

ΕΛΛΗΝΙΚΟ ΜΕΣΟΓΕΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ
ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ



ΘΕΜΑ

ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΕΦΑΡΜΟΓΕΣ
ΠΑΡΑΓΩΓΗΣ ΠΕΡΙΕΧΟΜΕΝΟΥ
ΕΡΕΥΝΑ ΚΑΙ ΑΝΑΠΤΥΞΗ ΕΠΙΔΕΙΚΤΙΚΗΣ
ΕΦΑΡΜΟΓΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΕΙΣΗΓΗΤΗΣ: ΚΟΝΤΟΓΙΑΝΝΗ ΕΥΑΓΓΕΛΙΑ ΤΠ4659
ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: κ. ΜΑΛΑΜΟΣ ΑΘΑΝΑΣΙΟΣ

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον καθηγητή κ. Αθανάσιο Μαλάμο για την κατοχύρωση του θέματος αυτής της πτυχιακής εργασίας.

Επίσης θα ήθελα να ευχαριστήσω τους γονείς μου Κωνσταντίνο Κοντογιάννη, Βαρβάρα Παραγιουδάκη και τους αδελφους μου Νίκο και Ιάκωβο οι οποίοι υπήρξαν στήριγμα για μένα όλο αυτόν τον καιρό.

Τέλος, θα ήθελα να ευχαριστήσω και τον αγαπημένο μου Μίλτο για την συνεχή συμπαράσταση σε όλο αυτό το ταξίδι.

Περίληψη

Η παρούσα πτυχιακή εργασία μελετά την ανάπτυξη της τεχνητής νοημοσύνης και επικεντρώνεται στα μοντέλα παραγωγής περιεχομένου και συγκεκριμένα στην ανάπτυξη ενός AI-based chat bot για το Ηράκλειο Κρήτης, χρησιμοποιώντας τις τεχνολογίες Node.js και PHP. Η μεθοδολογία ακολούθησε τα εξής βασικά βήματα:

1. Ανάλυση Απαιτήσεων και Σχεδιασμός Συστήματος: Καθορίστηκαν οι λειτουργικές ανάγκες του chat bot και σχεδιάστηκε η αρχιτεκτονική του συστήματος.
2. Επιλογή Τεχνολογιών και Εργαλείων: Επιλέχθηκαν οι κατάλληλες τεχνολογίες (Node.js, PHP, Nginx) και βιβλιοθήκες (LangChain, OpenAI GPT-4) για την υλοποίηση.
3. Ενσωμάτωση Frontend και Backend: Διαμορφώθηκε ο web server (nginx) για την επικοινωνία μεταξύ της PHP και του Node.js μέσω του endpoint /ask.
4. Εφαρμογή AI Μοντέλου: Χρησιμοποιήθηκε η βιβλιοθήκη LangChain σε συνδυασμό με το GPT-4 API για την επεξεργασία και ανάκτηση πληροφοριών από το αρχείο/βάση δεδομένων.
5. Διασφάλιση Ασφάλειας και Απόδοσης: Εγκαταστάθηκαν SSL πιστοποιητικά μέσω του Certbot για ασφαλή επικοινωνία και χρησιμοποιήθηκε ο PM2 για τη διαχείριση της εφαρμογής Node.js, εξασφαλίζοντας αξιοπιστία και σταθερότητα.
6. Δοκιμές και Αξιολόγηση: Έγιναν εκτεταμένες δοκιμές για την αξιολόγηση της λειτουργικότητας και της απόδοσης του chatbot, διασφαλίζοντας την παροχή ακριβών και αξιόπιστων απαντήσεων στους χρήστες.

Η εφαρμογή ακολούθησε μια ολοκληρωμένη προσέγγιση, εξασφαλίζοντας ότι το chatbot λειτουργεί αποτελεσματικά και ασφαλώς, προσφέροντας αξιόπιστες πληροφορίες στους χρήστες.

Παράλληλα με τα παραπάνω, έγινε μια μελέτη στα κοινωνικά ζητήματα που δημιουργούνται από τη χρήση της τεχνητής νοημοσύνης, έτσι ώστε να τονίσουμε την ανάγκη προσαρμογής της εκάστοτε υλοποίησης με βάση αυτά τα ζητήματα

Abstract

This undergraduate thesis explores the development of artificial intelligence, focusing on content generation models and specifically on the creation of an AI-based chatbot for Heraklion, Crete, utilizing Node.js and PHP technologies. The methodology followed these key steps:

1. **Requirements Analysis and System Design:** The functional needs of the chatbot were identified, and the system architecture was designed to meet these requirements effectively.
2. **Selection of Technologies and Tools:** Appropriate technologies (Node.js, PHP, Nginx) and libraries (LangChain, OpenAI GPT-4) were selected to ensure robust implementation and optimal performance.
3. **Integration of Frontend and Backend:** The web server (Nginx) was configured to facilitate seamless communication between the PHP frontend and the Node.js backend through the `/ask` endpoint.
4. **Implementation of AI Model:** The LangChain library, in combination with the GPT-4 API, was utilized to process and retrieve information from the data file/database, enabling the chatbot to generate accurate responses.
5. **Ensuring Security and Performance:** SSL certificates were installed using Certbot to secure communications, and PM2 was employed to manage the Node.js application, ensuring reliability and stability of the system.
6. **Testing and Evaluation:** Extensive testing was conducted to assess the functionality and performance of the chatbot, ensuring the provision of accurate and reliable responses to users.

The application adopted a comprehensive approach, ensuring that the chatbot operates efficiently and securely, providing reliable information to users. Additionally, a study was conducted on the social issues arising from the use of artificial intelligence, emphasizing the need to adapt each implementation based on these concerns.

Περιεχόμενα

Περίληψη.....	3
Abstract.....	4
Περιεχόμενα.....	5
Εισαγωγή.....	6
Παρουσίαση του Θέματος.....	6
Σκοπός και Στόχοι της εργασίας.....	7
Βασικές Έννοιες της Τεχνητής Νοημοσύνης.....	8
Τεχνητή νοημοσύνη και έννοιες.....	8
Τύποι Τεχνητής Νοημοσύνης, βασικά βήματα δημιουργίας και κύριες τεχνολογίες.....	9
Εφαρμογές της ΑΙ στην Παραγωγή Περιεχομένου.....	16
Δημιουργία Κειμένων: Εργαλεία όπως GPT-4, ChatGPT και άλλες πλατφόρμες.....	16
Δημιουργία Εικόνων και Βίντεο: Εφαρμογές όπως DALL-E, Midjourney.....	17
Άλλες Εφαρμογές: Δημιουργία μουσικής, ηχητικών εφέ, και περιεχομένου για social media.....	18
Περίπτωση Μελέτης: Το Demo ΑΙ για την Πόλη μου.....	18
Περιγραφή του Demo ΑΙ.....	18
Τεχνολογίες που Χρησιμοποιήθηκαν και επεξήγηση λειτουργίας.....	19
Αναλυτική δημιουργία/εγκατάσταση εφαρμογής.....	21
Προετοιμασία σέρβερ.....	21
Κύριος κώδικας και επιμέρους αρχεία.....	25
Εφαρμογές και Οφέλη.....	35
Προκλήσεις και Περιορισμοί.....	36
Οφέλη και Προκλήσεις της Χρήσης ΑΙ.....	37
Οφέλη.....	37
Προκλήσεις.....	38
Πνευματικά Δικαιώματα.....	39
Επιπτώσεις στην Αγορά Εργασίας.....	40
Ασφάλεια και Παραπληροφόρηση.....	41
Συμπεράσματα.....	42
Ευρήματα και επίτευξη στόχων.....	42
Βιβλιογραφία.....	43
Παράρτημα.....	44
Δημιουργία SSH keys & απενεργοποίηση password authentication.....	44
Nucleus Sampling.....	44
Retriever και Vector Store.....	45
RetrievalQChain & LangChain.....	46

Εισαγωγή

Παρουσίαση του Θέματος

Η τεχνητή νοημοσύνη είναι ένας από τους πιο γρήγορα εξελισσόμενος κλάδους της επιστήμης των υπολογιστών. Κύριος στόχος της είναι να δημιουργήσει αλγόριθμους και μοντέλα που θα δίνουν τη δυνατότητα στις μηχανές να εκτελέσουν εργασίες όπου υπο φυσιολογικές συνθήκες θα μπορούσα να εκτελεστούν μόνο από ανθρώπινη νοημοσύνη, όπως αναγνώριση μοτίβων, κατανόηση φυσικής γλώσσας και εκμάθηση. Με απλά λόγια μπορούμε να πούμε ότι η τεχνητή νοημοσύνη είναι η επιστήμη που διδάσκει τους υπολογιστές πως να σκέφτονται και να μαθαίνουν ακριβώς όπως θα έκανε και ένας άνθρωπος. Βασικός στόχος της είναι η δημιουργία μηχανών οι οποίες θα είναι σε θέση να λύσουν προβλήματα να πάρουν αποφάσεις και να μπορούν να προσαρμοστούν και να δράσουν όπως ακριβώς θα έκανε και ένας άνθρωπος στην εκάστοτε περίπτωση.

Τα τελευταία χρόνια οι εξελίξεις στη τεχνητή νοημοσύνη έχουν φέρει τεράστιες αλλαγές σε διάφορους τομείς, από την ιατρική και την οικονομία μέχρι την ψυχαγωγία και την επικοινωνία. Ειδικότερα στον τομέα της παραγωγής περιεχομένου, η τεχνητή νοημοσύνη θα μπορούσε να πει κανείς τι είναι το πιο κρίσιμο και σημαντικό εργαλείο που έχει δημιουργηθεί έως τώρα. Εφαρμογές όπως το chatgpt, dall-e και άλλα αυτοματοποιημένα συστήματα παραγωγής βίντεο, εικόνας και ήχου επιτρέπουν τη δημιουργία περιεχομένου με μεγάλη ποιότητα ταχύτητα αλλά και ακρίβεια αυξάνοντας την παραγωγικότητα στους κλάδους τους οποίους χρησιμοποιούνται

Αν κάνουμε μία ιστορική αναδρομή στην πορεία της τεχνητής νοημοσύνης θα δούμε ότι υπάρχει μία συνεχής εξέλιξη από τις πρώτες αυτόνομες μηχανές μέχρι τα σύγχρονα τεχνολογικά μοντέλα που βασίζονται σε εξελιγμένους αλγόριθμους, hardware υψηλών επιδόσεων αλλά και πρόσβαση σε μεγάλο όγκο των δεδομένων. Ορόσημα στον τομέα θεωρούνται επίσης η ανάπτυξη των πρώτων νευρωνικών δικτύων και η δημιουργία αλγορίθμων μηχανικής μάθησης τα οποία έχουν διευρύνει κατά πολύ τη δυναμική της τεχνητής νοημοσύνης ειδικά σε παραγωγή του περιεχομένου

Το πόσο σημαντική είναι η χρήση της τεχνητής νοημοσύνης φαίνεται αν κάτσουμε να αναλογιστούμε το πόσους πόρους μπορούμε να εξοικονομήσουμε (είτε από άποψη οικονομικού είτε από όπως ανθρώπινου δυναμικού) αυτοματοποιώντας τη διαδικασία

παραγωγής περιεχομένου δημιουργώντας ποιοτικό αλλά και πλήρως προσωποποιημένο περιεχόμενο το οποίο θα είναι σε θέση να καλύψει τις ανάγκες του χρήστη και παράλληλα να βελτιώσει την εμπειρία του

Τα τελευταία χρόνια οι εφαρμογές της τεχνητής νοημοσύνης έχουν μπει για τα καλά στην καθημερινότητά μας αφού όλο ένα και περισσότεροι κλάδοι τις εντάσσουν στις υπηρεσίες τους. Από Chatbot τα οποία είναι σε θέση να εξυπηρετήσουν αιτήματα και να λύσουν προβλήματα τα οποία μπορεί να αντιμετωπίζουμε σε μια υπηρεσία, μέχρι και τη δημιουργία πλήρως προσωποποιημένων λύσεων/προτάσεων όπως για παράδειγμα δημιουργία διατροφικών πλάνων ή προγραμμάτων εκγύμνασης.

Στο πλαίσιο λοιπόν της παρούσας εργασίας θα αναλύσουμε όλα τα παραπάνω εστιάζοντας κυρίως στη χρήση τεχνητής νοημοσύνης στην παραγωγή περιεχομένου ενώ παράλληλα θα δείξουμε την πρακτική εφαρμογή της μέσω της δημιουργίας ενός demo AI που θα έχεις σκοπό την παροχή πληροφοριών γύρω από την πόλη κατοικίας μας.

Σκοπός και Στόχοι της εργασίας

Η τεχνητή νοημοσύνη είναι ένας από τους πιο γρήγορα αναπτυσσόμενους κλάδους της επιστήμης των υπολογιστών, με εφαρμογές που συναντώνται σε κάθε πτυχή της καθημερινότητάς μας. Η ΤΝ έχει ως στόχο τη δημιουργία αλγορίθμων οι οποίοι με τη βοήθεια του hardware μπορούν να εκτελούν ενέργειες οι οποίες χρειάζονται "νοημοσύνη", όπως η κατανόηση ανθρώπινης γλώσσας και η εκμάθηση μέσα από μοτίβα και πρότυπα. Με απλά λόγια η τεχνητή νοημοσύνη προσπαθεί να κάνει τους υπολογιστές να μιλούν, να κινούνται και να συμπεριφέρονται όπως ένας άνθρωπος, εκτελώντας εργασίες οι οποίες μέχρι τώρα γίνονται αποκλειστικά από ανθρώπινο δυναμικό, βελτιώνοντας τη καθημερινότητά μας.

Ένας τομέας δραστηριότητας/εφαρμογής της τεχνητής νοημοσύνης είναι η παραγωγή περιεχομένου. Ένας κρίσιμος τομέας που επηρεάζει τόσο τη δημιουργική διαδικασία (συγγραφή κειμένων, στοίχων, σεναρίων, ειδήσεων κλπ) όσο και την αποτελεσματικότητα αυτών. Δημιουργία κειμένων, εικόνων, παραγωγή βίντεο ή ακόμα και μουσικής, η τεχνητή νοημοσύνη μπορεί να προσφέρει εργαλεία που να διευκολύνουν και να αυξήσουν στο μέγιστο τη δημιουργία περιεχομένου για τους χρήστες, συμβάλλοντας στη παραγωγικότητα και την ταχύτητα.

Στο πλαίσιο της μελέτης μας για τη παρούσα εργασία, εξετάζουμε τη τεχνητή νοημοσύνη στη παραγωγή περιεχομένου δίνοντας έμφαση σε ένα demo AI το οποίο θα δημιουργήσουμε/αναπτύξουμε. Το συγκεκριμένο εργαλείο θα είναι σε θέση να παρέχει πληροφορίες σχετικά με το Ηράκλειο Κρήτης, απαντώντας σε ερωτήσεις χρηστών με ακρίβεια και πλήρως ενημερωμένα στοιχεία/πληροφορίες για διάφορα θέματα που αφορούν τη πόλη μας όπως τοπικά events, ιστορικά γεγονότα, υπηρεσίες, αξιοθέατα και άλλα. Μέσω

αυτής της εφαρμογής και με βάση πάντα τη μελέτη που έχουμε κάνει και θα παρουσιάσουμε, έχουμε σκοπό να αναδείξουμε τις δυνατότητες της παραγωγής περιεχομένου με τη χρήση τεχνητής νοημοσύνης και να δείξουμε πως αυτή μπορεί να χρησιμοποιηθεί αποτελεσματικά από το ευρύ κοινό, εξυπηρετώντας τις ανάγκες του

Τέλος, πέρα από τα τεχνικά όμως θέματα, η εργασία μας θα αναπτυχθεί και γύρω από τα κοινωνικά και ηθικά ζητήματα που προκύπτουν από τη χρήση τεχνητής νοημοσύνης και που συνδέονται με ζητήματα πνευματικών δικαιωμάτων (για τις περιπτώσεις της παραγωγής κειμένου), επιπτώσεις στην αγορά εργασίας, ζητήματα ασφάλειας και ορθότητας πληροφοριών, ορθή χρήση και περιπτώσεις εξαπάτησης και άλλα παρόμοια ζητήματα τα οποία καθιστούν τη κατανόηση των συνεπειών της χρήσης της τεχνητής νοημοσύνης απαραίτητη για το ευρύ κοινό και όχι μόνο.

Βασικές Έννοιες της Τεχνητής Νοημοσύνης

Τεχνητή νοημοσύνη και έννοιες

Η ορολογία της τεχνητής νοημοσύνης είναι ο κλάδος της πληροφορικής ο οποίος εστιάζει στην σχεδίαση και την δημιουργία αλγορίθμων και μοντέλων όπου επιτρέπουν σε υπολογιστικά συστήματα να εκτελούν εργασίες μιμούμενα την ανθρώπινη νοημοσύνη. Ορισμένες από αυτές τις διαδικασίες είναι η ανάλυση και η μάθηση δεδομένων, η προσαρμοστικότητα αναλόγως το ζήτημα το οποίο εξυπηρετεί καθώς και η επίλυση σύνθετων προβλημάτων.

Η ΤΝ είναι μία επιστήμη η οποία συνδυάζει πληθώρα επιστημών όπως η ψυχολογία, η φιλοσοφία, η πληροφορική, η νευρολογία, η γλωσσολογία και η επιστήμη μηχανικών. Ο στόχος της είναι με τον συνδυασμό των παραπάνω επιστημών να συνθέσει μία ευφυής συμπεριφορά σε μία μηχανή ή σε υπολογιστή ειδικής κατασκευής, η οποία μιμείται την ανθρώπινη νοημοσύνη.

