identité pour limiter l'accès aux données uniquement aux utilisateurs autorisés.

Deuxièmement, nous avons défini des autorisations spécifiques pour chaque utilisateur afin de contrôler l'accès aux données.

Troisièmement, nous avons attribué un espace privé spécifique à chaque utilisateur pour restreindre l'accès aux autres.

En résumé, une stratégie complète a été suivie pour sécuriser la plateforme et protéger les données des utilisateurs contre les attaques externes et internes, en utilisant des technologies et des outils avancés dans le domaine de la sécurité et de la confidentialité.

2.3 Modèle d'IA pour la Détection des Intrusions sur une Plateforme d'Apprentissage

➤ Collecte des Données

La première étape pour développer un modèle d'IA pour la détection des intrusions consiste à collecter des données pertinentes sur les activités des utilisateurs. Ces données peuvent inclure des informations telles que les tentatives de connexion, les adresses IP, les actions effectuées, les horodatages, et les résultats des tentatives (succès ou échec). Les données doivent être recueillies de manière continue et stockées de manière sécurisée pour garantir leur intégrité et leur disponibilité pour l'analyse.

➤ Préparation des Données

Une fois les données collectées, la prochaine étape consiste à les préparer pour l'entraînement du modèle. Cela inclut le nettoyage des données pour supprimer les valeurs aberrantes ou incorrectes, la normalisation des valeurs pour assurer une distribution uniforme, et l'extraction des caractéristiques pertinentes qui aideront le modèle à identifier les schémas d'intrusion. Les caractéristiques peuvent inclure la fréquence des tentatives de connexion, les modèles d'adresse IP, les types d'actions effectuées, etc.

➤ Entraînement du Modèle

Avec des données préparées, un modèle d'IA peut être entraîné pour reconnaître les comportements d'intrusion. Les algorithmes de machine learning ou de deep learning tels que les réseaux de neurones, les arbres de décision, ou les machines à vecteurs de support (SVM) peuvent être utilisés. Le modèle est entraîné en utilisant un ensemble de données étiquetées où les comportements d'intrusion sont marqués, permettant au modèle d'apprendre à distinguer les activités normales des intrusions potentielles.

➤ **Validation et Évaluation**

Après l'entraînement, le modèle doit être validé et évalué pour s'assurer de sa précision et de sa fiabilité. Cela implique de tester le modèle avec un ensemble de données de validation distinct pour vérifier sa capacité à détecter correctement les intrusions. Les métriques d'évaluation telles que la précision, le rappel, la courbe ROC, et le score F1 sont utilisées pour mesurer les performances du modèle et ajuster les paramètres si nécessaire.

➤ **Déploiement du Modèle**

Une fois le modèle testé et validé, il peut être déployé pour une utilisation en temps réel. Le déploiement peut être effectué à l'aide de services cloud tels que Firebase Functions, permettant au modèle de s'exécuter dans un environnement évolutif et géré. Le modèle déployé analysera les nouvelles données d'activité des utilisateurs en temps réel pour détecter et alerter sur les comportements suspects.

➤ **Surveillance et Maintenance**

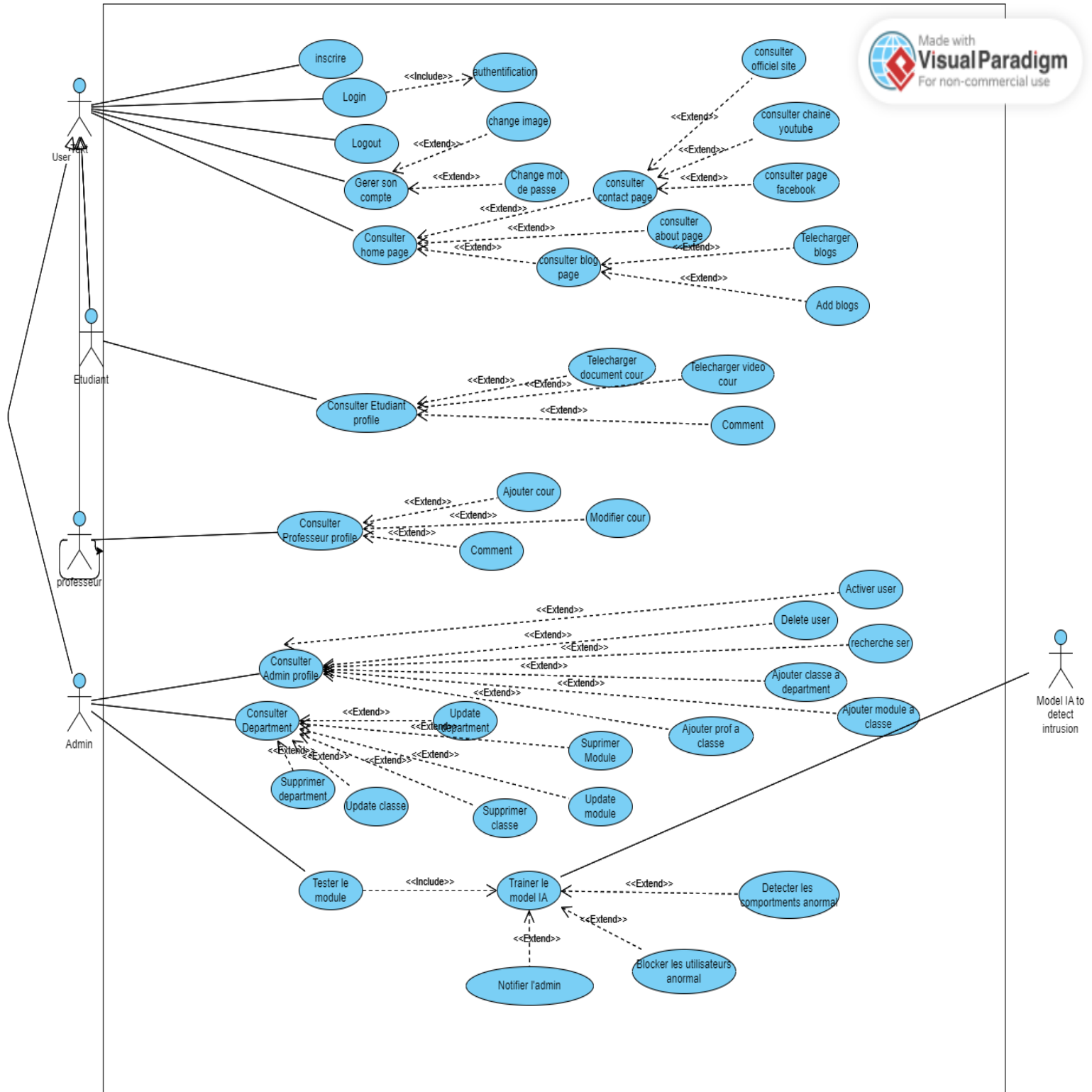
Le modèle de détection des intrusions nécessite une surveillance continue pour maintenir sa précision et son efficacité. Les données de performance doivent être régulièrement analysées, et le modèle doit être réentraîné avec de nouvelles données pour s'adapter aux nouvelles tactiques d'intrusion. La maintenance continue inclut également la mise à jour des algorithmes et l'amélioration des caractéristiques d'entrée pour répondre aux évolutions des menaces.

