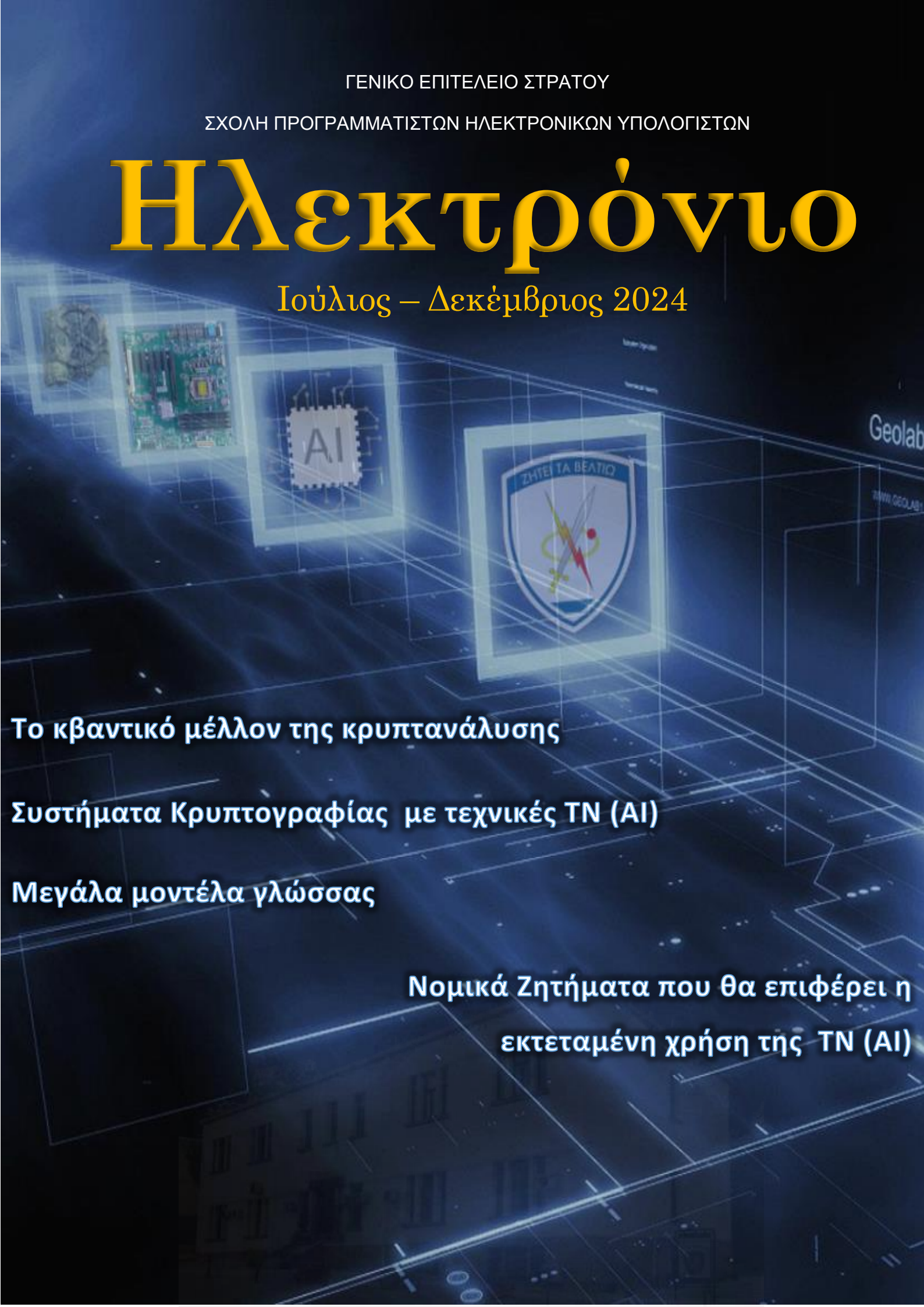
ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΣΤΡΑΤΟΥ

ΣΧΟΛΗ ΠΡΟΓΡΑΜΜΑΤΙΣΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Ηλεκτρόνιο

Ιούλιος – Δεκέμβριος 2024



Το κβαντικό μέλλον της κρυπτανάλυσης

Συστήματα Κρυπτογραφίας με τεχνικές ΤΝ (AI)

Μεγάλα μοντέλα γλώσσας

Νομικά Ζητήματα που θα επιφέρει η εκτεταμένη χρήση της ΤΝ (AI)

Σ.Π.Η.Υ
Σχολή Προγραμματιστών Ηλεκτρονικών Υπολογιστών

ΙΟΥΛΙΟΣ-ΔΕΚΕΜΒΡΙΟΣ 2024

ΓΕΣ/ΔΔΒ-ΕΠ

ΣΧΟΛΗ ΠΡΟΓΡΑΜΜΑΤΙΣΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΣΤΡΑΤΟΠΕΔΟ ΖΟΡΜΠΑ

Μεγάλου Αλεξάνδρου 2-4, Ζωγράφου

ΕΚΔΟΤΗΣ

ΤΜΗΜΑ ΜΕΛΕΤΩΝ ΣΠΗΥ

ΕΠΙΜΕΛΕΙΑ ΣΥΝΤΑΞΗΣ

Ανθστης (ΕΠ) Αναστάσιος Σιούτης

ΠΕΡΙΕΧΟΜΕΝΑ

ΧΑΙΡΕΤΙΣΜΟΣ ΔΙΟΙΚΗΤΟΥ ΣΠΗΥ

Αγαπητοί Αναγνώστες

Στη σύγχρονη εποχή η επιστήμη της πληροφορικής είναι βασικός πυλώνας για την υποστήριξη της ανάπτυξης των κοινωνιών. Οι εφαρμογές της αγγίζουν κάθε πτυχή της ανθρώπινης δραστηριότητας, από την επικοινωνία και την εργασία έως την ψυχαγωγία και την υγεία. Σε μεγάλο βαθμό διαμορφώνει τη συμπεριφορά του ανθρώπου και την αλληλεπίδραση του με το περιβάλλον του. Η εξειδικευμένη γνώση πλέον είναι βασικό ζητούμενο για την ανάπτυξη και διαχείριση σύνθετων συστημάτων, ανάλυση δεδομένων και αξιοποίηση των δυνατοτήτων της τεχνητής νοημοσύνης. Ο ρυθμός της τεχνολογικής προόδου, θέτει σε υψηλή προτεραιότητα την διατήρηση της επαφής με τις εξελίξεις. Προϋπόθεση για αυτό είναι η ουσιαστική επένδυση στην έρευνα και την καινοτομία, καθώς έτσι διασφαλίζεται η συμμετοχή στη διαμόρφωση του μέλλοντος. Είναι ο μόνος δρόμος για την ανάπτυξη αποκλειστικών προτύπων που προσφέρουν συγκριτικό πλεονέκτημα.

Η τεχνητή νοημοσύνη και η κβαντική τεχνολογία αναδεικνύουν νέες δυνατότητες που μεταβάλλουν τον τρόπο αλληλεπίδρασης με τα δεδομένα. Οι εφαρμογές της πρώτης συμβάλλουν στην ανάπτυξη ικανοτήτων για προσαρμογή σε μεταβαλλόμενες συνθήκες, αυτοματοποίηση διαδικασιών και υποστήριξη λήψης αποφάσεων. Η κβαντική τεχνολογία επιταχύνει ακόμα και τις πιο πολύπλοκες διαδικασίες. Η αξιοποίηση τους και η ταυτόχρονη αποτελεσματική αντιμετώπιση των αντίστοιχων προκλήσεων, δίνει σημαντική ώθηση στην πρόοδο.

Η Σχολή προσανατολίζεται στην υποστήριξη της έρευνας, την κατάρτιση του εξειδικευμένου προσωπικού ώστε να καταστεί ικανό να διαμορφώνει τις τεχνολογικές εξελίξεις και την εκπαίδευση του συνόλου των στελεχών ώστε να μπορούν να παρακολουθούν με άνεση τις τεχνολογικές εξελίξεις.

Καλή ανάγνωση.

Με εκτίμηση

Δημήτριος Ντόντος
Συνταγματάρχης (ΕΠ)

ΣΗΜΕΙΩΜΑ ΕΚΔΟΣΗΣ

Αγαπητοί Αναγνώστες,

Το δεύτερο τεύχος του περιοδικού είναι αφιερωμένο στην τεχνητή νοημοσύνη και την κβαντική τεχνολογία. Ο Ευάγγελος Γκούμας αναλύει το τρόπο με τον οποίο η κβαντική τεχνολογία μπορεί να ευεργετήσει τις διαδικασίες κρυπτανάλυσης. Οι Σπυρίδων Σταυρόπουλος και Παναγιώτης Μαυρομάτης παρουσιάζουν την εφαρμογή της τεχνητής νοημοσύνης στην ανάπτυξη γλωσσικών μοντέλων. Ο Θεόδωρος Πασχάλης αναλύει εφαρμογές της τεχνητής νοημοσύνης στην κρυπτογραφία. Η Άννα Παπαγγέλου καταγράφει τις νομικές προκλήσεις της εκμετάλλευσης της τεχνητής νοημοσύνης . Τέλος ο Γεώργιος Σπύρου καταγράφει εφαρμογές της επαυξημένης πραγματικότητας στον τομέα της άμυνας. Στο περιεχόμενο του τεύχους περιλαμβάνονται αναφορές στις δραστηριότητες της Σχολής για το πρώτο εξάμηνο του 2024.

Ξεκλειδώνοντας το κβαντικό μέλλον της κρυπτανάλυσης

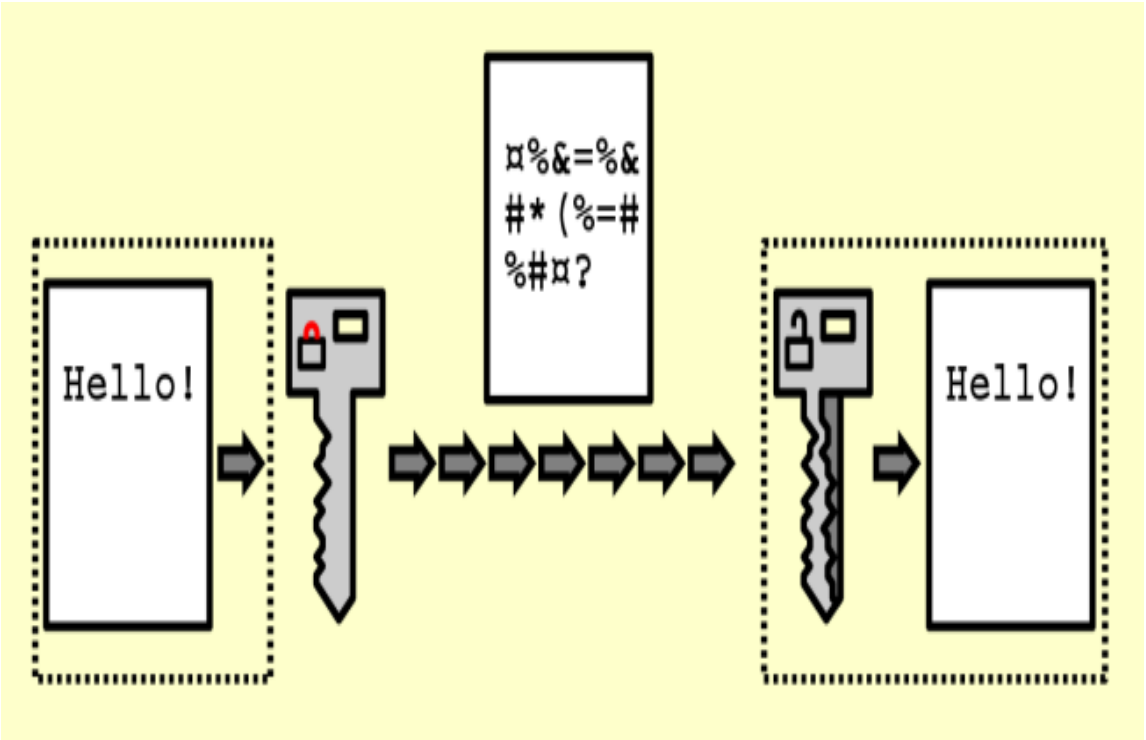
Ευάγγελος Γκούμας

Technische Universität Darmstadt

evangelos.gkoumas@tu-darmstadt.de

Εισαγωγή

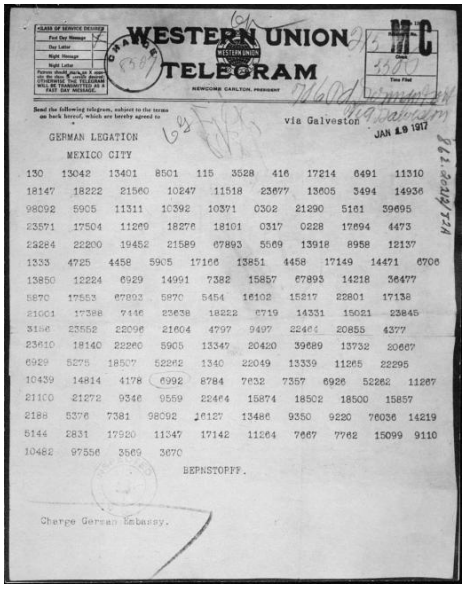
Η κρυπτολογία περιλαμβάνει δύο κύριους κλάδους: την Κρυπτογραφία και την Κρυπτανάλυση.



Η Κρυπτογραφία επικεντρώνεται στη κατασκευή και τη χρήση κωδίκων με στόχο να διασφαλίσει ότι δύο μέρη μπορούν να στείλουν μηνύματα διατηρώντας τα, κρυφά από ένα υποκλοπέα, ο οποίος μπορεί να παρακολουθεί όλη την επικοινωνία μεταξύ τους. Με αυτό τον τρόπο εξασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών.

Αντιθέτως, η κρυπτανάλυση πρόκειται για μια διαδικασία εύρεσης αδυναμιών σε κρυπτογραφικούς αλγορίθμους και χρήσης αυτών των αδυναμιών για την αποκρυπτογράφηση του κρυπτοκειμένου(cipher text) χωρίς τη χρήση του μυστικού

κλειδιού Οι επαγγελματίες της κρυπτανάλυσης, γνωστοί ως κρυπταναλυτές, διαδραματίζουν κρίσιμο ρόλο σε αυτόν τον τομέα.


WESTERN UNION
TELEGRAM
via Galveston
JAN 19 1917
GERMAN LEGATION
MEXICO CITY
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6928 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670
BERNSTORFF.
Charge German Embassy.

Εικόνα 1:Τηλεγράφημμα του Zimmermann

Στη συνέχεια του άρθρου θα παρουσιάσουμε κάποιες πιο αναλυτικές πληροφορίες σχετικά με τη κρυπτανάλυση. Θα ξεκινήσουμε με κάποιες ιστορικές πληροφορίες που θα μας εισάγουν στην σημαντικότητα της κρυπτανάλυσης. Εν συνεχεία, θα παρουσιάσουμε με όσο πιο απλό τρόπο μια κρυπταναλυτική τεχνική. Τέλος, θα μεταβούμε στην κβαντική κρυπτανάλυση αφού πρώτα δούμε κάποιους βασικούς αλγορίθμους.

Ιστορική εξέλιξη της κρυπτανάλυσης

Η κρυπτανάλυση, η επιστήμη της αποκρυπτογράφησης κωδικοποιημένων μηνυμάτων χωρίς προηγούμενη γνώση του κλειδιού, έχει εξελιχθεί σημαντικά με την πάροδο των αιώνων. Οι πρώιμες τεχνικές κρυπτογράφησης χρονολογούνται από τους αρχαίους πολιτισμούς[1], με απλές κρυπτογραφήσεις αντικατάστασης που χρησιμοποιήθηκαν από τον Ιούλιο Καίσαρα [2].

Κατά τη διάρκεια της Αναγέννησης αναπτύχθηκαν πιο σύνθετες μέθοδοι, όπως η κρυπτογράφηση Vigenère, η οποία παρέμεινε αδιάσπαστη για αιώνες . Τον 19ο αιώνα πρωτοπόροι όπως ο Charles Babbage και ο Friedrich Kasiski έσπασαν την κρυπτογράφηση Vigenère, σηματοδοτώντας σημαντικές εξελίξεις στην κρυπτανάλυση .

Τον 20ό αιώνα, η κρυπτανάλυση αποτέλεσε ένα κρίσιμο σταρτιωτικό εργαλείο. Ο Πρώτος Παγκόσμιος Πόλεμος ανέδειξε τη σημασία της με την υποκλοπή και αποκρυπτογράφηση του τηλεγραφήματος Zimmermann από τις βρετανικές μυστικές υπηρεσίες, η οποία επηρέασε την απόφαση των Ηνωμένων Πολιτειών να εισέλθουν στον πόλεμο [3]. Ωστόσο, ήταν κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου που η

κρυπτανάλυση έφτασε στο ζενίθ της με τις προσπάθειες να αποκρυπτογραφηθούν τα μηνύματα από τη γερμανική μηχανή Enigma .

Η μηχανή Enigma και ο Δεύτερος Παγκόσμιος Πόλεμος

Εικόνα 2: Γερμανική μηχανή Enigma , Μουσείο υπολογιστών Paderborn

Η μηχανή Enigma ήταν μια προηγμένη συσκευή κρυπτογράφησης που χρησιμοποιήθηκε από τη Γερμανία για τη διασφάλιση των στρατιωτικών επικοινωνιών [4]. Χρησιμοποιούσε ένα πολύπλοκο σύστημα περιστρεφόμενων ρότορων και ρυθμίσεων της πλακέτας, δημιουργώντας δισεκατομμύρια πιθανά κλειδιά κρυπτογράφησης . Αρχικά, το Πολωνικό Γραφείο Κρυπτογράφησης έκανε σημαντικές ανακαλύψεις στην κατανόηση της Enigma, αλλά ήταν οι Βρετανοί κωδικογράφοι, με επικεφαλής τον Alan Turing, που αποκρυπτογράφησαν πλήρως τα μηνύματα της Enigma [5].

Ο Turing και η ομάδα του ανέπτυξαν τη μηχανή Bombe, η οποία αυτοματοποίησε τη διαδικασία δοκιμής των ρυθμίσεων Enigma, μειώνοντας δραστικά το χρόνο που απαιτείται για την αποκωδικοποίηση των μηνυμάτων. Αυτή η ανακάλυψη επέτρεψε στους Συμμάχους να υποκλέψουν και να κατανοήσουν τα γερμανικά στρατιωτικά σχέδια, συμπεριλαμβανομένων των θέσεων των υποβρυχίων στον Ατλαντικό, οι οποίες ήταν ζωτικής σημασίας για τη διασφάλιση των νηοπομπών.

Κύριες κρυπταναλυτικές επιθέσεις

Στην κρυπτογραφία, η κατανόηση του μοντέλου απειλής είναι ζωτικής σημασίας για την αξιολόγηση της ασφάλειας των συστημάτων κρυπτογράφησης. Το μοντέλο απειλής ορίζει τις δυνατότητες ενός επιτιθέμενου χωρίς να περιορίζει τις στρατηγικές του, αναγνωρίζοντας ότι η πρόβλεψη συγκεκριμένων μεθόδων επίθεσης είναι εγγενώς αβέβαιη. Τα μοντέλα των απειλών παρουσιάζονται παρακάτω [6]:

Known-plaintext attack: Εδώ, ο αντίπαλος είναι σε θέση να μάθει ένα ή περισσότερα ζεύγη απλού κειμένου/κρυπτογραφημένου κειμένου που δημιουργούνται με τη χρήση κάποιου κλειδιού. Ο στόχος του αντιπάλου είναι στη συνέχεια να αντλήσει πληροφορίες

σχετικά με το υποκείμενο απλό κείμενο κάποιου άλλου κρυπτοκειμένου που παράγεται με το ίδιο κλειδί.

Chosen-plaintext attack: Σε αυτή την επίθεση, ο αντίπαλος μπορεί να αποκτήσει ζεύγη απλού κειμένου/κρυπτογραφημένου κειμένου, όπως παραπάνω, για κρυπτογραφημένα κείμενα της επιλογής του.

Ciphertext-only attack: Αυτή είναι η πιο βασική επίθεση, όπου ο αντίπαλος απλώς παρατηρεί ένα κρυπτογραφημένο κείμενο (ή πολλαπλά κρυπτογραφημένα κείμενα) και προσπαθεί να προσδιορίσει πληροφορίες σχετικά με το υποκείμενο απλό κείμενο (ή τα απλά κείμενα).

Man-In-The-Middle: Στην επίθεση Man-In-The-Middle Attack, ο επιτιθέμενος υποκλέπτει και ενδεχομένως τροποποιεί την επικοινωνία μεταξύ δύο μερών που πιστεύουν ότι επικοινωνούν απευθείας μεταξύ τους. Αυτό μπορεί να θέσει σε κίνδυνο την ασφάλεια του μηνύματος και τη διαδικασία ανταλλαγής κλειδιών [7].

Adaptive chosen-plaintext attack: Παρόμοια με την CPA, η παρούσα επιτρέπει στον επιτιθέμενο να ζητήσει κρυπτογραφήματα για πρόσθετα κρυπτογραφήματα αφού παρατηρήσει κάποια αρχικά κρυπτογραφήματα. Αυτή η επαναληπτική προσέγγιση μπορεί να αυξήσει τις πιθανότητες ανακάλυψης του κλειδιού κρυπτογράφησης.

Birthday attack: Αυτή η επίθεση αξιοποιεί το παράδοξο των γενεθλίων, το οποίο προβλέπει υψηλή πιθανότητα συγκρούσεων (δηλαδή δύο διαφορετικές είσοδοι να παράγουν την ίδια έξοδο) στις συναρτήσεις κατακερισμού(hash functions)*. Πρακτικά, είναι συναρτήσεις που λαμβάνουν εισόδους κάποιου μήκους και τις συμπιέζουν σε σύντομες εξόδους σταθερού μήκους. Στην κρυπτογραφία, χρησιμοποιείται για την εύρεση τέτοιων συγκρούσεων, υπονομεύοντας την ακεραιότητα της συνάρτησης κατακερματισμού.

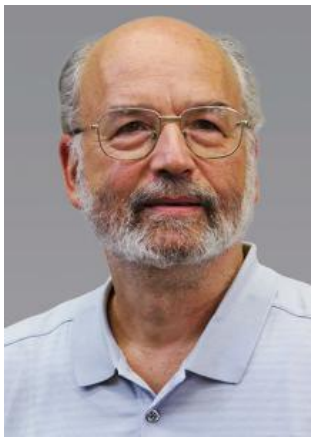
Side channel attack: Η επίθεση πλευρικού καναλιού εκμεταλλεύεται πληροφορίες που λαμβάνονται από τη φυσική υλοποίηση ενός κρυπτογραφικού συστήματος και όχι από αδυναμίες του ίδιου του αλγορίθμου. Παραδείγματα περιλαμβάνουν επιθέσεις χρονισμού, στατιστική ανάλυση ισχύος και ηλεκτρομαγνητική ανάλυση. Αυτές οι επιθέσεις μπορούν να αποκαλύψουν κρίσιμα δεδομένα, όπως τα κλειδιά κρυπτογράφησης.

Brute force attack: Μια επίθεση brute force attack περιλαμβάνει τη συστηματική δοκιμή κάθε δυνατού κλειδιού μέχρι να βρεθεί το σωστό. Αν και απλή στην εκτέλεση, αυτή η μέθοδος είναι χρονοβόρα και υπολογιστικά δαπανηρή, ειδικά με μεγαλύτερα κλειδιά.

Διαφορική κρυπτανάλυση: Αυτή η μέθοδος επίθεσης συγκρίνει ζεύγη απλών κειμένων και των αντίστοιχων κρυπτογραφημένων κειμένων για να εντοπίσει μοτίβα στον αλγόριθμο κρυπτογράφησης. Η διαφορική κρυπτανάλυση είναι ιδιαίτερα αποτελεσματική κατά ορισμένων κρυπτογραφήσεων μπλοκ, αποκαλύπτοντας τρωτά σημεία με βάση τις διαφορές μεταξύ ζευγών απλών κειμένων[8].

Στις επόμενες ενότητες του άρθρου, θα παρουσιάσουμε αναλυτικά την έννοια της κβαντικής διαφορικής κρυπτανάλυσης. Ωστόσο, πριν προχωρήσουμε σε λεπτομέρειες, θα ήταν χρήσιμο να εξετάσουμε συνοπτικά τη βασική ιδέα της διαφορικής κρυπτανάλυσης.

