Université Abbes Laghrour Khenchela

Faculté Science et technologie

Département Informatique

Spécialité : Sécurité et technologie web

Liste des PFE STW (Master 2) 2025-2026

	L'encadreur **Mail**	**Titre**
01	**Djezzar Meriem** *meriem.djezzar@univ-khenchela.dz*	**Titre : Protection des données médicales dans les systèmes e-santé** **Description:** Avec le développement des systèmes e-santé (comme les dossiers médicaux électroniques, la télémédecine ou les applications de suivi de santé), une grande quantité de données médicales personnelles est collectée, stockée et échangée entre différents acteurs du domaine de la santé. Ces données sont très sensibles et doivent être protégées contre tout accès non autorisé, toute perte ou toute modification. Ce projet a pour objectif d'étudier les principaux risques de sécurité liés à la gestion et au partage des données médicales, puis de proposer une solution simple pour les protéger. Une application web sera développée et une base de données SQL pour illustrer le fonctionnement du modèle de sécurité proposé.
02	**Djezzar Meriem** *meriem.djezzar@univ-khenchela.dz*	**Titre : Ontologie pour la modélisation des menaces en cybersécurité dans les systèmes IoT** **Description:** Avec le développement de l'Internet des Objets Médicaux (IoMT) — tels que les capteurs de santé, les dispositifs de surveillance à distance, ou encore les équipements hospitaliers connectés — la cybersécurité dans le domaine médical est devenue un enjeu majeur. Ces systèmes collectent et échangent des données sensibles sur la santé des patients, souvent via des réseaux vulnérables. L'objectif de ce projet est de concevoir une ontologie permettant de modéliser les menaces de cybersécurité spécifiques aux systèmes IoT médicaux. Cette ontologie doit représenter les dispositifs médicaux, leurs vulnérabilités, les types d'attaques possibles (accès non autorisé, injection de code, compromission de données, etc.), ainsi que les contre- mesures adaptées.
03	**Hioual Ouidad** *ouided.hioual@univ-khenchela.dz*	**Titre: Detection of Phishing Emails Using Machine Learning.** **Description** : Phishing is one of the most widespread and dangerous threats in cybersecurity. It consists of deceiving users into

		revealing sensitive information such as credentials, passwords, or banking data by impersonating a trusted entity through fraudulent emails. Despite the existence of anti-spam filters, many phishing attacks still bypass security systems, posing serious risks to individuals and organizations. To address this issue, machine learning techniques provide powerful and adaptive solutions to detect and prevent phishing in real time. By analyzing email content, metadata (sender, subject, links, attachments), and behavioral features, it becomes possible to build models capable of automatically distinguishing legitimate emails from fraudulent ones. The aim of this final-year project is to develop an intelligent system for automatic phishing email detection using machine learning algorithms. The student will collect a dataset of emails (phishing and legitimate), perform text preprocessing (cleaning, vectorization, feature extraction), and then train and evaluate various classification models such as Logistic Regression, SVM, Random Forest, or Neural Networks. The ultimate goal is to design an accurate, robust, and interpretable model that can be integrated into a mail system to enhance user security and data protection. This project will enable the student to gain practical skills in cybersecurity, text analysis (NLP), and machine learning.
04	**Abbas Fayçal** *abbas_faycal@univ-khenchela.dz*	**Titre:** LLM-Augmented Enterprise Cybersecurity: Real-Time Risk Analysis Intelligente **Description :** This project designs and evaluates a lightweight pipeline that embeds a local Large Language Model (LLM) into two high-risk enterprise workflows—email triage and source-code management. The LLM produces inline, explainable risk reports for messages (phishing, suspicious payment requests, risky links/attachments) and performs commit-time checks for exposed secrets, insecure patterns, and misconfigurations. The architecture prioritizes privacy with on-prem deployments (e.g., Llama 3, Mistral/Mixtral, Gemma, Falcon, DeepSeek) while remaining interoperable with cloud APIs (e.g., GPT-4o/4.1, Claude 3.5, Gemini 1.5) when heavier reasoning is needed. The evaluation covers latency, precision/recall, false-positive costs, and usability, and discusses prompt design, guardrails, and failure modes. The outcome is a practical, human-centered defense layer that complements existing email security gateways, secret scanners, and other tools. Real-world applications : - Phishing Detection in Corporate Enterprise Email Systems - Internal Threat Detection in Healthcare Environments - SaaS Product Security References 1. Tellache, A., et al. (2024). Leveraging LLMs and Cyber Threat Intelligence. 2. Huang, H., et al. (2024). Leveraging Large Language Models for Effective Phishing Email Detection. arXiv:2402.18093v2. 3. StrongestLayer (2025). AI-Generated Phishing: The Top Enterprise Threat of 2025.