Χωρίζεται σε δύο είδη η συγκεκριμένη επιστήμη, στην συμβολική τεχνητή νοημοσύνη η οποία προσπαθεί να αφομοιώσει την ανθρώπινη νοημοσύνη αλγοριθμικά χρησιμοποιώντας λέξεις, ιδέες και λογικούς κανόνες για να λύνουν προβλήματα και στην υπό συμβολική τεχνητή νοημοσύνη, η οποία προσπαθεί να αναπαράγει την ανθρώπινη νοημοσύνη χρησιμοποιώντας βασικά αριθμητικά μοντέλα συνδυαστικά με την εκμάθηση μέσα από την λήψη μεγάλων συνόλων δεδομένων. Η υπο συμβολική τεχνητή νοημοσύνη καταφέρνει να προσομοιάσει πραγματικές βιολογικές διαδικασίες όπως για παράδειγμα η λειτουργία του εγκεφάλου και κατά συνέπεια και η εξέλιξη .

Η διάκριση των δύο παραπάνω προσεγγίσεων σε συμβολικές και υποσυμβολικές έγκειται στα εργαλεία που την χρησιμοποιούν. Ωστόσο δεν είναι σπάνιος ο συνδυασμός πολλαπλών

προσεγγίσεων κατά την προσπάθει επίλυσης ενός προβλήματος. Η ΤΝ σύμφωνα με τον επιθυμητό στόχο κατηγοριοποιείται σε πολλούς ακόμη τομείς άλλου τύπου όπως είναι η επίλυση προβλημάτων, η μηχανική μάθηση, η δημιουργία και ανακάλυψη γνώσης, τα συστήματα γνώσεις κ.α. Αποτελεί πολύ επιστημονικό πεδίο με διασυνδέσεις σε άλλους κλάδους όπως η μηχανική όραση, η επεξεργασία φυσικής γλώσσας ή η ρομποτική, τα οποία εξελίσσονται ως ανεξάρτητα πεδία εντός του ευρύτερου πλαισίου της σύγχρονης και συνεχώς μεταβαλλόμενης τεχνητής νοημοσύνης.

Οι λογοτεχνικές και κινηματογραφικές απεικονίσεις της τεχνητής νοημοσύνης, κυρίως ως ανθρωποειδών ρομπότ με συνείδηση, έχουν διαμορφώσει σε μεγάλο βαθμό τις προσδοκίες του κοινού και έχουν επηρεάσει τις πρώτες έρευνες στον τομέα. Ωστόσο την πραγματικότητα η πλειονότητα των ερευνητών στην ΤΝ επικεντρώνεται στην ανάπτυξη συστημάτων που μπορούν να επιλύσουν συγκεκριμένα προβλήματα με υψηλή ακρίβεια (ασθενής ΤΝ), ενώ ένας μικρότερος αριθμός ερευνητών επιδιώκει την δημιουργία μηχανών με γενική νοημοσύνη που να προσομοιώνουν την ανθρώπινη σκέψη (ισχυρή ΤΝ). Βεβαίως μιλώντας για την σύγχρονη τεχνητή νοημοσύνη μπορούμε να πούμε ότι διαθέτει «μαθηματικοποιημένα» και ταχέως εξελισσόμενα πεδία πληροφορικής. Η τεχνητή νοημοσύνη έχει μεταμορφωθεί από έναν θεωρητικό κλάδο που είχε ως επίκεντρο λογικές αναλύσεις σε ένα πρακτικό πεδίο που αξιοποιεί μαθηματικά μοντέλα και μεγάλες ποσότητες δεδομένων. Η ανάπτυξη ισχυρών υπολογιστών, ειδικά των γραφικών καρτών, έχει επιταχύνει αυτή τη μετατόπιση, καθιστώντας εφικτή την εκπαίδευση πολύπλοκων αλγορίθμων.

Τύποι Τεχνητής Νοημοσύνης, βασικά βήματα δημιουργίας και κύριες τεχνολογίες

Reactive machines (Αντιδραστικά Μηχανήματα)

Αυτές οι μηχανές λειτουργούν μιμούμενες την ικανότητα του ανθρώπινου εγκεφάλου να λαμβάνει και να επεξεργάζεται διαφορετικά ερεθίσματα. Σε αντίθεση όμως με τον εγκέφαλο, δεν διαθέτουν μνήμη. Αυτό σημαίνει ότι δεν μπορούν να αξιοποιήσουν προηγούμενες εμπειρίες για να βελτιώσουν την απόδοσή τους, άρα στερούνται την ικανότητα της "μάθησης", πράγμα που σημαίνει ότι μια είσοδος παρέχει πάντα την ίδια έξοδο. Η λειτουργία τους περιορίζεται στην αυτόματη ανταπόκριση σε ένα προκαθορισμένο σύνολο ή συνδυασμό εισροών. Η μνήμη, ως παράγοντας βελτιστοποίησης, απουσιάζει.

Τα μοντέλα μηχανικής εκμάθησης τείνουν να είναι αντιδραστικά μηχανήματα, επειδή λαμβάνουν δεδομένα πελατών, όπως το ιστορικό αγορών ή αναζήτησης, και τα χρησιμοποιούν για να παρέχουν προτάσεις στους ίδιους πελάτες.

Αυτός ο τύπος ΑΙ είναι αντιδραστικός. Εκτελεί «σούπερ» τεχνητή νοημοσύνη, επειδή ο μέσος άνθρωπος δεν θα μπορούσε να επεξεργαστεί τεράστιες ποσότητες δεδομένων.

Η τεχνητή νοημοσύνη Reactive AI, όντας αξιόπιστη, τροφοδοτεί καινοτόμες εφευρέσεις, όπως τα αυτοοδηγούμενα οχήματα. Λειτουργεί άψογα, αντιδρώντας σε δεδομένα και καταστάσεις, στερείται όμως την ικανότητα πρόβλεψης μελλοντικών αποτελεσμάτων, αν δεν τροφοδοτηθεί με τις απαραίτητες πληροφορίες.

Αντιθέτως, η ανθρώπινη ύπαρξη διαφοροποιείται. Οι περισσότερες ενέργειές μας δεν βασίζονται σε αντιδράσεις, καθώς στερούμαστε το πλήθος πληροφοριών που απαιτούνται για άμεση ανταπόκριση. Διαθέτουμε όμως την ικανότητα αποθήκευσης και επεξεργασίας πληροφοριών, χτίζοντας μια βάση γνώσεων και εμπειριών. Βάσει αυτών, είτε επιτυχημένων είτε αποτυχημένων, διαμορφώνουμε την μελλοντική μας συμπεριφορά, προσαρμόζοντάς την σε παρόμοιες καταστάσεις.

Limited Memory (Περιορισμένης Μνήμης)

Ο επόμενος τύπος ΑΙ στην εξέλιξή του είναι η περιορισμένη μνήμη. Οι μηχανές περιορισμένης μνήμης είναι μηχανές που, εκτός από τις δυνατότητες αμιγώς αντιδραστικών μηχανών, είναι επίσης ικανές να μαθαίνουν από ιστορικά δεδομένα για να λαμβάνουν αποφάσεις. Σχεδόν όλες οι υπάρχουσες εφαρμογές που γνωρίζουμε εμπίπτουν σε αυτήν την κατηγορία ΑΙ. Όλα τα σημερινά συστήματα τεχνητής νοημοσύνης, όπως αυτά που χρησιμοποιούν βαθιά μάθηση, εκπαιδεύονται από μεγάλους όγκους δεδομένων εκπαίδευσης που αποθηκεύουν στη μνήμη τους για να σχηματίσουν ένα μοντέλο αναφοράς για την επίλυση μελλοντικών προβλημάτων.

Ένα πολύ καλό παράδειγμα στο πλαίσιο ΑΙ περιορισμένης μνήμης είναι τα αυτόνομα οχήματα. Χρησιμοποιείται για την παρακολούθηση της ταχύτητας και της κατεύθυνσης άλλων αυτοκινήτων, βοηθώντας τα να «καθοδηγούν το δρόμο» και να προσαρμόζονται εάν χρειάζεται. Τα αυτόνομα αυτοκίνητα χρησιμοποιούν τα δεδομένα που συλλέχθηκαν πρόσφατα στο παρελθόν για να λάβουν γρήγορες αποφάσεις. Με την κατανόηση και την ερμηνεία των εισερχόμενων δεδομένων, τα αυτοκίνητα μπορούν να είναι ασφαλή στους δρόμους. Όπως και τα αξιόπιστα για τον άνθρωπο αυτοκίνητα, μπορούν να οδηγούν και να λειτουργούν επαρκώς. Τα αυτοοδηγούμενα αυτοκίνητα παρακολουθούν το περιβάλλον τους και λαμβάνουν υπόψη την κίνηση άλλων συμμετεχόντων στην κυκλοφορία λαμβάνοντας υπόψη την κίνηση άλλων συμμετεχόντων στην τροχαία στο οπτικό πεδίο. Πριν από τα ΑΙ Περιορισμένης Μνήμης, προηγουμένως χρειαζόταν περισσότερο χρόνο περίπου 100 δευτερόλεπτα για να αντιδράσει και να λάβει αποφάσεις με βάση εξωτερικούς παράγοντες.

Theory of Mind (Η Θεωρία του Νου)

Μια τεχνητή νοημοσύνη επιπέδου θεωρίας του νου διαθέτει μία ριζικά αναβαθμισμένη ικανότητα κατανόησης των οντοτήτων με τις οποίες αλληλεπιδρά. Η τεχνητή νοημοσύνη θα

μπορεί να διακρίνει και να ερμηνεύει τις ανάγκες, τα συναισθήματα, τις προσθέσεις, τις πεποιθήσεις και τις διαδικασίες σκέψης των οντοτήτων αυτών.

Αυτή η βαθύτερη κατανόηση θα οδηγήσει σε βελτιωμένη επικοινωνία καθώς και την προσομοίωση ή μοντελοποίηση ανθρώπινων διαδικασιών σκέψης, καθώς ένα σύστημα ΑΙ θα μπορεί να προσαρμόσει τον τρόπο επικοινωνίας του στις ανάγκες και τα συναισθήματα της οντότητας. Η συνεργασία θα γίνει αποτελεσματικότερη, καθώς το σύστημα ΑΙ θα λαμβάνει υπόψη τις πεποιθήσεις και τον τρόπο σκέψης της οντότητας. Η ενσυναίσθηση θα αναπτυχθεί, καθώς το ΑΙ θα νιώθει και θα κατανοεί τα συναισθήματα της οντότητας, χτίζοντας μία πιο ουσιαστική σχέση.

Αν και η συμμετοχή της Θεωρία του Νου στα συστήματα ΑΙ βρίσκεται σε πρωταρχικό στάδιο, έχει κερδίσει αρκετή έλξη με μερικές από τις βασικές εξελίξεις αυτού του τομέα να περιλαμβάνουν τα εξής:

Αναγνώριση συναισθημάτων: Πλέον τα συστήματα ΑΙ μπορούν να αναγνωρίσουν τα ανθρώπινα συναισθήματα από πολλαπλά ερεθίσματα όπως ο τόνος της φωνής, οι εκφράσεις του προσώπου και η ανάλυση συναισθημάτων κειμένου. Αυτό είναι το πρώτο και πιο σημαντικό βήμα ώστε να καταφέρει ένας αλγόριθμος να κατανοήσει συναισθηματικές καταστάσεις των ανθρώπων.

Προγνωστική Μοντελοποίηση: Τα μοντέλα μηχανικής μάθησης χρησιμοποιούνται για την πρόβλεψη της ανθρώπινης συμπεριφοράς βάσει των ιστορικών δεδομένων. Ειδικότερα ως υποθέσουμε ότι έχουμε ένα σύστημα συστάσεων, εκείνο χρησιμοποιεί προγνωστικά μοντέλα ώστε να προχωρήσει σε κάποια πρόταση για προϊόν, τραγούδι ή ταινία με βάση τις προηγούμενες προτιμήσεις και συμπεριφορές των χρηστών.

Συνομιλητική τεχνητή νοημοσύνη: Τα chatbot και οι εικονικοί βοηθοί ενσωματώνουν πιο εξελιγμένα συστήματα διαλόγου που στοχεύουν στην κατανόηση του πλαισίου, της πρόθεσης και της συναισθηματικής κατάστασης των χρηστών. Μπορούν να ανταποκριθούν με μεγαλύτερη ενσυναίσθηση, κάνοντας τις αλληλεπιδράσεις πιο ανθρώπινες.

Προσομοίωση και Γνωσιακή Μοντελοποίηση: Η ανάπτυξη συστημάτων τεχνητής νοημοσύνης τα οποία μπορούν να προσομοιώσουν ανθρώπινες διαδικασίες σκέψης και επιτρέπουν την καλύτερη κατανόηση και πρόβλεψη της ανθρώπινης συμπεριφοράς σε διάφορες καταστάσεις.

Συστήματα πολλαπλών παραγόντων: Σε περιβάλλον στο οποίο υπάρχουν πολλαπλοί παράγοντες, τα συστήματα τεχνητής νοημοσύνης σχεδιάζονται με τέτοιο τρόπο ώστε να προβλέπουν τις προθέσεις και τις ενέργειες άλλων οντοτήτων είτε είναι ανθρώπινης είτε είναι τεχνητής νοημοσύνης. Αυτό είναι ζωτικής σημασίας σε εφαρμογές όπως τα αυτόνομα οχήματα όπου το σύστημα θα πρέπει να προβλέπει τις ενέργειες των άλλων οδηγών.

Συνολικά αξίζει να σημειωθεί η τεράστια ανάγκη για χρήση του Theory of Mind AI σε πολλές εφαρμογές και τομείς όπως για παράδειγμα στην υγειονομική περίθαλψη και την εξυπηρέτηση πελατών.

Ωστόσο είναι σημαντική η διασφάλιση του απορρήτου, η πρόληψη της κακής χρήσης και η αντιμετώπιση της μεροληψίας καθώς και η διατήρηση της διαφάνειας στην λήψη αποφάσεων τεχνητής νοημοσύνης αποτελούν πρωταρχικό μέλημα. Επιπλέον, η δυνατότητα των συστημάτων τεχνητής νοημοσύνης να χειραγωγούν τα ανθρώπινα συναισθήματα ή να εξαπατούν τους χρήστες πρέπει να παρακολουθείται προσεκτικά.

Ποια τα βασικά βήματα δημιουργίας ενός αντιδραστικού μηχανήματος τεχνητής νοημοσύνης

Η διαδικασία για την υλοποίηση μίας Reactive AI Machine έχει ως εξής:

Προσδιορισμός του προβλήματος καθώς και καθορισμός των στόχων

Το πρωταρχικό στάδιο για την ανάπτυξη της τεχνητής νοημοσύνης είναι ο καθορισμός σαφών και μετρήσιμων στόχων. Για παράδειγμα έχουμε την περίπτωση που θέλουμε να βελτιώσουμε την αποτελεσματικότητα, την ακρίβεια αλλά και την εμπειρία των πελατών σε μία επιχείρηση. Αυτό απαιτεί μία σταθερή κατανόηση των λειτουργιών της συγκεκριμένης επιχείρησης και των πιθανών προκλήσεων που καλείται να αντιμετωπίσει. Για τον λόγο αυτό εργαλεία όπως το λογισμικό οπτικοποίησης δεδομένων μπορούν να βοηθήσουν στην εύρεση μοτίβων βάση των υπάρχων δεδομένων.

Για τον προσδιορισμό των στόχων δεν θα πρέπει να ξεχάσουμε τα ακόλουθα:

- 1) Σκοπιμότητα: Είναι εφικτό η τεχνητή νοημοσύνη να αντιμετωπίσει αποτελεσματικά αυτό το ζήτημα;
- 2) Αντίκτυπος: Τι όφελος θα φέρει στην επιχείρησή σας η επίλυση του συγκεκριμένου ζητήματος;
- 3) Διαθεσιμότητα δεδομένων: Υπάρχουν επαρκή και ποιοτικά δεδομένα που σχετίζονται με το συγκεκριμένο ζήτημα;

Αυτοί είναι οι βασικοί παράγοντες οι οποίοι καθοδηγούν τον τρόπο προσέγγισης τον οποίο πρέπει να ακολουθήσετε ώστε να δημιουργήσετε μία τεχνητή νοημοσύνη η οποία θα ωφελεί πραγματικά την επιχείρησή σας.

Σύλλογή και προετοιμασία δεδομένων

Το συγκεκριμένο μοντέλο τεχνητής νοημοσύνης μαθαίνει από τα δεδομένα εκπαίδευσης. Συνεπώς είναι απαραίτητη η συλλογή σχετικών συνόλων δεδομένων υψηλής ποιότητας. Η συλλογή των δεδομένων μπορεί να πραγματοποιηθεί είτε από εσωτερικές βάσεις δεδομένων, αγορά δεδομένων ή προμήθεια ανοικτών συνόλων δεδομένων με μόνη προϋπόθεση ότι το σύνολο των δεδομένων αντιπροσωπεύει με ακρίβεια τον χώρο των προβλημάτων.

Έπειτα ακολουθεί η διαλογή των πληροφοριών που διαθέτουμε. Ειδικότερα ακολουθεί ο καθαρισμός δεδομένων, ο χειρισμός των τιμών που λείπουν ή οι ασυνεπείς καταχωρήσεις και τέλος η αφαίρεση των ακραίων στοιχείων. Για αυτό τον σκοπό εργαλεία όπως η βιβλιοθήκη Pandas της Python ή το dplyr του R μπορούν να φανούν χρήσιμα.