Διαφορική κρυπτανάλυση

Η διαφορική κρυπτανάλυση είναι μια επίθεση επιλεγμένου κειμένου, που σημαίνει ότι ο αντίπαλος είναι σε θέση να επιλέξει εισόδους και να εξετάσει τις εξόδους σε μια προσπάθεια εξαγωγής του κλειδιού. Πρόκειται για μια μορφή κρυπτανάλυσης που εφαρμόζεται σε αλγορίθμους συμμετρικού κλειδιού. Αναπτύχθηκε από τους Ισραηλινούς Eli Biham και Adi Shamir το 1991. Η συγκεκριμένη επίθεση εξετάζει τις διαφορές απλού κειμένου(plaintext) και τις διαφορές κρυπτοκειμένου(chipertext), αντί τα απλά κείμενα και κρυπτοκείμενα αυτά καθαυτά. Η διαφορά δυο απλών κειμένων ορίζεται από την αποκλειστική διάζευση (XOR) των κειμένων αυτών. Αντιστοίχως, η διαφορά δυο κρυπτοκειμένων ορίζεται από την αποκλειστική διάζευξη των κρυπτοκειμένων.

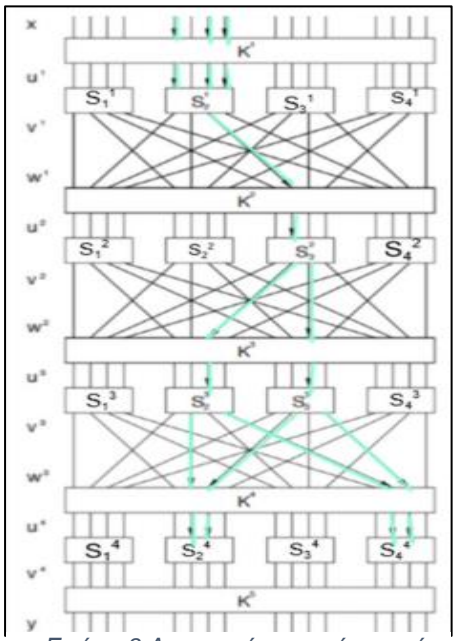
Το βασικό σχήμα της επίθεσης, εκμεταλλεύεται την υψηλή πιθανότητα ορισμένων εμφανίσεων διαφορών(εισόδων-εξόδων) και διαφορών απλού κειμένου στο τελευταίο γύρο της κρυπτογράφησης [9].

Παραλλαγές της διαφορικής Κρυπτανάλυσης

Η διαφορική κρυπτανάλυση θεωρείται η πιο αποτελεσματική κλασική μέθοδος κρυπτανάλυσης. Ανάλογα με το σημείο εστίασης της διαφορικής επίθεσης, υπάρχουν διάφορες παραλλαγές αυτής της μεθόδου. Οι κύριες παραλλαγές της διαφορικής κρυπτανάλυσης παρουσιάζονται συνοπτικά παρακάτω:

- Higher-Order Διαφορική Κρυπτανάλυση
- Truncated Διαφορική Κρυπτανάλυση
- Impossible Διαφορική Κρυπτανάλυση
- Multi-key Διαφορική Κρυπτανάλυση
- Επίθεση BOOMERANG

.Η διαφορική κρυπτανάλυση και η κρυπτογραφία SPN (Substitution-Permutation Network) συνδέονται μεταξύ τους μέσω της εστίασής τους στην ανάλυση και την ενίσχυση της ασφάλειας των κρυπτογραφήσεων μπλοκ.



Εικόνα 3:Διαφορικό μονοπάτι για ένα Δίκτυο Αντικατάστασης-Διάδοσης (SPN) 4 γύρων.

Το Δίκτυο αντικατάστασης-παρεμβολής (SPN)[6] είναι μια κρυπτογραφική δομή που χρησιμοποιείται σε αλγορίθμους κρυπτογράφησης μπλοκ για την εισαγωγή της μη γραμμικότητας και την εξασφάλιση της ασφάλειας των δεδομένων. Υλοποιεί το παράδειγμα της σύγχυσης-διάχυσης μέσω μιας σειράς συνδεδεμένων μαθηματικών πράξεων, που περιλαμβάνουν κυρίως αντικατάσταση και μετάθεση.

Σε ένα SPN, κάθε γύρος αποτελείται από τρία κύρια βήματα:

- Ανάμειξη κλειδιών: Το μπλοκ εισόδου γίνεται XOR με ένα υποκλειδί.

- Αντικατάσταση: Το μπλοκ διαιρείται σε μικρότερα τμήματα, καθένα από τα οποία μετασχηματίζεται χρησιμοποιώντας μια σταθερή συνάρτηση υποκατάστασης γνωστή ως S-box.
- Μετατροπή: Τα bits του μετασχηματισμένου μπλοκ ανακατεύονται στη συνέχεια σύμφωνα με ένα προκαθορισμένο μοτίβο μετατροπής.

Αυτός ο συνδυασμός λειτουργιών σε πολλαπλούς γύρους ενισχύει την αντίσταση της κρυπτογράφησης σε κρυπταναλυτικές επιθέσεις, καθώς αποκρύπτει τη σχέση μεταξύ του απλού κειμένου, του κρυπτοκειμένου και του κλειδιού. Τα δίκτυα SP αποτελούν τη ραχοκοκαλιά αρκετών γνωστών κρυπτογραφήσεων μπλοκ, όπως ο AES, ο PRESENT και ο SAFER.

Impossible διαφορική κρυπτανάλυση

Η impossible διαφορική κρυπτανάλυση είναι ένας τύπος επίθεσης επιλεγμένου απλού κειμένου που χρησιμοποιείται για την παραβίαση κρυπτογραφήσεων μπλοκ. Αποτελεί επέκταση της διαφορικής κρυπτανάλυσης, η οποία είναι μια γνωστή τεχνική κρυπτανάλυσης. Η Impossible διαφορική επίθεση προτάθηκε ταυτόχρονα από τους Biham, Shamir και Biryukov για πρώτη φορά το 1998 και έκτοτε έχει αποδειχθεί ότι είναι ένα ισχυρό εργαλείο για την κρυπτανάλυση. Στην πραγματικότητα, χρησιμοποιήθηκε για να σπάσει 31 από τους 32 γύρους του κρυπτογραφήματος Skipjack, το οποίο σχεδιάστηκε από την NSA και αποχαρακτηρίστηκε το 1998. Μια παρόμοια επίθεση χρησιμοποιήθηκε από τον Knudsen το 1998 για την κρυπτανάλυση 6 γύρων του κρυπτογραφήματος DEAL, το οποίο ήταν μια από τις προτάσεις του για το Advanced Encryption Standard (AES).

Η Impossible διαφορική επίθεση έχει επίσης εφαρμοστεί για να βελτιώσει τις πιο γνωστές επιθέσεις για άλλους ισχυρούς και μακροχρόνιους κρυπτογράφους μπλοκ, όπως ο IDEA και ο Khufu, σπάζοντας τις μειωμένες σε γύρους εκδόσεις αυτών των κρυπτογράφων[10].

Ο στόχος αυτής της τεχνικής κρυπτανάλυσης είναι να ανακτήσει ορισμένα bits του μυστικού κλειδιού ενός μαντείου κρυπτογράφησης black-box. Αυτό γίνεται απορρίπτοντας όλες τις λανθασμένες εικασίες για το κλειδί, με τη βοήθεια ενός ζεύγους απλών κειμένων που οδηγεί σε ένα impossible μοτίβο κάτω από τη μερική κρυπτογράφησή του με τις λανθασμένες εικασίες για το κλειδί. Η διαδικασία μιας impossible διαφορικής επίθεσης μπορεί να αναλυθεί σε δύο βασικά βήματα. Το πρώτο βήμα, επικεντρώνεται στην εύρεση ενός impossible διαφορικού με το μέγιστο δυνατό μήκος. Στο δεύτερο βήμα, που ονομάζεται φάση διαλογής κλειδιών, προστίθενται πρόσθετοι γύροι και στις δύο κατευθύνσεις για να εξακριβωθούν ποια πιθανά κλειδιά θα κρυπτογραφούν ή αποκρυπτογραφούν [11].

Έστω E ένας μπλοκ κρυπτογράφος n-bit με r γύρους. Γράφουμε:

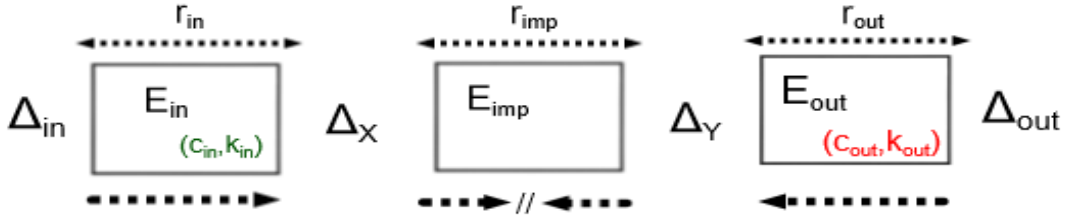
$$E = E_{out} \circ E_{imp} \circ E_{in},$$

όπου τα E_{out}, E_{imp} και E_{in} έχουν γύρους r_{out}, r_{imp} και r_{in} αντίστοιχα ($r = r_{in} + r_{imp} + r_{out}$).

Τα δύο βασικά βήματα της επίθεσης περιληπτικά είναι τα ακόλουθα:

Pair Generation

Πρέπει να δημιουργηθούν ζεύγη αριθμών που πληρούν συγκεκριμένες προϋποθέσεις χρησιμοποιώντας ένα ειδικό εργαλείο κρυπτογράφησης. Ο στόχος είναι να βρούμε πολλά ζεύγη όπου ο συνδυασμός των αριθμών με έναν συγκεκριμένο τρόπο ταιριάζει σε μια ομάδα που ονομάζεται Δ_{in}, και όταν αυτοί οι αριθμοί κρυπτογραφηθούν και στη συνέχεια συνδυαστούν, ταιριάζουν σε μια άλλη ομάδα που ονομάζεται Δ_{out}. Αυτό είναι σαν να λύνουμε ένα δύσκολο puzzle, και χρησιμοποιούμε μια μέθοδο από μια συγκεκριμένη εργασία για να το πετύχουμε αυτό. Το αποτέλεσμα είναι μια λίστα από ζεύγη, που ονομάζεται T_0, με κάθε ζεύγος να αποτελείται από δύο αριθμούς.



Εικόνα 4: Η Impossible διαφορική επίθεση. Η διαφορική ΔX ↔ ΔY μέσω των ενδιάμεσων γύρων Eimp είναι impossible

Pair Filtering

Ξεκινώντας με τη λίστα T_0 με πολλά ζεύγη, τα ελέγχουμε με μέρη του κλειδιού κρυπτογράφησης για να εντοπίσουμε ποια μέρη δεν λειτουργούν με αυτά τα ζεύγη. Για να κάνουμε αυτή τη διαδικασία ταχύτερη, χρησιμοποιούμε μια μέθοδο για να απορρίπτουμε γρήγορα τα μέρη του κλειδιού που δεν ταιριάζουν, αποφεύγοντας την ανάγκη να ελέγξουμε όλα τα ζεύγη έναντι όλων των μερών του κλειδιού. Αυτή η αποτελεσματική τεχνική περιγράφεται λεπτομερώς [12] και μας βοηθά να περιορίσουμε τα πιθανά σωστά μέρη του κλειδιού.

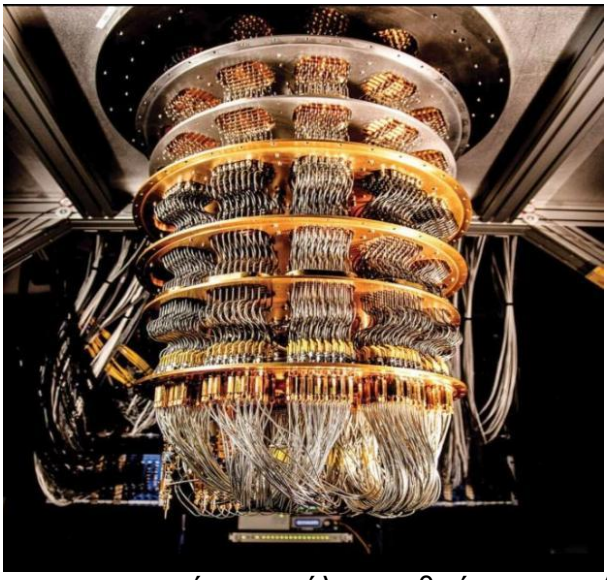
Όπως αναφέρθηκε παραπάνω η impossible διαφορική επίθεση βασίζεται σε ένα impossible διαφορικό μέγιστου μήκους, δηλαδή σε ένα ζεύγος διαφορικών Δ_X (Διαφορά εισόδου), Δ_Y (Διαφορά εξόδου), έτσι ώστε η πιθανότητα να διαδοθεί το Δ_X στο Δ_Y μετά από r_{imp} γύρους να είναι 0. Στη συνέχεια θα προσθέσουμε r_{in} και r_{out} γύρους του κρυπτογραφήματος αντίστοιχα πριν και μετά το impossible διαφορικό.

- Δ_x, Δ_y: Διαφορές εισόδου-εξόδου του impossible διαφορικού
- Δ_{in}, Δ_{out}:Σύνολο όλων των πιθανών εισόδων-εξόδων διαφορών του κρυπτρογραφήματος
- r_{in}: Αριθμός γύρων του διαφορικού διαδρομής (Δ_{in}, Δ_x)
- r_{out}: Αριθμός γύρων του διαφορικού διαδρομής (Δ_{in}, Δ_{out})
- r_{imp}: Αριθμός γύρων της impossible διαφοράς

Impossible μοτίβο ονομάζεται η πεντάδα των ποσοτήτων (Δ_X, Δ_Y, r_{imp}, r_{in}, r_{out}).

Θα ήταν αρκετά χρήσιμο για τον αναγνώστη που δεν είναι εξοικειωμένος με τον τομέα της κβαντικής πληροφορικής να κατανοήσει τους βασικούς αλγορίθμους που αποτελούν τη βάση αυτού του θέματος, δεδομένου ότι θα εξετάσουμε την κβαντική εκδοχή της κρυπτανάλυσης. Το σύμβολο “| ⟩” που εμφανίζεται στις επόμενες παραγράφους είναι το ket, το οποίο είναι το σύμβολο του Dirac.

Κβαντικοί Αλγόριθμοι



Η κβαντική πληροφορική έχει αποτελέσει θέμα μεγάλου ενδιαφέροντος και έρευνας τις τελευταίες δεκαετίες, υποσχόμενη να φέρει επανάσταση στον τομέα της πληροφορικής με την ικανότητά της να επιλύει προβλήματα εκθετικά ταχύτερα από τους κλασικούς υπολογιστές. Μια από τις σημαντικότερες ανακαλύψεις στον τομέα αυτό ήταν η ανακάλυψη του αλγορίθμου του Shor, ο οποίος κατέδειξε την αποτελεσματική παραγοντοποίηση μεγάλων αριθμών με τη χρήση κβαντικών κυκλωμάτων. Η ανακάλυψη αυτή είχε βαθύ αντίκτυπο στην κρυπτογραφία και προσέλκυσε την παγκόσμια προσοχή στις δυνατότητες των κβαντικών υπολογιστών.

Αλγόριθμος Deutsch-Jozsa

Ο αλγόριθμος Deutsch-Jozsa προτάθηκε από τους David Deutsch και Richard Jozsa το 1992 στην εργασία με τίτλο “Rapid solution of problems by quantum computation”[13]. Εκείνη την εποχή, ήταν ένας από τους πρώτους κβαντικούς αλγορίθμους που επέδειξε εκθετική επιτάχυνση σε σχέση με τους κλασικούς αλγορίθμους για ένα πρόβλημα που δεν είχε κατασκευαστεί τεχνητά για να επιλυθεί από έναν κβαντικό υπολογιστή. Ο αλγόριθμος έπαιξε σημαντικό ρόλο στην ανάπτυξη της κβαντικής πληροφορικής ως τομέα και συνέβαλε στην εδραίωση της δυνατότητας των κβαντικών υπολογιστών να επιλύουν προβλήματα που είναι δυσεπίλυτα για τους κλασικούς υπολογιστές.

Ο αλγόριθμος αντιμετωπίζει ένα πρόβλημα που αποτελεί ουσιαστικά επέκταση του προβλήματος που αντιμετωπίζει ο αλγόριθμος Deutsch. Στην πραγματικότητα, οι δύο αλγόριθμοι μοιράζονται την ίδια δομή. Στην περίπτωση του αλγορίθμου Deutsch-Jozsa, παρουσιάζεται ένα αντιστρέψιμο κύκλωμα που ενσωματώνει μια άγνωστη συνάρτηση f. Ωστόσο, σε αντίθεση με τον αλγόριθμο Deutsch, η f απεικονίζει n-bit συμβολοσειρές σε ένα μόνο bit [14].

Πρόβλημα του Αλγορίθμου Deutsch–Jozsa

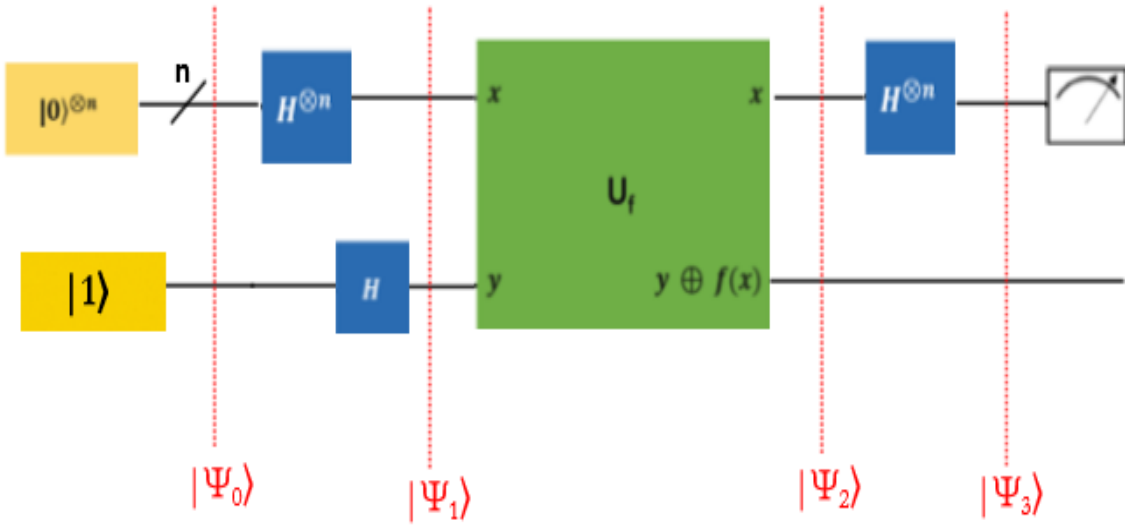
Input: Δεδομένου ενός black-box που υπολογίζει μια άγνωστη συνάρτηση $f:\{0,1\}^n \rightarrow \{0,1\}$

Promise: Αν η f είναι μια ισορροπημένη συνάρτηση ή μια σταθερή συνάρτηση

Problem: Προσδιορίστε αν η f είναι σταθερή ή ισορροπημένη κάνοντας ερωτήματα στο f.

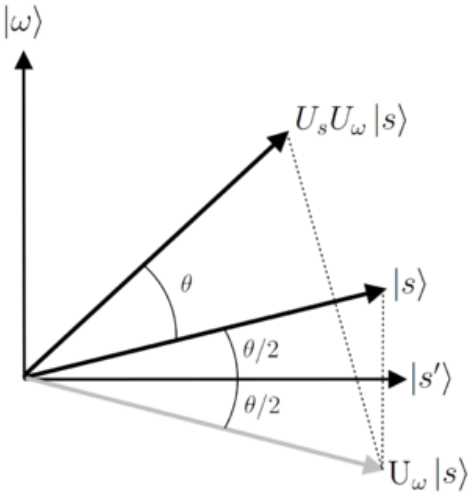
Αν έχουμε τη συνάρτηση f υλοποιημένη ως κβαντικό μαντείο, το οποίο αντιστοιχίζει την κατάσταση $|x\rangle|y\rangle$ σε $|x\rangle|y \oplus f(x)\rangle$ όπου $\oplus$ αντιπροσωπεύει την πρόσθεση modulo 2, τότε χρησιμοποιώντας έναν κβαντικό υπολογιστή, μπορούμε να λύσουμε αυτό το πρόβλημα με 100% εμπιστοσύνη αφού κάνουμε μόνο μία κλήση στη συνάρτηση $f(x)$[15].

Ακολουθεί το τυπικό κύκλωμα για τον αλγόριθμο Deutsch-Jozsa.



Εικόνα 5: Ο αλγόριθμος Deutsch-Jozsa

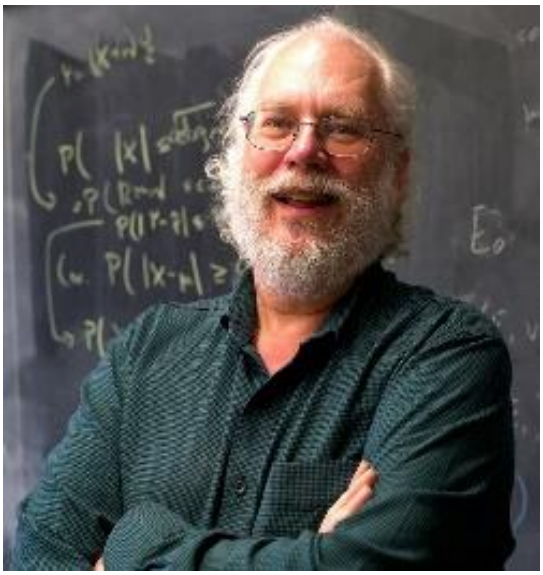
Αλγόριθμος Grover



Εικόνα 6: Η γεωμετρική ερμηνεία της πρώτης επανάληψης του αλγορίθμου του Grover.

Ο αλγόριθμος Grover χρησιμοποιείται για την αναζήτηση σε μια βάση δεδομένων. Ο συγκεκριμένος αλγόριθμος, αποτελεί το θεμέλιο λίθο σε κάθε κβαντική κρυπταναλυτική επίθεση. Ο αλγόριθμος αναζήτησης μπορεί να βρει μια καταχώρηση σε μια βάση δεδομένων με M καταχωρήσεις με O ($\sqrt{N}$) χρόνο και O(logN) χώρο[16]. Η μέθοδος αυτή ανακαλύφθηκε από τον Lov Grover το 1996. Διαπίστωσε ότι η μέθοδος του έδωσε τετραγωνική επιτάχυνση σε σύγκριση με άλλους κβαντικούς αλγορίθμους. Επιπλέον, η μέθοδος του Grover δίνει εκθετική ταχύτητα σε σχέση με τους αντίστοιχους κλασικούς.

Αλγόριθμος Shor



Ο αλγόριθμος του Shor είναι ένας κβαντικός αλγόριθμος που προτάθηκε από τον Αμερικανό μαθηματικό Peter Shor το 1994. Πρόκειται για έναν αλγόριθμο για την εύρεση των πρώτων παραγόντων ενός μεγάλου ακέραιου αριθμού, ένα πρόβλημα που είναι γνωστό ότι είναι δυσεπίλυτο για τους κλασικούς υπολογιστές. Ο αλγόριθμος του Shor έχει μεγάλη σημασία στον τομέα της κβαντικής πληροφορικής, καθώς αποτελεί ένα από τα πιο γνωστά παραδείγματα κβαντικού αλγορίθμου που μπορεί να λύσει ένα πρόβλημα ταχύτερα από οποιονδήποτε γνωστό κλασικό αλγόριθμο. Τέλος ο αλγόριθμος δεν είναι απλώς μια θεωρητική εργασία. Υπάρχει κάποια πειραματική απόδειξη ότι ο αλγόριθμος του Shor όντως λειτουργεί[17.

Πρόβλημα του Αλγορίθμου Shor

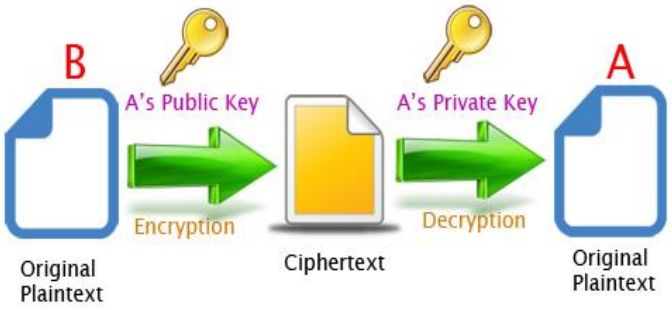
Input: Έστω ένας ακέραιος αριθμός N και δύο πρώτοι αριθμοί p και q, τέτοιο ώστε $N = p \cdot q$.

