

شبكات الحاسوب - COMPUTER NETWORKS

المحاضرة الاولى



Computer Networks

➤ مفهوم شبكات الحاسوب

➤ مكونات الشبكة

➤ ماهو البروتوكول

➤ فوائد شبكات الحاسوب

اعداد

د. وفاء حسن

د. حيدر عباس

م. صباح محمد

• ما هي شبكة الحاسوب COMPUTER NETWORK ؟

شبكة الحاسوب (COMPUTER NETWORK) عبارة عن مجموعة من الأجهزة الالكترونية (العقد) المتصلة مع بعضها البعض بأحد تقنيات الاتصال (سلكي - لاسلكي) حيث يكون لها القدرة على مشاركة عدد كبير من المستخدمين للبيانات DATA والبرمجيات SOFTWARE والأجهزة HARDWARE.

توفر شبكة الحاسوب سهولة التواصل بين الافراد والمؤسسات وارسال واستقبال الرسائل والمعلومات والوسائط المتعددة بسهولة وبوقت قصير مع توافر البيئة الامنة للاتصال .



مكونات الشبكات NETWORK COMPONENTS

- الشبكات هي مجموعة من أجهزة الكمبيوتر. تبدأ من جهازين على أقل تقدير وتنتهي بملايين الأجهزة.
- الشبكة تقسم الى خمسة مكونات رئيسية هي:-

1) وحدة الإرسال SENDING UNIT

هي المسؤولة عن إرسال البيانات والمعلومات إلى الحاسبات الأخرى داخل الشبكة.

2) وحدة الاستقبال RECEIVING UNIT

هي الوحدة المسؤولة عن استقبال البيانات والمعلومات والرسائل المرسلة من حاسبات وطرفيات أخرى داخل الشبكة أو الشبكات المتصلة بنفس الشبكة.

3) وسط الاتصال TRANSMISSION MEDIA

هي في الغالب خط تليفوني أو كابل اتصال من نوع معين مسئول عن نقل البيانات والمعلومات من / إلى الحاسبات المتصلة بالشبكة.

4) الرسالة THE MESSAGE

هي البيانات أو المعلومات التي نرغب بإرسالها عبر الشبكة.

5) البروتوكول THE PROTOCOL

هي مجموعة من القواعد RULES التي تتحكم بالاتصال.

• تتكون شبكة الحاسوب من عدة أجزاء لكل جزء وظيفته الخاصة في النظام الشبكي وهذه الأجزاء هي :

1. الحاسوب الرئيسي – الخادم SERVER

2. محطات العمل WORK STATIONS

3. خطوط الاتصال COMMUNICATION LINES

4. بطاقة الشبكة NETWORK INTERFACE CARD

5. المودم MODEM

6. الأجهزة الملحقة

7. محولات الشبكة COMMUNICATION SWITCHES

8. برامج الشبكة

1. الحاسوب الرئيسي – الخادم SERVER

• هو الجهاز الرئيسي لتشغيل الشبكة ويسمى جهاز الخدمة الرئيسي أو الخادم SERVER وهو عبارة عن حاسوب يتميز بالسرعة العالية والطاقة التخزينية الكبيرة لكي يستوعب البيانات والبرمجيات التي سوف يتداولها المشاركون في الشبكة. يقوم هذا الجهاز بالتحكم في جميع أجزاء الشبكة وذلك باستخدام برمجيات خاصة بتشغيل نظام الشبكة NETWORK OPERATING SYSTEM، مثل UNIX، WINDOWS SERVER2003 وغيرها.



2. محطات العمل WORK STATIONS

• وتسمى أيضا CLIENTS وهي الحاسبات الشخصية بكافة أنواعها (مكتبية – محمولة – مساعدات رقمية ...) أو الوحدات الطرفية TERMINALS والمتصلة بالجهاز الرئيسي ليستفيد مستخدموها من البيانات والبرمجيات المخزنة على جهاز الخدمة الرئيسي.



3. خطوط الاتصال COMMUNICATION LINES

- هي الوسائل التي سيتم بواسطتها تبادل البيانات بين الحاسوب الرئيسي والحاسبات الفرعية وتشمل الكيبلات بأنواعها المختلفة WIRE كما تشمل الخطوط اللاسلكية WIRELESS.