Οι στόχοι που πρέπει να υπάρχουν σε αυτό το σημείο είναι οι εξής:

- 1) Απόρρητο δεδομένων: Θα πρέπει να βεβαιωθούμε ότι τα δεδομένα συμμορφώνονται με τους κανονισμούς απορρήτου
- 2) Συνάφεια: Πρέπει να βεβαιωθούμε ότι τα δεδομένα είναι σχετικά με το πρόβλημα το οποίο έχετε καθορίσει
- 3) Όγκος: Πρέπει να έχουμε στα υπόψη ότι ο μεγάλος όγκος δεδομένων δεν είναι απαραίτητα καλύτερος. Ας θυμηθούμε ότι η το συγκεκριμένο μοντέλο τεχνητής νοημοσύνης μαθαίνει από τα δεδομένα τα οποία διαθέτει. Συνεπώς ο μεγάλος όγκος άσχετων δεδομένων μπορεί να παρεμποδίσουν την διαδικασία εκμάθησης της τεχνητής νοημοσύνης

Επιλογή εργαλείων και εφαρμογών

Ένα πολύ σημαντικό σημείο της υλοποίησης ενός ΑΙ είναι η επιλογή των κατάλληλων εργαλείων και εφαρμογών σύμφωνα με τις εκάστοτε ανάγκες. Μπορούμε να επιλέξουμε πλατφόρμες οι οποίες βασίζονται σε cloud όπως είναι το AWS ή το Google Cloud για επεκτασιμότητα ή τοπικούς διακομιστές για την αφάλεια των δεδομένων.

Η Python είναι μία δημοφιλής επιλογή γλώσσας προγραμματισμού χάρη στην απλότητα και την εκτεταμένη υποστήριξη βιβλιοθήκης για μηχανική εκμάθηση. Το R είναι επίσης χρήσιμο για στατιστικούς υπολογισμούς.

Παράγοντες επιλογής κατάλληλων εργαλείων:

- 1) Επεκτασιμότητα: Μπορεί μελλοντικά το συγκεκριμένο εργαλείο/πλατφόρμα να αντέξει ανάπτυξη;
- 2) Κόστος - Αποτελεσματικότητα: Η τιμή του είναι μέσα στα όρια του προϋπολογισμού σας σε σχέση με την αποτελεσματικότητά του
- 3) Συμβατότητα Λογισμικού: Είναι συμβατό το συγκεκριμένο εργαλείο με άλλα συστήματα που χρησιμοποιούνται ήδη;

Με την επιλογή του κατάλληλου εργαλείου ή της κατάλληλης πλατφόρμας μπορούμε να διασφαλίσουμε την αποδοτικότητα και την αποτελεσματικότητα της διαδικασίας ανάπτυξης του ΑΙ.

Δημιουργία αλγορίθμου ή επιλογή μοντέλου

Για την δημιουργία ενός αλγορίθμου ή την επιλογή προϋπάρχοντος μοντέλου τεχνητής νοημοσύνης θα πρέπει να εξετάσουμε την πολυπλοκότητα του προβλήματος, τον όγκο των δεδομένων καθώς και την τεχνογνωσία της ομάδας η οποία θα υλοποιήσει το μοντέλο.

Για την δημιουργία ενός αλγορίθμου απο την αρχή θα πρέπει να υπάρχει σχετική επάρκεια σε γλώσσες προγραμματισμού όπως η Python ή η R και μία καλή γνώση στην μηχανική μάθηση. Για την επιλογή μοντέλων εργαλεία όπως το TensorFlow ή το PyTorch προσφέρουν προεκπαιδευμένα μοντέλα που μπορούν να προσαρμοστούν με ακρίβεια στην εκάστοτε ανάγκη.

Οι βασικές εκτιμήσεις είναι οι εξής:

- 1) Υπολογιστικοί Πόροι: Μερικοί αλγόριθμοι/μοντέλα απαιτούν περισσότερη επεξεργαστική ισχύ
- 2) Ακρίβεια έναντι Ταχύτητας: Μοντέλα υψηλής ακρίβειας ενδέχεται να χρειαστούν περισσότερο χρόνο ώστε να εκπαιδευτούν ή για να εκτελεστούν
- 3) Ερμηνευσιμότητα: Θα πρέπει η διαδικασία λήψης αποφάσεων του μοντέλου να είναι κατανοητοί

Σε περίπτωση που αναφερόμαστε σε μία επιχείρηση μεσαίας κλίμακας που στοχεύει στην βελτίωση της αποτελεσματικότητας, την ακρίβεια αλλά και την εμπειρία των πελατών, η αξιοποίηση προϋπάρχοντων μοντέλων ίσως να είναι μία αποτελεσματική επιλογή. Μπορούμε με την χρήση εργαλείων όπως το TensorFlow ή το PyTorch να τελειοποιήσουμε ένα μοντέλο κατάλληλο για χρήση επεξεργασίας φυσικής γλώσσας.

Το ζήτημα το οποίο χρήζει μεγαλύτερης προσοχής είναι η εξισορρόπηση της ακρίβειας και της ταχύτητας, διασφαλίζοντας ότι οι αποκρίσεις του μοντέλου είναι ακριβείς. Σε αυτό όμως δεν θα πρέπει να ξεχάσουμε τους χρόνους απόκρισης οι οποίοι θα πρέπει να είναι εξίσου γρήγοροι.

Εκπαίδευση Αλγορίθμου

Ο τρόπος εκπαίδευσης ενός μοντέλου τεχνητής νοημοσύνης πραγματοποιείται με την συνεχή ανατροφοδότηση με πληθώρα δεδομένων τα οποία του δίνουν την δυνατότητα να βελτιώσει την απόδοση του. Για τον λόγο αυτό είναι αναγκαίο ένα σύνολο δεδομένων χωρισμένο σε δύο είδη, της εκπαίδευσης και της επικύρωσης. Για την συγκεκριμένη διαδικασία θα πρέπει να βεβαιωθούμε ότι τα δεδομένα είναι ορθά και σχετικά με το μοντέλο που θέλουμε να

δημιουργήσουμε.

Είναι σημαντικό να καταφέρουμε να πετύχουμε υπερπροσαρμογή. Υπερπροσαρμογή είναι όταν το μοντέλο εκπαιδεύεται πολύ καλά στα τωρινά δεδομένα αλλά δεν έχει καθόλου καλή απόδοση στα νέα δεδομένα που λαμβάνει.

Θα πρέπει ωστόσο να βεβαιωθούμε ότι υπολογιστικοί πόροι είναι επαρκείς, η εκπαίδευση μπορεί να είναι έντονη σε πόρους.

Δεν θα πρέπει να ξεχνάμε ότι η διαδικασία της εκπαίδευσης είναι μία δυναμική διαδικασία η οποία διαθέτει συνεχής κύκλους μάθησης και προσαρμογής στην οποία ο αλγόριθμος θα πρέπει να είναι ανοιχτός

Για να διαχειριστούμε την συγκεκριμένη διαδικασία μπορούμε να χρησιμοποιήσουμε εργαλεία όπως το TensorFlow, το Keras ή το PyTorch.

2.3 Εισαγωγή σε Machine Learning, Deep Learning, Νευρωνικά Δίκτυα, και Επεξεργασία Φυσικής Γλώσσας (NLP).

Machine Learning

Εξ ορισμού η μηχανική μάθηση ορίζεται ένα μερίδιο της τεχνητής νοημοσύνης το οποίο επικεντρώνεται στην εξέλιξη αλγορίθμων και στατιστικών μοντέλων που δίνουν την δυνατότητα σε υπολογιστές να εκτελούν συγκεκριμένες εργασίες χωρίς να έχουν οριστεί κανόνες. Ειδικότερα, τα συγκεκριμένα συστήματα μηχανικής μάθησης δεν προγραμματίζονται με προκαθορισμένους κανόνες αλλά χρησιμοποιούν δεδομένα προκειμένου να ανακαλύψουν μοτίβα και σχέσεις με σκοπό να μπορούν να κάνουν προβλέψεις ή να λαμβάνουν αποφάσεις. Ωστόσο η συγκεκριμένη διαδικασία εξετάζεται σε μεγάλα σύνολα δεδομένων με αποτέλεσμα να δίνει την δυνατότητα στους αλγόριθμο να βελτιώνουν την απόδοση τους καθώς έρχονται αντιμέτωποι με πολλαπλές πληροφορίες.

Deep Learning

Το Deep Learning είναι ένας κλάδος της μηχανικής μάθησης αρκετά περίπλοκος καθώς η λειτουργία του εμπνέεται από την λειτουργία του ανθρώπινου εγκεφάλου. Αυτό υλοποιείται βάση ενός αλγορίθμου ο οποίος ονομάζεται Artificial Neural Network. Για τον λόγο αυτό ο χρόνος δημιουργίας τέτοιων αλγορίθμων καθώς και ο χρόνος εκτέλεσης τους διαρκεί περισσότερο χρόνο από έναν αλγόριθμο machine learning

Νευρωνικά Δίκτυα

Τα νευρωνικά δίκτυα είναι επίσης ένας κλάδος της μηχανικής μάθησης ο οποίος μιμείται τα βιολογικά νευρωνικά δίκτυα που υπάρχουν στον ανθρώπινο εγκέφαλο. Τα νευρωνικά δίκτυα είναι ανεπτυγμένα μαθηματικά μοντέλα τα οποία εξυπηρετούν στην ανίχνευση μοτίβων καθώς έχουν την δυνατότητα να εκπαιδευθούν από μόνα τους μέσω αλγορίθμων καθώς και μέσω της ανάλυσης των δεδομένων που λαμβάνουν. Τα νευρωνικά δίκτυα αποτελούνται από πολλούς απλούς υπολογιστικούς κόμβους οι οποίοι ενώνονται μέσω πολλών διασυνδέσεων, οι λεγόμενοι νευρώνες.

Επεξεργασία Φυσικής Γλώσσας (NLP)

Η Επεξεργασία Φυσικής Γλώσσας αποτελεί έναν κεντρικό πυλώνα της σύγχρονης τεχνητής νοημοσύνης, συνδυάζοντας γλωσσολογία και επιστήμη των υπολογιστών. Στόχος της είναι να καταστήσει τους υπολογιστές ικανούς να κατανοούν, να ερμηνεύουν και να παράγουν ανθρώπινη γλώσσα. Λειτουργεί με τη βοήθεια αλγορίθμων μηχανικής μάθησης και νευρωνικών δικτύων, οι υπολογιστές αναλύουν τεράστιες ποσότητες κειμένου, αναγνωρίζοντας γραμματικά μοτίβα, συντακτικές δομές και το σημασιολογικό περιεχόμενο των λέξεων. Αυτή η βαθιά κατανόηση της ανθρώπινης γλώσσας επιτρέπει στους υπολογιστές να εκτελούν μια πληθώρα εργασιών, όπως η αναγνώριση ομιλίας (σημαντικός σταθμός για την δημιουργία chatbot και ψηφιακών βοηθών), αυτόματη μετάφραση ή ανάλυση συναισθημάτων.

Εφαρμογές της ΑΙ στην Παραγωγή Περιεχομένου

Η επιστήμη της Τεχνητής Νοημοσύνης έχει εφαρμογή σε πολλούς τομείς, ένας από αυτούς είναι η παραγωγή περιεχομένου η οποία έχει εξελιχθεί ραγδαία τα τελευταία έτη.

Δημιουργία Κειμένων: Εργαλεία όπως GPT-4, ChatGPT και άλλες πλατφόρμες.

Μερικά από τα πιο γνωστά εργαλεία δημιουργίας κειμένου είναι το GPT-4 και το ChatGPT. Είναι εργαλεία μεγάλων γλωσσικών μοντέλων που βασίζονται σε αρχιτεκτονική μετασχηματιστών. Τα μοντέλα αυτά έχουν εκπαιδευτεί σε τεράστιες ποσότητες κειμένου και έχουν την ικανότητα να παράγουν κείμενο όμοιο με κείμενο γραμμένο από τον άνθρωπο, να

μεταφράζουν γλώσσες, να δημιουργούν διαφορετικούς τύπους δημιουργικού περιεχομένου και να απαντούν στις ερωτήσεις των χρηστών με έναν ενημερωτικό τρόπο.

Το GPT-4 είναι η πιο πρόσφατη και εξελιγμένη έκδοση του GPT. Προσφέρει βελτιωμένες επιδόσεις σε μια σειρά από εργασίες, όπως η κατανόηση φυσικής γλώσσας, η δημιουργικότητα και η επίλυση προβλημάτων. Είναι σε θέση να χειριστεί πιο σύνθετες ερωτήσεις και να παράγει πιο συνεκτικό και συναφές κείμενο. Ωστόσο το ChatGPT είναι ένα μοντέλο που βασίζεται στο GPT-3.5 και έχει σχεδιαστεί ειδικά για διαλόγους. Είναι εξαιρετικά ικανό σε συνομιλίες, παρέχοντας φυσικές και συνεχείς αλληλεπιδράσεις.

Αλλα δημοφιλείς εργαλεία παραγωγής κειμένου είναι το Gemini το οποίο έχει σχεδιαστεί για δημιουργία διαλόγων, το Jasper.ai που ειδικεύεται στην δημιουργία διαφημιστικών κειμένων ή το Writesonic το οποίο έχει την ικανότητα να δημιουργεί περιεχόμενο σε πολλές γλώσσες. Ωστόσο η επιλογή του κατάλληλου εργαλείου εξαρτάται από τις υπάρχουσες ανάγκες..

Δημιουργία Εικόνων και Βίντεο: Εφαρμογές όπως DALL-E, Midjourney

Η τεχνητή νοημοσύνη δίνει την εξαιρετικά καινοτόμα δυνατότητα της δημιουργίας δημιουργικού περιεχομένου μέσω αλγορίθμου όπως η εικόνα, ο ήχος και το βίντεο. Η γενετική τεχνητή νοημοσύνη έχει φυσικά την δυνατότητα να μαθαίνει απο μοτίβο ή να κάνει προβέψεις καθώς και να παίρνει αποφάσεις αλλά έχει επίσης την δυνατότητα απο τα δεδομένα που λαμβάνει να δημιουργεί και νέες εκδοχές που μιμούνται τα χαρακτηριστικά απο τα δεδομένα εισόδου. Δύο απο τις πιο γνωστές εφαρμογές στον τομέα της δημιουργίας εικόνων και βίντεο είναι το DALL-E και το Midjourney. Οι συγκεκριμένες εφαρμογές μπορούν να παράγουν υψηλής ποιότητας οπτικό περιεχόμενο βάσει κειμένων τα οποία λαμβάνουν ως δεδομένα εισόδου μέσω της χρήσης προηγμένων τεχνικών μηχανικής μάθησης και νευρωνικών δικτύων.

Η πλατφόρμα DALL-E είναι μία πλατφόρμα δημιουργίας εικόνων AI που δημιουργήθηκε απο την OpenAI. Το όνομα του προήλθε απο τον καλλιτέχνη Salvador Dali και τον χαρακτήρα κινουμένων σχεδίων Wall-E υποδηλώνοντας την δυνατότητα που είχε ο καλλιτέχνης στον συνδυασμό δημιουργικότητας και τέχνης. Αυτή η πλατφόρμα λαμβάνει τα δεδομένα εισόδου σε μορφή κειμένου, τα συνδυάζει και τα μετατρέπει σε λεπτομερείς εικόνες που δεν υπάρχουν στην πραγματικότητα αλλά μοιάζουν πλήρως ρεαλιστικές και ανταποκρίνονται στην περιγραφή. Ένα χρήστης έχει την δυνατότητα να πειραματιστεί με διάφορες περιγραφές εικόνων καθώς η πλατφόρμα μπορεί να δημιουργήσει περιεχόμενο σε πολλαπλά και διαφορετικά στυλ σύμφωνα με τις ανάγκες πάντα του χρήστη.

Η πλατφόρμα Midjourney είναι μία πλατφόρμα παραγωγής δημιουργικής τεχνητής νοημοσύνης που αναπτύχθηκε απο το εργαστήριο του Midjourney και δίνει την δυνατότητα σε χρήστες να εκφραστούν δημιουργικά παράγοντας χαρακτήρες, εικόνες και απεικονίσεις μέσω σύντομων κειμένων οδηγιών. Το

Midjourney είναι παρόμοιο εργαλείο με το DALL-E και επικεντρώνεται στην δημιουργία υψηλής ποιότητας υλικού αλλά με έμφαση στην δημιουργική ελευθερία.

Άλλες Εφαρμογές: Δημιουργία μουσικής, ηχητικών εφέ, και περιεχομένου για social media

Η τεχνητή νοημοσύνη έχει εισχωρήσει και στον τομέα της μουσικής καθώς πλέον ένας χρήστης έχει την δυνατότητα να δημιουργήσει μουσική και τραγούδια πλήρους μήκους χωρίς δικαιώματα , ηχητικά εφέ ή ακόμη και περιεχόμενο στα μέσα κοινωνικής δικτύωσης. Μέσω αυτών των εφαρμογών παρατηρούμε ότι ανοίγονται νέοι ορίζοντες στην μουσική βιομηχανία καθώς απλοί χρήστες πλέον μπορούν να αυξήσουν τη δημιουργικότητα και την παραγωγικότητα τους προστίθοντας δικούς τους στίχους που έχουν επιλέξει σε μορφή κειμένου και μπορούν να δημιουργήσουν πολλαπλές σύνθετες μουσικές σύμφωνα με τις ανάγκες και τις προτιμήσεις τους. Η ύπαρξη τους είναι επαναστατική ωστόσο θα πρέπει να αξιολογηθεί σχετικά το πλαίσιο λειτουργίας τους ως προς την ηθική ώστε να προστατευτούν οι καλλιτέχνες και τα πνευματικά τους δικαιώματα.