05	**MAAROUK Toufik Messaoud** *maarouk.toufik@univ-khenchela.dz*	**Thème : Vérification formelle de la validité temporelle des sessions d'authentification dans les systèmes IoT.** **Description :** Les systèmes IoT (Internet of Things) regroupent de nombreux objets connectés (capteurs, caméras, dispositifs domotiques, etc.) qui communiquent via des protocoles souvent allégés et exposés à des vulnérabilités. L'un des points critiques de la sécurité IoT concerne la gestion des sessions d'authentification : durée de validité, renouvellement, expiration, et résistance aux attaques d'usurpation après expiration. Un grand nombre de failles proviennent d'erreurs de conception dans la logique temporelle : une session qui reste valide trop longtemps ou un délai d'expiration mal géré peut permettre à un attaquant de réutiliser un ancien jeton ou d'accéder à une ressource après la déconnexion d'un utilisateur. Les méthodes formelles permettent de modéliser de manière rigoureuse le comportement temporel des protocoles et de vérifier automatiquement que les propriétés de sécurité temporelles sont respectées.
06	**Tioura Abdelhamid** *atioura@yahoo.fr*	**Titre: Strengthening WSN Security through dynamic reorganization of the trusted network's nodes** **Description:** This work summarizes the process of dynamically selecting one or more sensors and then using them as a trusted authorities to implement a security policy. The selection can be made based on different metrics: random selection, allowing statistically good network coverage; selection based on the residual energy of the sensors, whose advantage is to offer better load distribution (in terms of energy consumption) in the network; and finally a democratic election process, based on reputation scores, which further improves the security of the device. The proposed solution will allow WSNs to organize themselves in a hierarchical manner, with a dynamically elected leader playing a central role in securing the overall network. The proposed solution will be simulated for testing and comparison with other solutions proposed in the literature.

07	**Mahdaoui Rafik** *Mahdaoui.rafik@univ-khenchela.dz*	**Titre: Optimisation de la Fiabilité des Systèmes Complexes à l'aide de l'Algorithme Gradient-Based Optimizer (GBO)** **Description:** La fiabilité des systèmes complexes (industriels, mécatroniques ou cyber-physiques) constitue un enjeu crucial dans le cadre de l'Industrie 4.0. L'évaluation et l'optimisation de cette fiabilité nécessitent souvent des modèles mathématiques non linéaires et fortement couplés, rendant leur résolution difficile par des méthodes classiques. Ce mémoire propose d'explorer l'application de l'algorithme Gradient-Based Optimizer (GBO) — une métaheuristique récente et performante — pour optimiser les paramètres influençant la fiabilité d'un système complexe. L'objectif est de trouver la configuration optimale minimisant le taux de défaillance ou maximisant la disponibilité du système. Le travail comportera plusieurs étapes : 1. Revue de la littérature sur les approches d'optimisation utilisées en fiabilité (PSO, GA, GWO, DE, etc.) et positionnement du GBO parmi elles. 2. Modélisation mathématique du système étudié (modèle de fiabilité série, parallèle, mixte, ou réseau de composants). 3. Application du GBO pour l'optimisation des paramètres clés (taux de panne, MTBF, disponibilité, coûts de maintenance, etc.). 4. Comparaison des performances du GBO avec d'autres métaheuristiques de référence. 5. Analyse de sensibilité et validation sur un cas réel ou simulé (ex. : système de production, robot industriel, ou réseau électrique). Possibilité d'application au monde réel : Oui
08	**Hichem Houassi** *haouassi.hichem@univ-khenchela.dz*	**Titre : Analyse Prédictive des Données pour la Détection et la Prévention des Cyberattaques .**
09	**Bekhouche Abd-el-ali** *bakhouche.abdelali@univ-khenchela.dz*	**Titre: AI-Based Intrusion Detection System Enhanced with Swarm Intelligence** **Description:** The main objective of this project is to design and implement an intelligent intrusion detection system (IDS) using artificial intelligence (AI) techniques, enhanced by swarm optimization algorithms. The system aims to detect and classify cyber-attacks in real time with improved accuracy and adaptability. The proposed system will use machine learning models (such as Random Forest, SVM, or Deep Neural