Promise: Έστω $\alpha \in \mathbb{Z}_N$ και μια συνάρτηση εκθετικοποίησης $f: \mathbb{Z}^+ \to \mathbb{Z}_N$ που ορίζεται ως $f(x) = \alpha^x \bmod N$ να ικανοποιεί τη συνθήκη, $f(x) = f(x_0) \iff x = x_0 + kr$, όπου r είναι η περίοδος της f, και k ένας ακέραιος αριθμός.

Problem: Προσδιορισμός της περιόδου r με την αναζήτηση της f.

Ο αλγόριθμος του Shor λειτουργεί με τη χρήση κβαντικού μετασχηματισμού Fourier για την εύρεση της περιόδου μιας συνάρτησης. Η συνάρτηση σε αυτή την περίπτωση είναι ο modular πολλαπλασιασμός ενός αριθμού. Η περίοδος χρησιμοποιείται στη συνέχεια για την εύρεση των παραγόντων του αριθμού. Η χρονική πολυπλοκότητα του αλγορίθμου του Shor είναι $O((\log N)^3)$ ενώ η χωρική πολυπλοκότητα $O(\log N)$, όπου N είναι ο ακέραιος αριθμός που θέλουμε να παραγοντοποιήσουμε, η οποία είναι σημαντικά ταχύτερη από τους καλύτερους γνωστούς κλασικούς αλγορίθμους για το ίδιο πρόβλημα.

Η χρήση του Shor αλγορίθμου έναντι του RSA

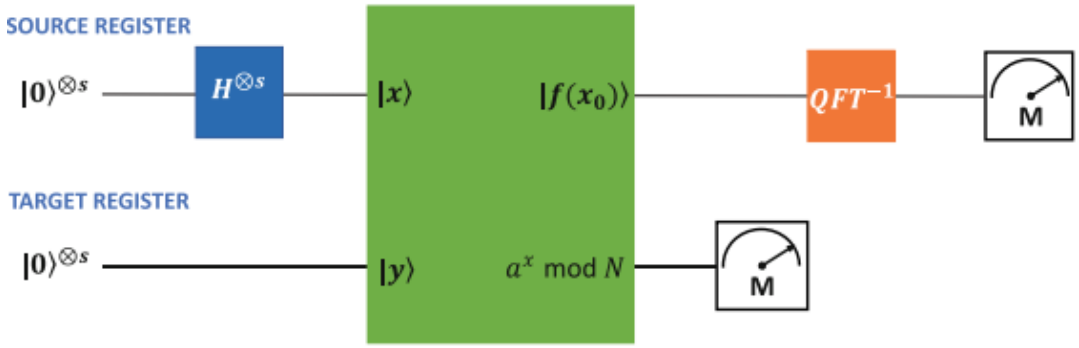


Εικόνα 7: Βασικό σχήμα του RSA

Το RSA (Rivest-Shamir-Adleman) [18] είναι ένα κρυπτοσύστημα δημόσιου κλειδιού, ένα από τα παλαιότερα που χρησιμοποιούνται ευρέως για την ασφαλή μετάδοση δεδομένων. Ένας χρήστης του RSA δημιουργεί και δημοσιεύει ένα δημόσιο κλειδί που βασίζεται σε δύο μεγάλους πρώτους αριθμούς, μαζί με μια βοηθητική τιμή. Τα μηνύματα μπορούν να κρυπτογραφηθούν από οποιονδήποτε, μέσω του δημόσιου κλειδιού, αλλά μπορούν να αποκρυπτογραφηθούν μόνο από κάποιον που γνωρίζει το ιδιωτικό κλειδί. Η ασφάλεια του RSA βασίζεται στην πρακτική δυσκολία της παραγοντοποίησης του γινομένου δύο μεγάλων πρώτων αριθμών, το “πρόβλημα της παραγοντοποίησης”. Το

RSA είναι ένας σχετικά αργός αλγόριθμος και δεν χρησιμοποιείται συνήθως για την άμεση κρυπτογράφηση δεδομένων χρηστών.

Ωστόσο, η έλευση των κβαντικών υπολογιστών και του αλγορίθμου του Shor επιτρέπει την παραγοντοποίηση σε πολυωνυμικό χρόνο, αποτελώντας δυνητική πρόκληση για τα παραδοσιακά κρυπτογραφικά συστήματα [19].

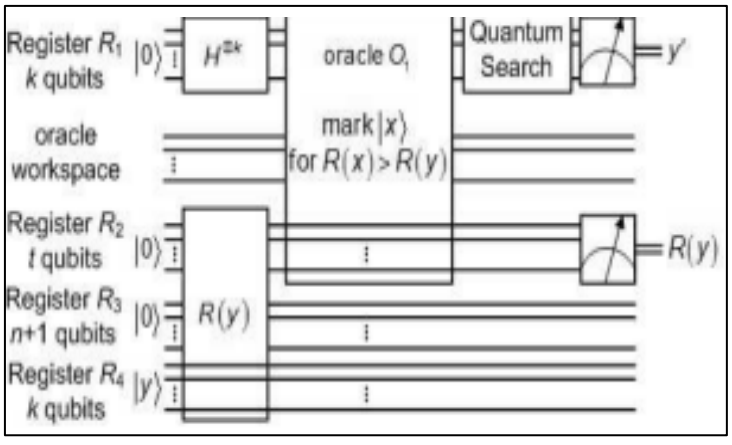


Εικόνα 8: Διάγραμμα που απεικονίζει τη διαδικασία του αλγορίθμου του Shor.

Με βάση τις προηγούμενες παραγράφους του άρθρου υπάρχουν ορισμένες βασικές γνώσεις στο πεδίο της κρυπτανάλυσης και των κβαντικών αλγορίθμων. Στις επόμενες παραγράφους, θα προσπαθήσουμε να περιγράψουμε συνοπτικά τα βασικό σχήμα της κβαντικής επίθεση .

Κβαντική προσέγγιση

Η κβαντική διαφορική κρυπτανάλυση είναι μια μέθοδος ανάλυσης και επίθεσης στην ασφάλεια κρυπτογραφικών συστημάτων με τη χρήση κβαντικών υπολογιστών. Πρόκειται για μια μορφή διαφορικής κρυπτανάλυσης, που



προτάθηκε στην εργασία[20] των Q. Zhou, S. Lu, Z. Zhang, J. Su του 2018 όπου δύο ελαφρώς διαφορετικές είσοδοι προετοιμάζονται ως κβαντικές καταστάσεις και επεξεργάζονται από έναν κβαντικό αλγόριθμο. Στη συνέχεια αναλύεται η διαφορά μεταξύ των εξόδων του κβαντικού αλγορίθμου για τις δύο εισόδους, αποκαλύπτοντας πληροφορίες σχετικά με το μυστικό κλειδί που χρησιμοποιείται από το κρυπτογραφικό σύστημα. Είναι εφικτή μόνο σε κβαντικούς υπολογιστές και πολλά κρυπτογραφικά συστήματα έχουν σχεδιαστεί για να αντιστέκονται σε κβαντικές επιθέσεις [19].

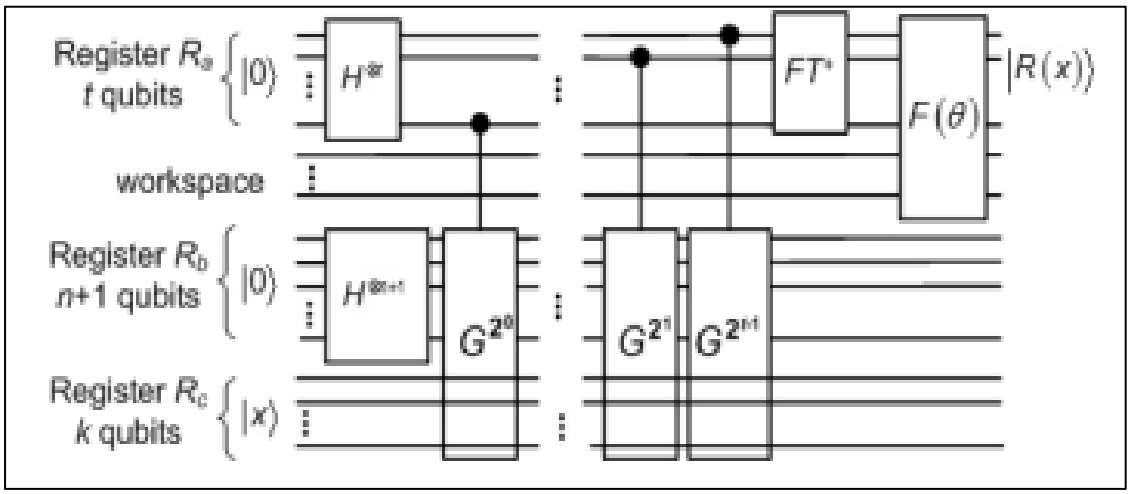
Η παρούσα διαδικασία επαναλαμβάνεται μέχρι η πιθανότητα του υποκλειδιού του κατωφλίου που έχει τα περισσότερα σωστά ζεύγη να είναι αρκετά μεγάλη.

Η κβαντική διαφορική κρυπτανάλυση περιλαμβάνει μια σειρά βημάτων για την αποκάλυψη του κλειδιού κρυπτογράφησης χρησιμοποιώντας τις δυνατότητες των κβαντικών υπολογισμών. Πρώτα, η μέθοδος υπολογίζει πώς οι διαφορές στις τιμές εισόδου επηρεάζουν την έξοδο στον τελικό γύρο της κρυπτογράφησης. Στη συνέχεια, συγκεντρώνει κρυπτογραφημένες εξόδους, ή κρυπτογραφήματα, για ζεύγη εισόδων (plaintexts) που έχουν γνωστές διαφορές. Επιλέγεται μια τυχαία τιμή κατωφλίου για να βοηθήσει στον εντοπισμό πιθανών υποψηφίων κλειδιών. Ο πυρήνας της διαδικασίας περιλαμβάνει την επανάληψη μέσω διαφόρων κβαντικών τεχνικών (Εικόνα 9): αρχικοποίηση κβαντικών καταχωρητών με πιθανές τιμές κλειδιών, χρήση κβαντικής καταμέτρησης για τον προσδιορισμό του αριθμού των σωστών ζευγών για κάθε υποψήφιο, εφαρμογή ενός κβαντικού μαντείου για την επισήμανση των πιο υποσχόμενων υποψηφίων και εκτέλεση κβαντικής αναζήτησης για την εύρεση του καλύτερου υποψήφιου κλειδιού. Καθ' όλη τη διάρκεια αυτής της διαδικασίας, το κατώφλι ενημερώνεται με βάση τον καλύτερο υποψήφιο που βρέθηκε. Τελικά, ο καλύτερος υποψήφιος επιστρέφεται ως το σωστό κλειδί κρυπτογράφησης, αξιοποιώντας την αποτελεσματικότητα και την ακρίβεια της κβαντικής υπολογιστικής.

Κύκλωμα για τον υπολογισμό του R(x)

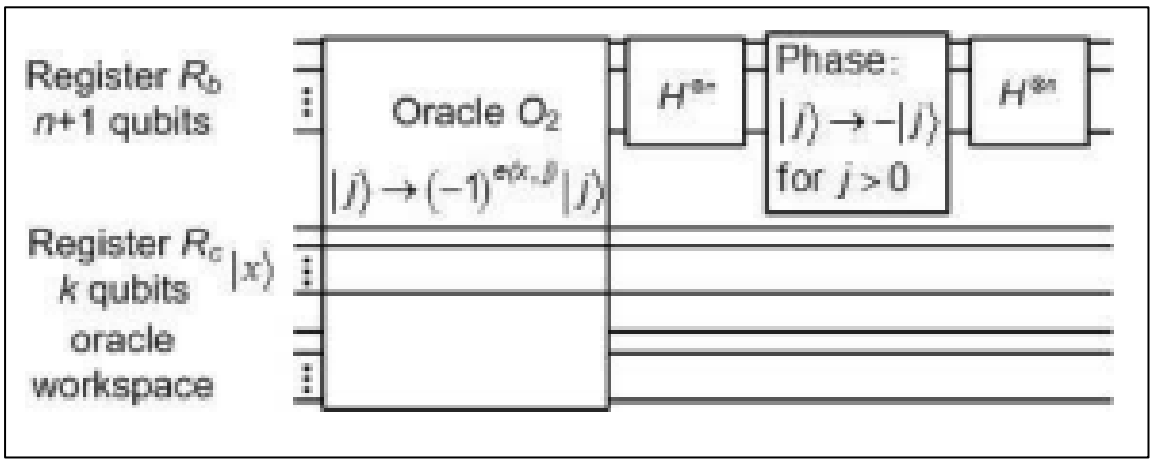
Το κύκλωμα που παρουσιάζεται στην Εικόνα 10 για την καταμέτρηση του αριθμού των σωστών ζευγών του υποκλειδιού x είναι γενικά το ίδιο με τα υπάρχοντα κυκλώματα κβαντικής καταμέτρησης, με τη διαφορά ότι περιλαμβάνεται ένας πρόσθετος καταχωρητής Rc που περιέχει το x και κάθε επανάληψη Grover G εμπλουτίζεται με ένα

μαντείο που λαμβάνει το x ως παράμετρο για να επισημάνει τις καταστάσεις που αντιστοιχούν στα σωστά ζεύγη του υποκλειδιού x.



Εικόνα 9: Κύκλωμα για τον υπολογισμό του R(x).

Ξεκινά με την κατανόηση του τρόπου με τον οποίο οι διαφορές στις τιμές εισόδου επηρεάζουν την έξοδο στον τελικό γύρο της κρυπτογράφησης. Οι κρυπτογραφημένες έξοδοι, ή κρυπτοκείμενα, συλλέγονται για ζεύγη εισόδων (plaintexts) με γνωστές διαφορές. Μια τυχαία τιμή κατωφλίου βοηθά στον εντοπισμό πιθανών υποψηφίων κλειδιών. Η διαδικασία χρησιμοποιεί κβαντικές τεχνικές, συμπεριλαμβανομένων κβαντικών καταχωρητών R και πυλών, για την επανάληψη των πιθανών κλειδιών.



Εικόνα 10: Κύκλωμα για την επανάληψη Grover G

Εφαρμόζοντας κβαντικές πύλες όπως ο αντίστροφος μετασχηματισμός Fourier και η επανάληψη Grover, το σύστημα βελτιώνει την αναζήτησή του για το σωστό κλειδί. Το κβαντικό κύκλωμα των επαναλήψεων Grover, όπως φαίνεται στην Εικόνα 11, απεικονίζει το G σε αυτή τη διαδικασία καταμέτρησης. Η συνάρτηση κβαντικού μαντείου βοηθά στον εντοπισμό υποσχόμενων υποψηφίων κλειδιών συγκρίνοντας τις αναμενόμενες και τις πραγματικές διαφορές εξόδου. Η διαδικασία κβαντικής καταμέτρησης ολοκληρώνεται όταν βρεθεί ο καλύτερος υποψήφιος, επιστρέφοντας αυτόν ως κλειδί κρυπτογράφησης, αξιοποιώντας έτσι τη δύναμη της κβαντικής πληροφορικής για αποτελεσματική και ακριβή κρυπτανάλυση.

Συμπεράσματα

Η κβαντική κρυπτανάλυση επηρεάζει σημαντικά τη σύγχρονη κυβερνοασφάλεια, καθώς απειλεί κλασικούς κρυπτογραφικούς αλγορίθμους όπως ο RSA και ο ECC, που είναι ζωτικής σημασίας για τις ψηφιακές επικοινωνίες και την προστασία των δεδομένων. Καθώς η κβαντική πληροφορική εξελίσσεται, η κρυπτανάλυση αυτών των αλγορίθμων καθίσταται εφικτή, γεγονός που καθιστά αναγκαία την ανάπτυξη κρυπτογραφικών τεχνικών ανθεκτικών στις κβαντικές επιθέσεις. Αυτό έχει ωθήσει μια παγκόσμια προσπάθεια έρευνας και επενδύσεων σε υποδομές για να εξασφαλιστεί η ασφαλής μετάβαση στη μετα-κβαντική κρυπτογραφία. Η συνεργασία μεταξύ ακαδημαϊκών, βιομηχανικών και ρυθμιστικών φορέων είναι ζωτικής σημασίας για την καθιέρωση ισχυρών προτύπων. Ενώ παρουσιάζει προκλήσεις, η κβαντική κρυπτανάλυση οδηγεί επίσης στην καινοτομία, οδηγώντας στη δημιουργία νέων, ανθεκτικών κρυπτογραφικών μεθόδων. Η προληπτική αντιμετώπιση αυτών των απειλών διασφαλίζει ένα ασφαλές ψηφιακό μέλλον μέσα στο εξελισσόμενο τοπίο της κυβερνοασφάλειας.

Βιογραφικό συντάκτη

Ο Ευάγγελος Γκούμας είναι απόφοιτος του τμήματος Μαθηματικών του Πανεπιστημίου Πατρών και είναι κάτοχος μεταπτυχιακού διπλώματος στην "Κρυπτογραφία, Ασφάλεια και Συστήματα Πληροφοριών" από τη Στρατιωτική Σχολή Ευελπίδων. Από το 2023, είναι διδακτορικός φοιτητής και μέλος της ομάδας Cryptography and Complexity Theory στο Τεχνολογικό Πανεπιστήμιο του Darmstadt στη Γερμανία, εστιάζοντας στην κβαντική κρυπτογραφία.

Αναφορές

[1] Singh, Simon. "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography." Anchor, 1999.
[2] Kahn, David. "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet." Scribner, 1996.
[3] Budiansky, Stephen. "Battle of Wits: The Complete Story of Codebreaking in World War II." Free Press, 2000.
[4] Welchman, Gordon. "The Hut Six Story: Breaking the Enigma Codes." McGraw-Hill, 1982.
[5] Hinsley, F. H., and Stripp, Alan. "Codebreakers: The Inside Story of Bletchley Park." Oxford University Press, 1993.
[6] Jonathan Katz and Yehuda Lindell. " Introduction to Modern Cryptography" Third Edition, CRC Press, 2021.
[7] https://en.wikipedia.org/wiki/Man-in-the-middle_attack.
[8] Douglas R. Stinson, Maura B. Paterson, "Cryptography Theory and Practice ",2019.
[9] Eli Biham, Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer, 1993.
[10] H. C. A. van Tilborg, S. Jajodia. Encyclopedia of Cryptography and Security. s.l. : Springer, 2011.
[11] Quantum impossible differential attacks: Applications to AES and SKINNY. N. David, M. Naya-Plasencia, A. Schrottenloher. s.l. : Cryptology ePrint Archive, Paper 2022/754, 2022.
[12] Brassard, G., Høyer, P., Tapp, A.: Quantum cryptanalysis of hash and claw-free functions. In: LATIN. Lecture Notes in Computer Science, vol. 1380, pp. 163–169. Springer (1998).
[13] Rapid solution of problems by quantum computation . D. Deutsch, R. Jozsa. 1907, s.l. : Proceedings of the Royal Society of London, Series A: Mathematical and Physical Sciences, 1992, Vol. 439, pp. 553-558.
[14] P. Kaye, R. Laflamme, M. Mosca. An Introduction to Quantum Computing. New York : Oxford University Press, 2007.
[15] Algorithms for quantum computation: discrete logarithms and factoring. Shor, P. W. s.l. : Proceedings 35th annual symposium on foundations of computer science, Ieee, 1994, pp. 124-134.
[16] M. A. Nielsen, I. L. Chuang. Quantum Computation and Quantum Information. UK : Cambridge University Press, 2010.
[17] Kasirajan, V. Fundamentals of Quantum Computing: Theory and Practice. USA: Springer, 2021.
[18] https://en.wikipedia.org/wiki/RSA_(cryptosystem).
[19] Hidary, J. D. Quantum Computing: An Applied Approach. s.l. : Springer, 2019.
[20]] Q. Zhou, S. Lu, Z. Zhang, J. Su, Quantum Differential Cryptanalysis.

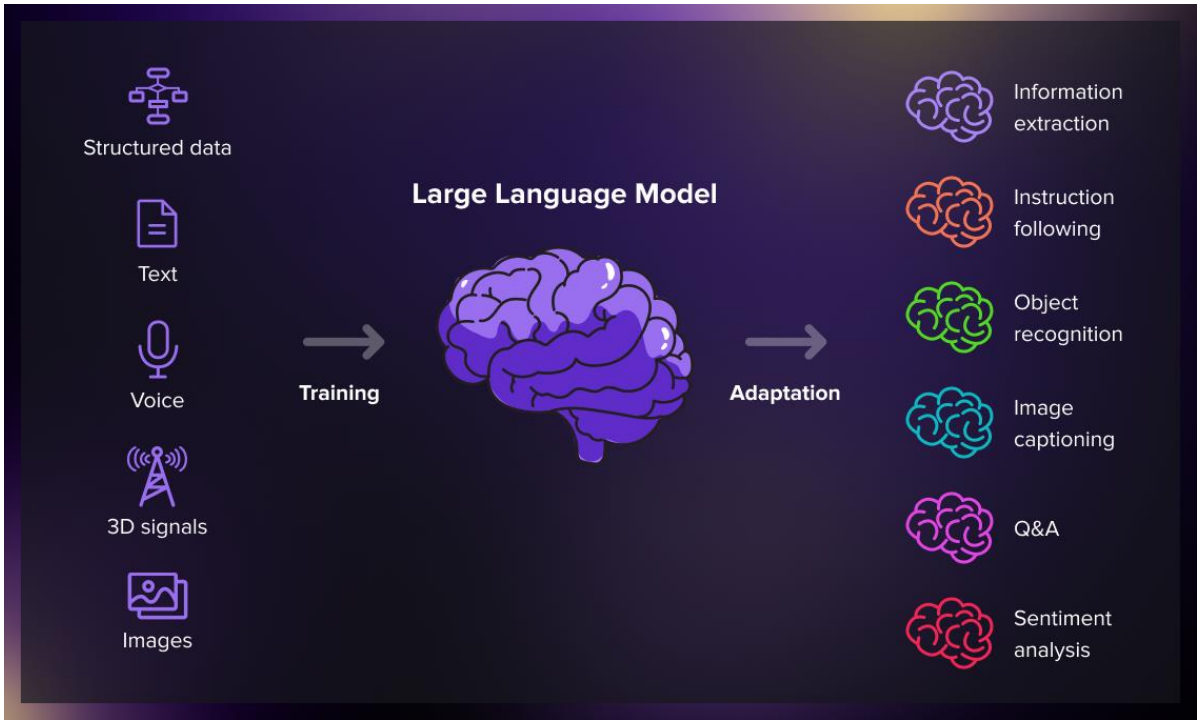
Μεγάλα μοντέλα γλώσσας: Μια επισκόπηση

Μαυρομάτης Παναγιώτης

Σταυρόπουλος Σπύρος

Εισαγωγή

Στο διαρκώς αναπτυσσόμενο τοπίο της τεχνητής νοημοσύνης (ΤΝ), οι συνεχείς εξελίξεις επαναπροσδιορίζουν συνεχώς τα όρια των δυνατοτήτων των μηχανών. Μεταξύ αυτών των εξελίξεων, η ανάπτυξη προηγμένων γλωσσικών μοντέλων αποτελεί απόδειξη της αξιοσημείωτης προόδου στον τομέα της επεξεργασίας φυσικής γλώσσας (Natural Language Processing - NLP). Καθώς η κοινωνία βασίζεται όλο και περισσότερο στην ΤΝ για την επικοινωνία, την κατανόηση και τη λήψη αποφάσεων, η κατανόηση των δυνατοτήτων και των επιπτώσεων αυτών των εξελιγμένων συστημάτων καθίσταται υψίστης σημασίας.



Τα μεγάλα μοντέλα γλώσσας (Large Language Models - LLM) αντιπροσωπεύουν ένα ορόσημο στη συνομιλητική ΤΝ. Εκπαιδευμένα σε τεράστια σύνολα δεδομένων που καλύπτουν ποικίλα γλωσσικά πρότυπα και ανθρώπινες αλληλεπιδράσεις, αυτά τα μοντέλα έχουν σχεδιαστεί για να μπορούν να εμπλακούν σε διάλογο που μιμείται την ανθρώπινη συνομιλία με εντυπωσιακή ρεαλιστικότητα. Η αρχιτεκτονική τους, βασισμένη σε βαθιά

νευρωνικά δίκτυα και μοντέλα μετασχηματιστών, τους επιτρέπει να κατανοούν κείμενο και να παράγουν απαντήσεις που είναι συναφείς και συνεκτικές με το περιεχόμενο μιας ερώτησης. Από την παροχή βοήθειας στους χρήστες με ερωτήματα έως τη δημιουργία δημιουργικού περιεχομένου, αυτά τα γλωσσικά μοντέλα καταδεικνύουν τη δυνατότητα της τεχνητής νοημοσύνης να επαυξάνει τις ανθρώπινες ικανότητες σε πολλούς τομείς. Εργαλεία όπως το ChatGPT και το Gemini χρησιμοποιούνται από εκατομμύρια χρήστες παγκοσμίως.