4. بطاقات الشبكة NETWORK INTERFACE CARD

- هي بطاقة تثبت بالحاسوب لتهيئته للاتصال بالشبكة، وتوجد البطاقة اما داخلية INTERNAL تثبت على اللوحة الأم MOTHERBOARD داخل الحاسوب أو خارجية EXTERNAL.

5. المودم MODEM

- عبارة عن لوحة أو شريحة الكترونية تضاف الى الحاسوب وتستخدم لتهيئة الحاسوب للاتصال بالانترنت من خلال خط الهاتف. يقوم المودم بتحويل الإشارات الرقمية DIGITAL SIGNALS التي يستخدمها الحاسوب MODULATE الى اشارات تماثلية ANALOG التي يستخدمها الهاتف ويقوم بالعملية العكسية ايضا؛ فكلما مودم

MODEM هو اختصار لكلمتي MODULATE – DEMODULATE



Network Interface Card (NIC)



6. الأجهزة الملحقة

- يمكن استخدام بعض الأجهزة وشبكها بالشبكة مثل الطابعات واجهزة الفاكس وغيرها ويستطيع اي مشترك في الشبكة استخدام هذه الأجهزة .



7. محولات الشبكة COMMUNICATION SWITCHES

- هي عبارة عن اجهزة تستخدم لربط حاسبات الشبكة ببعضها وفيما بين الشبكات وايضا لتوجيه البيانات بين حاسبات الشبكة، ومن هذه الأجهزة: الجسر / BRIDGE - البوابة - GATEWAY / الموزع - HUB / الموجه - ROUTER.



8. برامج الشبكة

- هي برامج الاتصالات التي ستنحكم في تشغيل نظام الشبكة ويتم تخزين هذه البرامج في الحاسوب الرئيسي SERVER ومن امثلتها PRTG

NAGIOS OPENNMS NETWORK MONITOR

ماهو البروتوكول PROTOCOL ؟

البروتوكول :- مجموعة من القوانين التي تنظم تنقل المعلومات بين الحواسيب.

كي تتمكن الحواسيب من الإتصال مع بعضها البعض، تم إبتكار طرق أساسية لنقل المعلومات ومُعالجتها. ويُطلق على هذه الطرق “البروتوكولات”. بعض هذه البروتوكولات شائعة مثل: POP, SMTP, TCP, IP, UDP, HTTP, FTP,

1. بروتوكول (HTTP) HYPERTEXT TRANSFER PROTOCOL

بروتوكول نقل النصوص التشعبية

لان الانترنت مكونة من شبكات واجهزة حاسوب مختلفة فأن الشبكة العالمية WWW تحتاج الى طريقة معرفة لتبادل المعلومات ، وبالتالي جاءت الحاجة إلى استخدام بروتوكول يسمح بانتقال النصوص التشعبية من حاسب إلى آخر ويطلق على هذا البرتوكول HYPERTEXT TRANSFER PROTOCOL واختصاره HTTP لذلك نجد ان بداية اي عنوان على الانترنت يبدأ ب HTTP ويستخدم وهذا البروتوكول في نقل الملفات المكونة للمواقع وصفحات الانترنت ويتم استعراض هذه النصوص باستخدام برمجيات متصفح الإنترنت مثل NETSCAPE ومستكشف الإنترنت INTERNET EXPLORER

2. بروتوكول (FTP) FILE TRANSFER PROTOCOL

- بروتوكول نقل الملفات FILE TRANSFER PROTOCOL واختصاره (FTP) يستخدم لنقل الملفات على الشبكة .
- وهو واحد من الأساليب المتبعة في نقل الملفات من خلال الانترنت وغالبا ما تتم هذه العملية باستخدام أداة التصفح من خلال الضغط على الارتباط التشعبي الخاص بالملف المراد نقله أو من خلال احد البرامج المتخصصة بتنزيل وتحميل الملفات باستخدام بروتوكول .
- لبروتوكول FTP عدة إستعمالات لكن وبشكل عام مهمته الرئيسية تتمثل في نقل الملفات عبر الشبكات، الأمر الذي يجعل منه مهما جدا خاصة لأصحاب المواقع حيث يتيح لهم رفع ملفات الموقع الى سيرفر الاستضافة، و تحميلها من السيرفر، بالاضافة إلى مختلف العمليات التي من الممكن القيام بها على الملفات المحملة على السيرفر، كحذفها، تعديلها أو نقلها من مسار الى اخر.
- نقل الملفات ينقسم الى قسمين

1- تنزيل الملفات : DOWNLOAD:

وهو جلب الملفات من الكمبيوتر المضيف HOST الى الجهاز المحلي LOCAL

2- ارسال الملفات : UPLAOD وهو ارسال الملفات من الكمبيوتر المحلي LOCAL الى الكمبيوتر المضيف HOST

- يستخدم الأشخاص FTP بشكل عام لجعل الملفات متوفرة للآخرين لتنزيلها و كذلك لتحميل صفحات ويب لإنشاء موقع على ويب أو لوضع صور رقمية على موقع لمشاركة الصور.