		Networks) to identify abnormal network behaviors. Swarm intelligence (e.g., Particle Swarm Optimization or Ant Colony Optimization) will be used to optimize the detection model parameters, improving performance in terms of precision, recall, and speed. The system can be tested on standard datasets such as NSL-KDD or CICIDS2017. Expected Results: - A prototype of an intrusion detection system capable of detecting network anomalies in real time. - Performance evaluation (accuracy, precision, recall, F1-score). - A comparison between standard AI models and swarm-enhanced models. - A detailed technical report and implementation guide. Tools and Technologies: - Programming Language: Python - Frameworks : Scikit-learn, TensorFlow/PyTorch - Optimization Library: PySwarms - Dataset: NSL-KDD or CICIDS2017 - Environment: Jupyter Notebook / Google Colab Keywords: Artificial Intelligence, Intrusion Detection System, Swarm Intelligence, Machine Learning, Cybersecurity
10	**Chergui Wahid** *wahidchergui@gmail.com*	**Titre : Détection d'intrusions basée sur l'apprentissage profond et l'analyse comportementale** **Description :** La cybersécurité est devenue un enjeu majeur dans les infrastructures informatiques modernes, en particulier avec la croissance exponentielle du volume de données et la complexité des attaques. Les systèmes de détection d'intrusions (IDS) traditionnels, souvent basés sur des signatures ou des règles statiques, montrent leurs limites face à des attaques nouvelles, polymorphes ou ciblées. L'émergence de l'apprentissage profond (Deep Learning) permet désormais de concevoir des systèmes capables d'apprendre automatiquement les comportements normaux et anormaux du trafic réseau, offrant ainsi une analyse comportementale plus fine et une détection proactive des menaces. L'objectif est de Mettre en œuvre un système intelligent de détection d'intrusions basé sur l'apprentissage profond, capable d'apprendre les schémas comportementaux du trafic réseau pour détecter les anomalies.
11	**Souidi Mouhamed El-habib** *souidi.mohammed@univ-khenchela.dz*	Titre : A novel intrusion detection approach based on mobile agents' coordination Description: This research proposes a novel intrusion detection approach based on mobile agents' coordination, primarily aimed at processing infected nodes and eliminating their susceptibility to further infection. Instead of relying on centralized monitoring, lightweight mobile agents traverse network hosts to collect logs, detect anomalies, and

		perform localized analysis. When compromise is suspected, agents negotiate and form coalitions to corroborate evidence, isolate infected nodes, remove persistent threats, and apply remediation policies (patching, configuration hardening, quarantine). Coordination mechanisms incorporate trust and game-theoretic strategies to prioritize responses and minimize collateral impact. By actively treating compromised hosts and reducing their attack surface, the system prevents lateral propagation and accelerates recovery. The distributed, adaptive architecture improves detection accuracy, lowers false positives, and enhances resilience, making it suitable for cloud, IoT, and critical infrastructures where rapid containment and elimination of susceptibility are essential. Evaluation demonstrates faster containment times and reduced infection rates across diverse network topologies.
12	**Djellab Issam** *Djellab_issam@univ-khenchela.dz*	Titre : Système intelligent de reconnaissance faciale pour le contrôle d'accès sécurisé Description : Ce projet vise à développer un système intelligent capable de reconnaître automatiquement les visages des individus à partir d'images , afin de gérer l'accès à un espace ou un service numérique. Le système repose sur des modèles de deep learning pré-entraînés tels que VGGFace (basé sur ResNet50) ou FaceNet, capables d'extraire des caractéristiques faciales (embeddings) très discriminantes à partir d'une image de visage. Une base de données est utilisée pour simuler un ensemble de personnes connues (autorisées) et inconnues (refusées). Le système compare le visage d'entrée avec les visages enregistrés à l'aide d'une mesure de distance euclidienne dans l'espace des caractéristiques. Si la distance est inférieure à un seuil déterminé automatiquement, l'accès est autorisé ; sinon, il est refusé. L'ensemble du traitement (prétraitement, extraction de caractéristiques, décision) est automatisé en Python à l'aide de bibliothèques comme TensorFlow/Keras, keras_vggface, OpenCV, et scikit-learn.
13	**Nessah Djamel** *nessah_djamel@univ-khenchela.dz*	Titre : Improving the Wu-Palmer Similarity Measure: Application to the SimLex-999 Dataset Description : The similarity measure is an important component for determining the degree of resemblance between terms, texts, documents, and so on. It is particularly useful in areas such as information retrieval, text comparison for plagiarism detection, recommendation systems, etc. This topic proposes an improvement to the Wu-Palmer similarity measure, which shows a weakness in the precision of its metric, and aims to evaluate its impact through results compared with a dataset based on human judgments. Keywords: Wu-palmer measure, edge counting method, similarity measure. Possibility of real-world application Text comparison, information retrieval.