Ωστόσο, η εξάπλωση των προηγμένων συστημάτων τεχνητής νοημοσύνης εγείρει επίσης σημαντικά ερωτήματα σχετικά με τη δεοντολογία, τη διαφάνεια και τον κοινωνικό αντίκτυπο. Καθώς τα συστήματα αυτά ενσωματώνονται όλο και περισσότερο στην καθημερινή ζωή και την επαγγελματική πρακτική, έρχονται στο προσκήνιο ανησυχίες σχετικά με τη μεροληψία, τη διαφάνεια και την ιδιωτικότητα. Η αντιμετώπιση αυτών των ανησυχιών απαιτεί όχι μόνο τεχνολογικές εξελίξεις αλλά και ισχυρά ηθικά πλαίσια και ρυθμιστικά μέτρα για να διασφαλιστεί η υπεύθυνη ανάπτυξη της ΤΝ.

Δυνατότητες

Τα LLM έχουν φέρει επανάσταση στον τομέα της τεχνητής νοημοσύνης, επιφέροντας σημαντικές εξελίξεις σε διάφορους τομείς. Αυτά τα εξελιγμένα συστήματα τεχνητής νοημοσύνης προσφέρουν πολλά πλεονεκτήματα που ενισχύουν τη χρησιμότητα και τον αντίκτυπό τους. Ακολουθούν ορισμένα από τα βασικά πλεονεκτήματα των LLMs:

Ενισχυμένη κατανόηση και παραγωγή φυσικής γλώσσας [1]

Τα LLM υπερέχουν στην κατανόηση και την παραγωγή κειμένου που μοιάζει με ανθρώπινο κείμενο. Η ικανότητά τους να κατανοούν το περιεχόμενο και να παράγουν συνεκτικές απαντήσεις τους καθιστά ανεκτίμητες για εφαρμογές που απαιτούν αλληλεπίδραση με φυσική γλώσσα. Αυτή η επάρκεια επιτρέπει στα LLM να εκτελούν εργασίες όπως η μετάφραση, η περίληψη και η δημιουργία περιεχομένου με αξιοσημείωτη ακρίβεια και ευχέρεια.

Ευελιξία σε όλους τους τομείς

Η εκπαίδευση των LLMs σε διάφορα σύνολα δεδομένων τους εξοπλίζει με μια ευρεία βάση γνώσεων, επιτρέποντάς τους να λειτουργούν αποτελεσματικά σε διάφορους τομείς. Είτε πρόκειται για τη συγγραφή κώδικα, τη δημιουργία νομικών εγγράφων, τη δημιουργία περιεχομένου μάρκετινγκ ή την παροχή υποστήριξης πελατών, τα LLM μπορούν να προσαρμοστούν σε διαφορετικά πλαίσια και να παρέχουν αποτελέσματα υψηλής ποιότητας. Αυτή η ευελιξία μειώνει την ανάγκη για μοντέλα ειδικού τομέα, εξορθολογίζοντας τις διαδικασίες και εξοικονομώντας πόρους.

Βελτιωμένη αποδοτικότητα και παραγωγικότητα

Αυτοματοποιώντας τις συνήθεις και επαναλαμβανόμενες εργασίες, τα LLM βελτιώνουν σημαντικά την αποδοτικότητα και την παραγωγικότητα. Για παράδειγμα, στην εξυπηρέτηση πελατών, τα LLM μπορούν να χειριστούν πολλά ερωτήματα ταυτόχρονα, παρέχοντας άμεσες και ακριβείς απαντήσεις. Στη δημιουργία περιεχομένου, μπορούν να συντάσσουν άρθρα, εκθέσεις και άλλα έγγραφα γρήγορα, επιτρέποντας στους ανθρώπινους εργαζόμενους να επικεντρωθούν σε πιο σύνθετες και δημιουργικές εργασίες. Αυτή η δυνατότητα αυτοματοποίησης οδηγεί σε εξοικονόμηση κόστους και ταχύτερους χρόνους διεκπεραίωσης σε διάφορες βιομηχανίες.

Εξατομίκευση και προσαρμογή [2]

Τα LLM μπορούν να ρυθμιστούν ώστε να ανταποκρίνονται σε συγκεκριμένες ανάγκες, επιτρέποντας εξατομικευμένες και προσαρμοσμένες αλληλεπιδράσεις. Σε εφαρμογές όπως οι εικονικοί βοηθοί και τα συστήματα συστάσεων, τα LLM μπορούν να μαθαίνουν τις προτιμήσεις των χρηστών και να παρέχουν εξατομικευμένες προτάσεις, βελτιώνοντας την εμπειρία και την ικανοποίηση των χρηστών. Αυτή η ικανότητα εξατομίκευσης είναι ιδιαίτερα πολύτιμη σε τομείς όπως το ηλεκτρονικό εμπόριο, η εκπαίδευση και η ψυχαγωγία, όπου οι εξατομικευμένες υπηρεσίες έχουν όλο και μεγαλύτερη ζήτηση.

Προσβασιμότητα

Καταρρίπτοντας τα γλωσσικά εμπόδια, τα LLMs προωθούν την προσβασιμότητα. Μπορούν να μεταφράζουν κείμενα μεταξύ πολλών γλωσσών, καθιστώντας τις πληροφορίες πιο προσιτές σε άτομα που δεν είναι φυσικοί ομιλητές. Επιπλέον, τα LLM μπορούν να βοηθήσουν τα άτομα με αναπηρίες μετατρέποντας κείμενο σε ομιλία και αντίστροφα, βελτιώνοντας την επικοινωνία και τις ευκαιρίες μάθησης. Αυτός ο εκδημοκρατισμός των πληροφοριών προάγει μια κοινωνία χωρίς αποκλεισμούς, όπου η γνώση και οι πόροι είναι διαθέσιμοι σε ένα ευρύτερο κοινό.

Καινοτομία και δημιουργικότητα

Τα LLM δεν είναι μόνο χρήσιμα στην αυτοματοποίηση επαναλαμβανόμενων εργασίων. Οδηγούν επίσης στην καινοτομία και τη δημιουργικότητα. Μπορούν να δημιουργήσουν νέες ιδέες, να βοηθήσουν σε συνεδρίες καταιγισμού ιδεών και να παρέχουν δημιουργικές εισροές σε τομείς όπως η τέχνη, η μουσική και η λογοτεχνία. Για παράδειγμα, τα LLM μπορούν να προτείνουν ανατροπές της πλοκής για συγγραφείς, να παράγουν μελωδίες για μουσικούς ή να δημιουργούν οπτικές ιδέες για σχεδιαστές. Αυτή η ικανότητα έμπνευσης και ενίσχυσης της ανθρώπινης δημιουργικότητας ανοίγει νέες δυνατότητες για καλλιτεχνικές και πνευματικές προσπάθειες.

Ενδείξεις με βάση τα δεδομένα

Αναλύοντας μεγάλους όγκους δεδομένων κειμένου, τα LLM μπορούν να εξάγουν πολύτιμες γνώσεις και τάσεις. Αυτή η αναλυτική ικανότητα είναι ιδιαίτερα χρήσιμη σε τομείς όπως η έρευνα αγοράς, η ανάλυση των μέσων κοινωνικής δικτύωσης και η υγειονομική περίθαλψη. Τα LLM μπορούν να εντοπίζουν μοτίβα, να ανιχνεύουν συναισθήματα και να δημιουργούν αναφορές που ενημερώνουν τις διαδικασίες λήψης αποφάσεων. Αυτές οι πληροφορίες που βασίζονται σε δεδομένα βοηθούν τους οργανισμούς να λαμβάνουν τεκμηριωμένες αποφάσεις, να βελτιστοποιούν τις στρατηγικές τους και να παραμένουν ανταγωνιστικοί.

Επεκτασιμότητα

Η επεκτασιμότητα των LLMs τα καθιστά κατάλληλα τόσο για εφαρμογές μικρής κλίμακας όσο και για μεγάλες επιχειρηματικές λύσεις. Μπορούν να αναπτυχθούν σε διάφορα περιβάλλοντα, από μεμονωμένες συσκευές χρηστών έως υποδομές που βασίζονται στο cloud, διασφαλίζοντας ότι επιχειρήσεις όλων των μεγεθών μπορούν να επωφεληθούν από τις δυνατότητές τους. Αυτή η επεκτασιμότητα διασφαλίζει ότι οι LLM μπορούν να αναπτυχθούν μαζί με τις ανάγκες ενός οργανισμού

Αδυναμίες

Ενώ τα LLM έχουν επιφέρει σημαντικές προόδους στον τομέα της τεχνητής νοημοσύνης, παρουσιάζουν επίσης μια σειρά από μειονεκτήματα και προκλήσεις. Τα ζητήματα αυτά μπορούν να επηρεάσουν την αποτελεσματικότητά τους, τις ηθικές εκτιμήσεις και τη συνολική ενσωμάτωση σε διάφορους τομείς. Ακολουθούν ορισμένα από τα βασικά μειονεκτήματα των LLM:

Μεροληψία και δικαιοσύνη [3]

Μια από τις μεγαλύτερες ανησυχίες για τα LLM είναι η παρουσία προκαταλήψεων στα αποτελέσματά τους. Δεδομένου ότι τα LLM εκπαιδεύονται σε μεγάλα σύνολα δεδομένων που αντικατοπτρίζουν την ανθρώπινη γλώσσα και συμπεριφορά, μπορούν ακούσια να μάθουν και να διαδώσουν κοινωνικές προκαταλήψεις που σχετίζονται με τη φυλή, το φύλο, την ηλικία και

άλλα χαρακτηριστικά. Αυτό μπορεί να οδηγήσει σε άδικα και μεροληπτικά αποτελέσματα, κάτι που είναι ιδιαίτερα προβληματικό σε ευαίσθητες εφαρμογές όπως οι προσλήψεις, η επιβολή του νόμου και η υγειονομική περίθαλψη.

Έλλειψη επεξηγηματικότητας [4]

Τα LLM λειτουργούν ως μοντέλα «μαύρου κουτιού», που σημαίνει ότι η εσωτερική τους λειτουργία δεν είναι εύκολα ερμηνεύσιμη από τον άνθρωπο. Αυτή η έλλειψη επεξηγηματικότητας καθιστά δύσκολο να κατανοηθεί πώς καταλήγουν σε συγκεκριμένες αποφάσεις ή αποτελέσματα. Σε κρίσιμες εφαρμογές όπως η νομική επιχειρηματολογία ή η ιατρική διάγνωση, αυτή η αδιαφάνεια μπορεί να υπονομεύσει την εμπιστοσύνη και τη λογοδοσία, καθώς οι χρήστες δεν μπορούν να επαληθεύσουν τη λογική πίσω από τις συστάσεις της ΤΝ.

Υψηλό υπολογιστικό κόστος [5]

Η εκπαίδευση και η ανάπτυξη των LLM απαιτούν σημαντικούς υπολογιστικούς πόρους, συμπεριλαμβανομένων ισχυρών GPU και μεγάλων ποσοτήτων ενέργειας. Αυτή η υψηλή κατανάλωση πόρων μπορεί να αποτελέσει εμπόδιο εισόδου για μικρότερους οργανισμούς ή ιδιώτες που δεν μπορούν να αντέξουν αυτά τα έξοδα. Επιπλέον, ο περιβαλλοντικός αντίκτυπος της λειτουργίας τέτοιων ενεργοβόρων μοντέλων αποτελεί αυξανόμενη ανησυχία, συμβάλλοντας στο αποτύπωμα άνθρακα των τεχνολογιών ΤΝ.

Κίνδυνοι ασφάλειας και απορρήτου

Τα LLM μπορεί να ενέχουν κινδύνους για την ασφάλεια και την προστασία της ιδιωτικής ζωής, ιδίως όταν έχουν να κάνουν με ευαίσθητες πληροφορίες. Υπάρχει ο κίνδυνος τα μοντέλα αυτά να απομνημονεύσουν και να αναπαράγουν ακούσια προσωπικά δεδομένα από τα σύνολα εκπαίδευσής τους. Επιπλέον, μπορεί να είναι ευάλωτα σε αντίπαλες επιθέσεις, όπου κακόβουλες είσοδοι διαμορφώνονται για να εξαπατήσουν το μοντέλο ώστε να παράγει εσφαλμένες ή επιβλαβείς εξόδους. Αυτά τα τρωτά σημεία καθιστούν αναγκαία ισχυρά μέτρα ασφαλείας για την προστασία των δεδομένων των χρηστών και την εξασφάλιση της ασφαλούς λειτουργίας.

Εξάρτηση από μεγάλα σύνολα δεδομένων

Η αποτελεσματικότητα των LLM εξαρτάται σε μεγάλο βαθμό από την ποιότητα και την ποσότητα των δεδομένων εκπαίδευσης. Εάν τα δεδομένα εκπαίδευσης είναι περιορισμένα, ξεπερασμένα ή μεροληπτικά, η απόδοση του μοντέλου θα τεθεί σε κίνδυνο. Επιπλέον, η απόκτηση και η επιμέλεια μεγάλων συνόλων δεδομένων μπορεί να είναι χρονοβόρα και

δαπανηρή. Αυτή η εξάρτηση εγείρει επίσης ηθικές ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής των δεδομένων και τη χρήση υλικού που προστατεύεται από πνευματικά δικαιώματα χωρίς την κατάλληλη συγκατάθεση

.Περιορισμένη κατανόηση του περιεχομένου

Παρά τις εντυπωσιακές τους δυνατότητες, τα LLM μπορεί να δυσκολεύονται να κατανοήσουν το βαθύ νόημα, τον σαρκασμό, το χιούμορ και τις αποχρώσεις της ανθρώπινης γλώσσας. Συχνά παράγουν αποτελέσματα που είναι εύλογα αλλά όχι απαραίτητα ακριβή ή κατάλληλα. Αυτός ο περιορισμός μπορεί να οδηγήσει σε παρανοήσεις και λάθη σε εφαρμογές που απαιτούν λεπτή κατανόηση, όπως η νομική ανάλυση, η δημιουργική γραφή και η υποστήριξη πελατών.

Ηθικά και δεοντολογικά διλήμματα

Η ανάπτυξη των LLM εγείρει διάφορα ηθικά και δεοντολογικά διλήμματα. Για παράδειγμα, η χρήση των LLMs για τη δημιουργία περιεχομένου βαθιάς απομίμησης ή παραπλανητικών πληροφοριών μπορεί να έχει σοβαρές κοινωνικές επιπτώσεις. Η δυνατότητα παραγωγής ρεαλιστικού κειμένου σε κλίμακα μπορεί να αξιοποιηθεί για εκστρατείες παραπληροφόρησης, απάτης και άλλες κακόβουλες δραστηριότητες. Η αντιμετώπιση αυτών των ηθικών προκλήσεων απαιτεί ένα συνδυασμό τεχνολογικών διασφαλίσεων και ρυθμιστικής εποπτείας.

Επιπτώσεις στην οικονομία και το εργατικό δυναμικό

Οι δυνατότητες αυτοματοποίησης των LLM μπορούν να οδηγήσουν σε σημαντικές οικονομικές διαταραχές και διαταραχές του εργατικού δυναμικού. Καθώς τα μοντέλα αυτά υιοθετούνται σε διάφορους κλάδους για την εκτέλεση καθηκόντων που παραδοσιακά εκτελούνταν από ανθρώπους, υπάρχει το ενδεχόμενο εκτόπισης θέσεων εργασίας. Ενώ τα LLM μπορούν να βελτιώσουν την παραγωγικότητα και την αποδοτικότητα, ενδέχεται επίσης να επιδεινώσουν τις οικονομικές ανισότητες, εάν τα οφέλη της αυτοματοποίησης δεν είναι ευρέως διανεμημένα.

Υπερβολική εξάρτηση από τα συστήματα τεχνητής νοημοσύνης

Η αυξανόμενη εξάρτηση από τα LLM και άλλα συστήματα ΤΝ μπορεί να οδηγήσει σε υπερβολική εξάρτηση, όπου οι χρήστες μπορεί να εμπιστεύονται τυφλά την ΤΝ χωρίς κριτική αξιολόγηση. Αυτό μπορεί να είναι ιδιαίτερα επικίνδυνο σε σενάρια υψηλού κινδύνου, όπου η ανθρώπινη κρίση είναι απαραίτητη. Η υπερβολική εξάρτηση από την ΤΝ μπορεί επίσης να καταπνίξει την ανθρώπινη δημιουργικότητα.

Εκπαίδευση

Πολλά LLMs χρησιμοποιούν μια διαφορετική αρχιτεκτονική νευρωνικού δικτύου, τον μετασχηματιστή.[6] Σε αντίθεση με τα παραδοσιακά επαναλαμβανόμενα νευρωνικά δίκτυα (RNN), ο μετασχηματιστής χρησιμοποιεί ένα μηχανισμό που ονομάζεται αυτοπροσοχή (self-attention). Αυτό επιτρέπει στο μοντέλο να παρακολουθεί ταυτόχρονα όλα τα μέρη της ακολουθίας εισόδου. Κάθε λέξη στην ακολουθία αναλύεται όχι μόνο από μόνη της αλλά και σε σχέση με κάθε άλλη λέξη. Αυτό επιτρέπει στο μοντέλο να συλλάβει εξαρτήσεις μεγάλης εμβέλειας μέσα στη γλώσσα, όπως το πώς μια αντωνυμία σχετίζεται με ένα όνομα αρκετές λέξεις πίσω στην πρόταση.

Οι μετασχηματιστές συνήθως ακολουθούν μια αρχιτεκτονική κωδικοποιητή-αποκωδικοποιητή. Ο κωδικοποιητής δέχεται την ακολουθία εισόδου (π.χ. μια πρόταση σε μια γλώσσα) και την επεξεργάζεται χρησιμοποιώντας την αυτοπροσοχή για να δημιουργήσει μια αναπαράσταση κάθε λέξης με βάση το περιεχόμενο. Αυτή η αναπαράσταση αποτυπώνει όχι μόνο τη σημασία της μεμονωμένης λέξης αλλά και τις σχέσεις της με άλλες λέξεις στην ακολουθία.

Στη συνέχεια, ο αποκωδικοποιητής χρησιμοποιεί την κωδικοποιημένη αναπαράσταση για να παράγει την ακολουθία εξόδου (π.χ. τη μετάφραση σε άλλη γλώσσα). Είναι σημαντικό ότι ο αποκωδικοποιητής χρησιμοποιεί επίσης έναν μηχανισμό προσοχής, αλλά αυτή τη φορά επικεντρώνεται στην κωδικοποιημένη αναπαράσταση που παράγεται από τον κωδικοποιητή. Αυτό επιτρέπει στον αποκωδικοποιητή να παρακολουθεί επιλεκτικά τα σχετικά μέρη της ακολουθίας εισόδου κατά τη δημιουργία της εξόδου.

Το βασικό πλεονέκτημα των μετασχηματιστών είναι η ικανότητά τους να παραλληλίζουν τους υπολογισμούς. Σε αντίθεση με τα RNN, τα οποία επεξεργάζονται τις πληροφορίες διαδοχικά και περιορίζουν τον παραλληλισμό, οι μετασχηματιστές μπορούν να αναλύουν όλα τα μέρη της ακολουθίας ταυτόχρονα. Αυτό τους καθιστά σημαντικά ταχύτερους στην εκπαίδευσή τους, ειδικά για μεγάλες ακολουθίες.

Η επιτυχία της αρχιτεκτονικής των μετασχηματιστών έχει οδηγήσει στην ευρεία υιοθέτησή τους σε διάφορες εργασίες επεξεργασίας φυσικής γλώσσας πέραν της μηχανικής μετάφρασης. Σε αυτές περιλαμβάνονται εργασίες όπως η περίληψη κειμένου, η απάντηση ερωτήσεων, ακόμη και η παραγωγή κώδικα. Η ικανότητα των μετασχηματιστών να συλλαμβάνουν εξαρτήσεις μεγάλης εμβέλειας και να αναλύουν τις σχέσεις εντός της γλώσσας τους καθιστά ένα ισχυρό εργαλείο για ένα ευρύ φάσμα εφαρμογών.

Επίλογος

Καθώς εξερευνούμε τα πλεονεκτήματα και τα μειονεκτήματα των Μεγάλων Γλωσσικών Μοντέλων, γίνεται σαφές ότι αυτές οι τεχνολογίες έχουν φέρει επανάσταση στον τομέα της τεχνητής νοημοσύνης. Ενώ προσφέρουν απαράμιλλη ικανότητα κατανόησης και παραγωγής φυσικής γλώσσας, υπάρχουν ακόμα προκλήσεις που πρέπει να αντιμετωπιστούν, όπως η ηθική χρήση, η προκατάληψη δεδομένων και η διαφάνεια των αλγορίθμων. Στο μέλλον, η συνεργασία μεταξύ επιστημόνων, μηχανικών και κοινωνίας θα είναι καθοριστική για τη διασφάλιση ότι αυτές τεχνολογίες θα χρησιμοποιηθούν προς όφελος όλων.

Βιογραφικό συντακτών

Ο Μαυρομμάτης Παναγιώτης Γεώργιος είναι απόφοιτος του Τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου. Δραστηριοποιείται στον τομέα των ανανεώσιμων πηγών ενέργειας αλλά και γενικά της πράσινης ανάπτυξης και διαθέτει καλές γνώσεις προγραμματισμού. Ως φοιτητής ασχολήθηκε εκτεταμένα με την επεξεργασία εικόνας μέσω της λήψης και ανάλυσης δορυφορικών δεδομένων από ραντάρ.

Ο Σταυρόπουλος Σπυρίδωνας είναι απόφοιτος του Τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών του Πανεπιστημίου Πατρών. Κατέχει καλές γνώσεις προγραμματισμού και ασχολείται με σύγχρονες τεχνολογίες σχετικά με την εκτεταμένη πραγματικότητα.

Αναφορές:

[1] Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D., Wu, J., Winter, C., Hesse, C., ... Amodei, D. (2020). Language models are few-shot learners. https://doi.org/10.48550/arXiv.2005.14165
[2] Murakhovs'ka, L., Laban, P., Xie, T., Xiong, C., & Wu, C.-S. (2023). Salespeople vs. SalesBot: Exploring the Role of Educational Value in Conversational Recommender Systems. Findings of the EMNLP (2023). https://doi.org/10.18653/v1/2023.findings-emnlp.657
[3] Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT '21), 610-623. https://doi.org/10.1145/3442188.3445922
[4] Sarker, I. H. (2024). AI-driven cybersecurity and threat intelligence: Cyber automation, intelligent decision-making and explainability. Springer.
[5] Shoeybi, M., Patwary, M., Puri, R., LeGresley, P., Casper, J., & Catanzaro, B. (2019). Megatron-LM: Training multi-billion parameter language models using model parallelism. arXiv. https://arxiv.org/abs/1909.08053
[6] Vaswani et al., (2017). Attention Is All You Need. arXiv:1706.03762

Συστήματα Κρυπτογραφίας με τεχνικές τεχνητής νοημοσύνης

ΥΕΑ (ΕΠ) Πασχάλης Θεόδωρος

Ασφάλεια Πληροφοριακών Συστημάτων

Στην ψηφιακή εποχή που ζούμε, η ασφάλεια των πληροφοριών έχει αποκτήσει ζωτική σημασία τόσο για τις επιχειρήσεις όσο και για τα άτομα. Οι συνεχώς αυξανόμενες απειλές, όπως οι κυβερνοεπιθέσεις,η κλοπή δεδομένων και η παραβίαση της ιδιωτικότητας, έχουν καταστήσει επιτακτική την ανάγκη για την ανάπτυξη και την υιοθέτηση προηγμένων συστημάτων ασφαλείας. Σε αυτό το πλαίσιο, η

κρυπτογραφία παίζει κεντρικό ρόλο, προσφέροντας αξιόπιστες λύσεις για την προστασία τηςεμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

Τα συστήματα ασφαλείας είναι πολυδιάστατα και περιλαμβάνουν μια σειρά από τεχνολογίες,διαδικασίες και πρακτικές που στοχεύουν στην προστασία των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση και καταστροφή. Μεταξύ των πιο κοινών στοιχείων των συστημάτων ασφαλείας περιλαμβάνονται τα τείχη προστασίας (firewalls), τα συστήματα ανίχνευσης και αποτροπής εισβολών (IDS/IPS), τα εργαλεία για την διαχείριση ταυτότητας και πρόσβασης (IAM), καθώς και οι στρατηγικές δημιουργίας αντιγράφων ασφαλείας και ανάκαμψης από καταστροφές.