• فوائد شبكات الحاسوب

1. المشاركة في استخدام الأجهزة : HARDWARE ونعني استفادة أي مستخدم للشبكة من إمكانيات الحاسوب الرئيسي بدلاً من اقتناء حاسوب مستقل، كذلك الاستفادة من جميع الأجهزة الملحقة بالشبكة مثل الطابعات .
2. المشاركة في البرمجيات : SOFTWARE ونعني استفادة أي مستخدم للشبكة من البرمجيات المخزنة في الحاسوب الرئيسي أو أي حاسوب آخر متصل بالشبكة مثل مشاركة الملفات واستخدام البريد الإلكتروني .
3. المشاركة في البيانات : DATA ونعني استخدام قاعدة بيانات واحدة تحتوي على جميع المعلومات يستخدمها جميع المتصلين بالشبكة كما هو متبع في البنوك وعند حجز تذاكر السفر .
4. سهولة التواصل بين الافراد والمؤسسات والشركات من خلال ارسال واستقبال الرسائل الالكترونية النصية والوسائط المتعددة بسرعة.
5. عقد المؤتمرات والندوات التفاعلية لأطراف متباعدة عبر شبكة الأنترنت .
6. التعليم عن بعد والطب عن بعد والتجارة الإلكترونية والحكومة الالكترونية .
7. تبادل الاخبار والمعلومات والتسوق عبر الانترنت ومواقع التواصل الاجتماعي.