14	**Chouhal Ouahiba** *Chouhal.ouahiba@univ-khenchela.dz*	Thème : Sûreté de fonctionnement intelligente d'un système de production industrielle Description : Les systèmes de production modernes exigent une surveillance continue et une optimisation intelligente afin de garantir une productivité élevée, une qualité constante et une réduction des coûts. Cependant, le suivi du fonctionnement en temps réel et la prise de décision automatique dans un environnement industriel complexe représentent un défi majeur. Comment concevoir un système capable de surveiller en continu le fonctionnement du processus de production et d'utiliser une méthode métaheuristique pour optimiser ses performances en termes de temps, qualité et fiabilité ? Étapes du travail □ Analyse et modélisation : Étudier le système industriel et identifier les paramètres de fonctionnement critiques. □ Mise en place du suivi : Développer un module de surveillance (collecte et traitement des données). □ Formulation du problème : Définir les fonctions objectif (minimiser le temps, maximiser la qualité). □ Application d'une méthode métaheuristique : Utiliser un algorithme d'optimisation (GA, PSO, Grey Wolf, etc.) pour ajuster les paramètres. □ Validation : Tester le système avant et après optimisation et évaluer les gains obtenus. .Possibilité d'application au monde réel : Oui
15	**Ridha mehalaine** *R_mahalaine@univ-khenchela.dz*	**Titre : Sécurité des données médicales dans l'Internet des objets médicaux tout en réduisant la consommation énergétique des objets.** **Description** Pour sécuriser les données médicales tout en réduisant la consommation énergétique des objets connectés (IoMT), il faut combiner des stratégies de sécurité robustes et des méthodes d'optimisation de l'énergie. Il est essentiel de mettre en place le chiffrement des données, une authentification forte et une segmentation des réseaux pour protéger les informations sensibles. Parallèlement, des techniques comme l'optimisation des algorithmes de traitement, la fréquence d'envoi des données et l'utilisation de capteurs basse consommation sont nécessaires pour réduire la consommation énergétique.

16	**Ridha mehalaine** *R_mahalaine@univ-khenchela.dz*	**Titre : La tolérance aux fautes pour les systèmes Embarqués.** **Description** Les systèmes embarqués traditionnels sont considérés comme des systèmes fermés au monde extérieur, exécutant des tâches bien précises et exposant un comportement avec des plages de variation bien définies. Actuellement les nouveaux usages donnés aux objets enfouis exigent des systèmes embarqués, plus intelligents et ouverts dans le sens où ils peuvent accéder à Internet, utilisent une connexion sans fil, exécutent des applications open source, et fonctionnent dans des environnements de nuage ce qui rend les systèmes embarqués actuels plus compliqués et leur sécurité une tâche très délicate. Pour les objets embarqués du quotidien, l'impact économique d'un dysfonctionnement impose de respecter des contraintes d'énergie, mais les techniques existantes sont très pénalisantes en termes de performances, en plus elles peuvent facilement échouer dans un contexte dynamique et adaptatif ce qui rend leurs adoption est une question n'est pas toujours évidente. L'objectif est de proposer un ordonnencement des tâches basée sur la tolérance aux fautes dans un système embarqué.
17	**MALIK Mohamed Mahdi** *malik.mohamed.mahdi@univ-khenchela.dz*	**Titre : An Explainable Machine Learning Approach for Network Intrusion Detection** **Description :** Explainable AI (XAI) techniques are methods and tools designed to make the decision-making process of machine learning models, especially complex ones like deep learning models, more understandable and interpretable to humans. These techniques help explain why and how a model arrived at a particular prediction, which is especially important in fields like sustainable environment, healthcare, finance, ... etc. where decisions have significant real-world impacts. A Network Intrusion Detection System (NIDS) is a cybersecurity tool that monitors network traffic or system

		activity to detect suspicious or malicious behavior, such as unauthorized access, Malware activity, Denial of Service (DoS) attacks, Data exfiltration (data theft), etc. It usually classifies network packets into: Normal traffic (safe), or Attack traffic (malicious). Traditionally, IDS tools rely on signatures (known attack patterns) or machine learning models or even deep learning to detect attacks accurately, but those models often act as "black boxes" and can't explain why an alert was triggered. That's a problem for cybersecurity analysts, who need to trust and understand the detection process before taking action. For this reason, this project employs interpretable and transparent models to interpret or explain model predictions. Explainable AI (XAI) solves this by: - Explaining why a network connection is classified as an attack. - Showing which features (like packet size, number of connections, protocol, etc.) triggered the alert. - Making the IDS transparent, auditable, and trustworthy. **Real-world application** • Enterprise Security: Explainable IDS helps cybersecurity teams understand and justify alerts, avoiding "false alarms." - Government and Critical Infrastructure: Transparency helps in audits, compliance, and risk reporting. - Cloud and IoT Security: Explaining anomalies in connected devices or cloud networks.
18	**Ziano Ahmed seghir** *zianou_ahmed_seghir@yahoo.fr*	**Titre : Protection et évaluation de la qualité d'images par ECC** **Description :** L'objectif de ce projet est de concevoir, implémenter et évaluer un système de chiffrement pour les images numériques fondé sur la cryptographie à courbe elliptique (ECC), tout en analysant la qualité visuelle des images chiffrées et déchiffrées à l'aide d'indicateurs objectifs tels que le PSNR, le SSIM et l'entropie. Dans un contexte où le partage d'images (médicales, industrielles, personnelles, etc.) est devenu omniprésent, la protection des données visuelles est un enjeu majeur. Les algorithmes classiques comme RSA ou AES offrent une sécurité robuste, mais peuvent être coûteux en ressources et inadaptés pour les systèmes nécessitant des échanges rapides et légers. La cryptographie à courbe elliptique (ECC) représente une solution moderne et efficace : elle permet d'obtenir un haut niveau de sécurité avec des clés beaucoup plus courtes, ce qui réduit la charge de calcul et rend le chiffrement plus performant pour les applications visuelles. Le projet vise donc à développer un modèle de chiffrement d'image basé sur ECC, puis à évaluer la qualité des