Τα τείχη προστασίας λειτουργούν ως φίλτρα, ελέγχοντας την κυκλοφορία δικτύου και αποτρέποντας την πρόσβαση σε ανεπιθύμητες συνδέσεις. Τα IDS και IPS παρακολουθούν τα δίκτυα και τα συστήματα για σημάδια κακόβουλης δραστηριότητας, ειδοποιώντας τους διαχειριστές ασφαλείας ή ακόμη και μπλοκάροντας τις ύποπτες ενέργειες. Τα συστήματα IAM εξασφαλίζουν ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε ευαίσθητες πληροφορίες και πόρους, μέσω μηχανισμών όπως η επαλήθευση ταυτότητας και η διαχείριση δικαιωμάτων πρόσβασης.

Ο Ρόλος της Κρυπτογραφίας

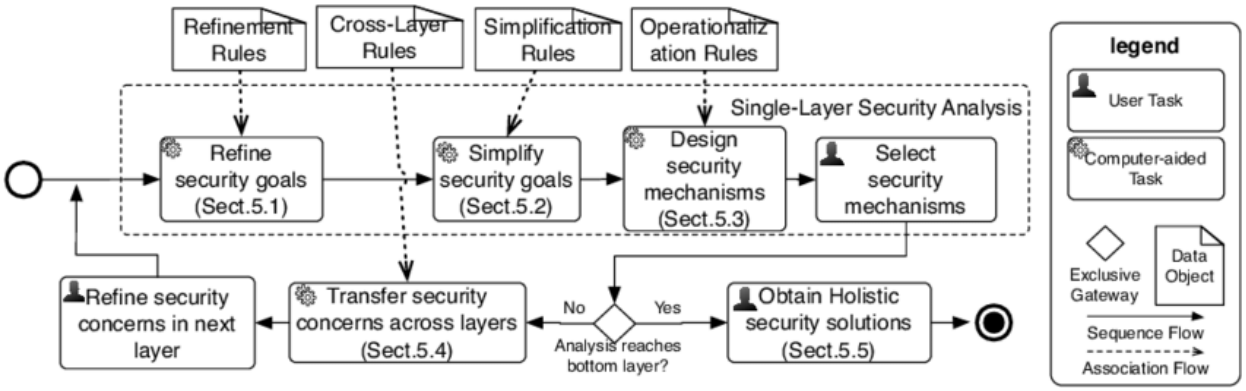
Η κρυπτογραφία είναι η επιστήμη που ασχολείται με τη μελέτη και την πρακτική των τεχνικώνγια την ασφαλή επικοινωνία, παρέχοντας μεθόδους για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Οι τεχνικές κρυπτογραφίας διασφαλίζουν ότι τα δεδομένα παραμένουν εμπιστευτικά κατά τη μεταφορά ή την αποθήκευσή τους, αποτρέποντας την ανάγνωση ή την αλλοίωσή τους από μη εξουσιοδοτημένα άτομα.

Υπάρχουν δύο κύριοι τύποι κρυπτογραφίας: η συμμετρική και η ασύμμετρη. Στη συμμετρικήκρυπτογραφία, το ίδιο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Παράδειγμα αυτής της τεχνικής είναι ο αλγόριθμος Advanced Encryption Standard (AES), που χρησιμοποιείται ευρέως λόγω της αποδοτικότηταςκαι της ασφάλειάς του. Στην ασύμμετρη κρυπτογραφία, χρησιμοποιούνται δύο διαφορετικά κλειδιά – ένα δημόσιο και ένα ιδιωτικό. Τα δημόσια κλειδιά χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων, ενώ τα ιδιωτικά για την αποκρυπτογράφησή τους. Αυτή η μέθοδος, γνωστή και ως κρυπτογραφία δημόσιου κλειδιού, χρησιμοποιείται σε πρωτόκολλα όπως το RSA (Rivest-Shamir-Adleman) και είναι θεμελιώδης για την ασφάλεια των συναλλαγών στο διαδίκτυο.

Η Σύνδεση των Συστημάτων Ασφαλείας με την Κρυπτογραφία

Η κρυπτογραφία ενσωματώνεται στα σύγχρονα συστήματα ασφαλείας με πολλούς τρόπους. Στα τείχη προστασίας και τα συστήματα IDS/IPS, χρησιμοποιούνται τεχνικές κρυπτογραφίας γιατην προστασία των επικοινωνιών και την εξασφάλιση ότι τα δεδομένα που διακινούνται μέσω των δικτύων παραμένουν ασφαλή από υποκλοπές και παραβιάσεις. Επιπλέον, η κρυπτογραφία συμβάλλει στην ασφαλή αποθήκευση δεδομένων, χρησιμοποιώντας αλγόριθμους κρυπτογράφησης για την προστασία ευαίσθητων πληροφοριών που αποθηκεύονται σε διακομιστές και βάσεις δεδομένων.

Ένας από τους πιο σημαντικούς ρόλους της κρυπτογραφίας στα συστήματα ασφαλείας είναι η επίτευξη της ακεραιότητας των δεδομένων και η επαλήθευση της ταυτότητας. Μέσω της χρήσης ψηφιακών υπογραφών και πιστοποιητικών, η κρυπτογραφία επιτρέπει την επαλήθευση της αυθεντικότητας των δεδομένων και των επικοινωνιών, προστατεύοντας τα από αλλοιώσεις και διασφαλίζοντας ότι οι πληροφορίες προέρχονται από έγκυρες πηγές.



Υλοποίηση ενός κρυπτογραφικού συστήματος

Βήμα 1: Καθορισμός Απαιτήσεων και Στόχων

Καθορισμός Απαιτήσεων Ασφάλειας

- Ανάλυση Αναγκών: Προσδιορίστε τις ανάγκες ασφαλείας του συστήματος, όπως την προστασία των δεδομένων, την ακεραιότητα και την αυθεντικότητα.
- Καθορισμός Απειλών: Προσδιορίστε τις πιθανές απειλές και τους κινδύνους που το σύστημα πρέπει να αντιμετωπίσει.

Ορισμός Στόχων

- Ασφάλεια: Εξασφάλιση ότι τα δεδομένα παραμένουν εμπιστευτικά και αμετάβλητα.
- Αποδοτικότητα: Το σύστημα πρέπει να είναι γρήγορο και αποδοτικό στη χρήση των πόρων.
- Ευκολία Χρήσης: Η κρυπτογράφηση και η αποκρυπτογράφηση πρέπει να είναι εύκολη στη χρήση για τους χρήστες.

Βήμα 2: Επιλογή Κρυπτογραφικών Αλγορίθμων

Συμμετρικοί και Ασύμμετροι Αλγόριθμοι

- Συμμετρική Κρυπτογραφία: Επιλογή αλγορίθμων όπως AES (Advanced Encryption Standard) για ταχύτητα και αποδοτικότητα.

- Ασύμμετρη Κρυπτογραφία: Επιλογή αλγορίθμων όπως RSA ή ECC (Elliptic Curve Cryptography) για ανταλλαγή κλειδιών και ψηφιακές υπογραφές.

Αλγόριθμοι Κατακερματισμού (SHA-256, SHA-3: Επιλογή ασφαλών αλγορίθμων κατακερματισμού για την διασφάλιση τηςακεραιότητας των δεδομένων)

Βήμα 3: Σχεδιασμός Πρωτοκόλλων

- Πρωτόκολλο Ανταλλαγής Κλειδιών
- Diffie-Hellman, ECDH: Χρησιμοποιήστε πρωτόκολλα για ασφαλή ανταλλαγή κλειδιών μεταξύ των μερών.
- Πρωτόκολλο Κρυπτογράφησης και Αποκρυπτογράφησης
- Συμμετρική Κρυπτογράφηση: Σχεδιάστε τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης χρησιμοποιώντας το επιλεγμένο συμμετρικό κλειδί.
- Ασύμμετρη Κρυπτογράφηση: Χρησιμοποιήστε ασύμμετρη κρυπτογράφηση για την ασφαλή αποστολή του συμμετρικού κλειδιού.

Βήμα 4: Ανάπτυξη Λογισμικου

- Επιλογή Γλώσσας Προγραμματισμού (ανάλογα με τις απαιτήσεις τουσυστήματος και τη γνώση της ομάδας ανάπτυξης).
- Υλοποίηση Αλγορίθμων (χρησιμοποίηση κρυπτογραφικών βιβλιοθηκών όπως OpenSSL,PyCryptodome, BouncyCastle για την υλοποίηση των αλγορίθμων).

Βήμα 5: Δοκιμή και Επαλήθευση

- Δοκιμές Ασφάλειας
- Penetration Testing: Εκτελέστε δοκιμές διείσδυσης για να εντοπίσετε και να διορθώσετε τυχόνευπάθειες.
- Ανθεκτικότητα σε Επιθέσεις: Ελέγξτε την ανθεκτικότητα του συστήματος σε γνωστές επιθέσειςόπως Brute Force, Man-in-the-Middle.
- Δοκιμές Λειτουργικότητας
- Δοκιμές Μονάδας: Εφαρμόστε δοκιμές μονάδας σε κάθε μέρος του συστήματος για ναδιασφαλίσετε ότι λειτουργεί σωστά.
- Ολοκληρωμένες Δοκιμές: Δοκιμάστε το σύστημα ως σύνολο για να επιβεβαιώσετε ότι όλες οιλειτουργίες συνεργάζονται σωστά.

Βήμα 6: Ανάπτυξη και Εφαρμογή

Εγκατάσταση του Συστήματος

- Διαμόρφωση: Ρυθμίστε το σύστημα σύμφωνα με τις απαιτήσεις ασφαλείας.
- Εκπαίδευση Χρηστών: Εκπαιδεύστε τους χρήστες στη σωστή χρήση του συστήματοςκρυπτογράφησης.
- Παρακολούθηση και Συντήρηση
- Συνεχής Παρακολούθηση: Παρακολουθήστε το σύστημα για ανωμαλίες και πιθανές απειλές.
- Τακτικές Ενημερώσεις: Εφαρμόστε τακτικές ενημερώσεις για να αντιμετωπίσετε νέες απειλέςκαι να βελτιώσετε την ασφάλεια.

Βήμα 7: Συνεχής Βελτίωση

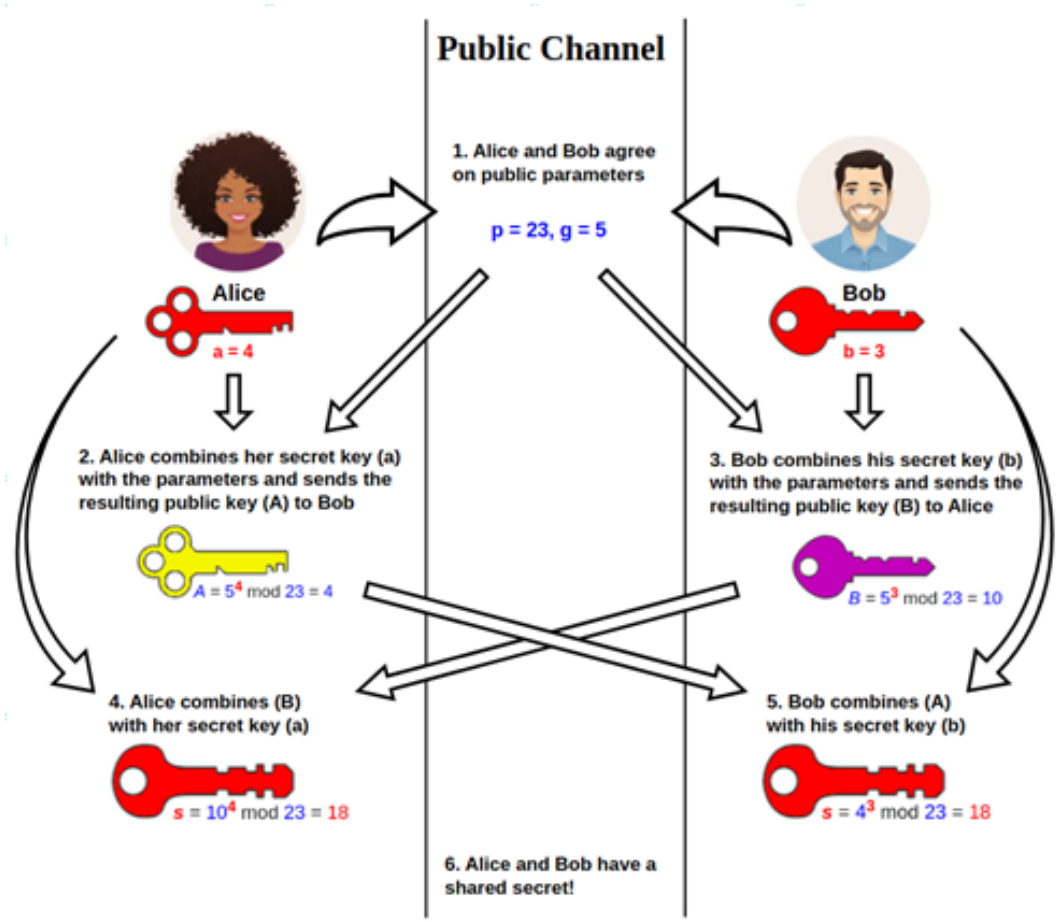
Συλλογή Ανατροφοδότησης

- Ανατροφοδότηση Χρηστών: Συλλέξτε ανατροφοδότηση από τους χρήστες για τη λειτουργικότητα και την ασφάλεια του συστήματος.

Βελτιστοποίηση

- Βελτιώσεις Αλγορίθμων: Βελτιστοποιήστε τους αλγορίθμους για καλύτερη απόδοση καιασφάλεια.
- Ενσωμάτωση Νέων Τεχνολογιών: Ενσωματώστε νέες τεχνολογίες και μεθόδους για τηνενίσχυση της ασφάλειας.

Η υλοποίηση ενός κρυπτογραφικού συστήματος απαιτεί μια συνδυασμένη προσπάθεια που περιλαμβάνει τον καθορισμό των απαιτήσεων, την επιλογή και τον σχεδιασμό των αλγορίθμων,την ανάπτυξη λογισμικού, τη δοκιμή και την επαλήθευση, την εφαρμογή και την παρακολούθηση, και τη συνεχή βελτίωση. Ακολουθώντας αυτά τα βήματα, μπορείτε να δημιουργήσετε ένα ισχυρό και αποδοτικό σύστημα κρυπτογράφησης που παρέχει ασφάλεια καιπροστασία για τα δεδομένα σας.



Τεχνητή νοημοσύνη

Η τεχνητή νοημοσύνη (ΤΝ) έχει εξελιχθεί ραγδαία τις τελευταίες δεκαετίες και έχει βρει εφαρμογές σε πολλούς τομείς της επιστήμης και της τεχνολογίας. Ένας από τους τομείς όπου ηΤΝ μπορεί να προσφέρει σημαντικά οφέλη είναι η κρυπτογραφία. Η κρυπτογραφία, η οποία είναι θεμελιώδης για την ασφάλεια των δεδομένων και την προστασία της ιδιωτικότητας, αντιμετωπίζει συνεχώς νέες προκλήσεις λόγω των εξελισσόμενων απειλών. Η ενσωμάτωση τεχνητής νοημοσύνης στα συστήματα κρυπτογραφίας μπορεί να βελτιώσει την αποδοτικότητα, την προσαρμοστικότητα και την ανθεκτικότητα αυτών των συστημάτων απέναντι σε σύγχρονεςαπειλές.

Βελτίωση Κρυπτογραφικών Αλγορίθμων

Η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί για την ανακάλυψη και τη βελτίωση κρυπτογραφικών αλγορίθμων. Μέσω της χρήσης αλγορίθμων μηχανικής μάθησης, οι ερευνητέςμπορούν να αναλύσουν τεράστια σύνολα δεδομένων και να ανακαλύψουν νέες μεθόδους κρυπτογράφησης που είναι πιο αποδοτικές και ανθεκτικές σε επιθέσεις. Για παράδειγμα, αλγόριθμοι γενετικών προγραμματισμών μπορούν να δημιουργήσουν και να

βελτιστοποιήσουν κρυπτογραφικές λειτουργίες με βάση συγκεκριμένα κριτήρια ασφαλείας και απόδοσης.

Ανίχνευση και Αντίδραση σε Απειλές

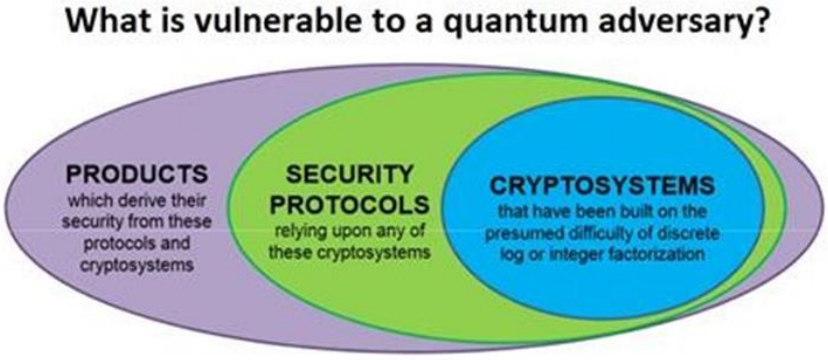
Η τεχνητή νοημοσύνη μπορεί να ενισχύσει την ανίχνευση και την αντίδραση σε κρυπτογραφικές επιθέσεις. Τα συστήματα ΤΝ, όπως τα νευρωνικά δίκτυα και τα συστήματα βαθιάς μάθησης, μπορούν να αναλύουν κυκλοφορία δεδομένων σε πραγματικό χρόνο και να εντοπίζουν ανωμαλίες που μπορεί να υποδεικνύουν προσπάθειες αποκρυπτογράφησης ή άλλες κακόβουλες δραστηριότητες. Μέσω της συνεχούς εκμάθησης, τα συστήματα αυτά μπορούν ναπροσαρμόζονται και να βελτιώνουν την ικανότητά τους να ανιχνεύουν νέες και άγνωστες απειλές.

Αυτόματη Δημιουργία Κλειδιών

Η δημιουργία κρυπτογραφικών κλειδιών είναι μια κρίσιμη διαδικασία για την ασφάλεια των δεδομένων. Η τεχνητή νοημοσύνη μπορεί να βελτιώσει αυτή τη διαδικασία μέσω της χρήσης αλγορίθμων τυχαίας γενεάς αριθμών που βασίζονται σε τεχνικές μηχανικής μάθησης. Αυτοί οι αλγόριθμοι μπορούν να παράγουν εξαιρετικά περίπλοκα και δύσκολα να προβλεφθούν κλειδιά,αυξάνοντας την ασφάλεια των συστημάτων κρυπτογράφησης.

Προστασία Εναντίον Κβαντικών Υπολογιστών

Οι κβαντικοί υπολογιστές αποτελούν μια σοβαρή απειλή για την παραδοσιακή κρυπτογραφία, καθώς έχουν τη δυνατότητα να αποκρυπτογραφούν γρήγορα δεδομένα που προστατεύονται απόκλασικούς αλγόριθμους κρυπτογράφησης. Η τεχνητή νοημοσύνη μπορεί να βοηθήσει στην ανάπτυξη κρυπτογραφικών αλγορίθμων ανθεκτικών σε κβαντικούς υπολογιστές. Με την ανάλυση των χαρακτηριστικών των κβαντικών επιθέσεων, οι αλγόριθμοι ΤΝ μπορούν να συμβάλλουν στη δημιουργία νέων μεθόδων κρυπτογράφησης που είναι ανθεκτικές σε τέτοιες επιθέσεις, διασφαλίζοντας την προστασία των δεδομένων στο μέλλον.



Ενίσχυση της Διαχείρισης Κρυπτογραφικών Κλειδιών

Η διαχείριση των κρυπτογραφικών κλειδιών είναι μια πολύπλοκη διαδικασία που απαιτεί ακρίβεια και προσοχή. Η ΤΝ μπορεί να αυτοματοποιήσει πολλές από τις διαδικασίες που εμπλέκονται στη διαχείριση των κλειδιών, όπως η αποθήκευση, η διανομή και η ανανέωση τους.Αυτό μπορεί να μειώσει τον ανθρώπινο παράγοντα και τις πιθανότητες σφάλματος, ενισχύοντας την ασφάλεια των συστημάτων.

Προγνωστική Ανάλυση

Τα συστήματα ΤΝ μπορούν να εκτελούν προγνωστική ανάλυση για να προβλέπουν πιθανούς κινδύνους και επιθέσεις προτού συμβούν. Μέσω της ανάλυσης ιστορικών δεδομένων και μοτίβων επιθέσεων, τα μοντέλα μηχανικής μάθησης μπορούν να εντοπίζουν σημάδια επικείμενων απειλών και να ειδοποιούν τους διαχειριστές ασφαλείας, επιτρέποντάς τους να λαμβάνουν προληπτικά μέτρα για την προστασία των συστημάτων κρυπτογράφησης.

Η βελτίωση των κρυπτογραφικών αλγορίθμων είναι μια συνεχής ανάγκη για την αντιμετώπιση των αυξανόμενων απειλών στην ασφάλεια των πληροφοριών. Οι αλγόριθμοι μηχανικής μάθησης και οι αλγόριθμοι γενετικών προγραμματισμών προσφέρουν νέους τρόπους για την ανακάλυψη και τη βελτιστοποίηση κρυπτογραφικών μεθόδων. Αυτές οι τεχνικές μπορούν να χρησιμοποιηθούν για την ανάπτυξη πιο ανθεκτικών και αποδοτικών κρυπτογραφικών αλγορίθμων που ανταποκρίνονται στις σύγχρονες απαιτήσεις ασφαλείας.

Βελτίωση Κρυπτογραφικών Αλγορίθμων μέσω Αλγορίθμων Μηχανικής Μάθησης και ΓενετικώνΠρογραμματισμών

Η βελτίωση των κρυπτογραφικών αλγορίθμων είναι μια συνεχής ανάγκη για την αντιμετώπιση των αυξανόμενων απειλών στην ασφάλεια των πληροφοριών. Οι αλγόριθμοι μηχανικής μάθησης και οι αλγόριθμοι γενετικών προγραμματισμών προσφέρουν νέους τρόπους για την ανακάλυψη και τη βελτιστοποίηση κρυπτογραφικών μεθόδων. Αυτές οι τεχνικές μπορούν να χρησιμοποιηθούν για την ανάπτυξη πιο ανθεκτικών και αποδοτικών κρυπτογραφικών αλγορίθμων που ανταποκρίνονται στις σύγχρονες απαιτήσεις ασφαλείας.

Αλγόριθμοι Μηχανικής Μάθησης

Οι αλγόριθμοι μηχανικής μάθησης μπορούν να συμβάλλουν στη βελτίωση των κρυπτογραφικών αλγορίθμων με διάφορους τρόπους:

- Ανίχνευση Ανωμαλιών και Αδυναμιών: Οι αλγόριθμοι μηχανικής μάθησης μπορούν να εκπαιδευτούν για την ανίχνευση ανωμαλιών σε κρυπτογραφικά συστήματα. Μέσω

της ανάλυσης μεγάλων συνόλων δεδομένων, αυτοί οι αλγόριθμοι μπορούν να εντοπίσουν μοτίβα που υποδεικνύουν αδυναμίες ή πιθανά σημεία επίθεσης. Για παράδειγμα, νευρωνικά δίκτυα και αλγόριθμοι υποστήριξης διανυσμάτων (SVM) μπορούν να χρησιμοποιηθούν για την αναγνώριση ασυνήθιστων συμπεριφορών που ενδέχεται να αποκαλύπτουν ευπάθειες σε κρυπτογραφικά πρωτόκολλα.

- Βελτιστοποίηση Παραμέτρων: Η μηχανική μάθηση μπορεί να βοηθήσει στη βελτιστοποίηση των παραμέτρων κρυπτογραφικών αλγορίθμων. Για παράδειγμα, οι αλγόριθμοι ενισχυτικής μάθησης (reinforcement learning) μπορούν να χρησιμοποιηθούν για την προσαρμογή των παραμέτρων κρυπτογράφησης έτσι ώστε να επιτυγχάνεται η βέλτιστη ασφάλεια και απόδοση. Μέσω συνεχούς εκπαίδευσης και προσαρμογής, οι αλγόριθμοι αυτοί μπορούν να βελτιώνουν τη συμπεριφορά τους με την πάροδο του χρόνου.
- Δημιουργία Νέων Κρυπτογραφικών Μεθόδων: Η μηχανική μάθηση μπορεί να χρησιμοποιηθεί για την ανάπτυξη νέων κρυπτογραφικών αλγορίθμων. Για παράδειγμα, οι γενετικοί αλγόριθμοι μπορούν να εφαρμόσουν τεχνικές όπως η γενετική βελτιστοποίηση για τη δημιουργία και την αξιολόγηση νέων κρυπτογραφικών λειτουργιών. Αυτοί οι αλγόριθμοι μπορούν να διερευνήσουν μεγάλες περιοχές του χώρου αναζήτησης για να εντοπίσουν καινοτόμες λύσεις που προσφέρουν αυξημένη ασφάλεια.