➤ **Conclusion**

La création d'un modèle d'IA pour la détection des intrusions sur une plateforme d'apprentissage implique une approche structurée de collecte de données, préparation des données, entraînement et validation du modèle, déploiement, et maintenance continue. En suivant ces étapes, une plateforme d'apprentissage peut être protégée efficacement contre les intrusions, garantissant la sécurité et l'intégrité des données utilisateur et des opérations de la plateforme.

Dans la partie relative aux base de donnée et au Backend, nous avons utilisé une base de donnée Nosql, voici la conception de note base de donnée :

3.1 Diagramme de cas d'utilisation



3.2 Schemas Diagramme

Il est difficile, voir impossible, de soumettre les bases de données Nosql, en particulier Firestore, aux diagrammes ou model de conception classique, en raison de la grande flexibilité dont bénéficient les bases de données firestore et de leur fonctionnement complètement différent des bases de données sql. Pour cette raison, nous avons décidé de représenter nos entités avec le (Schema diagram)

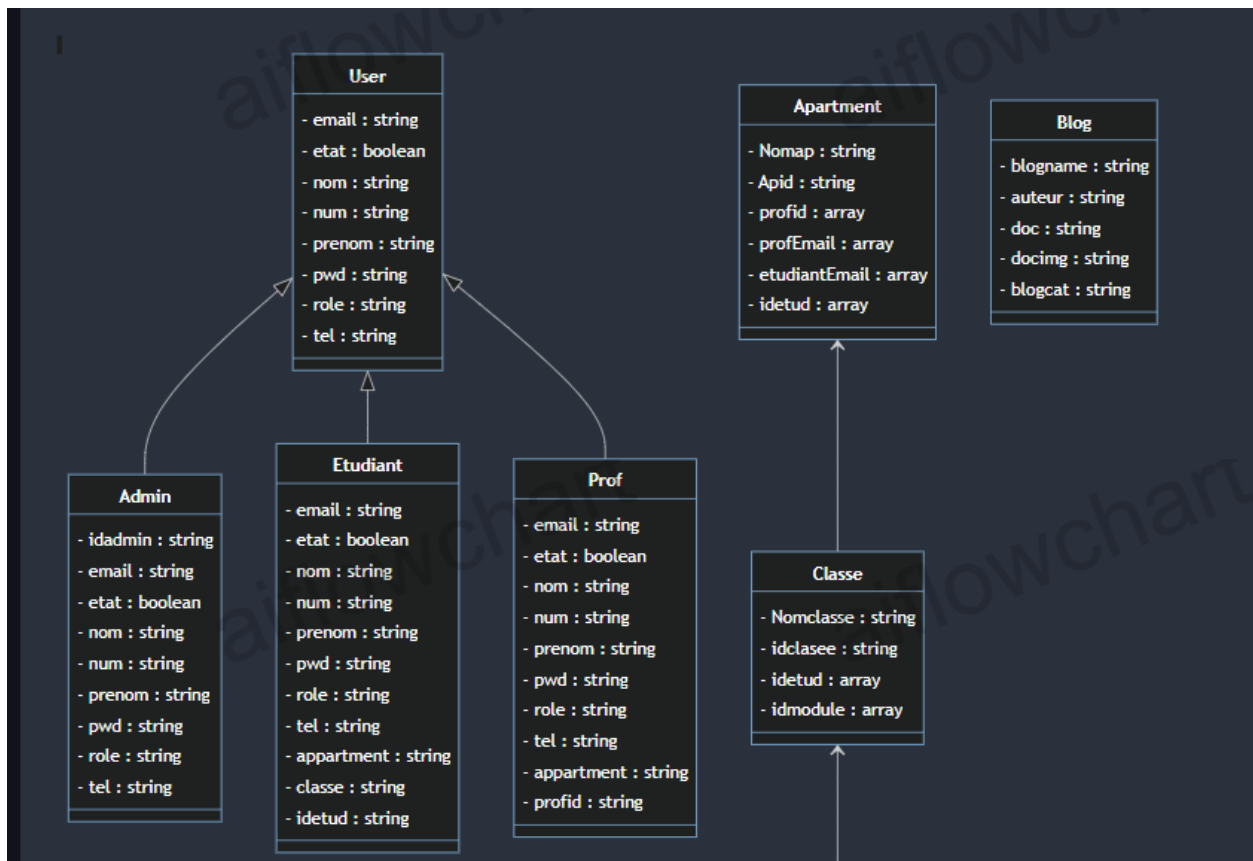




Figure 9 : Diagramme de schémas

4. Implémentation

4.1 Technologies utilisées : outils et environnement de développement

4.1.1 Outils

A fin de réaliser ce projet, nous avons utilisé plusieurs technologies, qui sont :



Firestore : est une base de données NoSQL entièrement gérée proposée par Google, qui fait partie de la plateforme Firebase. Elle est conçue pour stocker et synchroniser des données en temps réel entre les applications web, mobiles et les serveurs. Firestore offre des fonctionnalités puissantes telles que la prise en charge de requêtes complexes, la synchronisation des données en temps réel, la gestion des autorisations, les index automatiques et bien plus encore. Avec son modèle de données flexible et sa scalabilité automatique, Firestore est largement utilisé pour développer des applications modernes nécessitant une gestion efficace des données.