TYPES OF COMPUTER NETWORKS أنواع شبكات الحاسوب

المحاضرة الثانية



Computer Networks

- تصنيف شبكات الحاسوب حسب الحجم
- تصنيف شبكات الحاسوب حسب طريقة التوصيل

اعداد

د. وفاء حسن

د. حيدر عباس

م. صباح محمد

اولا: تصنيف الشبكات من حيث الحجم : SIZE

1. الشبكة المحلية LAN – LOCAL AREA NETWORK

2. الشبكة الواسعة WAN – WIDE AREA NETWORK

3. شبكة الانترنت INTRANET

4. شبكة الإكسترانت EXTRANET

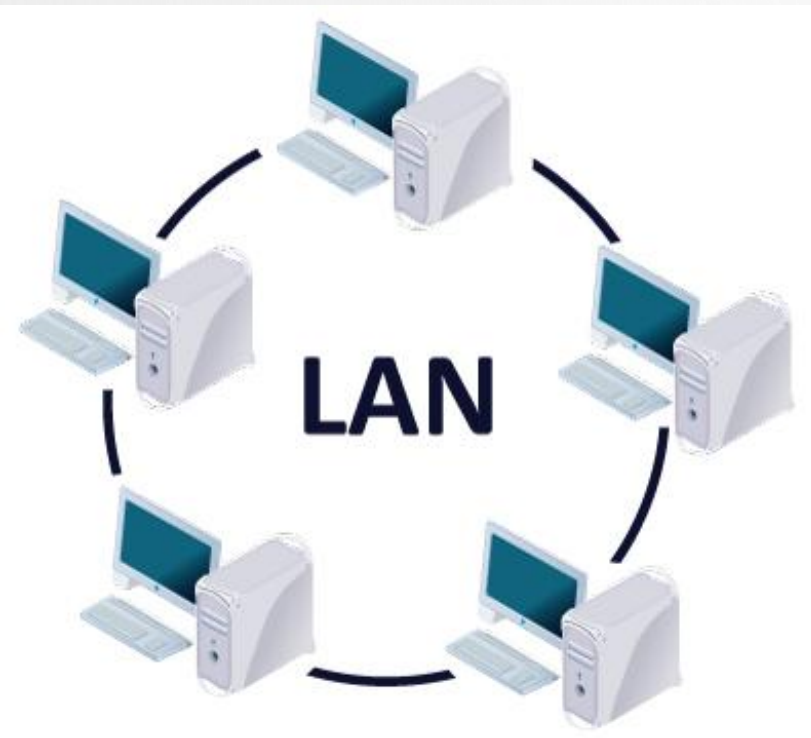
5. شبكة الانترنت INTERNET

1. الشبكة المحلية LAN – LOCAL AREA NETWORK

- هي اتصال مجموعة من الحاسبات بحاسوب رئيسي في أماكن متقاربة جغرافيا قد تكون غرفة أو مبنى واحد أو عدة مباني متقاربة، حيث يتم هذا الاتصال عن طريق وصلات سلكية مباشرة أو لاسلكية .تستخدم هذه الشبكات في الشركات الصغيرة، المدارس، المنازل و غيرها..

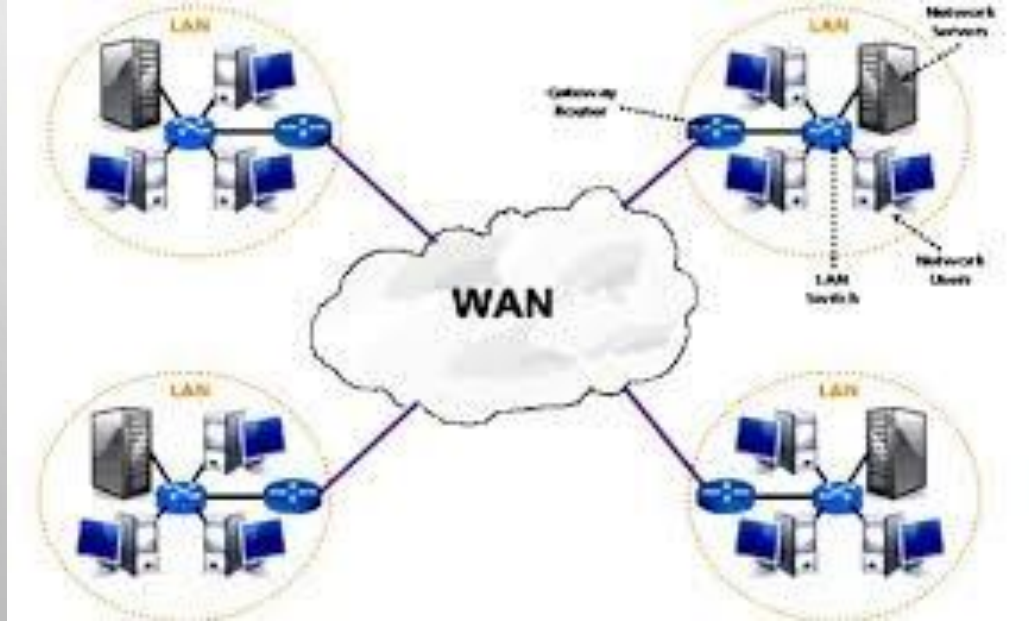
• مميزات الشبكة المحلية :

1. محدودة المكان فهي مخصصة لغرض محدد مثل المدرسة أو الجامعة أو شركة .
2. سرعة الإرسال لقصر المسافة بين الأجهزة .
3. يستخدمها عدد محدد من المستخدمين .
4. تدار هذه الشبكة في المدارس و الجامعات أو الشركات والمؤسسات الخاصة .