Μία από τις πιο γνωστές πλατφόρμες δημιουργία μουσικής είναι το Suno πού επικεντρώνεται στη δημιουργία μουσικών και ηχητικών εφέ χάρις την χρήση προηγμένων τεχνικών βαθιάς μάθησης και νευρωνικών δικτύων. Έχει την δυνατότητα αυτόματης σύνθεσης μουσικής και την επεξεργασία ήχων. Στο Suno ο χρήστης μπορεί να δημιουργήσει ολόκληρο τραγούδι από το μηδέν δίνοντας του ότι πληροφορία επιθυμεί σε σχέση με το επιθυμητό ύφος και εκείνο συνθέτει τραγούδι συμπεριλαμβανομένου και την δημιουργία στίχων. Ωστόσο δίνει και την δυνατότητα δημιουργίας τραγουδιού παραθέτοντας συγκεκριμένους στίχους και συγκεκριμένο ύφος.

Περίπτωση Μελέτης: Το Demo AI για την Πόλη μου

Περιγραφή του Demo AI

Όπως έχουμε ήδη αναφέρει και παραπάνω, στα πλαίσια της παρούσας εργασίας και με στόχο να δείξουμε και στη πράξη τα οφέλη αλλά και το τρόπο χρήσης της τεχνητής νοημοσύνης, θα δημιουργήσουμε ένα chatbot το οποίο θα είναι σε θέση να απαντήσει σε ερωτήσεις που θα κάνει ο χρήστης και θα σχετίζονται με τη πόλη του Ηρακλείου Κρήτης.

Κύριος στόχος είναι το να παρέχουμε στο χρήστη ενήμερες πληροφορίες και όχι τυχαία αποτελέσματα που μπορεί να βρει γενικότερα σε μηχανές αναζήτησης. Γι να το καταφέρουμε αυτό, θα χρησιμοποιήσουμε μια βάση δεδομένων η οποία θα περιέχει όλες τις πληροφορίες που θέλουμε να παρέχουμε στους χρήστες. Αυτές μπορεί να είναι από δρομολόγια μέσω μαζικής μεταφοράς, πληροφορίες για αξιοθέατα ή ιστορικά μνημεία έως και γενικές ιστορικές πληροφορίες για τη πόλη.

Το chatbot θα χρησιμοποιεί το AI chatgpt όπου μέσω ενός API θα παίρνει τις ερωτήσεις του χρήστη, θα αναζητά τη σχετική πληροφορία μέσα στη βάση την οποία θα έχουμε ήδη δημιουργήσει και θα παρέχει τη σχετική πληροφορία. Με αυτό θα καταφέρουμε να εκμεταλλευτούμε την ήδη υπάρχουσα AI τεχνολογία σε συνεργασία με πληροφορίες που θα εισάγουμε εμείς, ώστε να παρέχουμε ενήμερες και ακριβείς πληροφορίες.

Η εφαρμογή πέρα τη θεωρητική εφαρμογή της στο πλαίσιο της παρούσας εργασίας, θα μπορούσε να έχει και πολλές πρακτικές εφαρμογές. Όπως περιγράφεται παραπάνω θα μπορούσε να χρησιμοποιηθεί ως “οδηγός” καθοδήγησης τουριστών/επισκεπτών παρέχοντας καθοδήγηση με ενήμερες πληροφορίες ή και ως οδηγός/βοηθός μαθητών στα πλαίσια ενός μαθήματος, παρέχοντας πληροφορίες συναρτήσεων, παραδειγμάτων και άλλων σχετικών πληροφοριών.

Η χρήση της τεχνητής νοημοσύνης μπορεί να θεωρείται επίφοβη και σε πολλές περιπτώσεις μη ακριβής/αληθής, ωστόσο η χρήση της σε συνδυασμό με ένα προκαθορισμένο “κουβά” πληροφοριών μπορεί να φανεί εξαιρετικά χρήσιμη.

Τεχνολογίες που Χρησιμοποιήθηκαν και επεξήγηση λειτουργίας

Αρχικά για το κύριο μέρος του προγράμματος, χρησιμοποιήσαμε Node.JS η οποία είναι υπεύθυνη για την επεξεργασία των δεδομένων και την “επικοινωνία” μέσω του chatgpt.

Έπειτα, λόγω του ότι θέλαμε το chatbot να είναι διαθέσιμο προς επίδειξη, το έχουμε βγάλει online στη σελίδα <https://herbot.micohosting.com>. Οι αιτήσεις/ερωτήματα προς το chatbot μπορούν να γίνουν μέσω POST request προς τη διεπαφή /ask, ωστόσο για λόγους ευκολίας, δημιουργήσαμε ένα απλο php ώστε να υπάρχει ένα φιλικό προς το χρήστη interface.

Για τη παραπάνω λοιπόν υλοποίηση, χρησιμοποιήσαμε έναν VPS με Ubuntu, ο οποίος τρέχει έναν nginx web server και σε συνδυασμό με την PHP-FPM “σερβίρει” το endpoint /ask το οποίο μας παρέχει τη δυνατότητα να αλληλεπιδρούμε με το bot μας.

Διάγραμμα λειτουργίας



Ροή λειτουργίας

Χρήστης ⇨ Φόρμα PHP ⇨ Nginx ⇨ Node.js API ⇨ Chatgpt + databse ⇨ Node.js API ⇨ Nginx ⇨ Φόρμα PHP ⇨ Χρήστης

Παρακάτω ακολουθούν τα δομικά στοιχεία της υλοποίησης όπως ακριβώς χρησιμοποιήθηκαν.

Λειτουργικό Σύστημα: Ubuntu Server 22.04 LTS

Web Server: Nginx

Γλώσσα Προγραμματισμού για Backend: Node.js (με LangChain και OpenAI API)

Frontend: PHP με HTML και JavaScript

Process Manager για Node.js: PM2

SSL Πιστοποιητικά: Let's Encrypt (Certbot)

Βάση Δεδομένων: Χρήση αρχείου κειμένου ([heraklion_history.txt](#)) για αποθήκευση δεδομένων

Αναλυτική λειτουργία εφαρμογής

Φόρτωση της Ιστοσελίδας:

- Όταν ένας χρήστης επισκέπτεται το σύνδεσμο <https://herbot.micohosting.com/index.php>, φορτώνεται το PHP interface που περιλαμβάνει μια φόρμα για να υποβάλλει ερωτήσεις.

Υποβολή Ερώτησης:

- Ο χρήστης πληκτρολογεί μια ερώτηση στη φόρμα και πατά το κουμπί "Ρώτησε".
- Η φόρμα υποβάλλει μια αίτηση POST στο ίδιο αρχείο [index.php](#).

Επεξεργασία από PHP:

- Το PHP script λαμβάνει την ερώτηση, την επεξεργάζεται και δημιουργεί ένα JSON payload.
- Χρησιμοποιεί cURL για να στείλει μια αίτηση POST στον Node.js backend (<http://127.0.0.1:3000/ask>) με την ερώτηση.

Επεξεργασία από Node.js Backend:

- Ο Node.js server λαμβάνει την αίτηση στο endpoint [/ask](#).
- Χρησιμοποιεί τη βιβλιοθήκη LangChain για να αναλύσει το κείμενο από το αρχείο [heraklion_history.txt](#), δημιουργεί embeddings και διαχειρίζεται την ερώτηση μέσω ενός RetrievalQChain με GPT-4.
- Ανακτά τα σχετικά τμήματα κειμένου και απαντά με βάση τα δεδομένα που παρέχονται στο αρχείο κειμένου.

Απάντηση στον Χρήστη:

- Ο Node.js server επιστρέφει μια JSON απάντηση στο PHP frontend.
- Το PHP script επεξεργάζεται την απάντηση και την εμφανίζει στον χρήστη στην ιστοσελίδα.

Αναλυτική δημιουργία/εγκατάσταση εφαρμογής

Προετοιμασία σέρβερ

Αρχικά ξεκινάμε με το provisioning του σέρβερ. Για τις ανάγκες της υλοποίησης δεν έχουμε μεγάλες απαιτήσεις απο το σέρβερ που θα φιλοξενεί την εφαρμογή μας. Ένα απλό single core VPS/container με 2GB RAM θα είναι υπερ αρκετό. Επίσης θα χρειαστεί να έχουμε μια IPv4 ώστε να έχουμε δυνατότητα να στήσουμε το webserver μας.

Αφου ολοκληρωθεί το provisioning, συνδεόμαστε στο σέρβερ μέσω SSH και προχωράμε σε ενημέρωση του λειτουργικού.

```
root@ubuntu-4gb-nbg1-2: ~
kB]
Get:4 https://mirror.hetzner.com/ubuntu/security noble-security InRelease [126 k
B]
Hit:5 https://deb.nodesource.com/node 22.x nodistro InRelease
Get:6 https://mirror.hetzner.com/ubuntu/packages noble-updates/main amd64 Packag
es [759 kB]
Get:7 https://mirror.hetzner.com/ubuntu/packages noble-updates/universe amd64 Pa
ckages [965 kB]
Fetched 2,103 kB in 1s (3,266 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
10 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  apport apport-core-dump-handler cloud-init gir1.2-packagekitglib-1.0
  libpackagekit-glib2-18 packagekit python3-apport python3-problem-report
Progress: [ 9%] [.....]
10 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,766 kB of archives.
After this operation, 16.4 kB of additional disk space will be used.
Get:1 https://mirror.hetzner.com/ubuntu/packages noble-updates/main amd64 python3-problem-report all 2.28.1-0ubuntu3.3 [24.6 kB]
Get:2 https://mirror.hetzner.com/ubuntu/packages noble-updates/main amd64 python3-apport all 2.28.1-0ubuntu3.3 [92.3 kB]
Get:3 https://mirror.hetzner.com/ubuntu/packages noble-updates/main amd64 apport-core-dump-handler all 2.28.1-0ubuntu3.3 [17.5 kB]
Get:4 https://mirror.hetzner.com/ubuntu/packages noble-updates/main amd64 apport all 2.28.1-0ubuntu3.3 [84.5 kB]
Get:5 https://mirror.hetzner.com/ubuntu/packages noble-updates/main amd64 libpackagekit-glib2-18 amd64 1.2.8-2ubuntu1.1 [120 kB]
Get:6 https://mirror.hetzner.com/ubuntu/packages noble-updates/main amd64 gir1.2-packagekitglib-1.0 amd64 1.2.8-2ubuntu1.1 [25.6 kB]
Get:7 https://mirror.hetzner.com/ubuntu/packages noble-updates/main amd64 sosreport amd64 4.7.2-0ubuntu1~24.04.2 [356 kB]
Get:8 https://mirror.hetzner.com/ubuntu/packages noble-updates/main amd64 cloud-init all 24.4-0ubuntu1~24.04.2 [602 kB]
Get:9 https://mirror.hetzner.com/ubuntu/packages noble-updates/main amd64 packagekit amd64 1.2.8-2ubuntu1.1 [434 kB]
Get:10 https://mirror.hetzner.com/ubuntu/packages noble-updates/main amd64 ssh-import-id all 5.11-0ubuntu2.24.04.1 [10.1 kB]
Fetched 1,766 kB in 0s (19.0 MB/s)
Preconfiguring packages ...
Unpacking python3-problem-report (2.28.1-0ubuntu3.3) over (2.28.1-0ubuntu3.1) ...
Preparing to unpack .../1-python3-apport 2.28.1-0ubuntu3.3 all.deb ...
Unpacking python3-apport (2.28.1-0ubuntu3.3) over (2.28.1-0ubuntu3.1) ...
Preparing to unpack .../2-apport-core-dump-handler 2.28.1-0ubuntu3.3 all.deb ...
Unpacking apport-core-dump-handler (2.28.1-0ubuntu3.3) over (2.28.1-0ubuntu3.1) ...
```

Έπειτα δημιουργούμε έναν non-root user με sudo δικαιώματα

```
sudo usermod -aG sudo herbotuser
```

Ένα ακόμα προαιρετικό αλλά προτεινόμενο βήμα, είναι η δημιουργία SSH keys για την ασφαλή σύνδεση στο σέρβερ χωρίς τη χρήση κωδικών πρόσβασης (βλ. παράρτημα)

Συνεχίζουμε με την εγκατάσταση του webserver (nginx)

```
sudo usermod -aG sudo herbotuser
sudo apt install nginx -y
```

και ενεργοποιούμε την υπηρεσία ώστε να εκκινεί κατά την εκκίνηση του σέρβερ

```
sudo apt update && sudo apt upgrade -y
sudo adduser herbotuser
sudo usermod -aG sudo herbotuser
sudo apt install nginx -y
sudo systemctl enable nginx
sudo systemctl start nginx
```

κάπου εδώ τα πράγματα γίνονται αρκετά πιο περίπλοκα, καθώς θα χρειαστεί να ρυθμίσουμε τον nginx ώστε να λειτουργεί και με το subdomain herbot.micohosting.com αλλά και να χρησιμοποιεί SSL

Ξεκινάμε με τη δημιουργία του configuration file

```
touch /etc/nginx/sites-available/herbot.micohosting.com
```

και εισάγουμε το παρακάτω

```
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name herbot.micohosting.com;

    root /var/www/herbot.micohosting.com/html;
    index index.php index.html index.htm;

    # SSL Configuration managed by Certbot
    ssl_certificate /etc/letsencrypt/live/herbot.micohosting.com/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/herbot.micohosting.com/privkey.pem;
    include /etc/letsencrypt/options-ssl-nginx.conf;
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem;

    # Serve static files
    location / {
        try_files $uri $uri/ =404;
    }

    # PHP-FPM Handling
    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.3-fpm.sock;
    }

    # Proxy /ask to Node.js
```

```

        location /ask {
            proxy_pass http://127.0.0.1:3000;
            proxy_http_version 1.1;
            proxy_set_header Upgrade $http_upgrade;
            proxy_set_header Connection 'upgrade';
            proxy_set_header Host $host;
            proxy_cache_bypass $http_upgrade;
        }
    }

    server {
        if ($host = herbot.micohosting.com) {
            return 301 https://$host$request_uri;
        }

        listen 80;
        listen [::]:80;
        server_name herbot.micohosting.com;
        return 404;
    }

```

το παραπάνω, με λίγα λόγια, επιτρέπει στον nginx να διαχειρίζεται τα php αρχεία, να χρησιμοποιεί το SSL που έχουμε εγκαταστήσει μέσω της Certbot αλλά και να “σερβίρει” τη διεπαφή /ask του NodeJS μέσω της πόρτας 3000

τέλος δημιουργούμε ένα symlink του παραπάνω configuration file στο sites-enabled

```
sudo ln -s /etc/nginx/sites-available/herbot.micohosting.com /etc/nginx/sites-enabled/
```

και έπειτα τρέχουμε τα παρακάτω για να επιβεβαιώσουμε ότι το configuration file δεν έχει συντακτικά σφάλματα και κάνουμε re-load του webserver

```

sudo nginx -t
sudo systemctl reload nginx
sudo systemctl status nginx

```

```
root@ubuntu-4gb-nbgl-2: ~  
root@ubuntu-4gb-nbgl-2:~# sudo nginx -t  
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok  
nginx: configuration file /etc/nginx/nginx.conf test is successful  
root@ubuntu-4gb-nbgl-2:~# sudo systemctl reload nginx  
root@ubuntu-4gb-nbgl-2:~# sudo systemctl status nginx  
nginx.service - A high performance web server and a reverse proxy server  
Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)  
Active: active (running) since Sat 2024-12-07 23:05:34 UTC; 1 week 6 days ago  
Docs: man:nginx(8)  
Process: 381757 ExecReload=/usr/sbin/nginx -g daemon on; master_process on; -s reload (code=exited, status=0/SUCCESS)  
Main PID: 11619 (nginx)  
Tasks: 3 (limit: 4543)  
Memory: 3.6M (peak: 9.0M)  
CPU: 10.741s  
CGroup: /system.slice/nginx.service  
└─ 11619 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"  
   └─ 381759 "nginx: worker process"  
      └─ 381760 "nginx: worker process"  
  
Dec 07 23:05:34 ubuntu-4gb-nbgl-2 systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy server...  
Dec 07 23:05:34 ubuntu-4gb-nbgl-2 systemd[1]: Started nginx.service - A high performance web server and a reverse proxy server...  
Dec 21 16:38:48 ubuntu-4gb-nbgl-2 systemd[1]: Reloading nginx.service - A high performance web server and a reverse proxy server...  
Dec 21 16:38:48 ubuntu-4gb-nbgl-2 nginx[381757]: 2024/12/21 16:38:48 [notice] 381757#381757: signal process started  
Dec 21 16:38:48 ubuntu-4gb-nbgl-2 systemd[1]: Reloaded nginx.service - A high performance web server and a reverse proxy server.  
root@ubuntu-4gb-nbgl-2:~#
```

και προχωράμε σε επιδιόρθωση δικαιωμάτων για τα αρχεία/φакέλους

```
sudo chown -R www-data:www-data /var/www/herbot.micohosting.com/html  
sudo find /var/www/herbot.micohosting.com/html -type d -exec chmod 755 {} \  
sudo find /var/www/herbot.micohosting.com/html -type f -exec chmod 644 {} \;
```

Αφού επιβεβαιώσουμε πως ο nginx λειτουργει σωστα (μέσω ενός test html) συνεχίσουμε με την εγκατάσταση των php-fpm και των σχετικών modules

```
sudo apt install php8.3-fpm php8.3-curl -y
```

*σημείωση, η curl χρησιμοποιείται για τα POST/GET requests.