Αλγόριθμοι Γενετικών Προγραμματισμών

Οι αλγόριθμοι γενετικών προγραμματισμών είναι μια υποκατηγορία των εξελικτικών αλγορίθμων που χρησιμοποιούν έννοιες από τη βιολογία για την επίλυση προβλημάτων και μπορούν να βελτιώσουν τους κρυπτογραφικούς αλγόριθμους ως εξής:

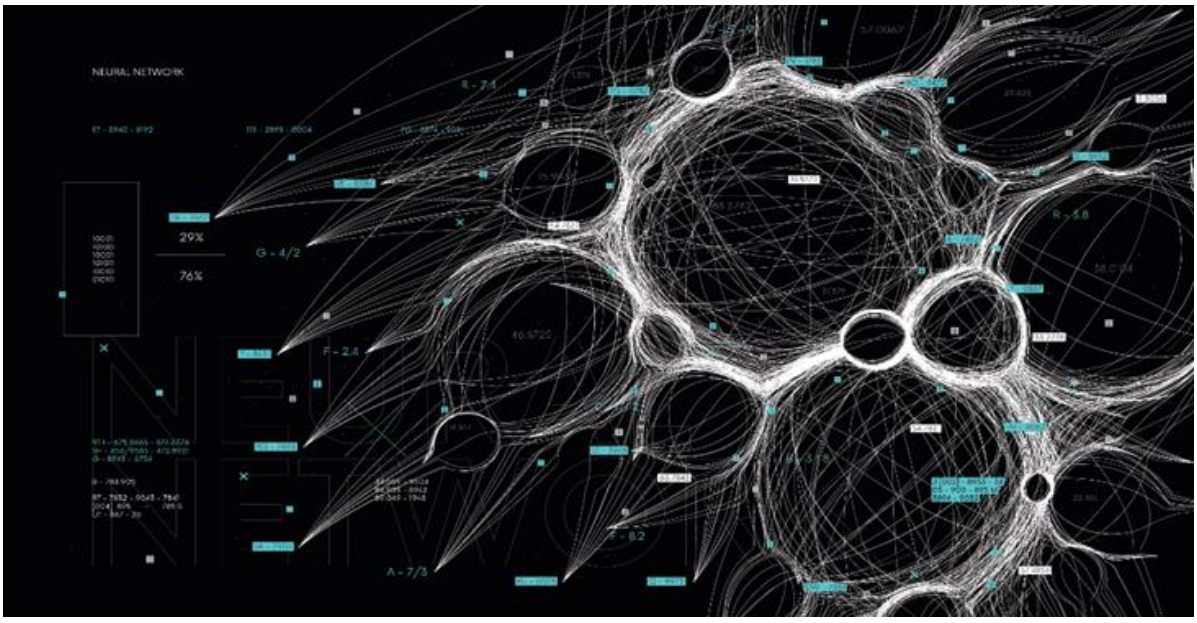
- Αυτόματη Ανακάλυψη Αλγορίθμων: Οι αλγόριθμοι γενετικών προγραμματισμών μπορούν να χρησιμοποιηθούν για την αυτόματη ανακάλυψη νέων κρυπτογραφικών αλγορίθμων. Χρησιμοποιώντας διαδικασίες όπως η αναπαραγωγή, η μετάλλαξη και η επιλογή, αυτοί οι αλγόριθμοι μπορούν να εξελίξουν νέες μορφές κρυπτογραφικών αλγορίθμων που δεν έχουν προκύψει από ανθρώπινη επινόηση. Αυτό μπορεί να οδηγήσεισε καινοτόμες και απρόσμενες λύσεις που προσφέρουν υψηλή ασφάλεια.
- Βελτιστοποίηση Υπαρχόντων Αλγορίθμων: Η βελτιστοποίηση των υφιστάμενων κρυπτογραφικών αλγορίθμων μπορεί να επιτευχθεί μέσω γενετικών

προγραμματισμών.Για παράδειγμα, ένας υπάρχων αλγόριθμος μπορεί να βελτιωθεί μέσω των γενετικών αλγορίθμων με την τροποποίηση συγκεκριμένων τμημάτων του κώδικα ή των παραμέτρων για την επίτευξη καλύτερης απόδοσης ή ασφάλειας. Αυτή η προσέγγιση επιτρέπει την ανακάλυψη των πιο αποδοτικών παραλλαγών ενός αλγορίθμου χωρίς ανθρώπινη παρέμβαση.

- Εξέλιξη και Προσαρμοστικότητα: Οι γενετικοί αλγόριθμοι είναι κατάλληλοι για την ανάπτυξη κρυπτογραφικών συστημάτων που μπορούν να εξελιχθούν και να προσαρμόζονται σε νέες απειλές. Μέσω συνεχούς εξέλιξης και προσαρμογής, αυτά τα συστήματα μπορούν να αναπτύσσουν νέες στρατηγικές κρυπτογράφησης για να ανταποκρίνονται σε νέες επιθέσεις και τεχνολογικές αλλαγές, διασφαλίζοντας ότι παραμένουν ανθεκτικά και επίκαιρα.

Η Συμβολή των Νευρωνικών Δικτύων και των Συστημάτων Deep Learning στην Ανίχνευση καιΑντιμετώπιση Απειλών

Η συνεχής αύξηση των ψηφιακών απειλών απαιτεί την ανάπτυξη προηγμένων τεχνολογιών για την ανίχνευση και την αντιμετώπισή τους. Τα νευρωνικά δίκτυα και τα συστήματα deep learningέχουν αποδείξει την αποτελεσματικότητά τους σε διάφορους τομείς της τεχνολογίας, και η ασφάλεια των πληροφοριών δεν αποτελεί εξαίρεση. Αυτές οι τεχνολογίες μπορούν να ενισχύσουν σημαντικά τις δυνατότητες ανίχνευσης και αντιμετώπισης απειλών, προσφέροντας ταχύτητα, ακρίβεια και προσαρμοστικότητα.



Ανίχνευση Ανωμαλιών

Τα νευρωνικά δίκτυα και τα συστήματα deep learning είναι εξαιρετικά αποτελεσματικά στην ανίχνευση ανωμαλιών σε μεγάλα σύνολα δεδομένων. Με τη χρήση αλγορίθμων επιτηρούμενης και μη επιτηρούμενης μάθησης, μπορούν να αναγνωρίζουν μοτίβα που υποδηλώνουν ασυνήθιστη ή κακόβουλη δραστηριότητα. Τα αυτοκωδικοποιημένα (autoencoders), για παράδειγμα, μπορούν να χρησιμοποιηθούν για την ανίχνευση ανωμαλιών με την εκπαίδευση ενός νευρωνικού δικτύου να αναπαράγει φυσιολογικά δεδομένα. Οποιαδήποτε απόκλιση από αυτά τα δεδομένα μπορεί να υποδεικνύει μια πιθανή απειλή.

Ταξινόμηση Απειλών

Τα συστήματα deep learning μπορούν να ταξινομούν διαφορετικούς τύπους απειλών με υψηλή ακρίβεια. Χρησιμοποιώντας μεγάλα σύνολα δεδομένων εκπαίδευσης που περιλαμβάνουν χαρακτηριστικά γνωστών απειλών, τα νευρωνικά δίκτυα μπορούν να μάθουν να αναγνωρίζουν και να ταξινομούν κακόβουλες δραστηριότητες, όπως ιούς, ransomware, και επιθέσεις phishing.Με τη χρήση δικτύων CNN (Convolutional Neural Networks) και RNN (Recurrent Neural Networks), τα συστήματα αυτά μπορούν να επεξεργάζονται και να αναλύουν μεγάλα καιπολύπλοκα δεδομένα, επιτυγχάνοντας εξαιρετικά αποτελέσματα.

Προγνωστική Ανάλυση

Τα συστήματα deep learning μπορούν να παρέχουν προγνωστική ανάλυση για την πρόβλεψη μελλοντικών απειλών. Μέσω της ανάλυσης ιστορικών δεδομένων και μοτίβων επιθέσεων, τα νευρωνικά δίκτυα μπορούν να εντοπίζουν σημάδια επικείμενων επιθέσεων και να προβλέπουν πιθανούς κινδύνους. Αυτή η προγνωστική ικανότητα επιτρέπει στους διαχειριστές ασφαλείας ναλαμβάνουν προληπτικά μέτρα για την προστασία των συστημάτων τους.

Ενίσχυση της Απόκρισης σε Επιθέσεις

Τα συστήματα deep learning μπορούν να αυτοματοποιήσουν και να ενισχύσουν την απόκρισησε επιθέσεις. Με τη χρήση τεχνικών reinforcement learning, τα συστήματα αυτά μπορούν να μάθουν να λαμβάνουν αποφάσεις σε πραγματικό χρόνο για την αντιμετώπιση κακόβουλων δραστηριοτήτων. Αυτό περιλαμβάνει την αυτόματη εφαρμογή κανόνων ασφαλείας, την απομόνωση μολυσμένων συστημάτων, και την προσαρμογή των ρυθμίσεων ασφαλείας για τηναποτροπή περαιτέρω επιθέσεων.

Ενίσχυση της Ανάλυσης Κακόβουλου Λογισμικού

Η ανάλυση κακόβουλου λογισμικού μπορεί να βελτιωθεί σημαντικά με τη χρήση deep learning. Τα νευρωνικά δίκτυα μπορούν να αναλύουν μεγάλες ποσότητες δεδομένων και να εντοπίζουν τα χαρακτηριστικά γνωρίσματα του κακόβουλου λογισμικού. Αυτό περιλαμβάνει την ανίχνευση υπογραφών κακόβουλου λογισμικού, την ανάλυση της συμπεριφοράς του και την αναγνώριση των μεθόδων που χρησιμοποιεί για την επίθεση και τη διασπορά.

Προστασία από Απειλές Μηδενικής Ημέρας (Zero-Day Threats)

Οι απειλές μηδενικής ημέρας είναι ιδιαίτερα επικίνδυνες επειδή εκμεταλλεύονται ευπάθειες που δεν έχουν ακόμη αναγνωριστεί και διορθωθεί. Τα συστήματα deep learning έχουν τη δυνατότητα να εντοπίζουν και να προστατεύουν τα συστήματα από τέτοιες απειλές, ακόμα και χωρίς την ύπαρξη συγκεκριμένων υπογραφών. Μέσω της ανάλυσης συμπεριφοράς και της ανίχνευσης ανωμαλιών, τα νευρωνικά δίκτυα μπορούν να εντοπίζουν ύποπτες δραστηριότητεςπου μπορεί να υποδεικνύουν μια επίθεση μηδενικής ημέρας.

Αυτοματοποίηση και Ενίσχυση της Δημιουργίας Κρυπτογραφικών Κλειδιών με Τεχνητή Νοημοσύνη

Η δημιουργία και διαχείριση κρυπτογραφικών κλειδιών αποτελεί βασικό στοιχείο για την ασφάλεια των πληροφοριών. Η τεχνητή νοημοσύνη (ΤΝ) μπορεί να προσφέρει σημαντικές βελτιώσεις σε αυτή τη διαδικασία, παρέχοντας αυτοματοποίηση, αυξημένη ασφάλεια και προσαρμοστικότητα. Σε αυτό το κείμενο, θα αναλύσουμε πώς η ΤΝ μπορεί να βοηθήσει στην αυτοματοποίηση της δημιουργίας κρυπτογραφικών κλειδιών και στην ενίσχυση της ασφάλειάς τους.

Η αυτοματοποίηση της διαδικασίας δημιουργίας κρυπτογραφικών κλειδιών μέσω της ΤΝ μπορεί να επιτευχθεί με διάφορους τρόπους:

- Χρήση Τυχαίων Γεννητριών Αριθμών με Τεχνικές Μηχανικής Μάθησης: Οι τυχαίοι αριθμοί είναι κρίσιμοι για τη δημιουργία ασφαλών κλειδιών. Παραδοσιακές μέθοδοι τυχαίας γεννήτριας αριθμών μπορεί να παρουσιάζουν προβλήματα προκαταληψίας ή προβλεψιμότητας. Η ΤΝ μπορεί να χρησιμοποιηθεί για την ανάπτυξη πιο εξελιγμένων τυχαίων γεννητριών αριθμών που βασίζονται σε τεχνικές μηχανικής μάθησης. Με την ανάλυση μεγάλων συνόλων δεδομένων, οι αλγόριθμοι μηχανικής μάθησης μπορούν να δημιουργήσουν εξαιρετικά τυχαίουςαριθμούς που είναι πιο δύσκολο να προβλεφθούν ή να αναπαραχθούν.
- Αυτόματη Ενημέρωση Κλειδιών: Η ΤΝ μπορεί να χρησιμοποιηθεί για την αυτοματοποίηση της διαδικασίας ενημέρωσης των κρυπτογραφικών κλειδιών. Με

την ανάλυση των δεδομένων και των μοτίβων χρήσης, τα συστήματα ΤΝ μπορούν να καθορίσουν πότε είναι η κατάλληλη στιγμή για την ανανέωση των κλειδιών, εξασφαλίζοντας ότι τα κλειδιά παραμένουν ασφαλή και επίκαιρα. Η αυτόματη ενημέρωση κλειδιών μπορεί να μειώσει τον κίνδυνο παραβίασης λόγω παλαιών ή συμβιβασμένων κλειδιών.

- Διαχείριση Κλειδιών: Τα συστήματα ΤΝ μπορούν να αυτοματοποιήσουν τη διαχείριση των κρυπτογραφικών κλειδιών, περιλαμβάνοντας τη δημιουργία, την αποθήκευση, τη διανομή και την ανανέωσή τους. Η αυτοματοποίηση αυτών των διαδικασιών μπορεί να μειώσει τον ανθρώπινο παράγοντα και τις πιθανότητες σφάλματος, ενώ παράλληλα αυξάνει την αποτελεσματικότητα και την ασφάλεια.

Ενίσχυση της Ασφάλειας των Κρυπτογραφικών Κλειδιών

Η ΤΝ μπορεί επίσης να ενισχύσει την ασφάλεια των κρυπτογραφικών κλειδιών με διάφορες μεθόδους:

- Ανίχνευση και Αντίδραση σε Απειλές: Τα συστήματα ΤΝ μπορούν να αναλύουν σε πραγματικό χρόνο την κυκλοφορία των δεδομένων και να εντοπίζουν πιθανές απειλές που στοχεύουν στα κρυπτογραφικά κλειδιά. Με τη χρήση τεχνικών μηχανικής μάθησης, μπορούν να αναγνωρίζουν ασυνήθιστες συμπεριφορές ή ανωμαλίες που μπορεί να υποδεικνύουν απόπειρες αποκρυπτογράφησης ή άλλες κακόβουλες δραστηριότητες. Αυτό επιτρέπει την άμεση αντίδρασηκαι την εφαρμογή μέτρων προστασίας.
- Ενίσχυση μέσω Πολυμορφισμού: Οι πολυμορφικοί αλγόριθμοι που βασίζονται σε ΤΝ μπορούν να ενισχύσουν την ασφάλεια των κρυπτογραφικών κλειδιών μεταβάλλοντας συνεχώςτη μορφή τους. Αυτή η τεχνική καθιστά πολύ πιο δύσκολη την αναγνώριση και την παραβίασητων κλειδιών από τους επιτιθέμενους, καθώς τα κλειδιά αλλάζουν συνεχώς σχήμα και δομή.
- Προστασία Εναντίον Κβαντικών Υπολογιστών: Οι κβαντικοί υπολογιστές αποτελούν μια σοβαρή απειλή για την παραδοσιακή κρυπτογραφία, καθώς μπορούν να αποκρυπτογραφούνδεδομένα πολύ γρηγορότερα από τους κλασικούς υπολογιστές. Η ΤΝ μπορεί να συμβάλλει στην ανάπτυξη κρυπτογραφικών κλειδιών που είναι ανθεκτικά σε κβαντικούς υπολογιστές. Με την ανάλυση των χαρακτηριστικών των κβαντικών επιθέσεων, οι αλγόριθμοι ΤΝ μπορούν να δημιουργούν κλειδιά που είναι πιο δύσκολο να σπάσουν ακόμα και από κβαντικούς υπολογιστές.

- Δημιουργία Ισχυρών Κλειδιών με Τεχνικές Βαθιάς Μάθησης: Τα συστήματα βαθιάς μάθησης (deep learning) μπορούν να αναλύουν τεράστια σύνολα δεδομένων και να μαθαίνουν μοτίβα που οδηγούν στη δημιουργία ισχυρών κρυπτογραφικών κλειδιών. Με τη χρήση νευρωνικών δικτύων, τα συστήματα αυτά μπορούν να δημιουργήσουν κλειδιά που είναι πιο περίπλοκα και πιο δύσκολα να παραβιαστούν. Η ικανότητα των συστημάτων βαθιάς μάθησης να μαθαίνουν και να προσαρμόζονται σε νέες απειλές καθιστά αυτά τα κλειδιά εξαιρετικά ασφαλή.

Εφαρμογές και Πλεονεκτήματα

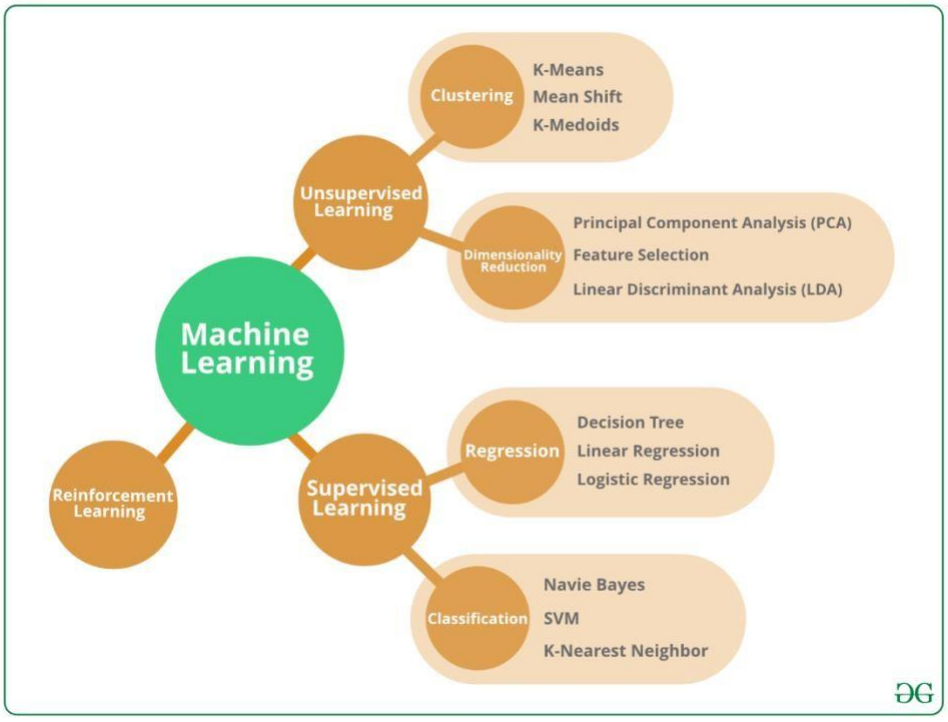
Η εφαρμογή της ΤΝ στη δημιουργία και ενίσχυση των κρυπτογραφικών κλειδιών προσφέρειπολλά πλεονεκτήματα:

- Αυξημένη Ασφάλεια: Η χρήση προηγμένων τεχνικών ΤΝ μπορεί να οδηγήσει στη δημιουργία κρυπτογραφικών κλειδιών που είναι πιο ανθεκτικά σε παραβιάσεις και επιθέσεις, αυξάνοντας την ασφάλεια των πληροφοριών. Μείωση Ανθρώπινου Παράγοντα: Η αυτοματοποίηση της διαδικασίας δημιουργίας καιδιαχείρισης κλειδιών μειώνει την ανάγκη για ανθρώπινη παρέμβαση, ελαχιστοποιώντας τα σφάλματα και τις αδυναμίες που μπορεί να προκύψουν από την ανθρώπινη εμπλοκή.
- Προσαρμοστικότητα: Τα συστήματα ΤΝ μπορούν να προσαρμόζονται συνεχώς σε νέες απειλές και να ενημερώνουν τα κλειδιά τους αναλόγως, εξασφαλίζοντας ότι παραμένουν επίκαιρα και ασφαλή.
- Αποτελεσματικότητα: Η αυτοματοποίηση των διαδικασιών δημιουργίας και διαχείρισης κλειδιών εξοικονομεί χρόνο και πόρους, επιτρέποντας στους διαχειριστές να επικεντρωθούν σε άλλες κρίσιμες πτυχές της ασφάλειας των πληροφοριών.

Βελτίωση της Προγνωστικής Ανάλυσης στα Συστήματα Κρυπτογραφίας

Η προγνωστική ανάλυση είναι μια κρίσιμη τεχνολογία για την ασφάλεια των πληροφοριών, καθώς επιτρέπει τον εντοπισμό και την αντιμετώπιση απειλών πριν αυτές προκαλέσουν ζημιά. Στα συστήματα κρυπτογραφίας, η προγνωστική ανάλυση μπορεί να χρησιμοποιηθεί για την πρόβλεψη επιθέσεων, την ενίσχυση της ασφάλειας και την προσαρμογή των κρυπτογραφικώνμεθόδων σε νέες απειλές. Υπάρχουν αρκετοί τρόποι με τους οποίους η

προγνωστική ανάλυσημπορεί να βελτιωθεί και να γίνει πιο αποτελεσματική στα συστήματα κρυπτογραφίας.

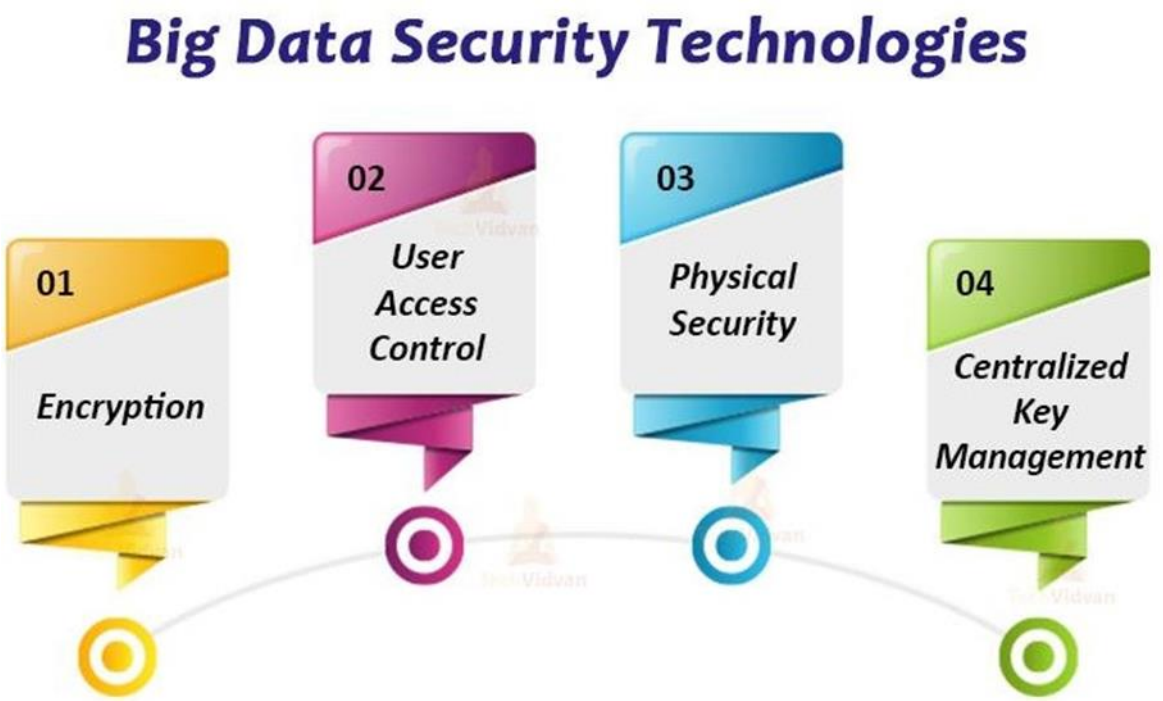


Η βελτίωση της προγνωστικής ανάλυσης μπορεί να επιτευχθεί με την ενσωμάτωση προηγμένων αλγορίθμων μηχανικής μάθησης και βαθιάς μάθησης. Οι αλγόριθμοι αυτοί μπορούν να αναλύουν μεγάλα σύνολα δεδομένων και να εντοπίζουν πρότυπα που υποδεικνύουν επικείμενεςαπειλές.