2. الشبكة الواسعة WAN – WIDE AREA NETWORK

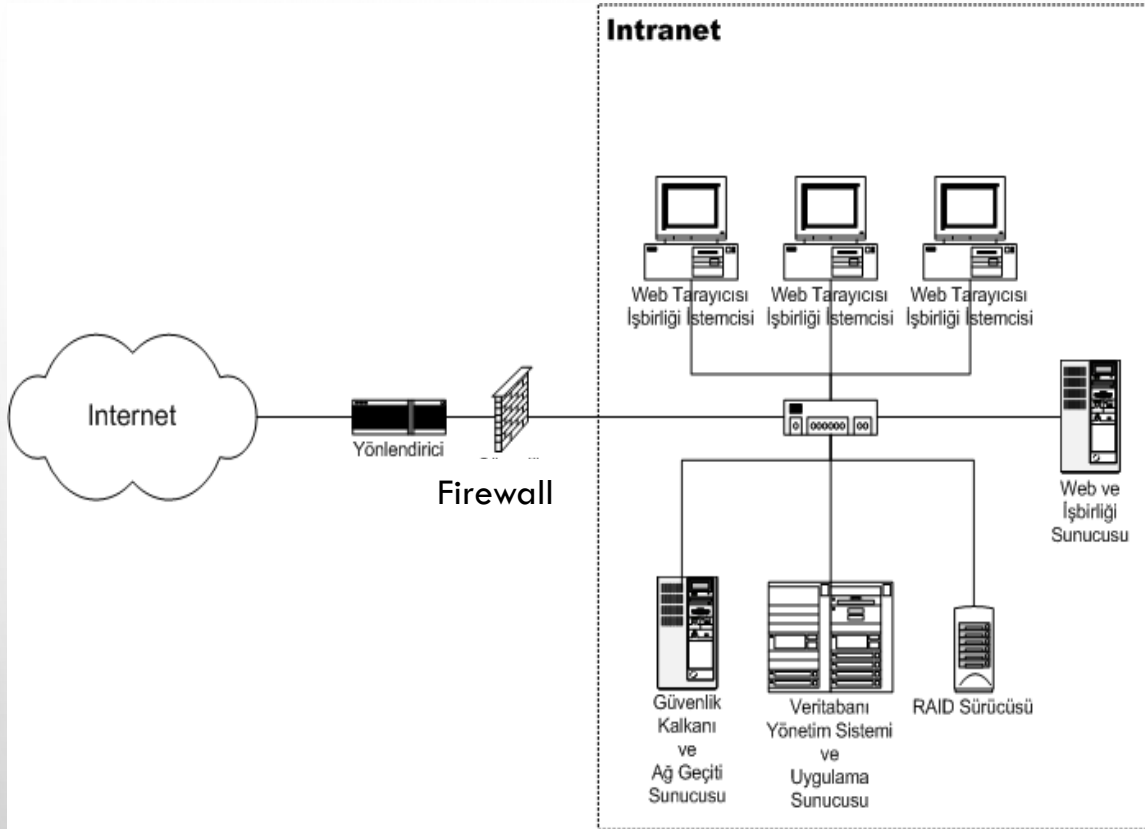
- هي اتصال مجموعة متباعدة من الحاسبات او مجموعة من الشبكات المحلية بحاسوب رئيسي، قد تكون في نفس البلد او في بلد آخر او قارة اخرى، وعادة ما يكون الحاسوب الرئيسي من النوع الكبير MAINFRAME او المتوسط MINICOMPUTER. تستخدم هذه الشبكات في الجهات الحكومية والمؤسسات والشركات الكبيرة التي لديها فروع متباعدة .



- مميزات الشبكة الواسعة :

1. تمتد بين المدن.
2. محدودة سرعة الإرسال لطول المسافات بين الوحدات المختلفة .
3. يستخدمها عدد كبير من المستخدمين .
4. تدار هذه الشبكة من هيئة عامة أو جهة حكومية .

3. شبكة الإنترنت



- تطلق تسمية الإنترنت على التطبيق العملي لاستخدام تقنيات الإنترنت في الشبكة الداخلية للمؤسسة أو الشركة، بغرض رفع كفاءة العمل الإداري ورفع الإنتاجية وتحسين آليات تشاؤرك الموارد والمعلومات والاستفادة من تقنيات الحوسبة المشتركة .

- تقدم شبكة الإنترنت خدمة الدخول إلى الإنترنت مع منع العكس (أي لا يمكن لغير المسجلين في شبكة الإنترنت الدخول إليها عن طريق الإنترنت)، وبذلك تؤمن الإنترنت سوراً منيعاً يُطلق عليه اسم (الجدار الناري FIREWALL) حول محتوياتها، مع المحافظة على حق وصول العاملين عليها إلى مصادر المعلومات الخارجية على الإنترنت .

4. شبكة الإكسترنات



- هي شبكة انترانت تسمح لبعض الأشخاص المخولين الدخول إليها و الإستفادة من بعض الخدمات دون الأماس بخصوصية الإنترنت المحلية .