Firebase Authentication : est un service fourni par Firebase pour gérer l'authentification des utilisateurs dans vos applications. Il prend en charge diverses méthodes d'authentification, notamment :

- Email et Mot de passe : Les utilisateurs peuvent s'inscrire et se connecter en utilisant leur adresse e-mail et leur mot de passe.
- Fournisseurs Sociaux : Intégration avec des plateformes sociales populaires telles que Google, Facebook, Twitter et GitHub pour l'authentification.
- Authentification Anonyme : Permet aux utilisateurs d'interagir avec votre application avant de créer un compte.
- Authentification par Numéro de Téléphone : Les utilisateurs peuvent se connecter avec leur numéro de téléphone en utilisant la vérification par SMS. Firebase Authentication gère les processus d'authentification sécurisée et s'intègre de manière transparente avec d'autres services Firebase.



Firebase Hosting : est un service d'hébergement web fourni par Google, faisant partie de la plateforme Firebase, conçu pour déployer des applications web et des sites statiques. Il offre une distribution de contenu rapide grâce à un réseau de diffusion de contenu (CDN) mondial, SSL automatique pour des connexions sécurisées, un déploiement facile avec Firebase CLI, et une intégration transparente avec d'autres services Firebase. Il est idéal pour l'hébergement



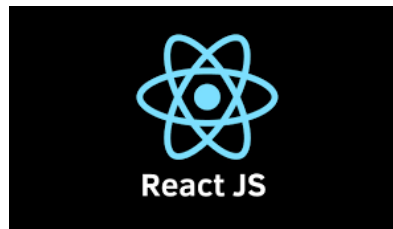
d'applications monopages (SPAs), de sites statiques, d'applications rendues côté serveur et d'applications web progressives (PWAs).

Firestore : est un service qui offre un moyen évolutif et sécurisé de stocker et de servir du contenu généré par l'utilisateur tel que des images, des vidéos et d'autres fichiers. Les principales caractéristiques incluent :

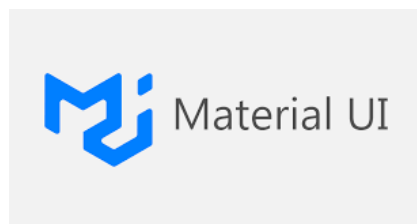
- **Stockage évolutif :** Conçu pour gérer de grands volumes de données avec une haute disponibilité.
- **Sécurité :** Utilise les Règles de Sécurité Firestore pour contrôler l'accès aux fichiers.
- **Intégration Facile :** S'intègre aux SDK Firestore pour des téléchargements et des téléversements de fichiers transparents au sein de votre application.
- **Support des Métadonnées :** Vous permet de stocker des métadonnées personnalisées avec les fichiers. Firestore est idéal pour stocker et servir du contenu généré par l'utilisateur dans les applications mobiles et web.



Les Firebase Functions, également connues sous le nom de Cloud Functions pour Firebase, sont un cadre de travail sans serveur qui vous permet d'exécuter du code backend en réponse à des événements déclenchés par les fonctionnalités de Firebase et des requêtes HTTPS. Avec Firebase Functions, vous pouvez écrire et déployer des fonctions qui sont automatiquement mises à l'échelle, gérées et exécutées dans le cloud, éliminant ainsi le besoin de gestion de serveurs. Ces fonctions peuvent gérer des tâches telles que le traitement d'événements de base de données en temps réel, l'envoi de notifications, l'exécution de logique métier et l'intégration avec d'autres services. Elles sont écrites en JavaScript ou TypeScript et s'exécutent dans un environnement géré, garantissant une haute disponibilité et évolutivité.



ReactJS : est une bibliothèque JavaScript développée par Facebook, utilisée pour construire des interfaces utilisateur interactives et dynamiques pour les applications web. Elle se distingue par son approche basée sur les composants, où chaque élément de l'interface est représenté par un composant réutilisable et autonome. ReactJS utilise une syntaxe déclarative pour décrire comment l'interface utilisateur devrait se comporter en fonction de l'état des données. Grâce à son architecture efficace basée sur le concept de Virtual DOM, ReactJS offre des performances élevées et une mise à jour optimisée de l'interface utilisateur, ce qui en fait un choix populaire pour le développement d'applications web modernes et réactives.



Material-UI : est une bibliothèque de composants React qui implémente les principes de conception de Material Design de Google. Elle offre une gamme complète de composants prêts à l'emploi, tels que des boutons, des champs de saisie, des barres de progression, des cartes, des icônes, et bien d'autres, conformément aux directives de Material Design. Material-UI permet aux développeurs de créer rapidement et facilement des interfaces utilisateur attrayantes et cohérentes pour leurs applications web, en utilisant une syntaxe intuitive et une personnalisation flexible des composants. Cette bibliothèque est largement utilisée dans la communauté React pour son esthétique moderne et ses fonctionnalités avancées, facilitant ainsi le développement d'applications web élégantes et réactives.



Node.js : est un environnement d'exécution JavaScript côté serveur, basé sur le moteur JavaScript V8 de Google Chrome. Il permet aux développeurs d'écrire des applications web et des serveurs côté serveur en utilisant JavaScript, un langage principalement associé au développement côté client. Node.js utilise un modèle d'événements non bloquants et asynchrones, ce qui le rend adapté aux applications en temps réel et aux opérations d'entrée/sortie intensives. Grâce à son écosystème de modules et de bibliothèques extensibles, Node.js est largement utilisé pour créer des applications web évolutives et performantes.

Node.js est largement utilisé pour construire des applications web rapides et évolutives, des API RESTful, des applications en temps réel comme les chats et les jeux en ligne, et bien plus encore.

{JSON}

JSON : (JavaScript Object Notation) est un format de données léger et textuel utilisé pour représenter et échanger des données structurées. Il est souvent utilisé dans le développement web pour transférer des données entre un serveur et un client. JSON est basé sur deux structures de données simples : des paires clé-valeur et des listes ordonnées de valeurs. Son format texte le rend facile à lire et à écrire pour les humains, et son utilisation est largement répandue en raison de sa simplicité et de sa compatibilité avec de nombreux langages de programmation.



JSX : (JavaScript XML) est une extension de syntaxe pour JavaScript, souvent utilisée avec des bibliothèques comme React. Elle permet aux développeurs de définir la structure des composants d'interface utilisateur de manière déclarative en utilisant une syntaxe proche de XML ou HTML. JSX est ensuite transformé en code JavaScript standard lors de la compilation, ce qui permet d'écrire du code plus lisible et plus facile à maintenir pour la création d'interfaces utilisateur dynamiques et réactives dans les applications web.