Τα νευρωνικά δίκτυα, ειδικά τα συστήματα βαθιάς μάθησης (deep learning), έχουν τη δυνατότητα να αναλύουν πολύπλοκα δεδομένα και να μαθαίνουν από αυτά. Με τη χρήση δικτύων CNN (Convolutional Neural Networks) και RNN (Recurrent Neural Networks), τα συστήματα αυτά μπορούν να προβλέπουνεπιθέσεις με βάση ιστορικά δεδομένα και μοτίβα δραστηριότητας.

Η ενισχυτική μάθηση (reinforcement learning) μπορεί να χρησιμοποιηθεί για την προσαρμογή των κρυπτογραφικών συστημάτων σε πραγματικό χρόνο. Οι αλγόριθμοι αυτοί μπορούν να μάθουν από το περιβάλλον και να βελτιώνουν συνεχώς τις στρατηγικές ασφάλειας, λαμβάνοντας υπόψη τις αλλαγές στα μοτίβααπειλών.

Ενσωμάτωση Μεγάλων Δεδομένων (Big Data)



Η ανάλυση μεγάλων δεδομένων μπορεί να προσφέρει σημαντική βελτίωση στην προγνωστική ανάλυση κρυπτογραφικών συστημάτων. Η συλλογή και ανάλυση μεγάλων ποσοτήτων δεδομένων από διαφορετικές πηγές μπορεί να προσφέρει μια πιο ολοκληρωμένη εικόνα των πιθανών απειλών.

Προσαρμοστικότητα και Αυτονομία

Η ικανότητα των κρυπτογραφικών συστημάτων να προσαρμόζονται σε νέες απειλές είναι κρίσιμη για την αποτελεσματική προγνωστική ανάλυση. Η χρήση της ΤΝ μπορεί να ενισχύσει αυτή την προσαρμοστικότητα.

Συμπέρασμα

Η υλοποίηση ενός σύγχρονου και ασφαλούς κρυπτογραφικού συστήματος αποτελεί μια σύνθετη και πολυδιάστατη διαδικασία που περιλαμβάνει τον καθορισμό απαιτήσεων, την επιλογή αλγορίθμων, τον σχεδιασμό πρωτοκόλλων, την ανάπτυξη λογισμικού, τη δοκιμή και επαλήθευση, την εφαρμογή και την παρακολούθηση, καθώς και τη συνεχή βελτίωση. Οι βασικέςπτυχές της διαδικασίας αυτής, όπως έχουν αναλυθεί, μπορούν να συνοψιστούν ως εξής:

- Καθορισμός Απαιτήσεων και Στόχων: Η αρχική φάση περιλαμβάνει την ανάλυση των αναγκών ασφαλείας και την ταυτοποίηση πιθανών απειλών. Ο καθορισμός σαφών στόχων είναι κρίσιμος για την κατεύθυνση της ανάπτυξης του συστήματος.
- Επιλογή Κρυπτογραφικών Αλγορίθμων: Η επιλογή των κατάλληλων κρυπτογραφικώναλγορίθμων, είτε συμμετρικών (όπως το AES) είτε ασύμμετρων (όπως το RSA), είναι θεμελιώδης για την ασφάλεια και την απόδοση του συστήματος. Οι αλγόριθμοι κατακερματισμού όπως οι SHA-256 και SHA-3 εξασφαλίζουν την ακεραιότητα των δεδομένων.
- Σχεδιασμός Πρωτοκόλλων: Η δημιουργία ασφαλών πρωτοκόλλων ανταλλαγής κλειδιών (όπως το Diffie-Hellman) και η διασφάλιση της διαδικασίας κρυπτογράφησης και αποκρυπτογράφησης είναι απαραίτητες για την αποτελεσματικότητα του συστήματος.
- Ανάπτυξη Λογισμικού: Η χρήση κρυπτογραφικών βιβλιοθηκών και η επιλογή κατάλληλων γλωσσών προγραμματισμού διευκολύνει την ανάπτυξη αποδοτικού και ασφαλούς λογισμικού. Η υλοποίηση των αλγορίθμων και των πρωτοκόλλων πρέπει ναείναι ακριβής και ασφαλής.
- Δοκιμή και Επαλήθευση: Η εκτενής δοκιμή και επαλήθευση, μέσω τεχνικών όπως οι δοκιμές διείσδυσης και οι δοκιμές μονάδας, διασφαλίζουν ότι το σύστημα είναι ασφαλέςκαι λειτουργικό. Οι δοκιμές αυτές είναι κρίσιμες για την ανθεκτικότητα του συστήματοςαπέναντι σε επιθέσεις.
- Ανάπτυξη και Εφαρμογή: Η εγκατάσταση και η σωστή διαμόρφωση του συστήματος, καθώς και η εκπαίδευση των χρηστών, είναι ζωτικής σημασίας για την επιτυχία της εφαρμογής του. Η σωστή χρήση και η συνεχής παρακολούθηση του συστήματος βοηθούν στην έγκαιρη ανίχνευση και αντιμετώπιση τυχόν προβλημάτων.
- Συνεχής Βελτίωση: Η συλλογή ανατροφοδότησης και η συνεχιζόμενη βελτίωση του συστήματος εξασφαλίζουν την προσαρμογή του στις νέες απειλές και την ενσωμάτωσηνέων τεχνολογιών. Η τακτική ενημέρωση και η βελτιστοποίηση των αλγορίθμων διατηρούν την ασφάλεια και την αποδοτικότητα του συστήματος σε υψηλό επίπεδο.
- Η συνεργασία των ανθρώπων με τις μηχανές, μέσω της χρήσης τεχνητής νοημοσύνης και αλγορίθμων μηχανικής μάθησης, μπορεί να βελτιώσει σημαντικά την ανίχνευση ανωμαλιών και αδυναμιών, να αυτοματοποιήσει τη δημιουργία και ενίσχυση κρυπτογραφικών κλειδιών και να βελτιώσει τη συνολική απόδοση και ασφάλεια του συστήματος. Η χρήση τεχνολογιών όπως τα νευρωνικά δίκτυα και το

deep learning προσφέρει νέες δυνατότητες στην κρυπτογραφία, συμβάλλοντας στην ανίχνευση και αντιμετώπιση απειλών με πιο αποδοτικό και αποτελεσματικότρόπο.

Συνολικά, η προσεκτική και συστηματική προσέγγιση σε κάθε βήμα της υλοποίησης ενός κρυπτογραφικού συστήματος, σε συνδυασμό με την αξιοποίηση των δυνατοτήτων της τεχνητήςνοημοσύνης, μπορεί να οδηγήσει σε δημιουργία ισχυρών, ασφαλών και αποδοτικών συστημάτων που ανταποκρίνονται στις σύγχρονες ανάγκες και απειλές

.

Βιογραφικό συντάκτη

Ο ΥΕΑ (ΕΠ) Πασχάλης Θεόδωρος είναι απόφοιτος του τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστήμιου Αιγαίου. Κατέχει γνώσεις προγραμματισμού και εκτενείς γνώσεις πάνω σε θέματα κυβερνοασφάλειας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

S. Katzenbeisser, I. Polian, F. Regazzoni and M. Stöttinger, "Security in Autonomous Systems," 2019 IEEE European Test Symposium (ETS), Baden-Baden, Germany, 2019, pp. 1-8, doi: 10.1109/ETS.2019.8791552. keywords: {Autonomous systems;Cryptography;Automobiles;Sensors;Computer security;Machine learning algorithms},
Blackledge, J. & Mosola, N. (2020) Applications of Artificial Intelligence to Cryptography,Transactions onMachine Learning & Artifical Intellengence6th June 2020. doi:10.14738/tmlai.83.8219

Almalawi, A., Hassan, S., Fahad, A. et al. A Hybrid Cryptographic Mechanism for Secure Data Transmission in Edge AI Networks. Int J Comput Intell Syst 17, 24 (2024). https://doi.org/10.1007/s44196-024-00417-8
Ali, S.; Rehman, S.U.; Imran, A.; Adeem, G.; Iqbal, Z.; Kim, K.-I. Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection. Electronics 2022, 11, 3934. https://doi.org/10.3390/electronics11233934
Bin Li, Yuhao Feng, Zenggang Xiong, Weidong Yang, Gang Liu,Research on AI security enhanced encryption algorithm of autonomous IoT systems,Information Sciences,Volume 575,2021,Pages 379-398,ISSN 0020-0255 https://doi.org/10.1016/j.ins.2021.06.016. https://www.sciencedirect.com/science/article/pii/S0020025521006071
Stypiński, M.; Niemiec, M. Security of Neural Network-Based Key Agreement Protocol for Smart Grids. Energies 2023, 16, 3997. https://doi.org/10.3390/en16103997
Mohammed M. Alani. 2019. Applications of machine learning in cryptography: a survey. In Proceedings of the 3rd International Conference on Cryptography ,
Security and Privacy (ICCSP '19). Association for Computing Machinery, New York, NY, USA, 23–27. https://doi.org/10.1145/3309074.3309092
Nandkumar Niture . Machine Learning and Cryptographic Algorithms -- Analysis and Design in Ransomware and Vulnerabilities Detection. TechRxiv. October 29, 2020.
DOI: 10.36227/techrxiv.13146866.v1
R. Aiyshwariya Devi, A.R. Arunachalam,
Enhancement of IoT device security using an Improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM,High- Confidence Computing,Volume 3, Issue 2,2023,100117,ISSN 26672952, https://doi.org/10.1016/j.hcc.2023.100117. https://www.sciencedirect.com/science/article/pii/S2667295223000156

Nair, M.M., Deshmukh, A. and Tyagi, A.K. (2024). Artificial Intelligence for Cyber Security. In Automated Secure Computing for Next-Generation Systems, A.K. Tyagi (Ed.). https://doi.org/10.1002/9781394213948.ch5
Tianqi Zhou, Chen Wang, Wenying Zheng, Haowen Tan,
Secure and efficient authenticated group key agreement protocol for AI-based automation systems,ISA Transactions,Volume 141,2023,Pages 1-9,ISSN 0019-0578, https://doi.org/10.1016/j.isatra.2023.04.010.
MANOHARAN, Ashok; SARKER, Mithun. Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. DOI: https://www. doi. org/10.56726/IRJMETS32644, 2023, 1.

Παρουσίαση των νομικών ζητημάτων που επιφέρει ή πιθανολογείται ότι θα επιφέρει η εκτεταμένη χρήση της τεχνητής νοημοσύνης

Υπλγος(ΝΟΜ) Παπαγγέλου Άννα

Εισαγωγή

Οι αρχές του 21ου αιώνα αποτέλεσαν σημείο εκκίνησης μιας περιόδου ραγδαίων τεχνολογικών εξελίξεων για την ανθρωπότητα. [1] Η ταχύτητα ανάπτυξης, το εύρος της καινοτομίας και η εκ βάθρων αναθεώρηση των υφιστάμενων δυνατοτήτων συνέβαλλαν στη θεώρηση ότι βιώνουμε μια τέταρτη βιομηχανική επανάσταση. [2] Πρόκειται για ένα νέο κεφάλαιο στην ανθρώπινη εξέλιξη που περιλαμβάνει τεχνολογίες όπως η τεχνητή νοημοσύνη, οι οποίες συνδέουν άρρηκτα τον πραγματικό με τον ψηφιακό κόσμο [3] και υπόσχονται πολλαπλά οφέλη για τις κοινωνίες και τους ανθρώπους. [4]

Η τεχνητή νοημοσύνη αποτελεί καθοριστικής σημασίας τεχνολογία με πολυάριθμες εφαρμογές. [5] Συνοπτικά, αναφέρεται στην υλοποίηση υπολογιστικών συστημάτων που αναπαράγουν τις γνωστικές λειτουργίες ενός ανθρώπου, όπως είναι ενδεικτικά η μάθηση, ο σχεδιασμός και η δημιουργικότητα, η προσαρμοστικότητα, η εξαγωγή συμπερασμάτων και η επίλυση προβλημάτων. [6] Τα συστήματα τεχνητής νοημοσύνης είναι συστήματα λογισμικού που σχεδιάζονται αποσκοπώντας στην επίτευξη ενός σύνθετου στόχου, αντιλαμβάνονται το περιβάλλον τους μέσω της απόκτησης δεδομένων, προβαίνουν σε συλλογισμούς βάσει της ερμηνείας των εισαγόμενων δεδομένων και προβαίνουν στις βέλτιστες απαιτούμενες ενέργειες για την υλοποίηση του επιδιωκόμενου στόχου. [1] [7] [8] Τα σύγχρονα συστήματα τεχνητής νοημοσύνης είναι ικανά να προσαρμόζουν ως ένα βαθμό τη συμπεριφορά τους αναλύοντας τις συνέπειες προηγούμενων δράσεων και επιλύοντας προβλήματα με αυτονομία. [9]

Η τεχνητή νοημοσύνη διαδραματίζει κεντρικό ρόλο στον ψηφιακό μετασχηματισμό της κοινωνίας μας. [10] Χρησιμοποιείται ευρέως σε επιστημονικές, εμπορικές και

στρατιωτικές εφαρμογές, καθώς και σε ποικίλες διαδικασίες λήψης αποφάσεων, όπως σε νομικές και ιατρικές διεργασίες, αποφέροντας σημαντικά οφέλη. [5] Ωστόσο, ορισμένες εφαρμογές ΤΝ, μπορεί επίσης να έχουν αρνητικές επιπτώσεις, οι οποίες ενδεχομένως να είναι δύσκολο να προβλεφθούν, να προσδιοριστούν ή να μετρηθούν. [4]

Είναι γεγονός ότι η εκθετική διάδοση των συστημάτων τεχνητής νοημοσύνης δημιούργησε ένα σοβαρό κενό δικαίου, δεδομένου ότι η ανθρώπινη δραστηριότητα αποτελούσε παραδοσιακά το ρυθμιστικό αντικείμενο των νομικών διατάξεων. [11] Επιπρόσθετα, η αυξανόμενη αυτονομία των συστημάτων τεχνητής νοημοσύνης κατέστησε παρωχημένη κάθε προηγούμενη απόπειρα νομοθετικής ρύθμισης της δράσης τους. [5] Τα σύγχρονα νομικά συστήματα καλούνται λοιπόν να αντιμετωπίσουν μια άνευ προηγουμένου σειρά από προκλήσεις. [6]

Πιθανές συγκρούσεις με θεμελιώδη δικαιώματα

Τεχνητή νοημοσύνη και ανθρώπινη αξιοπρέπεια

Πρωταρχικό ζήτημα αποτελεί η συμμόρφωση των συστημάτων τεχνητής νοημοσύνης με τα θεμελιώδη δικαιώματα, όπως η αξιοπρέπεια, οι ελευθερίες, η ισότητα, τα δικαιώματα των πολιτών και η δικαιοσύνη. [4] Η κοινή βάση που συνενώνει τα εν λόγω δικαιώματα μπορεί να θεωρηθεί ότι εδράζεται στον σεβασμό στην ανθρώπινη αξιοπρέπεια, θεμελιώδη αρχή του διεθνούς δικαίου των ανθρωπίνων δικαιωμάτων και μήτρα των αρχών της ελευθερίας, της δικαιοσύνης και της ειρήνης, της ισότητας, της πνευματικής ανάπτυξης, και της κοινωνικής προόδου και ανάπτυξης. [7] Η ανθρώπινη αξιοπρέπεια περικλείει την ιδέα ότι κάθε ανθρώπινο ον έχει μια εγγενή αξία, η οποία δεν πρέπει ποτέ να υποβαθμίζεται, να παραβιάζεται ή να καταστέλλεται. [10] Επομένως, τα συστήματα τεχνητής νοημοσύνης θα πρέπει να αναπτυχθούν κατά τέτοιον τρόπο ώστε να σέβονται, να εξυπηρετούν και να προστατεύουν τη σωματική και πνευματική ακεραιότητα του ανθρώπου, την προσωπική και πολιτισμική αίσθηση της ταυτότητας και την ικανοποίηση των βασικών αναγκών του. [7]

Διακινδύνευση της αξιοπρέπειας και της ελευθερίας του ατόμου

Η αξιοπρέπεια και η ελευθερία του ατόμου παραβλάπτονται σε περιπτώσεις διακινδύνευσης της αυτονομίας και της ψυχικής υγείας, αδικαιολόγητης επιτήρησης, εξαπάτησης και αθέμιτης χειραγώγησης. [10] Η τεχνητή νοημοσύνη αποτελεί αυξανόμενη απειλή για το δικαίωμα των ανθρώπων να λαμβάνουν αυτόνομες αποφάσεις. [5]

Παρατηρείται έλλειμα διαφάνειας κατά την εφαρμογή τεχνολογιών τεχνητής νοημοσύνης, καθώς συχνά οι χρήστες βρίσκονται σε σύγχυση αναφορικά με την αλληλεπίδρασή τους με συστήματα τεχνητής νοημοσύνης ή με φυσικά πρόσωπα, ενώ παράλληλα δεν έχουν επίγνωση του τρόπου λειτουργίας και λήψης αποφάσεων των αλγορίθμων που χρησιμοποιούνται, (νοημοσύνη, 2019) είτε εξαιτίας της πολυπλοκότητάς τους, είτε επειδή οι πληροφορίες αυτές αποκρύπτονται στο πλαίσιο προστασίας της πνευματικής ιδιοκτησίας των δημιουργών τους. [5] Επιπρόσθετα, η τεχνητή νοημοσύνη απαιτεί πρόσβαση σε εκτεταμένα σύνολα δεδομένων, σε πολλές περιπτώσεις, ευαίσθητα, συμπεριλαμβανομένων δεδομένων για τη φυλή, εθνικότητα, φύλο και άλλα χαρακτηριστικά. [9] Ενδεικτικό παράδειγμα αποτελούν τεχνολογίες που συγκεντρώνουν δεδομένα κινητικότητας, καθώς συσκευές Internet των Πραγμάτων (IoT) που συλλέγουν ευαίσθητα δεδομένα, όπως δεδομένα υγείας). [12] Αθέμιτες μορφές αξιοποίησης των δεδομένων αυτών παραβιάζουν το δικαίωμα στην προστασία της ιδιωτικότητας των χρηστών. [13] Προσβολή των ανωτέρω δικαιωμάτων υφίσταται και σε περιπτώσεις αυθαίρετης χρήσης προσωπικών και μη δεδομένων για την ταξινόμηση και δημιουργία προφίλ ατόμων, [3] με σκοπό την εκμετάλλευση πιθανών ευπαθειών και δημιουργία προβλέψεων για την χειραγώγησή τους. [6]

Διακινδύνευση της ισότητας και της απαγόρευσης των διακρίσεων

Η χρήση της τεχνητής νοημοσύνης μπορεί να διακινδυνεύσει την ισότητα και την απαγόρευση των διακρίσεων. [5] Η εφαρμογή αλγορίθμων τεχνητής νοημοσύνης σε τομείς όπως οι κοινωνικές υπηρεσίες δύναται να δημιουργήσει ψηφιακούς φραγμούς για εκείνους που δεν έχουν πρόσβαση στην τεχνολογία ή δεν έχουν ψηφιακές δεξιότητες. [7] Αυτό μπορεί να επηρεάσει αρνητικά δικαιώματα, όπως η πρόσβαση στην εργασία, τη διατροφή και τη στέγαση. [5] Οι αλγόριθμοι είναι δυνατό να οδηγούν σε αποτελέσματα που χαρακτηρίζονται από αθέμιτη μεροληψία, όταν τα δεδομένα που τους τροφοδοτούν εμπεριέχουν προκαταλήψεις, είτε τα δεδομένα αυτά είναι ελλιπή ή μη αντιπροσωπευτικά. [13] Αυτό μπορεί να οδηγήσει σε αθέμιτες διακρίσεις και να ενισχύσει υφιστάμενες κοινωνικές ανισότητες. [6] Για παράδειγμα, εάν τροφοδοτούμε την βάση δεδομένων του αλγόριθμου με δεδομένα που δείχνουν ότι η πλειονότητα των θέσεων ευθύνης στο εργασιακό περιβάλλον καταλαμβάνονται από άνδρες, ο αλγόριθμος τεχνητής νοημοσύνης κατανοεί ότι η εταιρεία προσπαθεί να προσλάβει έναν άνδρα, ακόμα και όταν αυτό δεν αποτελεί εμφανές και σαφές κριτήριο της θέσης εργασίας. [8] Επιπλέον, η προκατάληψη στα δεδομένα μπορεί να προκαλέσει διακρίσεις, τόσο στα εργαλεία

προβλέψεων της αστυνόμευσης όσο και στις εφαρμογές αναγνώρισης προσώπου σε πραγματικό χρόνο. [5]

Διακινδύνευση των δικαιωμάτων των πολιτών

Τα συστήματα ΤΝ προσφέρουν σημαντικές ευκαιρίες βελτίωσης στην έκταση και στην αποτελεσματικότητα της διακυβέρνησης, ενισχύοντας την παροχή δημόσιων υπηρεσιών και αγαθών προς την κοινωνία. [14] Ταυτόχρονα όμως, τα δικαιώματα των πολιτών, μεταξύ των οποίων το δικαίωμα ψήφου, το δικαίωμα στη χρηστή διοίκηση, την πρόσβαση σε δημόσια έγγραφα και το δικαίωμα υποβολής αναφοράς στη διοίκηση, είναι δυνατό να επηρεαστούν αρνητικά από τις εφαρμογές της τεχνητής νοημοσύνης. [10] Η χρήση τεχνητής νοημοσύνης στη διαχείριση πληροφοριών μπορεί να οδηγήσει σε περιορισμό της πρόσβασης των πολιτών σε δημόσια έγγραφα ή πληροφορίες που επηρεάζουν τις αποφάσεις της διοίκησης. [13] Επιπρόσθετα, η επηρεασμένη ή ψευδής πληροφορία που διαδίδεται μέσω αλγορίθμων τεχνητής νοημοσύνης μπορεί να απειλήσει την αντικειμενική διαμόρφωση της δημόσιας άποψης και να παρεμποδίσει την ελεύθερη και ενημερωμένη συζήτηση για πολιτικά θέματα. [9] [8] Ακόμη, η χρήση τεχνητής νοημοσύνης σε πολιτικές αποφάσεις μπορεί να αυξήσει τον κίνδυνο κατάχρησης εξουσίας, καθώς οι αλγόριθμοι μπορεί να εφαρμόζονται χωρίς την αναγκαία διαφάνεια και εποπτεία. [14]

Διακινδύνευση των δικαιωμάτων πνευματικής ιδιοκτησίας

Αναφορικά με την προστασία της πνευματικής ιδιοκτησίας, η αυθαίρετη αξιοποίηση έργων πνευματικής ιδιοκτησίας από εφαρμογές τεχνητής νοημοσύνης δύναται να εγείρει ζητήματα πνευματικής κλοπής ή παραβίασης πνευματικών δικαιωμάτων. [15] Επιπρόσθετα, ανακύπτουν προβληματισμοί σχετικά με την απόδοση ευθύνης για τυχόν παραβιάσεις πνευματικών δικαιωμάτων που σχετίζονται με τα έργα που παράγονται από τεχνητή νοημοσύνη. Εν γένει, η δημιουργία έργων χρησιμοποιώντας την τεχνητή νοημοσύνη απαιτεί νέες νομικές προσεγγίσεις. [16] Παραδοσιακά, η προστασία της πνευματικής ιδιοκτησίας αφορούσε σε έργα που είναι ανθρώπινες δημιουργίες. [9] Για τον λόγο αυτό, η κυριότητα των έργων που δημιουργούνται με τη χρήση υπολογιστή δεν ήταν υπό αμφισβήτηση, επειδή το πρόγραμμα ήταν απλώς ένα εργαλείο που υποστήριζε τη δημιουργική διαδικασία. [16] Ωστόσο, πλέον η τεχνητή νοημοσύνη χρησιμοποιείται για να δημιουργεί έργα μουσικής, δημοσιογραφίας, καθώς και παιχνίδια, λαμβάνοντας αποφάσεις επί της δημιουργικής διαδικασίας, χωρίς ανθρώπινη παρέμβαση. [9]