5. الشبكة العالمية الموسعة WWW (الانترنت):

- عبارة عن شبكة عالمية تربط بين ملايين الشبكات. ومن أهم ما يميز الإنترنت هو الكم الهائل من البيانات الذي يمكنك الوصول اليه من خلال هذه الشبكة وبسرعة كبيرة وكذلك نقل الملفات والمعلومات بين المستخدمين ولكن يجب توخي الحذر من مدى دقة المعلومات المتاحة على هذه الشبكة .



يتم ربط شبكات الانترنت بطريقة سلكية او لاسلكية وتوصيل أجهزة الحاسوب والأجهزة الحديثة من خلال شبكة خطية او نجمية في جميع أماكن العمل في الشركة، المصنع، الفندق، المكتب، المؤسسة والهيئات والمصالح الحكومية حيث يتم ربطها معا لتوفر سهولة نقل وتبادل البيانات والمعلومات إضافة الى ربط الأماكن بجميع الخدمات مع تأمين الحماية من الاختراق بأقوى بروتوكولات التشفير. كل ذلك يتم وفق ضوابط وقواعد يطلق عليها بروتوكولات الانترنت.



• أنواع و طرق ربط شبكات الانترنت

• **شبكات الوصلات السلكية** ويتم ربط الاجهزة هنا باستخدام الاسلاك والكابلات التي نراها متصلة بأجهزة الحاسب الآلي منها الكابلات المحورية، والكابلات الزوجية المجدولة المحمية (STP)، والكابلات الزوجية المجدولة غير المحمية (UTP)، أو الألياف الضوئية.

• **شبكات الوصلات اللاسلكية** وهي شبكات تعمل بدون توصيلات سلكية بين أجهزة الشبكة ولكن تتم عن طريق الواي فاي (WIFI) لعمل بث موجات أشبه بموجات الراديو. وتستقبله أجهزة الحاسوب المزودة بـ كارت WIFI ويتم تبادل البيانات والمعلومات عن طريق الموجات التي تنشرها اجهزة WIFI.

• **ربط الشبكات اللاسلكية لمسافة بعيدة:** يتم استخدام اكسس بوينت ACCESS POINT للعمل على ربط شبكة الكمبيوتر في مكان ما باجهزة اخرى في مكان آخر كأن تربط مبنين لشركة ويقوم جهاز WIFI REPEATER باستقبال الاشارة اللاسلكية وتقويتها ويقوم بارسالها ومن هنا تنتسح المساحة الجغرافية التي تغطيها الشبكة ويتضاعف عدد المستخدمين. يتم ربط الشبكات عن طريق عدة خطوات وهناك عدة أنواع من ربط الشبكات.

ثانيا: تصنيف الشبكات من حيث طريقة التوصيل : **TOPOLOGY**

1. شبكة المسار الخطي BUS NETWORK

2. الشبكة الحلقية TOKEN RING NETWORK

3. الشبكة النجمية STAR NETWORK

4. الشبكة المتداخلة MESH NETWORK

أولاً: شبكة المسار الخطي BUS NETWORK

- يتم توصيل جميع الأجهزة داخل الشبكة في سلك واحد محوري شبيه بسلك التلفزيون ونهاية وبداية هذا السلك لا يتقابلان، ويتم نقل البيانات من حاسوب لآخر في أي اتجاه . تعمل هذه الشبكة بنفس الطريقة التي يتحدث بها الأشخاص حيث ينتظر كل حاسوب في الشبكة دوره ليقوم بإرسال المعلومات .
- يعتبر هذا النوع من التوصيل بطيئاً في نقل البيانات وعند توقف الكابل الرئيسي فان الشبكة بأكملها تتعطل غير ان هذا النوع بسيط في توصيل هذه الشبكة وغير مكلف حيث ان جميع الأجهزة تقع على نفس السلك بينما طرق التوصيل الاخرى تحتاج الى المزيد من الاسلاك .