Javascript : est un langage de programmation polyvalent utilisé principalement pour développer des applications web interactives. Il est souvent utilisé pour ajouter des fonctionnalités dynamiques aux pages web, telles que la manipulation du contenu HTML, la gestion des événements utilisateur, les animations, la validation des formulaires, et bien plus encore. JavaScript est un langage de script côté client, ce qui signifie qu'il est exécuté dans le navigateur web de l'utilisateur, offrant ainsi une expérience interactive et réactive. De plus, JavaScript peut également être utilisé côté serveur avec des plateformes comme Node.js pour créer des applications web complètes.

Lucidchart : est une application en ligne de création de diagrammes et de schémas.



Elle permet aux utilisateurs de concevoir et de partager facilement des diagrammes professionnels, tels que des organigrammes, des diagrammes de flux, des plans d'architecture, des diagrammes UML et bien d'autres. Avec son interface intuitive et ses nombreuses fonctionnalités de collaboration en temps réel, Lucidchart est largement utilisé par les professionnels et les équipes pour visualiser des concepts, organiser des idées, planifier des projets et communiquer efficacement des informations complexes.



Visual Studio Code est un éditeur de code source gratuit et open-source développé par Microsoft. Il offre une interface utilisateur conviviale, une grande variété de fonctionnalités et une extensibilité grâce à son écosystème d'extensions. VSCode est largement utilisé par les développeurs pour écrire, éditer et déboguer du code dans de nombreux langages de programmation, notamment JavaScript, TypeScript, Python, Java, et bien d'autres. Il est apprécié pour sa légèreté, sa rapidité, sa personnalisation et sa prise en charge de nombreuses fonctionnalités telles que la coloration syntaxique, la complétion automatique, le débogage intégré, le contrôle de version, et bien plus encore.



Word, Microsoft Word est un traitement de texte publié par Microsoft. C'est l'une des applications de productivité bureautique incluses dans la suite Microsoft Office. Développé à l'origine par Charles Simonyi et Richard Brodie, il a été publié pour la première fois en 1983.

4.1.2 Environnement

Environnement matériel Pour la réalisation de ce projet on a disposé d'un :

- Un ordinateur : - Marque : HP
- processeur : Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz(4 CPUs), ~2.5GHz
- Ram : 8 GB - Disque dur : 256 GB SSD

4.2 Implémentation de l'application

4.2.1 Création u projet en utilisant reactjs

- Pour créer un application avec reactjs et firebase il faut les commandes suivants :
- Pour créer un aplication reactjs

```
npx create-react-app my-firebase-app  
cd my-firebase-app
```

Code 1 : create-react-app

- Install Firebase SDK

```
npm install firebase
```

Code 2 : Install-firebase-Sdk

- Page de configuration de firebase dans l'application

```
import firebase from 'firebase/app';  
import 'firebase/auth';  
import 'firebase/firestore';  
import 'firebase/storage';  
  
const firebaseConfig = {  
  apiKey: "YOUR_API_KEY",  
  authDomain: "YOUR_AUTH_DOMAIN",  
  projectId: "YOUR_PROJECT_ID",  
  storageBucket: "YOUR_STORAGE_BUCKET",  
  messagingSenderId: "YOUR_MESSAGING_SENDER_ID",  
  appId: "YOUR_APP_ID"  
};  
  
firebase.initializeApp(firebaseConfig);  
  
const auth = firebase.auth();  
const firestore = firebase.firestore();  
const storage = firebase.storage();  
  
export { auth, firestore, storage }
```

Code 3 : Configuration-firebase

- Installer Firebase CLI:

```
npm install -g firebase-tools
```

Code 4 : Install firebase- CLI

- Se connecter à Firebase:

```
firebase login
```

Code 5 : Connecter au firebase

- Initialiser Firebase dans votre projet:

```
firebase init
```

Code 6 : Intialisation de projet

- Construire votre application React:

```
npm run build
```

Code 7 : Construction app

- Déployer sur Firebase Hosting:

```
firebase deploy
```

Code 8 : Deploy app

4.2.2 Création du model IA

- Pour créer un model IA pour detecter les intrusions sur notre site web il faut les commandes suivantes :

Initialisation de Firebase dans l'application Web

```
import { initializeApp } from "firebase/app";
import { getAuth } from "firebase/auth";
import { getFirestore } from "firebase/firestore";
import { getStorage } from "firebase/storage";

const firebaseConfig = {
  apiKey: "*****",
  authDomain: "firestoretest-3615c.firebaseio.com",
  projectId: "firestoretest-3615c",
  storageBucket: "firestoretest-3615c.appspot.com",
  messagingSenderId: "3*****",
  appId: "*****",
  measurementId: "*****"
};

export const app = initializeApp(firebaseConfig);

const auth = getAuth();
const db = getFirestore(app);
const storage = getStorage(app);

export { db, auth, storage };
```

Code 9: Intialisation firebase

Collecter des données pour entraîner le modèle

```
function logRequest(requestDetails) {
  db.collection("requests").add({
    timestamp: firebase.firestore.FieldValue.serverTimestamp(),
    ...requestDetails
  })
  .then(() => {
    console.log("Request logged successfully!");
  })
  .catch((error) => {
    console.error("Error logging request: ", error);
  });
}

// Example usage
logRequest({ userId: "12345", action: "login", ipAddress: "192.168.1.1", status: "failed"

```

Code 10 : Coollection de donnees

Former le modèle d'IA

```
html

<script src="https://cdn.jsdelivr.net/npm/@tensorflow/tfjs"></script>

```

Code 11: Incluez TensorFlow.js dans le code HTML

```

async function trainModel() {
  // Fetch your data from Firestore
  const snapshot = await db.collection('requests').get();
  const data = snapshot.docs.map(doc => doc.data());

  // Prepare your training data
  const inputs = data.map(d => [/* features, e.g., request time, user activity, etc. */]);
  const labels = data.map(d => [/* target, e.g., 1 for hacking attempt, 0 for normal */]);

  // Define a model for binary classification.
  const model = tf.sequential();
  model.add(tf.layers.dense({units: 10, activation: 'relu', inputShape: [inputs[0].length]}));
  model.add(tf.layers.dense({units: 1, activation: 'sigmoid'}));

  model.compile({optimizer: 'adam', loss: 'binaryCrossentropy', metrics: ['accuracy']});

  const xs = tf.tensor2d(inputs);
  const ys = tf.tensor2d(labels);

  await model.fit(xs, ys, {
    epochs: 50,
    callbacks: {