		images après chiffrement et déchiffrement, afin de mesurer la fidélité visuelle et la robustesse de la méthode proposée. Le travail de recherche consistera à : • Faire une revue de la littérature sur les méthodes de chiffrement d'images et sur la cryptographie à courbe elliptique. • Concevoir et implémenter un modèle de chiffrement d'image basé sur ECC. • Évaluer la qualité des images avant et après chiffrement à l'aide de mesures objectives (PSNR, SSIM, MSE, entropie).
19	**Mounir Hemam** *hemam.mounir@univ.khenchela.dz*	**Thème : Système de détection d'intrusion sémantique et intelligent pour les réseaux IoT** **Description :** L'Internet des Objets (IoT) connecte des milliards de dispositifs hétérogènes (capteurs, caméras, objets connectés, machines industrielles, etc.) à travers le monde. Cette interconnexion massive engendre un volume considérable de données et une superficie d'attaque étendue. Les solutions de sécurité classiques (pare-feux, antivirus, etc.) ne sont plus suffisantes, car les attaques deviennent plus intelligentes, distribuées et contextuelles. Les systèmes de détection d'intrusion (IDS) basés sur l'IA permettent d'identifier des comportements anormaux dans les réseaux. Cependant, ces modèles sont souvent dépendants des données d'entraînement et ne peuvent pas raisonner sur le contexte des événements. L'ajout d'une couche sémantique, à travers les ontologies, permet de donner du sens aux événements réseau, de représenter les relations entre entités (utilisateur, appareil, service, protocole, comportement), et d'effectuer un raisonnement logique pour détecter des attaques plus subtiles.
20	**Mounir Hemam** *hemam.mounir@univ.khenchela.dz*	**Thème : Système intelligent de détection d'activités anormales dans un réseau IoT médical** **Description :** Avec la croissance rapide de l'Internet des objets médicaux (IoMT – Internet of Medical Things), de

		nombreux dispositifs connectés tels que les capteurs de surveillance, les pompes à insuline, les moniteurs cardiaques ou les équipements hospitaliers échangent en permanence des données sensibles sur l'état de santé des patients. Cette connectivité améliore la qualité des soins et la réactivité médicale, mais elle expose également les réseaux IoMT à de nombreuses menaces de sécurité : attaques par déni de service, accès non autorisés, altération de données ou comportements anormaux de dispositifs médicaux. L'objectif de ce projet est de concevoir un système intelligent capable de détecter automatiquement les activités anormales dans un réseau IoT médical en se basant sur des techniques d'intelligence artificielle. Le système analysera le trafic réseau ou les données d'activité des dispositifs médicaux afin de distinguer les comportements "normaux" de ceux potentiellement malveillants. Sur le plan pratique, le travail consistera à : Utiliser ou simuler un jeu de données IoMT (réel ou généré). Effectuer un prétraitement des données (nettoyage, sélection de caractéristiques). Appliquer un ou plusieurs algorithmes de détection d'anomalies (par exemple : Random Forest, Isolation Forest, K-Means). Évaluer les performances du modèle selon des indicateurs tels que la précision, le rappel ou le taux de fausses alertes.
21	**Messaoudi Nabil** *Messaoudi.nabil@univ-khenchela.dz*	**Thème : Thème : Sécurisation des Modèles de Machine Learning Contre les Attaques Adversariales.** **Description:** Les modèles de Machine Learning sont de plus en plus utilisés dans des systèmes de sécurité informatique (détection d'intrusions, classification des menaces, etc.). Cependant, ces modèles peuvent être vulnérables aux attaques adversariales, où des perturbations subtiles dans les données d'entrée sont utilisées pour tromper le modèle et obtenir des résultats erronés. Comment utiliser les attaques adversariales pour évaluer la robustesse des modèles de Machine Learning dans des environnements de sécurité et comment les