επιβεβαίωση λειτουργίας του php-fpm service

```
root@ubuntu-4gb-nbg1-2: ~  
root@ubuntu-4gb-nbg1-2:~# sudo systemctl status php8.3-fpm.service  
● php8.3-fpm.service - The PHP 8.3 FastCGI Process Manager  
   Loaded: loaded (/usr/lib/systemd/system/php8.3-fpm.service; enabled; preset: enabled)  
   Active: active (running) since Sat 2024-12-14 06:14:21 UTC; 1 week 0 days ago  
     Docs: man:php-fpm8.3(8)  
  Main PID: 189312 (php-fpm8.3)  
    Status: "Processes active: 0, idle: 2, Requests: 207, slow: 0, Traffic: 0req/sec"  
   Tasks: 3 (limit: 4543)  
  Memory: 8.2M (peak: 8.5M)  
    CPU: 1min 5.365s  
   CGroup: /system.slice/php8.3-fpm.service  
           └─189312 "php-fpm: master process (/etc/php/8.3/fpm/php-fpm.conf)"  
             └─189314 "php-fpm: pool www"  
               └─189315 "php-fpm: pool www"  
  
Dec 14 06:14:21 ubuntu-4gb-nbg1-2 systemd[1]: Starting php8.3-fpm.service - The PHP 8.3 FastCGI Process Manager...  
Dec 14 06:14:21 ubuntu-4gb-nbg1-2 systemd[1]: Started php8.3-fpm.service - The PHP 8.3 FastCGI Process Manager.  
root@ubuntu-4gb-nbg1-2:~#
```

τέλος, ολοκληρώνουμε τη προετοιμασία του σέρβερ με την εγκατάσταση του NodeJS

```
curl -fsSL https://deb.nodesource.com/setup_18.x | sudo -E bash -  
sudo apt install -y nodejs
```

μόλις ολοκληρωθεί το παραπάνω (θα χρειαστεί λίγος χρόνος), επιβεβαιώνουμε πως όλα είναι εντάξει

```
node -v  
npm -v
```

```
root@ubuntu-4gb-nbg1-2: ~  
root@ubuntu-4gb-nbg1-2:~# node -v  
v22.12.0  
root@ubuntu-4gb-nbg1-2:~# npm -v  
10.9.0  
root@ubuntu-4gb-nbg1-2:~#
```

Αφού έχουν ολοκληρωθεί με επιτυχία όλα τα παραπάνω, μπορούμε να προχωρήσουμε στην εισαγωγή των επιμέρους αρχείων του κώδικα

Κύριος κώδικας και επιμέρους αρχεία

Δημιουργούμε αρχικά τους φακέλους οι οποίοι θα χρησιμοποιηθούν για να “σερβίρουν” τα αρχεία της εφαρμογής μας

```
sudo mkdir -p /var/www/herbot.micohosting.com/html/herbot  
sudo chown -R jerbotuser:www-data /var/www/herbot.micohosting.com/html/herbot
```

και μπαίνουμε στο directory ώστε να δημιουργήσουμε μέσα τα αρχεία του κώδικα

```
cd /var/www/herbot.micohosting.com/html/herbot
```

δημιουργούμε το index.js και βάζουμε μέσα το παρακάτω κώδικα

```
import { config } from "dotenv";
config(); // Load environment variables from .env

import fs from 'fs';
import express from 'express';
import { OpenAI } from "langchain/llms/openai";
import { OpenAIEmbeddings } from "langchain/embeddings/openai";
import { RecursiveCharacterTextSplitter } from "langchain/text_splitter";
import { RetrievalQAChain } from "langchain/chains";
import { MemoryVectorStore } from "langchain/vectorstores/memory";

// Load your OpenAI API key from .env
const openAiApiKey = process.env.OPENAI_API_KEY;
if (!openAiApiKey) {
  console.error("Error: OPENAI_API_KEY not set in .env");
  process.exit(1);
}

// Read the text file
const text = fs.readFileSync('heraklion_history.txt', 'utf8');

// Split the text into smaller chunks
const splitter = new RecursiveCharacterTextSplitter({
  chunkSize: 500, // Increased chunk size to keep related data together
  chunkOverlap: 100 // Increased overlap to ensure context continuity
});
const docs = await splitter.createDocuments([text]);

// Prepare embeddings
const embeddings = new OpenAIEmbeddings({ openAIApiKey: openAiApiKey });

// Define an even stricter prompt template
const template = `
You are a highly accurate assistant that answers questions solely based on the provided context
about Heraklion.
You must:
- Use only the information present in the context exactly as written, word for word.
- Not add, rename, or reinterpret any information.
- If the requested information is not explicitly and exactly stated in the context, respond with
"Λυπάμαι, δεν μπορώ να σε βοηθήσω με αυτό."
- Do not use synonyms if the context does not use them, do not guess or infer data not stated
```

verbatim in the context.
- All responses must be in Greek.

Context:
{context}

Question: {query}

Answer:
`;
`;

// Initialize the LLM with stricter parameters

```
const llm = new OpenAI({  
  openAIApiKey: openAiApiKey,  
  temperature: 0,           // Keep deterministic responses  
  top_p: 0.1,              // Further reduce token selection variety  
  modelName: "gpt-4"       // Using GPT-4 for better accuracy  
});
```

// Initialize variables for lazy loading

```
let vectorStore = null;  
let chain = null;
```

// Set up an Express server

```
const app = express();  
app.use(express.json());
```

```
app.post('/ask', async (req, res) => {  
  const { question } = req.body;  
  if (!question) return res.status(400).json({ error: "No question provided" });  
  
  try {  
    if (!vectorStore) {  
      vectorStore = await MemoryVectorStore.fromDocuments(docs, embeddings);  
    }  
  
    // Configure the retriever with a higher k to return more chunks  
    const retriever = vectorStore.asRetriever({ k: 10 }); // Increased k to 10  
  
    if (!chain) {  
      chain = RetrievalQAChain.fromLLM(  
        llm,  
        retriever,  
        {  
          promptTemplate: template,  
          chainType: "stuff" // Use "stuff" chainType to pass all text directly  
        }  
      );  
    }  
  }  
});
```

```

    );
  }

  // Debug: Log retrieved docs
  const retrievedDocs = await retriever.getRelevantDocuments(question);
  console.log("Retrieved Docs:", retrievedDocs.map(doc => doc.pageContent));

  // Retrieve and answer the question
  const response = await chain.call({ query: question });
  // Trim the answer
  const answer = response.text.trim();

  res.json({ answer });
} catch (error) {
  console.error("Error processing request:", error);
  res.status(500).json({ error: "Error processing request" });
}
});

app.get('/', (req, res) => {
  res.send("Node.js Chatbot Server Running");
});

const port = process.env.PORT || 3000;
app.listen(port, () => console.log(`Chatbot running on port ${port}`));

```

επίσης δημιουργούμε το αρχείο .env με τα παρακάτω στοιχεία τα οποία ουσιαστικά είναι variables ώστε να υπάρχει η δυνατότητα να τροποποιηθεί η εφαρμογή χωρίς άμεση επέμβαση στο κώδικα

```

OPENAI_API_KEY=your_openai_api_key_here
PORT=3000

```

τέλος δημιουργούμε το heraklion_history.txt το οποίο και θα περιέχει τις πληροφορίες βάσης των οποίων θα θέλουμε να απαντάει το chatbot.

Τώρα που έχουν ολοκληρωθεί όλα τα παραπάνω και τα αρχεία έχουν ανέβει, τρέχουμε τα παρακάτω για την εγκατάσταση των επιμέρους πακέτων

```

npm init -y
npm install express dotenv langchain openai

```

Προαιρετικά προχωράμε και στην εγκατάσταση/ενεργοποίηση του process manager ώστε να είμαστε σίγουροι για τη συνεχή λειτουργία του NodeJS

```

sudo npm install -g pm2
pm2 start index.js --name
herbot pm2 save

```

```
pm2 startup systemd
```

Σε αυτό το σημείο ο κώδικας του NodeJS θα πρέπει να τρέχει σωστά και να είναι σε θέση να δεχτεί αλλά και να απαντήσει σε POST requests μέσω του /ask

Απο το παραπάνω κώδικα του NodeJS, αξίζει να επικεντρωθούμε για λίγο στα παρακάτω κομμάτια.

Για αρχή στο

```
// Initialize the LLM with stricter parameters
const llm = new OpenAI({
  openAIApiKey: openAiApiKey,
  temperature: 0,           // Keep deterministic responses
  top_p: 0.1,              // Further reduce token selection variety
  modelName: "gpt-4"       // Using GPT-4 for better accuracy
});
```

σε αυτό το σημείο, ορίζεται το πως το μοντέλο της τεχνητής νοημοσύνης που χρησιμοποιούμε (openai), αλληλεπιδρά με το κώδικά μας.

Αφού ορίσουμε τη κλάση και το API key, είναι σημαντική η ύπαρξη του `temperature: 0`

αυτό πρακτικά “περιορίζει” τη δημιουργικότητα του μοντέλου και το κατευθύνει ώστε να απαντά πιο αυστηρά βάση των πληροφοριών που του δίνονται παρακάτω στο κώδικα.

Το δεύτερο επίσης σημαντικό κομμάτι είναι το `top_p: 0.1`. Πρόκειται για μια αρκετά σημαντική παράμετρο η οποία είναι μια ρύθμιση που ελέγχει πώς το μοντέλο επιλέγει τις λέξεις όταν δημιουργεί απαντήσεις. Ειδικότερα, η `top_p` χρησιμοποιεί μια τεχνική που ονομάζεται **nucleus sampling** (δειγματοληψία πυρήνα).

Όταν το μοντέλο σκέφτεται ποια λέξη να βάλει στη συνέχεια, κάθε πιθανή λέξη έχει μια βαθμολογία (πιθανότητα). Το nucleus sampling διαλέγει μόνο από τις λέξεις με τις υψηλότερες πιθανότητες, ώστε η επιλογή να είναι πιο ελεγχόμενη και λιγότερο τυχαία.

Ρυθμίζοντας το στο 0.1, επιλέγει τις 10% πιο πιθανές λέξεις περιορίζοντας ακόμα περισσότερο (σε συνδυασμό με το `temperature:0`) τη δημιουργικότητα του μοντέλου, παράγοντας πιο αυστηρά τις απαντήσεις που δίνει.

Περισσότερες πληροφορίες σχετικά με το **nucleus sampling** παρέχονται στο παράρτημα της εργασίας

Τέλος το modelName καθορίζει το ποιο μοντέλο θα χρησιμοποιηθεί.

Το δεύτερο κομμάτι κώδικα που θα πρέπει να εστιάσουμε, είναι το παρακάτω

```
// Configure the retriever with a higher k to return more chunks
const retriever = vectorStore.asRetriever({ k: 10 }); // Increased k to 10
```

Αυτό το κομμάτι κώδικα διαμορφώνει έναν **retriever** για να επιστρέφει περισσότερα "chunks" (κομμάτια πληροφορίας) από έναν **vector store**.

Το vector store είναι μια δομή δεδομένων (στη περίπτωση μας το 'heraklion_history.txt') η οποία αποθηκεύει τις πληροφορίες ως vectors (διανύσματα) για γρήγορη προσπέλαση. Έπειτα το .asRetriever μετατρέπει το διάνυσμα αυτό σε retriever (δηλαδή μια διεπαφή) ώστε να μπορεί να γίνει ανάκτηση των πληροφοριών. Ορίζοντας το k στο 10 σημαίνει ότι ο retriever θα επιστρέψει τις 10 πιο σχετικές εγγραφές/πληροφορίες του vector store.

Ανάλογα την υλοποίηση που θέλουμε να πετύχουμε, ενδέχεται να χρειαστεί να τροποποιήσουμε κατάλληλα το k. Στη περίπτωση μας, το έχουμε αυξήσει στο 10, το οποίο και φαίνεται να λειτουργεί σωστά βάσει της υπάρχουσας βάσης δεδομένων.

Περισσότερες πληροφορίες σχετικά με τα chunks, retrievers και vector stores παρέχονται στο παράρτημα της εργασίας.

Στη συνέχεια, όπως έχουμε αναφέρει ήδη παραπάνω, θα δημιουργήσουμε ένα php ώστε να μπορεί ένας χρήστης να αλληλεπιδρά με το NodeJS μέσω ενός interface φιλικό προς το χρήστη.

Πρόκειται για μια πολύ απλή υλοποίηση η οποία έχει τη παρακάτω μορφή

Heraklion Chatbot

Ρώτησε οπδήποτε για το Ηράκλειο:

δημιουργούμε το index.php στο directory του subdomain μας

```
touch /var/www/herbot.micohosting.com/html/index.php
```

εισάγοντας το παρακάτω κώδικα

```
<?php
// index.php

if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    // Get the question from the POST data
    $question = isset($_POST['question']) ? trim($_POST['question']) : "";

    if ($question === "") {
        $error = "Παρακαλώ εισάγετε μια ερώτηση.";
    } else {
```

```

// Prepare the JSON payload
$data = json_encode(["question" => $question]);

// Initialize cURL
$ch = curl_init();

// Set cURL options
curl_setopt($ch, CURLOPT_URL, "http://127.0.0.1:3000/ask");
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS, $data);
curl_setopt($ch, CURLOPT_HTTPHEADER, [
    'Content-Type: application/json',
    'Content-Length: ' . strlen($data)
]);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_TIMEOUT, 10); // Timeout after 10 seconds

// Execute the request
$response = curl_exec($ch);

// Check for errors
if ($response === false) {
    $error = "Σφάλμα κατά την εκτέλεση του αιτήματος: " . curl_error($ch);
} else {
    $http_code = curl_getinfo($ch, CURLINFO_HTTP_CODE);
    if ($http_code === 200) {
        // Decode the JSON response
        $json = json_decode($response, true);
        if (isset($json['answer'])) {
            $answer = htmlspecialchars($json['answer'], ENT_QUOTES, 'UTF-8');
        } else {
            $error = "Μη αναμενόμενο format απάντησης.";
        }
    } else {
        $error = "Απάντηση διακομιστή με κωδικό: " . $http_code;
    }
}

// Close cURL resource
curl_close($ch);
}
?>

<!DOCTYPE html>
<html lang="el">
<head>

```

```

<meta charset="UTF-8">
<title>Herbot Chatbot</title>
<style>
body {
font-family: Arial, sans-serif;
margin: 40px;
background-color: #f9f9f9;
}
.container {
max-width: 700px;
margin: auto;
background: #fff;
padding: 30px;
border-radius: 8px;
box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
}
input[type="text"] {
width: 100%;
padding: 12px;
margin-bottom: 15px;
border: 1px solid #ccc;
border-radius: 4px;
}
button {
background-color: #4CAF50;
color: white;
padding: 12px 20px;
border: none;
border-radius: 4px;
cursor: pointer;
font-size: 16px;
}
button:hover {
background-color: #45a049;
}
.response {
margin-top: 20px;
padding: 15px;
background-color: #e7f3fe;
border-left: 6px solid #2196F3;
border-radius: 4px;
}
.error {
margin-top: 20px;
padding: 15px;
background-color: #fdecea;
border-left: 6px solid #f44336;

```

```

        border-radius: 4px;
    }
</style>
</head>
<body>
<div class="container">
    <h1>Herbot Chatbot</h1>
    <p>Ρώτησε οτιδήποτε για το Ηράκλειο:</p>
    <form method="POST" action="index.php">
        <input type="text" name="question" placeholder="Πληκτρολόγησε την ερώτησή σου..."
required>
        <button type="submit">Ρώτησε</button>
    </form>

    <?php if (isset($answer)): ?>
    <div class="response">
        <strong>Απάντηση:</strong>
        <p><?php echo $answer; ?></p>
    </div>
    <?php elseif (isset($error)): ?>
    <div class="error">
        <strong>Σφάλμα:</strong>
        <p><?php echo htmlspecialchars($error, ENT_QUOTES, 'UTF-8'); ?></p>
    </div>
    <?php endif; ?>
</div>
</body>
</html>

```

Στο παραπάνω κώδικα, η php ελέγχει αν το request αφορά POST request, λαμβάνει το query από τη φόρμα, ελέγχει αν είναι κενό και έπειτα δημιουργεί ένα JSON payload με την ερώτηση του χρήστη και τη στέλνει μέσω curl στο nodejs στην 127.0.0.1 στη πόρτα 3000 όπου “ακούει” η διεπαφή /ask. Τέλος, λαμβάνει την απάντηση και εφόσον δεν υπάρχουν σφάλματα τη προωθεί στο χρήστη.

Μαζί με την php, έχουν εισαχθεί και τα ανάλογα html/css ώστε να δημιουργήσουν μια φιλική εμφάνιση για το χρήστη.