```

Code 12 : Entraîner le modèle-IA

```

      onEpochEnd: (epoch, logs) => {
        console.log(`Epoch ${epoch}: loss = ${logs.loss}`);
      }
    }
  });

  // Save the model to local storage
  await model.save('localstorage://my-model');
}

trainModel();

```

Code 13 : Entraîner le modèle-2

Déployer le modèle à l'aide des fonctions Firebase

Après avoir entraîné le modèle, vous devez le déployer à l'aide des fonctions Firebase. Vous pouvez enregistrer le modèle localement, puis le charger dans une fonction Firebase pour faire des prédictions :

1. Install Firebase CLI and initialize functions:

```
npm install -g firebase-tools
firebase init functions
```

Code 14 : Firebase-function

2. Implement the function in functions/index.js:

```
const functions = require("firebase-functions");
const admin = require("firebase-admin");
const tf = require("@tensorflow/tfjs-node");
const path = require("path");

admin.initializeApp();
const db = admin.firestore();

exports.detectAnomaly = functions.https.onRequest(async (req, res) => {
  const { requestDetails } = req.body;

  // Load the pre-trained model
  const modelPath = path.join(__dirname, 'my-model');
  const model = await tf.loadLayersModel(`file://${modelPath}/model.json`);

  // Prepare input data for prediction
  const inputData = tf.tensor2d([/* normalized request details */], [1, /* input sh

  // Make a prediction
  const prediction = model.predict(inputData);
```

Code 15 : Implement-function-1A

```
const prediction = model.predict(inputData);
const data = await prediction.array();

res.json({ prediction: data[0][0] });
});
```

Code 16 : Implement-function-2

3. déployer la fonction:

```
firebase deploy --only functions
```

Code 17 : déployer la fonction

4.Intégrez le modèle à votre application Web

```
async function detectAnomaly(requestDetails) {
  const response = await fetch("https://<YOUR_PROJECT_ID>.cloudfunctions.net/detectAnomaly", {
    method: "POST",
    body: JSON.stringify({ requestDetails }),
    headers: { "Content-Type": "application/json" }
  });
  const data = await response.json();
  if (data.prediction > /* threshold */) {
    console.log("Possible hacking attempt detected!");
    // Take appropriate action (e.g., log, alert, block user)
  }
}

// Example usage
detectAnomaly({ userId: "12345", action: "login", ipAddress: "192.168.1.1", status: "failed" });
```

Code 18 : Integrate-model

5.Présentation du système

5.1 Capture des pages

Ci-dessous se trouvent les captures d'écran de notre plateforme :

Login

Dans cette page vous pouvez accéder à notre plateforme si vous avez un compte ou vous pouvez inscrire si vous n'avez pas un compte en cliquant sur s'inscrire .

Login

Email Address *

Password *

LOGIN

Forgot your password?

RESET PASSWORD

Nouvel utilisateur

INSCRIVEZ-VOUS ICI

Figure 10 : Login

Page d’inscription

Apartment *

Informatique

Select Role *

Etudiant

Classe *

M2-SII

S'INSCRIRE

LOGIN

Dans cette page vous pouvez s'inscrire a la plateforme en saisissant votre informations

S'inscrire

First Name *

Cheikh Essouvi

Last Name

Ahmed Elhadj

Email Address *

cheikhessouvi@gmail.com

Password *

.....

Numero *

8MRT10096

Telephone *

0774602096

Apartment *

Informatique ▼

Select Role *

Etudiant ▲

Admin

Prof

Etudiant

S'INSCRIRE

LOGIN

Figure 11 : Inscription

Page Admin

Cette page est accessible que par l'admin, c'est la page principale d'admin qu'elle lui permet de gérer la plateforme

Welcome admin test

[PAGE HOME](#) [LOGOUT](#)

This is the Admins page

NOMINATION DES PROFESSEURS

Email

R...

E...

SEARCH

Nom	Prenom	Email	Numero	Role	Etat	Telephone	Actions
admin	test	admin@gmail.com	09876543	Admin	Active	07733321	DELETE DEACTIVATE
test2	test2	test2312@gmail.com	09948464	Prof	Active	09980009	DELETE DEACTIVATE
prof-chimmie1	prof-chimmie1	prof-chimmie1@gmail.com	jhgfz	Prof	Active	09990979	DELETE DEACTIVATE
prof-math1	prof-math1	prof-math1@gmail.com	0774602096	Prof	Active	07733321	DELETE DEACTIVATE
prof-info1	prof-info1	prof-info1@gmail.com	0774602096	Prof	Active	07733321	DELETE DEACTIVATE
etud-math5	etud-math5	etud-math5@gmail.com	jhgfz	Etudiant	Active	09587	DELETE DEACTIVATE

Figure 12 : page admin

Page d’Ajout de Département

Dans cette page l’admin peut ajouter des departments, classes et Modules

Welcome admin test

[PAGE HOME](#) [LOGOUT](#)

Ajouter Département

Apartment Name

AJOUTER DÉPARTEMENT

Ajoutez classe pour un département

Class Name

Select Apartment ▼

REGISTRER

Ajouter Module a un classe

Module Name

Select Apartment ▼
Informatique

Select Class ▼
M1-info

AJOUTER MODULE

Figure 13 : Page d'ajout department

a. Page d’affectation des profs aux Modules

Dans cette page l'admin Affecte un professeur a un Module

Nommer Professeur pour un Module

Select Apartment

Informatique

Select Class

M1-info

Select Module

Module1-M1-info

Select Professor

prof-math1

NOMMER UN PROFESSEUR

Figure 14 : Page de modules

Page de Prof

Cette page et le page de professeur

Welcome prof-info1 prof-info1

[PAGE HOME](#) [LOGOUT](#)

[AJOUTER NOUVELLE COUR](#)

this the page of professeurs

Figure 15 : Page de prof

Page d'ajout de cours

Dans cette page le professeur peut ajouter des cours videos et documents dans un module s' il est affecter a ce module

L'ajout d'un cour

Select Module

▼

Course Name

Choose File No file chosen

Choose File No file chosen

ADD MODULE

Figure 16 : Page d'ajouter cour

Page cour d'Etudiant

C'est la page communs entre les etudiants d'une classe, ou il ya leurs cours

Welcome etud-info1 etud-info1

[PAGE HOME](#) [LOGOUT](#)