		sécuriser contre ces attaques ? Objectif : L'objectif de ce travail est de développer des techniques pour tester la robustesse des modèles de Machine Learning dans un contexte de sécurité, en générant des attaques adversariales visant à perturber leur fonctionnement. Par la suite, il s'agira de proposer des méthodes de défense pour rendre ces modèles plus résistants aux attaques adversariales. Cela inclura l'utilisation de méthodes comme les perturbations adversariales, les méthodes de défense (adversarial training), et l'évaluation de la performance des modèles sous attaque. Key words: Attaques et defense adversariales ; Machine Learning ; Sécurité des modèles ; Python Possibilité d'application au monde réel : Ce travail peut être appliqué à des systèmes de sécurité en entreprise ou dans des environnements critiques, où des modèles de Machine Learning sont utilisés pour des tâches telles que la détection d'intrusions, l'analyse de malwares, ou la surveillance de réseaux. Les attaques adversariales étant un vecteur de risque croissant, les défenses proposées permettront de sécuriser les systèmes en ligne contre des attaques destinées à contourner ou perturber ces modèles.
22	**Saadi Souad** *saadi.souad@uni-khenchela.dz*	**Titre : Détection et réponse automatique aux cyberattaques par Intelligence Artificielle** **Description :** Ce projet a pour objectif de concevoir et de développer un système intelligent de détection et de réponse automatique aux cyberattaques à l'aide des techniques d'intelligence artificielle. Face à la multiplication et à la sophistication des attaques informatiques, les approches traditionnelles basées sur des signatures ou des règles prédéfinies ne suffisent plus. Le système proposé s'appuie sur le Machine Learning

		pour analyser le trafic réseau, identifier les comportements anormaux et détecter les intrusions en temps réel. Une fois une anomalie repérée, le module de réponse automatique agit instantanément en appliquant des contre-mesures adaptées, telles que le blocage de l'adresse IP malveillante ou l'isolement du poste compromis. Ce travail vise à renforcer la cybersécurité des entreprises et des infrastructures critiques tout en offrant une base solide pour le développement futur d'une solution commerciale locale orientée vers la surveillance intelligente des réseaux. Mots-clés : Cybersécurité , Apprentissage automatique, Détection d'anomalies , Réponse automatique, Intelligence artificielle, Système de détection d'intrusion , Analyse du trafic réseau, Deep Learning
23	**Abdeldjalil LEDMI** **abdeldjalil.ledmi@univ-khenchela.dz**	**Thème: Decentralized Multi-Agent Intrusion Detection with Supervised Learning** **Description :** Centralized IDS architectures struggle under high traffic volumes and are vulnerable to denial-of- service and single-point failures, while distributed, agent-based designs improve scalability, resilience, and responsiveness through autonomous, mobile agents collaborating across the network. Traditional signature-based detection misses novel threats, motivating supervised and anomaly-based learning on labeled traffic features to detect both known and emerging attack behaviors in near real time. Problem statement Design a distributed IDS that leverages mobile multi-agents for on-host sniffing, local preprocessing, and classifier-driven decisions, while coordinating across nodes to reduce false positives and recover from manager failure without degrading detection accuracy under realistic traffic loads. Objectives Architect a fault-tolerant MAS-IDS with agents for management, sniffing, analysis, and model provisioning,

		including leader election upon manager failure and threshold-based coordination to limit chatter.
24	**LEDMI Makhlouf** *ledmi.makhlouf@univ-khenchela.dz*	**Titre : Frequent Sequence Mining for Identifying Anomalous Access Patterns in Networked Systems.** **Description :** Cybersecurity monitoring systems generate extensive streams of event logs that chronologically record user authentication attempts, access behaviors, and network transactions. Analyzing these temporal event sequences is essential for distinguishing legitimate activity patterns from those indicative of security breaches or coordinated attacks. Sequential Pattern Mining (SPM) provides an effective computational framework for extracting frequent and recurrent event sequences from such log data. This project proposes the application of SPM techniques to identify characteristic behavioral patterns associated with both normal system usage and potential intrusions. By detecting deviations from frequent patterns, the study aims to uncover anomalous or high-risk event sequences that may signal emerging security threats. The anticipated outcome is the development of an SPM-based analytical approach that enhances proactive intrusion detection and contributes to intelligent cybersecurity decision support systems. Possibilité d'application au monde réel : Yes.
25	**BEGROUN BRAHIM** *belgroune.brahim@univ_khenchelaa.dz*	**Thème : Behavioral Biometrics for Continuous Authentication in Information Systems** **Description:** This project aims to develop a behavioral biometrics system for continuous user authentication in information systems. The system analyzes unique behavioral traits such as typing rhythm, mouse movement, and touchscreen interactions to verify user identity. Students will experiment with real- world datasets — including the CMU Keystroke Dynamics, Balabit Mouse Dynamics, and Aalto Touchscreen Swipe datasets — to train and evaluate models using classical machine learning techniques like SVM, KNN, and Random Forests. The approach