Τέλος, τρέχουμε (προαιρετικά) τα παρακάτω ώστε να εγκαταστήσουμε ένα SSL στο subdomain μας μέσω της Certbot ώστε να απαλλαγούμε από οποιαδήποτε προειδοποίηση ασφαλείας των browser και να αυξήσουμε την ασφάλεια της σελίδας κρυπτογραφώντας τα δεδομένα.

```

sudo apt install certbot python3-certbot-nginx -y
sudo certbot --nginx -d herbot.micohosting.com

```

Επίσης προαιρετικό είναι το παρακάτω, ώστε να ανανεώνεται αυτόματα το SSL που έχουμε εκδόσει.

```
sudo certbot renew --dry-run
```

Ενδεικτικό POST request που μπορεί να δεχτεί απευθείας η διεπαφή /ask

```
curl -X POST "http://127.0.0.1:3000/ask" \
  -H "Content-Type: application/json" \
  -d '{"question": "\u03a0\u03b9\u03bf\u03c3 \u03b7\u03c4\u03b1\u03bd \u03bf \u03c0\u03bb\u03b7\u03b8\u03c5\u03c3\u03bc\u03cc\u03c2 \u03c4\u03bf\u03c5 \u0397\u03c1\u03b1\u03ba\u03bb\u03b5\u03b9\u03bf\u03c5 \u03c4\u03bf 1991;\u201d}'
```

Με βάση τα παραπάνω, η όλη εφαρμογή θα πρέπει να λειτουργεί ως εξής.

Φόρτωση της Ιστοσελίδας:

- Όταν ένας χρήστης επισκέπτεται <https://herbot.micohosting.com/index.php>, φορτώνεται η rhr που περιλαμβάνει τη φόρμα για να υποβάλλει ερωτήσεις.

Υποβολή Ερώτησης:

- Ο χρήστης πληκτρολογεί μια ερώτηση στη φόρμα και πατά το κουμπί "Ρώτησε".
- Η φόρμα υποβάλλει ένα POST στο ίδιο αρχείο index.php.

Επεξεργασία από PHP:

- Η ρηρ λαμβάνει την ερώτηση, την επεξεργάζεται και δημιουργεί ένα JSON payload.
- Χρησιμοποιεί cURL για να στείλει μια αίτηση POST στο Node.js (<http://127.0.0.1:3000/ask>) με την ερώτηση.

Επεξεργασία από Node.js Backend:

- Το Node.js λαμβάνει την αίτηση στη διεπαφή/ask.
- Χρησιμοποιεί τη βιβλιοθήκη LangChain για να αναλύσει το κείμενο από το αρχείο heraklion_history.txt, δημιουργεί embeddings και διαχειρίζεται την ερώτηση μέσω ενός RetrievalQAChain με GPT-4.
- Ανακτά τα σχετικά τμήματα κειμένου και απαντά με βάση τα δεδομένα που παρέχονται στο αρχείο κειμένου.

Απάντηση στον Χρήστη:

- Το Node.js επιστρέφει μια JSON απάντηση στη php.
- Η php επεξεργάζεται την απάντηση και την εμφανίζει στον χρήστη στην ιστοσελίδα.

Πληροφορίες σχετικά με τα RetrievalQChain και LangChain παρέχονται επίσης στο παράρτημα της εργασίας.

Εφαρμογές και Οφέλη

Η εξέλιξη της τεχνητής νοημοσύνης και η χρήση της σε πολλαπλές εφαρμογές για πολλαπλές λειτουργίες έχει πραγματικά ωφελήσει την καθημερινή ζωή και την αλληλεπίδραση των πολιτών και των επισκεπτών στις πόλεις. Στα πλαίσια αυτά προχώρησα στην ανάπτυξη ενός Demo AI για την πόλη μου, το Ηράκλειο Κρήτης, το οποίο απεικονίζει εφαρμογές και οφέλη που μπορούν να προκύψουν από την χρήση ενός Chatbot για τους κατοίκους και τους επισκέπτες της πόλης με την παροχή των κατάλληλων πληροφοριών που αναζητούν.

Το Demo AI έχει δημιουργηθεί για εξυπηρετεί ως ψηφιακός βοηθός και να απαντά στις ερωτήσεις των χρηστών σε σχέση ποικίλα θέματα που αφορούν την πόλη. Το Chatbot μπορεί να παρέχει τόσο στους κατοίκους της πόλης όσο και στους επισκέπτες σημαντικές πληροφορίες για το Ηράκλειο όπως πληροφορίες για τοπικά γεγονότα, πληροφορίες για αξιοθέατα, για ιστορικά δεδομένα, για αθλητικά γεγονότα, για εκδηλώσεις, για καλλιτεχνικά δρώμενα αλλά και πληροφορίες για υπηρεσίες με βάση τα ενδιαφέροντα και τις προτιμήσεις των χρηστών προσφέροντας μία προσωποποιημένη εμπειρία. Επίσης μία σημαντική δυνατότητα κυρίως για τους επισκέπτες της πόλης είναι η εύρεση πληροφοριών για εστιατόρια, ξενοδοχεία και υπηρεσίες μεταφοράς σε πολλαπλές γλώσσες που σαφώς βελτιώνουν την εμπειρία του επισκέπτη στην πόλη μας. Επιπλέον μπορεί να παρέχει πληροφορίες σχετικά με τις δημόσιες υπηρεσίες όπως πληροφορίες για δομές δημόσιας υγείας, εκπαίδευσης ή ασφάλειας εξυπηρετώντας τους πολίτες για την ευκολότερη πρόσβαση τους σε αυτές.

Συμπερασματικά καταλήγουμε ότι ένας τέτοιος ψηφιακός βοηθός που απαντάει σε ερωτήσεις χρηστών για το Ηράκλειο Κρήτης προσφέρει πολυάριθμα οφέλη τόσο στους χρήστες και τους επισκέπτες όσο και στην ίδια την πόλη. Οι χρήστες του ψηφιακού βοηθού μπορούν να λάβουν απαντήσεις στις ερωτήσεις τους άμεσα και με ακρίβεια εξοικονομώντας τον χρόνο τον οποίο θα σπαταλούσαν σε διαφορετική περίπτωση. Επίσης οι χρήστες μπορούν να λάβουν προσωποποιημένες συστάσεις μέσω της ανάλυσης των προτιμήσεων τους κάνοντας την εμπειρία πιο ευχάριστη και αποτελεσματική. Συν τούτοις, το Demo AI είναι διαθέσιμο όλες τις ώρες της ημέρας επιτρέποντας στους χρήστες να λαμβάνουν πληροφορίες και βοήθεια οποιαδήποτε ώρα και στιγμή ανεξάρτητα από τις ώρες λειτουργίας των υπηρεσιών. Επιπλέον δίνει την δυνατότητα της ευκολότερης πρόσβασης σε πληροφορίες, όπως για παράδειγμα σε άτομα διαφορετικών εθνοτήτων ή άτομα με κινητικές και οπτικές δυσκολίες, αντίστοιχα όμως βέβαια παρέχει ευκολότερη πρόσβαση και σε όσους προτιμούν τις ψηφιακές λύσεις στην καθημερινότητα τους. Ωστόσο δεν μπορούμε να παραλείψουμε τα οφέλη που αποκομίζει η ίδια η πόλη καθώς με την παροχή όλων των πληροφοριών για την πόλη σε ένα μόλις ψηφιακό βοηθό για τις τοπικές επιχειρήσεις και τα αξιοθέατα ωθεί τον τουρισμό στην ενίσχυση και την υποστήριξη της τοπικής οικονομίας. Ένα επίσης σημαντικό ακόμη όφελος είναι η συλλογή πολύτιμων δεδομένων μέσω της αλληλεπίδρασης με τους χρήστες. Τα δεδομένα αυτά θα μπορούν να τα λάβουν οι δημοτικές αρχές και να τα χρησιμοποιήσουν ώστε να κατανοήσουν καλύτερα τις ανάγκες και τις προτιμήσεις των πολιτών ώστε να βελτιώσουν πιο στοχευμένα την βιωσιμότητα των πολιτών στην πόλη.

Η δημιουργία ενός ψηφιακού βοηθού με αυτή την ιδιότητα σε οποιαδήποτε πόλη μπορεί να δημιουργήσει μία πιο συνδεδεμένη και ενημερωμένη κοινότητα βελτιώνοντας την ποιότητα ζωής των κατοίκων και διευκολύνοντας τους την πρόσβαση σε πληροφορίες και υπηρεσίες διευκολύνοντας επίσης την εξερεύνηση των επισκεπτών στην πόλη. Τέλος, η συνεχής εξέλιξη του AI εξασφαλίζει ότι οι χρήστες θα λαμβάνουν διαρκώς ενημερωμένες πληροφορίες σύμφωνα με τις μεταβαλλόμενες ανάγκες.

Προκλήσεις και Περιορισμοί

Κατά την ανάπτυξη και τη χρήση του chatbot, αντιμετωπίσαμε διάφορες τεχνικές και λειτουργικές προκλήσεις που μας επηρέασαν άμεσα στην υλοποίηση αλλά και στην απόδοση του συστήματος.

Ενσωμάτωση και χρήση διαφόρων τεχνολογιών

Ο κύριος κώδικας του chatbot είναι σε NodeJs. Θα μπορούσαμε οι ερωτήσεις και οι απαντήσεις να λειτουργούν απευθείας μέσω του κύριου κώδικα, ωστόσο αυτό δε θα ήταν και τόσο “φιλικό” ως προς τη χρήση. Για αυτό το λόγο, προχωρήσαμε στη χρήση κώδικα php για το frontend τον οποίο το “σερβίρουμε” μέσω του web server (nginx). Η κύρια πρόκληση που έπρεπε να αντιμετωπίσουμε σε αυτό το στάδιο, ήταν η σωστή προώθηση των request από την php στο NodeJS (backend) μέσω του proxy_pass του nginx. Επιπροσθέτως, για να λειτουργήσει ο κώδικας php, χρειάζεται η ρύθμιση και η εγκατάσταση ενός handler (php-fpm). Αυτό αν και δεν απαιτεί τόσο περίπλοκη ρύθμιση, παραμένει ένα κρίσιμο βήμα το οποίο είναι απαραίτητο για την όλη υλοποίηση.

Διαχείριση request/responce

Η χρήση της LangChain για την επεξεργασία και την ανάκτηση των πληροφοριών από το αρχείο-βάση δεδομένων απαιτεί προσεκτική διαμόρφωση όλων των παραμέτρων (chhunksize, chunkoverlap και k) όπως έχει ήδη αναφερθεί. Στα πλαίσια της εργασίας και με δεδομένο πως η συγκεκριμένη εφαρμογή παρέχεται ως demo, δεν ήταν απαραίτητο να εμβαθύνουμε τόσο πολύ στη ρύθμιση αυτών, ωστόσο σε πιο περίπλοκες εφαρμογές ή όταν η βάση δεδομένων τείνει να είναι πολύ μεγάλη, η σωστή ρύθμισή τους είναι υψηλής σημασίας ώστε να διασφαλίσουμε ότι οι απαντήσεις που θα επιστρέφουν θα είναι στα πλαίσια του αποδεκτού βάσης των προδιαγραφών της εφαρμογής. Στις δοκιμές που κάναμε, διαπιστώσαμε πολλές φορές πως το μοντέλο AI που χρησιμοποιούσαμε δε χρησιμοποιούσε αποκλειστικά τα δεδομένα που εισάγαμε, αλλά πολλές φορές δημιουργούσε περιεχόμενο ανεξάρτητα των δικών μας πληροφοριών (hallucinations). Για να έχουμε το βέλτιστο αποτέλεσμα και να λειτουργεί η εφαρμογή μας με τον επιθυμητό τρόπο, έπρεπε να ρυθμίσουμε σωστά τις παραπάνω παραμέτρους.

Ασφάλεια και επικοινωνία

Αν και πρόκειται για δοκιμαστική εφαρμογή, είναι αρκετά σημαντικό να σταθούμε στο κομμάτι της ασφάλειας των δεδομένων κατά την αλληλεπίδραση με το χρήστη. Παρόλο που οι ερωτήσεις και οι απαντήσεις δε περιέχουμε ευαίσθητα δεδομένα, προχωρήσαμε στην εγκατάσταση SSL πιστοποιητικών μέσω του Certbot, ώστε τα δεδομένα που ανταλλάσσονται μεταξύ του χρήστη και της εφαρμογής να είναι κρυπτογραφημένα. Αυτό απαιτούσε κάποιες πρόσθετες ενέργειες στο configuration του nginx, χωρίς ωστόσο να πρόκειται για κάτι εξαιρετικά δύσκολο. Το σημαντικό κομμάτι στο οποίο πρέπει να σταθούμε, είναι η διαχείριση των API keys. Ο κώδικας κάνει χρήση του μοντέλου CHAT-GPT το οποίο παρέχεται επι πληρωμή με τη δημιουργία/χρήση API keys. Για να είμαστε σίγουροι πως δε θα έχουμε προβλήματα με μια πιθανή διαρροή του κλειδιού μας, χρησιμοποιούμε το αρχείο .env ώστε να περνάμε το κλειδί στην εφαρμογή με ασφάλεια.

Εξάρτηση από την Open AI

Λόγω της χρήσης του μοντέλου CHAT-GPT, η απόδοση αλλά και γενικότερα η εύρυθμη λειτουργία της εφαρμογής μας εξαρτάται από την αξιοπιστία και την απόδοση του Open AI API. Οποιοδήποτε outage ή καθυστέρηση από την υπηρεσία της Open AI επιδρά άμεσα και στην εμπειρία του χρήστη. Επίσης καθώς η υπηρεσία παρέχεται με χρέωση, υπάρχει περίπτωση αυτό να επηρεάζει τη λειτουργία της εφαρμογής, καθώς ενδέχεται να πρέπει να ορίσουμε με τη σειρά μας περιορισμούς ως προς το εύρος χρήσης, το ρυθμό των ερωτήσεων που μπορεί να κάνει κάθε χρήστης και άλλα, ώστε να μπορούμε να διατηρούμε τις χρεώσεις σε επιθυμητά επίπεδα.

Πρόσβαση σε πληροφορίες

Με την υπάρχουσα ρύθμιση των παραμέτρων (όπως αναφέρθηκε παραπάνω), το chatbot στηρίζεται αποκλειστικά στα δεδομένα που έχουμε ήδη εισάγει στο αρχείο μας. Θα πρέπει λοιπόν οι πληροφορίες που παρέχουμε να είναι ολοκληρωμένες έτσι ώστε η εφαρμογή να είναι σε θέση να απαντάει σε όσο των δυνατόν περισσότερες ερωτήσεις. Παρόλα αυτά το σύστημα θεωρείται αρκετά ευέλικτο καθώς η προσθήκη πληροφοριών ή η ενημέρωση των υπαρχόντων είναι ανεξάρτητη από το κύριο κώδικα και μπορεί να γίνει και από χρήστες χωρίς προγραμματιστικές γνώσεις. Ωστόσο θα πρέπει πάντα να ελέγχεται η ορθότητα και η εγκυρότητά τους ώστε η απαντήσεις να είναι ακριβείς και αποτελεσματικές.

Βελτιστοποίηση απόδοσης

Για υλοποιήσεις οι οποίες πρόκειται να διατεθούν στο ευρύ κοινό, είναι πολύ σημαντικό να σημειωθεί πως ενδέχεται να χρειάζεται να γίνουν περαιτέρω ρυθμίσεις / τροποποιήσεις. Ο σέρβερ που φιλοξενεί την υπάρχουσα εφαρμογή δεν είναι σε θέση να διαχειριστεί μεγάλο όγκο ταυτόχρονων επισκεπτών. Σε αυτή τη περίπτωση, θα ήταν χρήσιμο να γίνει μια σχετική μελέτη ώστε να προβλεφθεί ο εκτιμώμενος αριθμός επισκεπτών, ώστε να επιλεγεί ο κατάλληλος σέρβερ με τα απαραίτητα resources. Επίσης η χρήση εργαλείων όπως nginx caching ίσως να βοηθήσει στη βελτιστοποίηση της απόδοσης. Να σημειωθεί πως μέσω του PM2 μπορεί να επιτευχθεί η παρακολούθηση του nodeJS ώστε αν ελέγχεται και η κατανάλωση μνήμης.

Όπως καταλαβαίνουμε από τους παραπάνω περιορισμούς και τις προκλήσεις που αντιμετωπίσαμε, είναι σημαντικό η διαμόρφωση του συστήματος να γίνει με προσοχή και να υπάρχει συνεχής παρακολούθηση / συντήρηση ώστε να έχουμε το βέλτιστο επιθυμητό αποτέλεσμα. Παρά τις όλες δυσκολίες, η σωστή λειτουργία της εφαρμογής μπορεί να επιβεβαιωθεί και να χρησιμοποιηθεί ως πρότυπο και για άλλες πρακτικές εφαρμογές.

Οφέλη και Προκλήσεις της Χρήσης AI

Οφέλη

Ο κλάδος της τεχνητής νοημοσύνης είναι ένας κλάδος ταχείας ανάπτυξης ο οποίος έχει ενσωματωθεί για τα καλά στην καθημερινότητα πολλών ανθρώπων καθώς έχει λάβει θέση σε πολλούς κλάδους της ζωής. Χάρη αυτό το εργαλείο, παρέχονται στους χρήστες άμεσες λύσεις που βελτιώνουν την ποιότητα ζωής καθώς μπορούν να κερδίσουν χρόνο λαμβάνοντας άμεσες και προσωποποιημένες λύσεις. Ένα τέτοιο εξαιρετικό παράδειγμα αυτής της ενσωμάτωσης είναι το παραπάνω Demo AI όπου έχει αναπτυχθεί για το Ηράκλειο Κρήτης το οποίο μπορεί να προσφέρει πολυάριθμα οφέλη στους χρήστες και στην τοπική κοινότητα.