Your Modules

Module1-M2-info

Module2-M2-info

Figure 17 : Page de cour etudiants

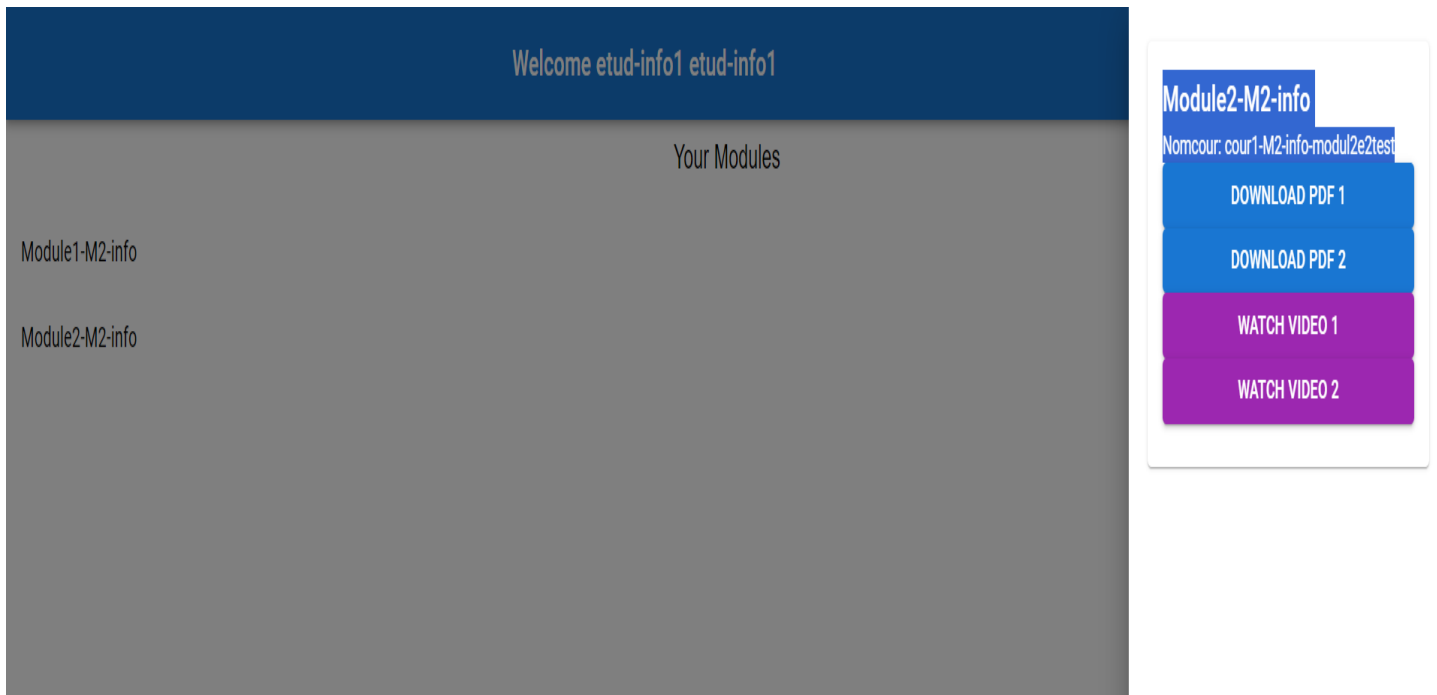
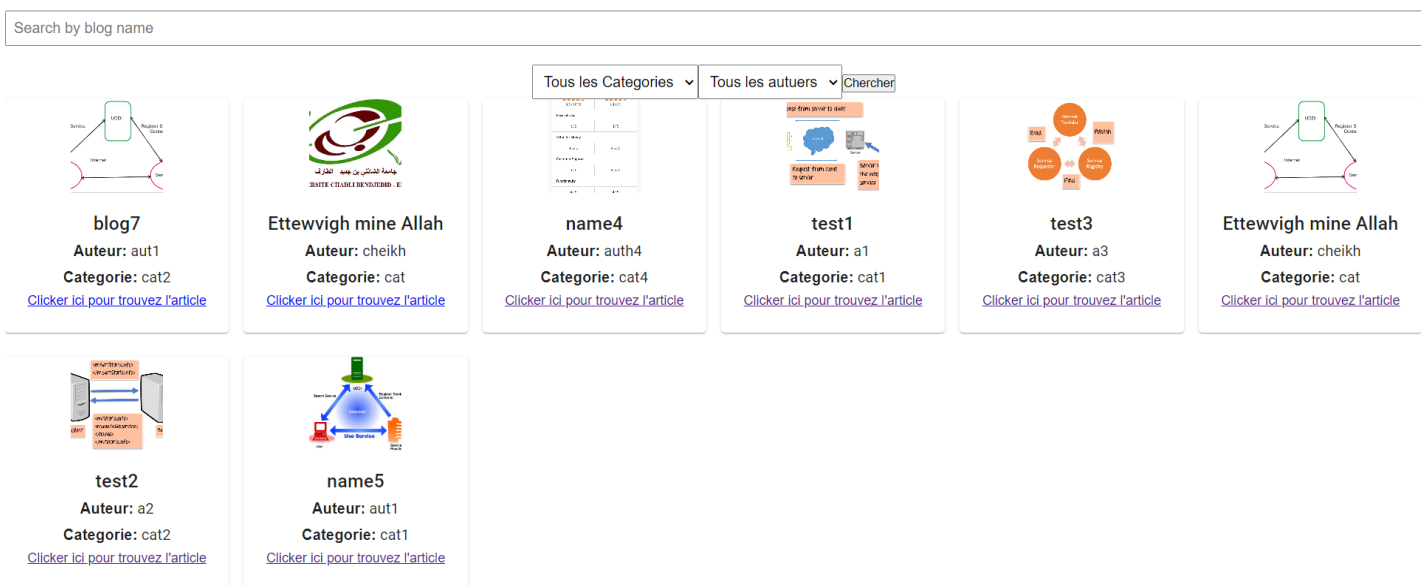


Figure 18 : Page cour

Page de Blogs

La page ou il ya des articles, l'utilisateur peut chercher une article par sa titra ou son auteur et par son categories et en fin il peut telecharger l'article

Page d'articles



Page D'ajout Blog

L'utilisateur peut ajouter un article



Add Blog

Name:

Category:

Author:

PDF File: Choose File No file chosen

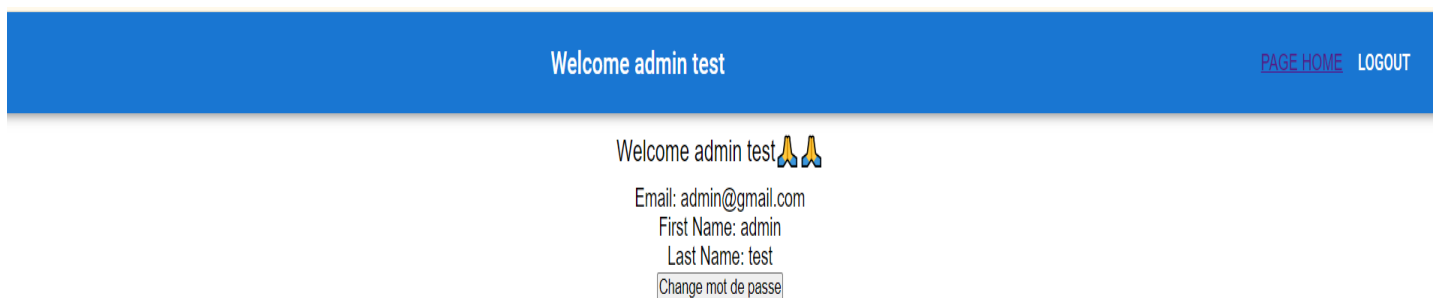
Image: Choose File No file chosen

Add Blog

Figure 20 : Add blog

Page de profile

C'est la page de profile de chaque utilisateur, où ses informations sont affichées lors de sa connexion et identifiées par son identifiant unique



Welcome admin test

[PAGE HOME](#) [LOGOUT](#)

Welcome admin test 

Email: admin@gmail.com

First Name: admin

Last Name: test

Change mot de passe

Figure 21 : Profile

Page Home

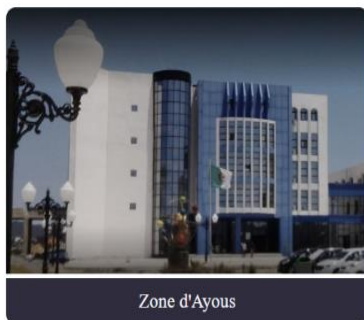
C'est la page general de l'application



Figure 22 : page de home

L'enciente Universitaire

La campus Universitaire est disperse dans plusieurs zones proches les unes des autres a l'intérieur de la ville d'el-taref.



Les Cours que nous proposons !

We have the most varied and most sought after courses for your graduation.

Les Cours que nous proposons !

We have the most varied and most sought after courses for your graduation.

Cours que nous proposons

Nous proposons les cours les plus variés et les plus recherchés pour votre diplôme.

Degré

les différentes formations de l'espace Diplôme sont disponibles sur nos plateformes en ligne

Après être diplômé

les différentes formations de l'espace Post Graduation sont disponibles sur nos plateformes en ligne

Notre Facultés

Notre Accompagnateur est bien conçu, bien organisé et équipé des dernières technologies.



Faculté de science de la vie



Faculte de langues et de lettres



Faculte de science et technologies



Faculté de des sciences humaines et sociales



Faculte de droit et de sciences politiques



Faculte de gestion economies et affaires

Notre Accompagnateurs

r Notre Accompagnateur est bien concus, bien organisé et équipé des dernières technologies.



Ce que disent nos étudiants

Sachons un peu ce que pensent nos étudiants



J'ai beaucoup aimé les installations, les professeurs, les cours proposé par l'université... et bien c'est un lieu d'immersion dans apprentissage!!

Cheikh Essouvi



Je suis très satisfait de tout le soutien apporté par cette université moi. Maintenant, je veux transmettre cette expérience à mes amis.

Cheikhena

Nos étudiants peuvent s'inscrire a nos cours en ligne partout dans le monde,
Clicker sur le bouton ci-dessous pour en savoir plus.

About US

CONTACT US

Vous pouvez en apprendre davantage sur notre enseignement, nos cours, nos professeurs et bien plus encore. plus. Si vous avez encore des questions, nous sommes à votre disposition, contactez-nous à tout moment.



6. Conclusion

Dans ce chapitre on a parlé de :

- Dans la partie Introduction, Nous avons présenté une introduction générale sur le fonctionnement du projet.
- Dans la partie Approches proposées, Nous avons discuté des méthodes suivies
- Dans la partie Conception et Architecture , nous avons présenté les Diagrammes de conception de données adoptés .
- Dans la partie Implémentation ; nous avons parlé des technologies utilisées et de l'environnement de travail . et on a donné les captures de la plateforme

Conclusion et Perspectives

Ce projet est un modèle de base qui comprend toutes les fonctionnalités nécessaires de backend pour créer et développer une plateforme d'apprentissage à distance relativement sécurisée sur le plan cybernétique, car une sécurité totale est impossible à atteindre.

Il vise à prévenir les menaces externes liées à la connexion à la plateforme, ainsi que les menaces internes liées aux autorisations des utilisateurs et à leur confidentialité. C'est pourquoi nous ne nous sommes pas beaucoup concentrés sur les interfaces dans ce projet, mais plutôt sur le backend. L'application fonctionne entièrement et chaque page remplit sa fonction.

Comme je l'ai dit, il s'agit d'un prototype qui peut être développé davantage en ajoutant d'autres fonctionnalités et améliorations, telles que l'interaction entre les utilisateurs, l'amélioration des interfaces et l'ajout de nouvelles fonctionnalités.

Nous aspirons également à améliorer l'efficacité de notre modèle d'intelligence artificielle pour la détection des intrusions et des menaces imminentes. Le backend de cette plateforme a été développé avec Firestore et JavaScript. Firestore est une base de données très flexible qui diffère des bases de données traditionnelles.

Pendant le développement de cette plateforme, nous avons appris ReactJS et Firebase à partir de zéro, car nous n'avions aucune connaissance préalable de ces technologies. Leur découverte a été une expérience incroyable.