		enhances system security while maintaining usability and privacy in modern digital environments. Possibilité d'application au monde réel : This project can be applied in systems requiring strong and continuous authentication, such as online banking, enterprise networks, and mobile applications. By monitoring user behavior, it detects anomalies and prevents unauthorized access, providing a seamless and non-intrusive layer of security for modern digital environments.
26	**BARDOU Dalal** *dalal.bardou@univ-khenchela.dz*	**Thème: Reconnaissance d'Empreintes Digitales par Réseaux de Neurones Convolutifs pour les Systèmes de Sécurité** **Description :** La reconnaissance d'empreintes digitales est une technologie biométrique cruciale pour l'authentification sécurisée dans divers domaines. Ce projet de master propose de développer un système complet de reconnaissance d'empreintes digitales basé sur des réseaux de neurones convolutifs (CNN). Le système implémentera un pipeline complet incluant le prétraitement des images d'empreintes (amélioration de la qualité, segmentation), l'extraction des caractéristiques (minuties, motifs de crêtes) et la comparaison/matching. Le modèle sera entraîné et évalué sur des bases de données standards d'empreintes digitales en utilisant des métriques de performance standards (TAR, FAR, FRR). Possibilité d'application au monde réel : Ce système peut être déployé dans les contrôle d'accès physiques et logiques, les appareils mobiles, les systèmes bancaires et les applications gouvernementales nécessitant une authentification biométrique fiable et sécurisée.
27	**Boussalem Mohamed** *boussalem_mohamed@univ-khenchela.dz*	**Thème : Improving Diagnostic Models in the Presence of Incomplete Clinical Data** **Description :** In recent years, machine learning has become a vital tool in healthcare for disease prediction and diagnosis. However, one of the main challenges in applying these models to real-world medical data is the frequent

		presence of missing or incomplete information. Missing data can arise from various sources such as incomplete tests, recording errors, or patient dropouts, and can severely impact the accuracy and reliability of predictive models. This work focuses on improving disease prediction models in the presence of incomplete medical datasets, a common and critical challenge in healthcare data analysis. The specific case study will be defined later based on available datasets and clinical relevance. The primary goal of this work is to propose and evaluate an effective approach to handle missing data, thereby enhancing the performance and robustness of disease prediction models, ultimately supporting better clinical decision-making even when faced with imperfect data. Possibilité d'application au monde réel : This work can be applied in the healthcare field to assist doctors in predicting and detecting diseases, even in cases of incomplete datasets.
28	**Bechoua Khaled** **k.bechoua@univ-khenchela.dz**	**Thème : Vers une détection transparente des attaques de phishing grâce au machine learning et à XAI** **Description :** Ce projet vise à concevoir un système intelligent capable de détecter les attaques de phishing à partir de données tabulaires (ex. caractéristiques d'e-mails ou de sites web) en utilisant des modèles de machine learning. L'objectif principal est non seulement d'obtenir une détection précise, mais aussi de rendre les décisions du modèle compréhensibles et interprétables grâce aux techniques d'intelligence artificielle explicable (XAI) telles que LIME ou SHAP. L'étudiant(e) développera un pipeline complet incluant la collecte et le prétraitement des données, l'entraînement de modèles de classification (SVM, Random Forest, etc.), puis l'application des méthodes XAI pour analyser et visualiser les facteurs influençant chaque prédiction. Ce projet vise à concevoir un système intelligent capable de détecter les attaques de phishing à partir de données tabulaires (ex. caractéristiques d'e-mails ou de sites web) en utilisant des modèles de machine learning.

		L'objectif principal est non seulement d'obtenir une détection précise, mais aussi de rendre les décisions du modèle compréhensibles et interprétables grâce aux techniques d'intelligence artificielle explicable (XAI) telles que LIME ou SHAP. L'étudiant(e) développera un pipeline complet incluant la collecte et le prétraitement des données, l'entraînement de modèles de classification (SVM, Random Forest, etc.), puis l'application des méthodes XAI pour analyser et visualiser les facteurs influençant chaque prédiction.
29	**Zahrouri Ahmed** **ahmed.zahrouri@univ_khenchela.dz**	**Thème : Using optimization algorithms to improve the performance of deep learning models for distributed denial-of-service (DDoS) attack detection and classification.** **Description:** Our work consists of designing and implementing an optimized deep learning approach to improve the accuracy and speed of DDoS attack detection in network traffic. We are particularly interested in the problems of real-time attack detection, attack type classification, and early warning systems, focusing on traffic flow patterns and statistical features. Moreover, we explore the possibilities of improving the performance of this approach by using metaheuristic optimization algorithms to optimize model hyperparameters and ensemble weights. Real-world application possibility: yes, using several tools • Python programming language • TensorFlow or PyTorch: Deep learning frameworks for model development • DDoS datasets: CICDDoS2019, CICIDS2017 available on the internet • Optimization libraries: PySwarm, PyGAD for metaheuristic algorithms implementation
30	**Azizi Nabil** **azizi.nabil@univ-khenchela.dz**	**Théme: Modélisation et Prédiction des Trajectoires de Soins par l'Extraction des Motifs Séquentiels Fermés sur des Données de Santé à Grande Échelle** **Description :**