Ένα πολύ σημαντικό όφελος είναι η άμεση πρόσβαση σε ενημερωμένες πληροφορίες. Οι χρήστες μπορούν με την χρήση φυσικής γλώσσας να ρωτήσουν τον αλγόριθμο ότι επιθυμούν σχετικά με το Ηράκλειο Κρήτης για ζητήματα όπως τοπικά γεγονότα, αξιοθέατα ή πληροφορίες για δημόσιες υπηρεσίες και να ενημερωθούν πάρα πολύ άμεσα εξοικονομώντας αρκετό χρόνο που θα σπαταλούσαν σε διαφορετική περίπτωση. Επιπλέον η ενημέρωση των πληροφοριών εντός του αλγορίθμου όπως και η ενημέρωση του ίδιου του αλγορίθμου είναι συστηματική και

πραγματοποιείται πάρα πολύ άμεσα με αποτέλεσμα οι χρήστες να λαμβάνουν ενημερωμένες και ακριβείς πληροφορίες.

Επιπλέον το ΑΙ προσφέρει προσωποποιημένη εμπειρία στον εκάστοτε χρήστη. Ο κάθε χρήστης μπορεί να αναζητήσει ότι επιθυμεί σύμφωνα με τις δικές του προτιμήσεις και ενδιαφέροντα με αποτέλεσμα να λάβει εξατομικευμένες συστάσεις για τοποθεσίες προς επίσκεψη, εκδηλώσεις, δραστηριότητες κ.α. Λόγω αυτού οι χρήστες έχουν το αίσθημα ότι λαμβάνουν βοήθεια και υποστήριξη που ανταποκρίνεται στις ατομικές τους ανάγκες.

Το ΑΙ δίνει επίσης στους χρήστες την δυνατότητα για εύκολη πρόσβαση στις δημόσιες υπηρεσίες καθώς μπορούν να βρουν εύκολα πληροφορίες σχετικά με τις δημόσιες υπηρεσίες, όπως υπηρεσίες υγειονομικού ενδιαφέροντος εκπαιδευτικά ιδρύματα ή πληροφορίες για τα μέσα μαζικής μεταφοράς, με την χρήση ενός εύχρηστου ψηφιακού βοηθού. Ωστόσο έχοντας τον ψηφιακό οδηγό ο οποίος μπορεί να απαντάει και να κατευθύνει τους χρήστες σε συχνές ερωτήσεις βελτιώνεται ακόμη η αποτελεσματικότητα της δημόσιας διοίκησης.

Ακόμη ο ψηφιακός βοηθός μπορεί να πληροφορήσει τους χρήστες για τις τοπικές επιχειρήσεις, όπως τα εστιατόρια και τα καταστήματα παροχής υπηρεσιών, με αποτέλεσμα την αύξηση της επισκεψιμότητας και κατά συνέπεια των πωλήσεων και την ενίσχυση της τοπικής οικονομίας. Αυτό εξυπηρετεί ιδιαίτερα στην προώθηση της τοπικής αγοράς προς τους επισκέπτες της πόλης εφόσον τους παρέχονται άμεσα και εύκολα όλες οι χρήσιμες πληροφορίες για την πόλη σύμφωνα με τις δικές τους ανάγκες και προτιμήσεις για τα αξιοθέατα ή τις δραστηριότητες που μπορούν να απολαύσουν ερχόμενοι στο Ηράκλειο.

Ωστόσο αυτό περιλαμβάνει και την αύξηση της αποδοτικότητας στις Δημοτικές υπηρεσίες, καθώς με την αυτοματοποιημένη διαχείριση αιτημάτων μειώνεται σημαντικά ο χρόνος επίλυσης ενός προβλήματος μειώνοντας και την ανάγκη για ανθρώπινη παρέμβαση και μειώνοντας τα έξοδα της Δημοτικής Αρχής. Η συλλογή και η επεξεργασία πληροφοριών μπορεί να γίνει εύκολα και άμεσα μέσω της αλληλεπίδρασης των χρηστών με τον ψηφιακό βοηθό, εκμηδενίζοντας σχεδόν τον χρόνο αποστολής των τελικών πληροφοριών στην Δημοτική Αρχή ώστε να βοηθήσει στην λήψη κατάλληλων στρατηγικών αποφάσεων.

Αυτό δίνει την δυνατότητα σε όλους τους πολίτες να συμμετέχουν πιο ενεργά σε κοινωνικά ζητήματα και ζητήματα ενημέρωσης. Όλοι οι πολίτες μπορούν να ενημερωθούν για τα κοινωνικά δρώμενα, για νέους νόμους και κανονισμούς και να συμμετέχουν πιο ενεργά στην παράθεση των απόψεων τους για τη λήψη καλύτερων και πιο εξυπηρετικών αποφάσεων σχετικά με την πόλη τους.

Προκλήσεις

Όπως διαπιστώσαμε η χρήση ενός ψηφιακού βοηθού για κάθε πόλη, όπως και για το Ηράκλειο Κρήτης, επιφέρει ποικίλα και πολυδιάστατα οφέλη. Ωστόσο δεν μπορούμε να μην εξετάσουμε τις προκλήσεις τις οποίες πρέπει να ελέγξουμε και να τις να αντιμετωπίσουμε για να εξασφαλίσουμε τόσο την ηθική και την αξιοπιστία, όσο και την ορθή νομική υπόσταση του συστήματος.

Ένα από τα πιο κρίσιμα ζητήματα το οποίο θα πρέπει να εξεταστεί εξονυχιστικά είναι τα ηθικά ζητήματα. Ο ψηφιακός βοηθός λαμβάνει και επεξεργάζεται πολλές πληροφορίες που αφορούν προσωπικά δεδομένα, λόγω αυτού θα πρέπει να διασφαλιστεί τόσο η προστασία των δεδομένων όσο και η ιδιωτικότητα των πληροφοριών των χρηστών. Σε τέτοια ζητήματα η παραβίαση των

προσωπικών δεδομένων μπορεί να οδηγήσει τους χρήστες στο να ακολουθήσουν νομική οδό καθώς και στο να χάσουν κάθε εμπιστοσύνη προς οποιονδήποτε ψηφιακό βοηθό απομακρύνοντας τους από την λειτουργία τόσο σημαντικών για την καθημερινότητα τους εργαλείων. Ο αλγόριθμός θα πρέπει να λειτουργεί με διαφάνεια ώστε οι χρήστες να μπορούν να κατανοούν τον τρόπο λειτουργίας του και να κατανοούν πως χρησιμοποιούνται οι πληροφορίες οι οποίες μοιράζονται μαζί του. Επιπλέον ο αλγόριθμός του ΑΙ θα πρέπει στις πληροφορίες τις οποίες χρησιμοποιεί να διαθέτει προκαθορισμένες ηθικές αρχές και αξίες οι οποίες να συμβαδίζουν με αυτές τις κοινωνίας. Ειδικότερα οι ψηφιακοί βοηθοί που λαμβάνουν αποφάσεις θα πρέπει να προγραμματίζονται με υπευθυνότητα και να είναι σαφές να μην δημιουργηθούν υποψίες για καταχρήσεις ή ηθικά διλήμματα.

Ένα ακόμη σημαντικό ζήτημα είναι η εξασφάλιση των ορθών πληροφοριών. Ο ψηφιακός βοηθός θα πρέπει να είναι ακριβής στις απαντήσεις του και τα δεδομένα που χρησιμοποιεί να είναι ακριβή και αξιόπιστα. Η μη ανανέωση των πληροφοριών του αλγορίθμου ή η μη επαρκής ποιότητα των δεδομένων του είναι πιθανό να ελαττώσουν την αποτελεσματικότητα του ή ακόμη να παρέχει στους χρήστες λανθασμένες και παραπλανητικές πληροφορίες με αποτέλεσμα να τους οδηγούν στην λήψη λανθασμένων αποφάσεων. Κάτι τέτοιο θα πλήξει σοβαρά την αξιοπιστία των ψηφιακών βοηθών. Ακόμη θα πρέπει να είναι σε θέση να αντιμετωπίζει λάθη βάση των πληροφοριών που διαθέτει και να χειρίζεται τις αβεβαιότητες προειδοποιώντας τους χρήστες όταν η πληροφορία που παρέχει δεν είναι εξακριβωμένη. Αυτό δημιουργεί την ανάγκη της συνεχής αναβάθμισης του μοντέλου για την συνεχή βελτίωση του καθώς κρίνεται αναγκαία για να παρέχει ορθές πληροφορίες στους χρήστες και να ελαχιστοποιεί τα σφάλματα.

Τέλος ένα εξίσου σημαντικό ζήτημα το οποίο θα πρέπει να εξεταστεί είναι τα πνευματικά δικαιώματα. Τα μοντέλα ΑΙ εκπαιδεύονται μέσω πληροφοριών που λαμβάνουν, οι οποίες μπορεί να περιέχουν προστατευμένο περιεχόμενο. Η χρήση και επεξεργασία πληροφοριών τέτοιου είδους θα πρέπει να τηρεί τους νόμους σχετικά με την πνευματική ιδιοκτησία και να αποφεύγει την παράνομη χρήση και επεξεργασία δεδομένων. Ας μην ξεχνάμε ωστόσο ότι μέσω των μοντέλων ΑΙ ο χρήστης μπορεί να παράξει περιεχόμενο. Το περιεχόμενο αυτό μπορεί να δημιουργήσει απορίες σχετικά με τα δικαιώματα ιδιοκτησίας και χρήσης του. Γι' αυτό θα πρέπει η πληροφορία αυτή θα πρέπει εξ αρχής να οριστεί σαφώς. Επίσης ο αλγόριθμος θα πρέπει να διαθέτει άδεια χρήσης στις συγκεκριμένες περιπτώσεις και να ακολουθεί συγκεκριμένους κανονισμούς προστατεύοντας ταυτόχρονα και των δημιουργό περιεχομένου μέσω του ΑΙ αλλά και τον χρήστη. Ωστόσο το συγκεκριμένο ζήτημα θα το αναλύσουμε εκτενέστερα σε επόμενη παράγραφο.

Πνευματικά Δικαιώματα

Με την πάροδο του χρόνου έχουμε παρατηρήσει πως η τεχνητή νοημοσύνη έχει ανατρέψει πλήρως τους τρόπου παραγωγής περιεχομένου όπως η παραγωγή εικόνας, βίντεο, μουσικής ή άλλης μορφής δημιουργικού περιεχομένου καθώς πλέον μπορεί εύκολα οποιοσδήποτε χρήστης να δημιουργήσει κάποιο έργο με αυτοματοποιημένο τρόπο. Ωστόσο αυτή η καινοτομία έχει επιφέρει σημαντικές αναταραχές στον τομέα των πνευματικών δικαιωμάτων. Η τεχνολογία αναπτύσσεται ωστόσο μαζί της θα πρέπει να τροποποιηθούν και να προσαρμοστούν οι νομοθεσίες ώστε να είναι κατάλληλες πλέον και να μπορούν να καλύψουν τις νέες ανάγκες που έχουν δημιουργηθεί.

Είναι σημαντικό να ορίσουμε σε ευδιάκριτο πλαίσιο τον κάτοχο των δικαιωμάτων για το παραγόμενο περιεχόμενο. Παραδοσιακά, τα πνευματικά δικαιώματα συνδέονται άμεσα με τα άτομα όπου παράγουν το περιεχόμενο. Στην δεδομένη περίπτωση το άτομο είναι ο χρήστης ο οποίος προσθέτει και ορίζει συγκεκριμένες εισροές. Βέβαια αντίστοιχα κάτοχος των πνευματικών δικαιωμάτων μπορεί

να οριστεί και ο δημιουργός του του εκάστοτε ΑΙ παραγωγής περιεχομένου. Δεν έχει ωστόσο οριστεί ακόμη ποιος κατέχει τα πνευματικά δικαιώματα για αυτά τα έργα αλλά η ανάγκη για να οριστούν νέες νομικές αρχές εντείνεται διαρκώς.

Επιπτώσεις στην Αγορά Εργασίας

Η ανάπτυξη της τεχνητής νοημοσύνης είναι διαρκώς εξελισσόμενη και εξυπηρετεί άμεσα στην βελτίωση της καθημερινότητας και της ποιότητας ζωής των ανθρώπων. Οι επιπτώσεις ωστόσο των συγκεκριμένων αλγορίθμων έχουν ξεκινήσει να κάνουν την εμφάνισή τους και ως άμεσο ζήτημα έχει παρατηρηθεί ο μετασχηματισμός της οικονομίας, της κοινωνίας και κατά συνέπεια έχουν φτάσει οι αλλαγές και στην αγορά εργασίας.

Όπως είναι φυσικό ο κυρίως προβληματισμός σχετικά με τις επιπτώσεις στην αγορά εργασίας με την εμφάνιση του ΑΙ είναι η μείωση των θέσεων εργασίας. Ένα εργαλείο ΑΙ όπως είναι το ΑΙ για την πόλη του Ηρακλείου Κρήτης μπορεί να αυτοματοποιήσει αρκετές διαδικασίες και να αντικαταστήσει ανθρώπινο δυναμικό σε θέσεις εργασίας που παρέχουν εξυπηρέτηση πελατών, η διαχείριση και επεξεργασία δεδομένων ή παραγωγή περιεχομένου. Άμεσες θέσεις εργασίας οι οποίες απειλούνται είναι σε επαγγέλματα όπως ο τομέας της γραμματειακής υποστήριξης, η υποστήριξη πελατών αλλά και η λιανική πώληση υπό προϋποθέσεις.

Αντίστοιχα βέβαια, παρά την απειλή μείωσης θέσεων εργασίας σε ορισμένους τομείς, δημιουργεί νέες θέσεις εργασίας σε διαφορετικούς τομείς. Τα συστήματα ΑΙ χρειάζονται επαγγελματίες για την συντήρηση αλλά και για την ανάπτυξη τους ώστε να ακολουθούν και να προσαρμόζονται στα νέα δεδομένα της κάθε εποχής. Αντίστοιχα νέες θέσεις εργασίας δημιουργούνται και στην ανάλυση δεδομένων, ώστε κατά την είσοδο δεδομένων σε ένα πληροφοριακό σύστημα ΑΙ να φέρει στον χρήστη την βέλτιστη προσωποποιημένη απάντηση. Χρήσιμες ακόμη θέσεις εργασίας οι οποίες αναγκαία θα δημιουργηθούν είναι η θέσεις για την ασφάλεια των πληροφοριών και θέσεις για την διαχείριση έργων τεχνολογίας. Ωστόσο οι νέες θέσεις εργασίας απαιτούν από τους εργαζομένους να διαθέτουν νέες δεξιότητες και γνώσεις. Για παράδειγμα την εκπαίδευση σε εξειδικευμένους τομείς όπως η διαχείριση συστημάτων ΑΙ, η επεξεργασία και ανάλυση δεδομένων και η εκπαίδευση στην μηχανική μάθηση.

Ως εκ τούτου παρατηρούμε ότι με τον καιρό η ανάγκη για εργαζομένους με τεχνικές δεξιότητες αυξάνονται. Θα πρέπει οι εργαζόμενοι να είναι σε θέση να αντιλαμβάνονται τις νέες τεχνολογίες οι οποίες διαρκώς εξελίσσονται, επίσης γνώσεις σε θέματα προγραμματισμού θα είναι επίσης χρήσιμα. Ο τομέας της τεχνητής νοημοσύνης δημιουργεί την ανάγκη για συνεχή επανακατάρτιση στις νέες τεχνολογίες ώστε να είναι δυνατή η προσαρμογή του ατόμου στις συνεχείς αλλαγές της αγοράς εργασίας.

Ωστόσο όπως είναι λογικό ένα μέρος των εργαζομένων δεν διαθέτει την απαραίτητη εξοικείωση με την τεχνολογία με αποτέλεσμα η επέκταση της τεχνητής νοημοσύνης στην καθημερινότητα μας να ενισχύει την ανισότητα στην αγορά εργασίας σε σχέση με τους εργαζομένους που κατέχουν τεχνικές δεξιότητες. Αυτό έχει ως αποτέλεσμα την μείωση των θέσεων εργασίας στην συγκεκριμένη κοινωνική ομάδα και πιθανόν την αύξηση της ανεργίας και της οικονομικής ανασφάλειας.

Συμπερασματικά η άνθιση της τεχνητής νοημοσύνης αποτελεί σημαντικό παράγοντα για τον μετασχηματισμό της αγοράς εργασίας καθώς δημιουργεί νέες ευκαιρίες αλλά φυσικά και νέες προκλήσεις σε σχέση με τις παραδοσιακές θέσεις εργασίας. Δημιουργεί νέες θέσεις εργασίας στους τομείς της τεχνολογίας, του προγραμματισμού, της ανάλυσης δεδομένων, της ασφάλειας των δεδομένων αλλά και της μηχανικής μάθησης με προϋπόθεση την άριστη σχέση με την τεχνολογία και

την ανάγκη για δια βίου μάθησης. Παρόλα αυτά η πρόκληση για άτομα μη εξοικειωμένα με την τεχνολογία αυξάνεται με αύξηση του ρίσκου για τις επιπτώσεις στην ποιότητα ζωής τους.

Ασφάλεια και Παραπληροφόρηση

Η εξέλιξη της τεχνητής νοημοσύνης έχει επιφέρει σημαντικές αλλαγές στην δημιουργία περιεχομένου όπως την δημιουργία υψηλής ποιότητας κειμένων, εικόνων, βίντεο και άλλων δημιουργικών έργων με την χρήση αυτοματοποιημένων αλγορίθμων. Παρά τις σημαντικές εξελίξεις που έχει επιφέρει η χρήση του ΑΙ στην παραγωγή περιεχομένου έχει αφυπνήσει σημαντικούς κινδύνους κυρίως σε τομείς ηθικής, ασφάλειας και παραπληροφόρησης. Κρίνεται αναγκαία ωστόσο η ανάλυση των κινδύνων ώστε να κατανοήσουμε τις επιπτώσεις που πιθανόν να επιφέρει στην κοινωνία η ανάπτυξη της τεχνητής νοημοσύνης ώστε να βρεθούν οι κατάλληλοι τρόποι αντιμετώπισης τους.