Συνεπώς, μη εντασσόμενα στο υφιστάμενο νομικό πλαίσιο, τα έργα αυτά δεν απολαμβάνουν νομικής προστασίας. [16]

Νομικοί προβληματισμοί από τις εφαρμογές της τεχνητής νοημοσύνης σε κρίσιμους τομείς

Η χρήση της τεχνητής νοημοσύνης στην απονομή της δικαιοσύνης

Η ενσωμάτωση εφαρμογών τεχνητής νοημοσύνης στο δικαστικό σύστημα εγείρει πολλούς νομικούς προβληματισμούς. [3] Ειδικότερα, είναι δυνατό να προκύψουν ζητήματα δικαιοσύνης, όπως η έλλειψη διαφάνειας, αντικειμενικότητας και ισότητας πρόσβασης στη δικαιοσύνη. [8] Οι πρώτες απόπειρες χρήσης της τεχνητής νοημοσύνης στο νομικό κόσμο αφορούσαν κυρίως στην οργάνωση πληροφοριών. [7] Σήμερα, εργαλεία τεχνητής νοημοσύνης δύνανται να συμβουλεύουν επαγγελματίες, να προβλέπουν πιθανά αποτελέσματα των δικαστικών αποφάσεων, ενώ σε πειραματικό στάδιο εφαρμόζονται και προς επικουρία ή προς υποκατάσταση του φυσικού δικαστή. [7] Οι κίνδυνοι που προκύπτουν από την αξιοποίηση της τεχνητής νοημοσύνης στην απονομή της δικαιοσύνης περιλαμβάνουν την αυξημένη μεροληπτικότητα απέναντι σε συγκεκριμένες κατηγορίες κατηγορούμενων. [7] Σε περιπτώσεις που οι αλγόριθμοι αναπαράγουν στερεοτυπικές αντιλήψεις, είτε λόγω ελαττωμάτων στον προγραμματισμό τους, είτε λόγω των δεδομένων που τους τροφοδοτούν, είναι δυνατό να προκύψουν διαφορετικά αποτελέσματα για άτομα που κατηγορούνται για το ίδιο έγκλημα. [13] Επιπρόσθετα, η έλλειψη διαφάνειας ως προς τα δεδομένα και τις μεθόδους που χρησιμοποιούν οι αλγόριθμοι υποβαθμίζει το δικαίωμα στη δίκαιη δίκη. [7] Όσον αφορά στην υποκατάσταση του φυσικού δικαστή, το βασικό επιχείρημα για την αμφισβήτηση της αποτελεσματικότητας μιας τέτοιας προσπάθειας, συνίσταται στο γεγονός ότι οι δικαστικές αποφάσεις αποτυπώνουν πέρα από την αξιολόγηση των πραγματικών περιστατικών και αξιολογήσεις που προκύπτουν με βάση τη συνείδηση και την ηθική του δικαστή, οι οποίες μάλιστα αντανακλούν κάθε φορά την κρατούσα κοινή αντίληψη των μελών μιας συγκεκριμένης γεωγραφικά κοινωνίας. [8] Η προοπτική συνεπώς, να δημιουργηθούν υπολογιστικά συστήματα στα οποία θα ανατεθεί αυτή η ηθική αξιολόγηση αντιμετωπίζεται με σκεπτικισμό. [8]

Η χρήση της τεχνητής νοημοσύνης στον τομέα της υγείας

Η χρήση τεχνητής νοημοσύνης σε ευαίσθητους τομείς, όπως η ιατρική διάγνωση και θεραπεία, εγείρει προβληματισμούς σχετικά με την ασφάλεια, τη διαφάνεια, τη διαλειτουργικότητα, την αποτελεσματικότητα και την αξιοπιστία των συστημάτων τεχνητής νοημοσύνης. [10] Ειδικότερα, η τροφοδότηση των αλγορίθμων με μη έγκυρα ή ελλιπή δεδομένα μπορεί να οδηγήσει σε λανθασμένη διάγνωση ή ανεπιθύμητα αποτελέσματα. [7] Ομοίως, είναι δυνατό να διαιωνίζονται προκαταλήψεις και να σημειώνονται περιστατικά διακριτικής μεταχείρισης των ασθενών. [6] Είναι κρίσιμη συνεπώς, η τροφοδότηση των αλγορίθμων με αξιόπιστα δεδομένα. Ένα ακόμα κρίσιμο ζήτημα, αποτελεί η πιθανή επιδείνωση των ανισοτήτων στην παροχή υγειονομικής περίθαλψης, όταν δεν λαμβάνονται υπόψη παράγοντες, όπως η δυνατότητα πρόσβασης στην τεχνολογία και οι κοινωνικοοικονομικές διαφορές. [17] Επιπρόσθετα, ενδέχεται να παραβιάζονται δικαιώματα των ασθενών, όπως η ενημέρωση, η συγκατάθεση και το απόρρητο, εξαιτίας της έλλειψης διαφάνειας σχετικά με τις διαδικασίες που ακολουθούν οι εφαρμογές τεχνητής νοημοσύνης, καθώς και εξαιτίας του τρόπου που διαχειρίζονται τα ευαίσθητα ιατρικά δεδομένα. [17]

Η χρήση της τεχνητής νοημοσύνης στις στρατιωτικές επιχειρήσεις

Η χρήση της τεχνητής νοημοσύνης στον τομέα της άμυνας και της ασφάλειας αναμένεται να αλλάξει άρδην τον τρόπο που διεξάγονται έως σήμερα οι στρατιωτικές επιχειρήσεις. [18] Η εισαγωγή αυτόνομων συστημάτων για τον καθοδήγηση πυραύλων ή drones, έχει προκαλέσει προβληματισμό ως προς τη συμμόρφωση σε αρχές του διεθνούς δικαίου του πολέμου, όπως οι αρχές της διάκρισης, της αναλογικότητας και της ανθρωπιάς. [7] Πιο συγκεκριμένα, ανάλογα το επίπεδο αυτονομίας τους, απαντώνται συστήματα, όπου οι κύριες αποφάσεις, όπως η εκτόξευση όπλων, λαμβάνονται πάντα από ένα άτομο, άλλα συστήματα που λειτουργούν αυτόνομα υπό την επίβλεψη ενός ανθρώπου που μπορεί να διακόψει δραστηριότητες, και άλλα συστήματα που ολοκληρώνουν την αποστολή τους χωρίς καμία ανθρώπινη επίβλεψη. [18] Τα τελευταία έχουν προκαλέσει σοβαρές ανησυχίες και συζητήσεις σε πολλά επίπεδα [6] Ειδικότερα, επισημαίνεται ο κίνδυνος της απουσίας ανθρώπινης επίβλεψης και παρέμβασης, που μπορεί να οδηγήσει σε ατυχήματα ή ακόμα και σε εγκλήματα πολέμου. [7] Επιπρόσθετα, η ικανότητα ενός αυτόνομου συστήματος να αναγνωρίζει στόχους θέτει προβληματισμούς όσον αφορά στη σωστή αναγνώριση και διάκριση στόχων, καθώς και στον κίνδυνο σφαλμάτων ή συστηματικών αστοχιών. [7] Ακολούθως, η απουσία

ανθρώπινης επίβλεψης μπορεί να δυσκολεύει την προσδιορισμό της ευθύνης σε περίπτωση ατυχήματος ή κατάχρησης. [5]

Ζητήματα λογοδοσίας

Η εισαγωγή υπερβολικής αυτονομίας σε συστήματα τεχνητής νοημοσύνης θέτει σημαντικά ζητήματα ποινικής και αστικής ευθύνης, όταν προκαλούνται ζημίες σε τρίτους. [5] [8] Η δυνατότητα των μηχανών να λαμβάνουν αποφάσεις με τόσο μεγάλο βαθμό αυτονομίας, που δεν μπορούν αποτελεσματικά να ελεγχθούν από τον άνθρωπο και να αποδοθούν στην ανθρώπινη κρίση, όπως στην περίπτωση συστημάτων που μαθαίνουν από την εμπειρία τους, καθιστά την υπαιτιότητα δυσδιάκριτη. [3] Δεδομένου ότι, η αρχική προγραμματιστική διαδικασία δεν προβλέπει όλες τις πιθανές επιλογές που μπορεί να κάνει η μηχανή, δυσχεραίνεται ο καθορισμός της ανθρώπινης ευθύνης για τις παραγόμενες ενέργειες. [5] Ταυτόχρονα όμως, η ανάγκη για λογοδοσία επιτάσσει να δημιουργηθούν επαρκείς μηχανισμοί για την ανάληψη ευθυνών αναφορικά με τις ενέργειες των συστημάτων τεχνητής νοημοσύνης και τα αποτελέσματά τους, τόσο πριν όσο και μετά την εφαρμογή τους. [4] [10]

Συμπεράσματα - Προτάσεις

Από την ανωτέρω απόπειρα ανάλυσης των προκλήσεων που σχετίζονται με την αυξανόμενη χρήση συστημάτων τεχνητής νοημοσύνης, προκύπτει αδιαμφισβήτητα η αναγκαιότητα μιας ολιστικής προσέγγισης βασισμένης σε κοινές αξίες και θεμέλια. [10] Προκειμένου να επιτευχθεί αυτό, κεντρικό ρόλο στην ανάπτυξη, χρήση και παρακολούθηση των εφαρμογών τεχνητής νοημοσύνης θα πρέπει να διαδραματίζουν η διαφάνεια, η δικαιοσύνη, η πρόταξη του ανθρωποκεντρικού χαρακτήρα, καθώς και η εξασφάλιση εποπτείας και ελέγχου. [12] [4]

Η επίτευξη διαφάνειας στη λειτουργία και τις αποφάσεις των συστημάτων τεχνητής νοημοσύνης ικανοποιεί την ανάγκη για κατανόηση και εμπιστοσύνη από τους ανθρώπους που επηρεάζονται από αυτά. [12] Η εφαρμογή της δικαιοσύνης στην ανάπτυξη και χρήση τους εξασφαλίζει την ισότητα μεταχείρισης και την αναγνώριση των δικαιωμάτων των ατόμων. [7] Η ενίσχυση του ανθρωποκεντρικού χαρακτήρα των νέων τεχνολογιών, μέσω της εξασφάλισης του σεβασμού στα θεμελιώδη δικαιώματα, όπως η ανθρώπινη αξιοπρέπεια, αποτελεί κρίσιμο ζήτημα για την εξασφάλιση της εμπιστοσύνης

και της αποδοχής τους από τις κοινωνίες. [6] Στο πλαίσιο αυτό τα συστήματα τεχνητής νοημοσύνης θα πρέπει να σχεδιάζονται έτσι ώστε να αυξάνουν, να συμπληρώνουν και να ενισχύουν τις ανθρώπινες γνωστικές, κοινωνικές και πολιτισμικές δεξιότητες. [4] Επιπρόσθετα, η ενίσχυση της ανθρώπινης εποπτείας και ελέγχου στα συστήματα τεχνητής νοημοσύνης είναι αναγκαία για την εξασφάλιση της κατάλληλης λειτουργίας και την αποφυγή ανεπιθύμητων συνεπειών. [10] [11] Παράλληλα, η δημιουργία μηχανισμών λογοδοσίας και η θεσμοθέτηση επαρκούς έννομης προστασίας αποτελούν προαπαιτούμενο για την ανεμπόδιστη πρόσβαση στη δικαιοσύνη από άτομα, των οποίων τα δικαιώματα παραβιάζονται εξαιτίας της λειτουργίας συστημάτων τεχνητής νοημοσύνης. [5] [8]

Συνοψίζοντας, είναι σημαντικό να θυμόμαστε ότι η τεχνητή νοημοσύνη δεν αποτελεί αυτοσκοπό, [6] αλλά ένα πολλά υποσχόμενο μέσο για την ανθρώπινη ευημερία, που μπορεί να προάγει την ατομική και κοινωνική ευζωία και το κοινό καλό, καθώς και να συντελέσει στην πρόοδο και την καινοτομία. [11] [8] Υπό το πρίσμα αυτό αναγκαία η εφαρμογή της αρχής της αναλογικότητας, με σκοπό την εξισορρόπηση των ωφελειών και των πιθανολογούμενων δυσμενών επιπτώσεων από τη χρήση της τεχνητής νοημοσύνης. [10]

Καταληκτικά, δεδομένης της αυξανόμενης σημασίας που διαδραματίζουν οι εφαρμογές τεχνητής νοημοσύνης στις σύγχρονες κοινωνίες, είναι ζωτικής σημασίας να προκύψει σε εθνικό, αλλά και σε διεθνές επίπεδο, ένα ολοκληρωμένο νομοθετικό πλαίσιο, που να λαμβάνει υπόψη τις υφιστάμενες προκλήσεις και να προβλέπει της παραμέτρους για τη αξιοποίηση των πολυάριθμων ωφελειών που παρέχουν οι νέες τεχνολογίες, περιορίζοντας τους κινδύνους και την προσβολή των κατοχυρωμένων δικαιωμάτων. [8] Εκτιμώντας ότι η ραγδαία τεχνολογική πρόοδος δύναται να επιφέρει σταδιακά μετασχηματισμούς στις κοινωνικές δομές, κρίνεται εξίσου σκόπιμο να δημιουργηθούν μηχανισμοί διαβούλευσης και συμμετοχής του κοινού στη διαδικασία λήψης αποφάσεων για την εφαρμογή και τη ρύθμιση των συστημάτων τεχνητής νοημοσύνης, ώστε να λαμβάνονται υπόψη οι ανάγκες, οι προτεραιότητες και οι ανησυχίες των πολιτών. [6]

Βιογραφικό συντάκτη

Η Υπλγός (ΝΟΜ) Παπαγγέλου Άννα γεννήθηκε στη Θεσσαλονίκη το 1993. Αποφοίτησε από τη Στρατιωτική Σχολή Αξιωματικών Σωματων το 2015 ως Ανθυπολοχαγός. Υπηρετεί ως Επιτελής στο Γραφείο του Γενικού Γραμματέα ΥΠΕΘΑ. Είναι απόφοιτος της 143ης ΕΣ του Τμήματος Αναλυτών-Προγραμματιστών της ΣΠΗΥ.

Αναφορές

[1] «Τεχνητή Νοημοσύνη,» [Ηλεκτρονικό]. Available: 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.
[2] W. E. Forum, «Fourth Industrial Revolution,» 2024.
[3] D. Bourcier, «De l'intelligence artificielle à la personne virtuelle : émergence d'une entité juridique ?,» Droit et société 2001/3 (n°49), 2001.
[4] T. Madiega, «EU guidelines on ethics in artificial intelligence: Context and implementation,» 2019.
[5] M. Kritikos, «Artificial Intelligence ante portas:Legal & ethical reflections,» 2019.
[6] P. Boucher, «Why artificial intelligence matters,» 2019.
[7] G. L. Moli, «Intelligence artificielle vs dignité humaine : quand la sous-performance humaine est légalement requise,» RED 2022/1 (N° 4), 2022.
[8] Σ. Τάσσης, «Το Δίκαιο στην εποχή της Τεχνητής Νοημοσύνης,» 2019. [Ηλεκτρονικό]. Available: https://www.lawspot.gr/nomika-blogs/spiros_tassis/dikaio-stin-epohi-tis-tehnitis-noimosynis.
[9] P. Boucher, «How artificial intelligence works,» 2019.
[10] Ο. ε. υ. ε. γ. τ. τ. νοημοσύνη, «ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΓΙΑ ΑΞΙΟΠΙΣΤΗ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ,» European Commission, 2019.
[11] D. D. P. Authority, «AI and Algorithmic Risks Report Netherlands,» 2023.
[12] S. M. K. P. Julien Cloarec, «L'intelligence artificielle au service de la prise de décision en marketing,» Décisions Marketing 2023/4 (N° 112), 2024.
[13] E. Y. Nick Bostrom, The Ethics of Artificial Intelligence, 2011.
[14] «What is artificial intelligence and how is it used?,» 2020. [Ηλεκτρονικό]. Available: https://www.europarl.europa.eu/topics/en/article/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used.
[15] T. Tompkins, «New York Times Sues OpenAI Over ChatGPT's Alleged Copyright Infringement,» 2023. [Ηλεκτρονικό]. Available: https://www.investopedia.com/new-york-times-sues-openai-over-chatgpt-s-alleged-copyright-infringement-8420351.
[16] A. Guadamuz, «Artificial intelligence and copyright,» WIPO Magazine, 2017.
[17] T. M. G. C. Sara Gerke, Ethical and legal challenges of artificial intelligence-driven healthcare, 2020.
[18] «Τεχνητή νοημοσύνη: Πολεμικές επιχειρήσεις μέσω AI… και όμως είναι το παρόν,» Οικονομικός Ταχυδρόμος, 2024.
[19] S. Murshed, C. Murphy, D. Hou, N. Khan, G. Ananthanarayanan και F. Hussain, «Machine Learning at the Network Edge: A Survey,» 23 Μαΐου 2021. [Ηλεκτρονικό]. Available: https://arxiv.org/abs/1908.00080.
[20] E. E. Γ. Τ. Α. Τ. Δ. (CEPEJ), «Ευρωπαϊκός Χάρτης Δεοντολογίας για τη χρήση της Τεχνητής Νοημοσύνης στα δικαστικά συστήματα και στο περιβάλλον τους,» 2018.

ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Αποφοίτηση Σχολείου Διαχειριστών Πληροφοριακών Συστημάτων

Την 02 Φεβ. 24 πραγματοποιήθηκε στη ΣΠΗΥ, η αποφοίτηση του Σχολείου Διαχειριστών Πληροφοριακών Συστημάτων (Α΄ ΕΣ 2024)

Επίσκεψη των 142 και 143 Εκπαιδευτικών Σειρών Αναλυτών – Προγραμματιστών στο ΚΕΤΑΚ

Την 14 Φεβ. 24 πραγματοποιήθηκε επίσκεψη στο ΚΕΤΑΚ των 142 και 143 Εκπαιδευτικών Σειρών Αναλυτών – Προγραμματιστών της ΣΠΗΥ

Αποφοίτηση

142 Εκπαιδευτικής Σειράς Αξκών Αναλυτών – Προγραμματιστών

Την 23η Φεβρουαρίου 2024 πραγματοποιήθηκε στη ΛΑΕΔ, η αποφοίτηση της 142ης Εκπαιδευτικής Σειράς Αξκών Αναλυτών-Προγραμματιστών της ΣΠΗΥ, παρουσία του Υδντή του ΓΕΣ/ΔΔΒ-ΕΠ Ταξιάρχου Χρήστου Δαϊλίδη, ο οποίος απένειμε τα πτυχία στους αποφοιτήσαντες.

Στην ίδια τελετή τιμήθηκαν με αναμνηστική πλακέτα, από το Δκτή της ΣΠΗΥ, Συνταγματάρχη (ΕΠ) Ιγνάτιο Χάρο οι καθηγητές της Σχολής κκ Βασσάλος Παρασκευάς, Καράμπελας Παναγιώτης, Πασκαλής Σαράντης, Παυλάτος Χρήστος, Σέκκας Οδυσσέας και Χατζηευθυμιάδης Ευστάθιος προς αναγνώριση της πολυετούς πολύτιμης συνεισφοράς τους στο εκπαιδευτικό έργο της Σχολής.

Αποφοίτηση

Σχολείου Ασφάλειας Πληροφοριακών Συστημάτων (Α΄ ΕΣ 2024).

Την 08 Μαρ 24 ολοκληρώθηκε στη ΣΠΗΥ, η φοίτηση της Α' ΕΣ 2024 του Σχολείου Ασφαλείας Πληροφοριακών Συστημάτων (Α΄ ΕΣ 2024). Αποφοίτησαν 11 στελέχη του ΣΞ, 2 του ΠΝ, 2 της ΠΑ και 1 του ΝΟΜ.

Επίσκεψη της 143 Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών στο Τμήμα Προσομοίωσης ΓΕΕΘΑ/Α3/4

Στις 08 Μαρ 24 πραγματοποιήθηκε επίσκεψη στο Τμήμα Προσομοίωσης ΓΕΕΘΑ/Α3/4, της 143ης Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών της ΣΠΗΥ. Οι σπουδαστές ενημερώθηκαν για τις δραστηριότητες του Τμήματος και για τεχνικά στοιχεία ανάπτυξης προσομοιώσεων.

Αποφοίτηση

5ου Βασικού Σχολείου Πληροφορικής

Στις 12 Απρ 24 πραγματοποιήθηκε στη ΣΠΗΥ, η αποφοίτηση του 5ου Βασικού Σχολείου Πληροφορικής. Αποφοίτησαν 24 στελέχη του ΣΞ, 9 του ΠΝ, 3 της ΠΑ, 4 του ΝΟΜ, 4 του ΓΕΕΦ και 2 της ΕΛ.ΑΣ.

Διεξαγωγή Επιμορφωτικών Προγραμμάτων ΔΙΜΑ ΠΠ ΥΠΕΘΑ

Η ΣΠΗΥ οργάνωσε και υλοποίησε προγράμματα εκπαίδευσης για το χειρισμό Η/Υ και τη διαχείριση αρχείων, βασικού και προχωρημένου επιπέδου γνώσεων επεξεργασίας κειμένου, υπολογιστικών φύλλων, παρουσιάσεων καθώς και υπηρεσιών διαδικτύου για το πολιτικό προσωπικό του ΥΠΕΘΑ. Η εκπαίδευση ολοκληρώθηκε με τη μέθοδο της διαδικτυακής μάθησης και φυσικής παρουσίας στη Σχολή

Αποφοίτηση Σχολείου Μ. Λοχιών τάξεων 2022-2023

Στις 07 Ιουνίου 24 πραγματοποιήθηκε στη ΣΠΗΥ, η αποφοίτηση του Σχολείου Μ. Λοχιών τάξεων 2022-2023.

Επίσκεψη της 143 Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών στην εταιρεία ALTUS-LSA

Στις 12 Ιουν 24 πραγματοποιήθηκε επίσκεψη της 143ης Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών της ΣΠΗΥ, στις εγκαταστάσεις της εταιρείας ALTUS-LSA. Ο αντιπρόεδρος της εταιρείας, Υποστράτηγος ε.α. κ. Ταξιάρχης Σαρδέλλης παρουσίασε τις δραστηριότητες της στους σπουδαστές. Επιπλέον επιδείχθηκαν από τεχνικό προσωπικό της, οι εφαρμογές της πληροφορικής στη διαχείριση των μη επανδρωμένων ιπτάμενων μέσων.


Ολοκλήρωση Επιμορφωτικών Προγραμμάτων Η/Υ ΔΙΜΑ και ΦΠ

Στις 14 Ιουν 24 και 21 Ιουν 24 ολοκληρώθηκαν Επιμορφωτικά Προγράμματα για το Πολιτικό Προσωπικό του ΥΠΕΘΑ με ΔΙΜΑ και ΦΠ. Η εκπαίδευση εκάστου είχε διάρκεια μία εβδομάδα και συμμετείχαν συνολικά σε αυτά 26 Μόνιμοι Υπάλληλοι.

Όροι Συνεργασίας

Σκοπός

Το περιοδικό «ΗΛΕΚΤΡΟΝΙΟ» εκδίδεται από τη ΣΠΗΥ κάθε εξάμηνο με σκοπό την προώθηση πληροφοριών σχετικά με τις εξελίξεις στο χώρο της πληροφορικής και τις εφαρμογές της.

Η θεματολογία του περιοδικού περιλαμβάνει κείμενα σχετικά με:

- επιστημονικές εργασίες
- εφαρμογές της πληροφορικής
- νέες μεθοδολογίες και τεχνικές
- την ιστορική εξέλιξη της πληροφορικής
- τις δραστηριότητες της Σχολής

Τα κείμενα που δημοσιεύονται εκφράζουν τον συντάκτη και δεν απηχούν απαραίτητα τις απόψεις της Σχολής.

Τα προς δημοσίευση άρθρα θα πρέπει να πληρούν τους παρακάτω κανόνες:

- Τα κείμενα δεν θα πρέπει να υπερβαίνουν τις 5.000 λέξεις. Επιπλέον θα πρέπει να περιλαμβάνουν επαρκή τεκμηρίωση και βιβλιογραφία.
- Η υποβολή των κειμένων θα πρέπει να γίνεται σε ηλεκτρονική επεξεργάσιμη μορφή στη διεύθυνση ηλεκτρονικού ταχυδρομείου sphy_3@army.gr.
- Οι συντάκτες των άρθρων θα πρέπει να υποβάλλουν και ένα σύντομο βιογραφικό (με φωτογραφία προαιρετικά) το οποίο θα προστίθεται στο τέλος του κειμένου.
- Τα κείμενα δεν θα πρέπει να περιλαμβάνουν διαβαθμισμένες πληροφορίες.