		Les systèmes de santé modernes génèrent des quantités massives de données sur les parcours des patients (diagnostics, prescriptions, hospitalisations, actes médicaux). L'analyse de ces séquences d'événements est un enjeu majeur pour améliorer la qualité des soins, optimiser les ressources et anticiper les complications. Cependant, la complexité et le volume de ces données rendent les algorithmes traditionnels d'extraction de motifs inefficaces. Ils produisent souvent un nombre explosif de motifs redondants (ex: si <diagnostic A> → <traitement B> est fréquent, <diagnostic A> l'est aussi), ce qui noie l'information pertinente. L'algorithme CloFAST [1] a démontré son efficacité pour extraire des motifs fermés, une représentation compacte et complète des séquences fréquentes. L'enjeu est d'appliquer et d'adapter cette approche pour analyser des cohortes de plusieurs millions de patients. Objectifs Scientifiques et Techniques : L'objectif principal de ce master est de développer un framework pour identifier les trajectoires de soins typiques et atypiques à partir de données de santé réelles et anonymisées, et d'utiliser ces modèles pour la prédiction. 1. Adaptation et Implémentation : Adapter les structures de données efficaces de CloFAST (sparse id-lists, vertical id-lists) pour une exécution distribuée sur une plateforme Big Data comme Apache Spark, en s'inspirant des architectures décrites dans le survey sur le PSPM [2].
31	**Lehis Saida** **lehis.saida@univ-khenchela.dz**	**Théme: Cooperative Control of Urban Traffic Light Systems using Multi-Agent Reinforcement Learning** **Description :** This research aims to develop a cooperative traffic light control system using multi-agent reinforcement learning (MARL), where each intersection acts as an intelligent agent that learns optimal signal timing based on real-time traffic conditions. The system adopts a centralized training and decentralized execution framework to enable coordination among intersections, overcoming the limitations of traditional fixed-time and independent reinforcement learning controllers. Algorithms of reinforcement learning will be explored to enhance

		cooperation and adaptability. The simulation environment will be implemented using SUMO or CityFlow, and performance will be evaluated through key metrics such as average waiting time, queue length, and throughput. By comparing MARL with conventional and independent approaches under dynamic traffic scenarios, the study aims to demonstrate significant reductions in congestion and improved network-wide efficiency. Ultimately, this work contributes to smart city research by introducing a scalable, intelligent, and adaptive approach to urban traffic management.
32	**BEN ATTIA HASIBA** **ben.attia.hasiba@gmail.com**	**Thème : Design and Implementation of a Network Packet Sniffer and Anomaly Analyzer for Intrusion Detection** **Description :** This project aims to design and implement a system that captures, inspects, and analyzes network traffic in real time to detect potential security threats or abnormal behaviors. The system acts as a "packet sniffer," intercepting packets at the network interface level, and then classifying them according to their type, source, destination, protocol, and security relevance. Through statistical and rule-based analysis, the tool can identify suspicious activities such as ARP spoofing, port scanning, and DNS poisoning. Possibilité d'application au monde réel : 100%
33	**BAKHOUCHE Abderaouf** **bakhouche_abderraouf@univ-khenchela.dz**	**Sujet : Développement d'un système de prédiction des performances des étudiants basé sur l'IA** **Description :** Ce mémoire s'intéresse à l'application de l'intelligence artificielle dans le domaine de l'éducation, à travers la conception d'un système de prédiction des performances des étudiants. L'objectif est de développer un modèle capable d'analyser les interactions d'un apprenant avec des exercices (réponses correctes ou incorrectes, temps de réponse, type de question) et de prédire sa réussite future. Le projet reposera dans un premier temps sur l'exploitation de datasets éducatifs publics tels que ASSISTments, EdNet ou KDD Cup 2010, largement utilisés dans la recherche sur les systèmes éducatifs intelligents (Intelligent

		Tutoring Systems). En complément, une mini-plateforme éducative pourra être développée (par exemple via Flask, Streamlit ou autres), permettant à de vrais utilisateurs de répondre à des exercices simples (mathématiques, logique, algorithmique, etc.). Les interactions générées constitueront un dataset personnalisé, venant enrichir ou illustrer les expériences. Cette démarche permet d'ancrer le projet dans un contexte réel et de démontrer la faisabilité d'un système de tutorat intelligent adapté aux besoins locaux. Le mémoire combinera donc : □ Une approche expérimentale : entraînement et comparaison de modèles de Machine Learning (régression logistique, forêts aléatoires, XGBoost, MLP simple) appliqués aux datasets publics. □ Une approche pratique : création éventuelle d'un dataset propre via une mini-plateforme éducative, permettant de tester le système dans un environnement réel.