Το κυριότερο ζήτημα είναι οι πολυποίκιλοι κίνδυνοι ασφαλείας. Για την χρήση του ΑΙ για παραγωγή περιεχομένου είναι αναγκαία η συλλογή και η επεξεργασία μεγάλου όγκου δεδομένων τα οποία μπορεί να περιλαμβάνουν και εξατομικευμένες προσωπικές πληροφορίες. Λόγω αυτού θα πρέπει να διασφαλιστεί η προστασία των δεδομένων ώστε να μην υπάρχει ο κίνδυνος παραβίασης προσωπικών δεδομένων ή κακόβουλης επεξεργασίας κοινόχρηστων πληροφοριών και παραβίαση της ιδιωτικότητας.

Μία ακόμη σημαντική ανησυχία είναι τα αποτελέσματα από την εξάρτηση με την τεχνολογία. Οι δυνατότητες που παρέχει ένας ψηφιακός βοηθός έχουν δημιουργήσει ανησυχία σχετικά με την εξάρτηση των χρηστών καθώς υπάρχει το ενδεχόμενο απώλειας δεξιοτήτων στους χρήστες λόγω της συνεχούς διευκόλυνσης μέσω το ΑΙ. Το πρόβλημα αυτό εντείνεται σε περίπτωση εσφαλμένης απάντησης της τεχνητής νοημοσύνης ή σε περίπτωση ελλιπής γνώσεις καθώς οι χρήστες μπορεί να μην έχουν μετέπειτα επαρκείς δεξιότητες για την επίλυση του ζητούμενου προβλήματος.

Με την κακόβουλη χρήση της τεχνητής νοημοσύνης μπορεί να παραχθεί δημιουργικό περιεχόμενο όπως ρεαλιστικές εικόνες και βίντεο τα οποία να αναπαριστούν ψευδές περιεχόμενο με σκοπό να παραπλανήσει το κοινό. Συνεπώς η ανάπτυξη της συγκεκριμένης δυνατότητας εντείνει την τον κίνδυνο διάδοσης ψευδών ειδήσεων με σκοπο την παραπληροφόρηση. Επιπλέον οι αυτοματοποιημένες διαδικασίες είναι σε θέση να επιταχύνουν την διαδικασία διάδοσης ψευδών πληροφοριών. Αυτό εντείνει την ανάγκη το κοινό να εκπαιδεύεται και να διαθέτει κριτική σκέψη ώστε να είναι σε θέση να επιλέγει τις πληροφορίες που απορροφά. Βέβαια η κακόβουλη παραγωγή ψευδούς περιεχομένου μέσω του ΑΙ έχει ως αποτέλεσμα να υπονομεύσει την εμπιστοσύνη των χρηστών προς τα μέσα ενημέρωσης και τις πηγές πληροφόρησης.

Για τον λόγο αυτό η λογοδοσία αλλά και η ευθύνη για το παραγόμενο περιεχόμενο σχετικά με την ορθότητα των απαντήσεων και την ηθική μέσω ΑΙ αναπτύσει πολλά ερωτήματα. Θα πρέπει να οριστεί υπαίτιο άτομο για την παραγωγή του περιεχομένου καθώς ένας αλγόριθμος ΑΙ αλληλεπιδρά με πολλαπλά άτομα από τον δημιουργό του έως και τον τελικό χρήστη.

Συμπεράσματα

Ευρήματα και επίτευξη στόχων.

Κατά τη διάρκεια της εργασίας, κάναμε μια ιστορική αναδρομή στην εξέλιξη της τεχνητής νοημοσύνης στο πέρασμα του χρόνου και μελετήσαμε διάφορα μοντέλα παραγωγής περιεχομένου. Η χρήση τεχνητής νοημοσύνης για τη παραγωγή περιεχομένου στις μέρες μας, είναι η πιο δημοφιλής, αφού κυρίως με την εμφάνιση του chat-gpt από την Open AI, η TN έγινε γνωστή στο ευρύ κοινό. Όλο και περισσότερος κόσμος άρχισε να χρησιμοποιεί τη τεχνητή νοημοσύνη στη καθημερινότητά του, από χρήστες οι οποίοι απλά αναζητούν κάποιες πληροφορίες, μέχρι και κάποιους που παράγουν multimedia και λόγους ψυχαγωγίας. Η δωρεάν διάθεση των μοντέλων αυτών, έχει δημιουργήσει τα τελευταία χρόνια ένα αυξημένο ενδιαφέρον προς τη τεχνολογία αυτή και άσχετα από το επίπεδο του κάθε χρήστη ολοένα και περισσότεροι φαίνεται να είναι οικείοι στη χρήση της.

Πέρα από τις βασικές έννοιες και τα συγκεκριμένα μοντέλα που αναφέραμε, βλέπουμε πως αυτή η μαζική χρήση της TN φέρνει στην επιφάνεια πολύ σημαντικά κοινωνικά ζητήματα, τα οποία στο μέλλον ενδέχεται να φέρουν στην επιφάνεια την ανάγκη για νομικές ρυθμίσεις. Η παραγωγή εικόνων και γενικότερα multimedia ή η συγγραφή σεναρίων θέτει ζητήματα περι ιδιοκτησίας και πνευματικών δικαιωμάτων και οι συζητήσεις γύρω από αυτό έχουν ήδη ξεκινήσει.

Για να δείξουμε τις πρακτικές εφαρμογές που μπορεί να έχει η χρήση της τεχνητής νοημοσύνης στη βελτίωση της καθημερινότητάς μας, προχωρήσαμε στη δημιουργία ενός chat bot το οποίο με βάση πληροφορίες που έχουμε ήδη εισάγει, είναι σε θέση να απαντάει σε ερωτήσεις χρηστών σχετικά με τη πόλη μας (Ηράκλειο Κρήτης). Βλέποντας πως η εφαρμογή λειτουργεί ορθά, συμπεραίνουμε πως παρόμοιες υλοποιήσεις μπορεί να έχουμε σημαντικές πρακτικές εφαρμογές σε διάφορους κλάδους, βελτιώνοντας τις ζωές μας. Αντίστοιχες εφαρμογές θα μπορούσαν να χρησιμοποιηθούν από δήμους ώστε να παρέχουν πληροφορίες σχετικά με τις υπηρεσίες τους ή ακόμα και από εταιρείες ώστε να απαντούν σε ερωτήσεις πελατών σχετικά με τη χρήση ενός προϊόντος ή μιας υπηρεσίας. Αντίστοιχα, εκπαιδευτικά ιδρύματα θα μπορούσαν να διατηρούν σχετικές βάσης δεδομένων βάση των οποίων θα μπορούν να παρέχουν πληροφορίες στους σπουδαστές ή να βελτιώνουν την απόδοση στα πλαίσια των μαθημάτων.

Η αρχική ιδέα για τη δημιουργία της εφαρμογής, ήταν καθαρά η επίλυση καθημερινών προβλημάτων που μπορεί να αντιμετωπίζει κάποιος και η ανάδειξη της αναγκαιότητας για τη χρήση της συγκεκριμένης τεχνολογίας. Οι στόχοι μας φαίνεται πως έχουν επιτευχθεί καθώς μέσω του chat bot που δημιουργήσαμε, σε πρώτη φάση μπορούμε να παρέχουμε στο χρήστη τη δυνατότητα να λάβει απαντήσεις χωρίς να χρειάζεται να ψάχνει σε πολλαπλές πηγές και να ελέγχει την ορθότητά τους και σε δεύτερη φάση, οι απαντήσεις που λαμβάνει να είναι προσωποποιημένες αφού το chat bot είναι σε θέση να απαντάει σε διαφορετικές γλώσσες. Επιπροσθέτως, παρουσιάζουμε κοινωνικές πτυχές οι οποίες ενδεχομένως να αγνοούνται από τη πλειοψηφία των χρηστών της τεχνητής νοημοσύνης και οι οποίες σε βάθος χρόνου ενδέχεται να είναι σε κέντρο των συζητήσεων γύρω από τη TN. Παρόλο που ο κύριος στόχος της εργασίας δεν είναι να ασχοληθεί με κοινωνικά ζητήματα, είναι σημαντικό να καταλάβουμε πως οποιαδήποτε πρακτική εφαρμογή της TN (ειδικά στη παραγωγή περιεχομένου) θα πρέπει λαμβάνει υπόψη της σχετικά ζητήματα που μπορεί να προκύπτουν.

Βιβλιογραφία

Europarl:

<https://www.europarl.europa.eu/topics/el/article/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoieitai>

Wikipedia:

https://el.wikipedia.org/wiki/%CE%A4%CE%B5%CF%87%CE%BD%CE%B7%CF%84%CE%AE_%CE%BD%CE%BF%CE%B7%CE%BC%CE%BF%CF%83%CF%8D%CE%BD%CE%B7

Forbes: <https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/>

Coursera: <https://www.coursera.org/articles/types-of-ai>

Medium:

<https://medium.com/@camilajohn001/theory-of-mind-ai-the-next-frontier-in-artificial-intelligence-92cb1963ab5d>

Sap: <https://www.sap.com/greece/products/artificial-intelligence/what-is-generative-ai.html>

Instantai Prompt: <https://www.instantaiprompt.com/a-i-tools/dall-e/>

Nginx Documentation: <https://nginx.org/en/docs/>

PHP Documentation: <https://www.php.net/docs.php>

Node.js Documentation: <https://nodejs.org/en/docs/>

PM2 Documentation: <https://pm2.keymetrics.io/docs/usage/quick-start/>

LangChain Documentation: <https://langchain.readthedocs.io/>

OpenAI API Documentation: <https://beta.openai.com/docs/>

Certbot Documentation: <https://certbot.eff.org/docs/>

Παράρτημα

Δημιουργία SSH keys & απενεργοποίηση password authentication.

Αρχικά τρέχουμε το παρακάτω **τοπικά** για τη δημιουργία του κλειδιού
`ssh-keygen -t rsa -b 4096 -C "your\_email@example.com"`

έπειτα αντιγράφουμε το public key στο remote server
`ssh-copy-id yourusername@your_server_ip`

ανοίγουμε το `/etc/ssh/sshd_config`
`sudo vi /etc/ssh/sshd_config`

και τροποποιούμε το `PasswordAuthentication` ως εξής
`PasswordAuthentication no`

τέλος επανεκκινούμε την υπηρεσία `sshd`
`sudo systemctl restart sshd`

Nucleus Sampling

Όταν το μοντέλο σκέφτεται ποια λέξη να βάλει στη συνέχεια, κάθε πιθανή λέξη έχει μια βαθμολογία (πιθανότητα). Το nucleus sampling διαλέγει μόνο από τις **λέξεις με τις υψηλότερες πιθανότητες**, ώστε η επιλογή να είναι πιο ελεγχόμενη και λιγότερο τυχαία.

- **top_p** είναι ένα ποσοστό (π.χ., 0.1, 0.5, 1.0) που λέει στο μοντέλο να λαμβάνει υπόψη **μόνο τις πιο πιθανές λέξεις που συνολικά αποτελούν το X% της συνολικής πιθανότητας**.
 - Για **top_p: 1.0**, όλες οι πιθανές λέξεις λαμβάνονται υπόψη.
 - Για **top_p: 0.1**, λαμβάνονται υπόψη μόνο οι πιο πιθανές λέξεις που αθροίζουν το 10% των συνολικών πιθανοτήτων.

Παράδειγμα

Ας υποθέσουμε ότι το μοντέλο πρέπει να συμπληρώσει την πρόταση:

"The cat is on the..."

Το μοντέλο υπολογίζει τις πιθανότητες για τις επόμενες λέξεις:

Λέξη	Πιθανότητα	Σωρευτική πιθανότητα
roof	0.4	0.4

table	0.3	0.7
floor	0.2	0.9
moon	0.05	0.95
car	0.03	0.98
refrigerator	0.02	1.00

top_p = 1.0

- Όλες οι πιθανές λέξεις περιλαμβάνονται. Το μοντέλο μπορεί να επιλέξει οποιαδήποτε από τις λέξεις, ακόμα και "refrigerator" ή "moon".

top_p = 0.9

- Επιλέγονται μόνο οι λέξεις που καλύπτουν το 90% των συνολικών πιθανοτήτων.
- Άρα οι πιθανές επιλογές είναι: roof, table, και floor.

top_p = 0.1

- Επιλέγονται μόνο οι λέξεις που καλύπτουν το 10% των συνολικών πιθανοτήτων.
- Άρα η μοναδική επιλογή είναι η λέξη: roof.

Ας πούμε ότι ρωτάς το μοντέλο:

"What is the capital of France?"

Με top_p = 1.0

Το μοντέλο μπορεί να επιστρέψει:

- "Paris" (0.9 πιθανότητα)
- "Marseille" (0.05 πιθανότητα)
- "London" (0.03 πιθανότητα)
- "Berlin" (0.02 πιθανότητα)

Με top_p = 0.1

Το μοντέλο θα επιστρέψει μόνο:

- "Paris" (η μόνη λέξη που είναι εντός του πρώτου 10% των πιθανοτήτων).

Retriever και Vector Store

Ένα **retriever** είναι μια "έξυπνη" μηχανή αναζήτησης που μπορεί να βρει τα πιο σχετικά δεδομένα από ένα σύνολο εγγραφών, με βάση την ομοιότητα μεταξύ ερωτήματος (query) και δεδομένων που είναι αποθηκευμένα ως διανύσματα.

Ένα **vector store** αποθηκεύει πληροφορίες με τη μορφή **διανυσμάτων** (vectors), δηλαδή αριθμητικών αναπαραστάσεων που περιγράφουν τη σημασιολογική έννοια της πληροφορίας. Κάθε ερώτημα μετατρέπεται επίσης σε διάνυσμα, και το retriever βρίσκει τα πιο κοντινά (σχετικά) διανύσματα χρησιμοποιώντας μεθόδους όπως:

- **Cosine Similarity**: Υπολογίζει την γωνία μεταξύ των διανυσμάτων.
 - **Euclidean Distance**: Υπολογίζει την απόσταση στο χώρο.
-

χρησιμοποιώντας το παρακάτω `vectorStore.asRetriever({...})` μπορούμε να χρησιμοποιήσουμε το retriever ώστε να ανακτήσουμε πληροφορίες από το vector store. Στη παραπάνω κλάση ορίζουμε ένα chunk (το ονομάζω k) το οποίο καθορίζει πόσα αποτελέσματα επιστρέφει το retriever:

- **Χαμηλό k**: Επιστρέφονται μόνο λίγα κομμάτια πληροφορίας (π.χ., τα 3 πιο σχετικά).
 - Χρήσιμο όταν θέλεις γρήγορες και στοχευμένες απαντήσεις.
- **Υψηλό k**: Επιστρέφονται περισσότερα κομμάτια (π.χ., 10).
 - Χρήσιμο όταν:
 - Θέλεις να έχεις περισσότερες πληροφορίες για να δουλέψεις.
 - Θέλεις να αποφύγεις την πιθανότητα να παραλειφθούν σημαντικές πληροφορίες.

RetrievalQChain & LangChain

Το **LangChain** είναι μια βιβλιοθήκη Python (και άλλων γλωσσών) σχεδιασμένη να διευκολύνει την ανάπτυξη εφαρμογών που βασίζονται σε μεγάλα γλωσσικά μοντέλα (**LLMs**), όπως το GPT-4. Προσφέρει εργαλεία και αφαιρέσεις για την ενσωμάτωση γλωσσικών μοντέλων σε πιο περίπλοκες εφαρμογές.

Το **RetrievalQChain** είναι μια μέθοδος ή εργαλείο στη βιβλιοθήκη **LangChain** που χρησιμοποιείται για την ανάπτυξη εφαρμογών ερωτήσεων-απαντήσεων (Q&A). Βασίζεται στη δυνατότητα να συνδυάζει την αναζήτηση πληροφοριών από δεδομένα (retrieval) με την παραγωγή απαντήσεων (QA).

Πώς λειτουργεί το RetrievalQChain;

1. **Ερώτημα από τον χρήστη (Query)**:
 - Ο χρήστης θέτει μια ερώτηση, όπως π.χ., "Ποια είναι η πρωτεύουσα της Γαλλίας;"

2. **Retriever:**

- Ένα εργαλείο (όπως το vector store retriever) αναζητά τα πιο σχε σχετικά δεδομένα από μια βάση δεδομένων ή ένα αποθηκευμένο corpus, χρησιμοποιώντας τεχνικές όπως:
 - **Semantic search:** Εύρεση πληροφοριών με βάση τη σημασιολογία του ερωτήματος.
 - **Cosine similarity:** Μέτρηση της ομοιότητας μεταξύ του ερωτήματος και των αποθηκευμένων δεδομένων.

3. **Language Model:**

- Ένα μεγάλο γλωσσικό μοντέλο (π.χ., GPT-4) χρησιμοποιείται για να επεξεργαστεί τα αποτελέσματα που επέστρεψε ο retriever.
- Το μοντέλο παράγει μια περιεκτική και κατανοητή απάντηση, συνδυάζοντας τα σχετικά δεδομένα.

4. **Παραγωγή Απάντησης:**

- Το τελικό αποτέλεσμα είναι μια πλήρης και ακριβής απάντηση που εμφανίζεται στον χρήστη.