References

- Ahmed Tlili, M. C. (2021, 12). *A Systematic Literature Review of Empirical Studies on Learning Analytics in Educational Games*. Récupéré sur ResearchGate: <https://www.researchgate.net/publication/350037959>
- Anandhavalli Muniasamy, A. A. (2020, 01 15). *Deep Learning: The Impact on Future eLearning*. Récupéré sur IJET: <https://doi.org/10.3991/ijet.v15i01.11435>
- Automatic modeling learner's personality using learning analytics approach in an intelligent Moodle learning platform*. (2019., 07 03). Récupéré sur Taylor & Francis: <https://doi.org/10.1080/10494820.2019.1636084>
- Ghelani, D. (2022, 09 22). *Cyber Security, Cyber Threats, Implications and Future*. Récupéré sur Authorea: <https://www.authorea.com/users/506161/articles/587239-cyber-security-cyber-threats-implications-and-future-perspectives-a-review>
- Ido Roll, R. W. (2016, 02 22). *Evolution and Revolution in Artificial*. Récupéré sur SpringerLink: <https://doi.org/10.1007/s40593-016-0110-3>
- Ilie Gligorea, M. C.-T. (2023, December 6). *Adaptive Learning Using Artificial Intelligence in e-Learning*:. Récupéré sur mdpi: <https://doi.org/10.3390/educsci13121216>
- Johan van Niekerk, R. v. (2013, 10). *From information security to cyber security*. Récupéré sur ScienceDirect: <https://doi.org/10.1016/j.cose.2013.04.004>
- Kai-Yu Tang, C.-Y. C.-J. (2021, 01). *Trends in artificial intelligence-supported e- learning: a systematic review and co-citation network analysis (1998-2019)*. Récupéré sur ResearchGate: <https://www.researchgate.net/publication/348648921>
- MIR MURTAZA, Y. A. (2022, July 26). *AI-Based Personalized E-Learning Systems*:. Récupéré sur IEEE Access: <https://ieeexplore.ieee.org/abstract/document/9840390>
- Naveed Naeem Abbas, T. A. (2019, June 16). Récupéré sur Springer Link: <https://link.springer.com/article/10.1007/s11192-019-03222-9>

- Naveed Naeem Abbas, T. A. (2019, 01 16). *Investigating the applications of artificial intelligence*. Récupéré sur SpringerLink: <https://doi.org/10.1007/s11192-019-03222-9>
- Neerja Kashive, L. P. (2020, 12). *Understanding user perception toward artificial intelligence (AI) enabled e-learning*. Récupéré sur ResearchGate: <https://www.researchgate.net/publication/347516230>
- O.J. Falana, I. E. (2021, 04). *Se-LMS: Secured learning management systems for smart school*. Récupéré sur ResearchGate: https://www.researchgate.net/publication/350838302_Se-LMS_Secured_learning_management_systems_for_smart_school
- Peng Gao, J. L. (2021, April 30). *An Introduction to Key Technology in Artificial Intelligence and big*. Récupéré sur SpringerLink: <https://link.springer.com/article/10.1007/s11036-021-01777-7>
- Rian Andrian, A. F. (2020, 02). *Security Scanner for Web Applications Case Study: Learning Management System*. Récupéré sur ResearchGate: https://www.researchgate.net/publication/341124176_Security_Scanner_For_Web_Applications_Case_Study_Learning_Management_System
- Rossouw von Solms, J. v. (2013, April 11). *From information security to cyber security*. Récupéré sur Elseiver: <https://dx.doi.org/10.1016/j.cose.2013.04.004>
- Yao Jun, A. C. (2021, October 27). *Artificial Intelligence Application in Cybersecurity*. Récupéré sur Hindawi: <https://doi.org/10.1155/2021/3329581>
- Yosr Chamekh, M. A. (2020). *Ways Artificial Intelligence Will Shape eLearning*. Récupéré sur International Journal of Sciences:: <https://core.ac.uk/download/pdf/288306482.pdf>

ملخص

المشروع يهدف إلى تحسين تجربة التعلم عبر الإنترنت لطلاب الجامعات من خلال توفير أقصى درجات الأمان والخصوصية للمستخدمين. الهدف الرئيسي هو إنشاء منصة تعليمية عبر الإنترنت تتيح للطلاب الوصول بسهولة وخصوصية إلى المحتوى التعليمي. لضمان حماية البيانات الشخصية للمستخدمين، سيتم تنفيذ آليات أمان قوية مثل التشفير المتقدم وأنظمة المصادقة القوية. بالإضافة إلى ذلك، سيتم تطوير نظام إدارة حقوق الوصول المتقدم لضمان أن كل طالب ومعلم يمكنه فقط الوصول إلى الموارد المخصصة لهم وأخيراً لدينا نموذج ذكاء اصطناعي لكشف السلوك المريب للمستخدمين وإبلاغ المسؤولين وحظرهم في حالات معينة. بشكل عام، يهدف هذا المشروع إلى إنشاء تجربة تعليمية عبر الإنترنت آمنة وخاصة وثرية لطلاب الجامعات، مع التركيز بشكل كبير على حماية البيانات وخصوصية المستخدمين.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، التعلم الإلكتروني

Résumé

Le projet vise à améliorer l'expérience d'apprentissage en ligne des étudiants universitaires en offrant une sécurité et une confidentialité maximales aux utilisateurs. L'objectif principal est de créer une plateforme d'apprentissage en ligne permettant aux étudiants d'accéder facilement et en toute confidentialité au contenu éducatif. Pour garantir la protection des données personnelles des utilisateurs, des mécanismes de sécurité solides tels que le cryptage avancé et des systèmes d'authentification robustes seront mis en place. De plus, un système de gestion des droits d'accès sophistiqué sera développé pour s'assurer que chaque étudiant et enseignant ne puisse accéder qu'aux ressources qui leur sont attribuées. Enfin, nous disposons d'un modèle d'intelligence artificielle pour détecter les comportements suspects des utilisateurs, informer les administrateurs et les bloquer dans certains cas. Globalement, ce projet vise à créer une expérience d'apprentissage en ligne sécurisée, privée et enrichissante pour les étudiants universitaires, en mettant fortement l'accent sur la protection des données et la confidentialité des utilisateurs.

Mots clés : IA, cybersécurité, E-Learning

Abstract

The project aims to improve the online learning experience for university students by providing maximum security and privacy for users. The main objective is to create an online learning platform that allows students to easily and privately access educational content. To ensure the protection of users' personal data, strong security mechanisms such as advanced encryption and robust authentication systems will be implemented. Additionally, a sophisticated access rights management system will be developed to ensure that each student and teacher can only access the resources assigned to them. Finally, we have an artificial intelligence model to detect suspicious user behavior, notify administrators, and block them in certain cases. Overall, this project aims to create a secure, private, and enriching online learning experience for university students, with a strong focus on data protection and user privacy.

Keywords : AI, cybersecurity, E-Learning