ثانياً: الشبكة الحلقية TOKEN RING NETWORK

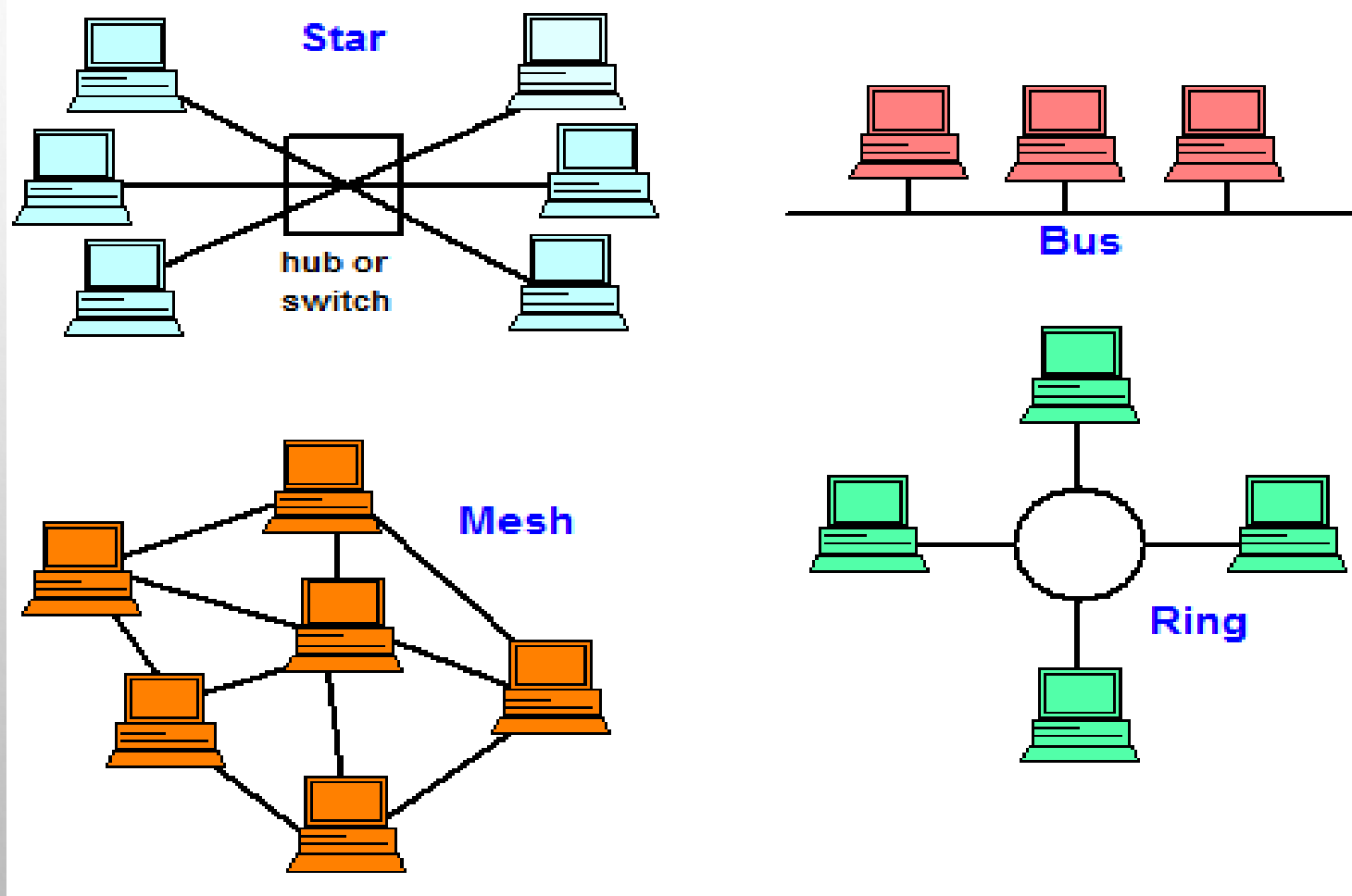
- يتم توصيل الحاسبات على سلك واحد على شكل حلقة حيث يلتقي طرفا السلك ويتم نقل البيانات بين الحاسبات في اتجاه واحد عبر السلك الى ان تصل الى الحاسوب المطلوب .
- من عيوب هذا التوصيل ان الشبكة تتوقف بالكامل عند تعطل احدى الوحدات الطرفية غير انها تتميز بالسرعة والكفاءة .

ثالثاً: الشبكة النجمية STAR NETWORK

- أبسط انواع التوصيل ويتم توصيل الحاسوب الرئيسي بالحاسبات الطرفية مباشرة عن طريق سلك او اتصال لاسلكي، ولا يتم اي اتصال بين حاسوب و آخر او شبكة اخرى الا عن طريق الحاسوب الرئيسي .
- يتميز هذا التوصيل بالفعالية والكفاءة نظرا لاتصال جميع الحاسبات الطرفية اتصالا مباشرا بالحاسوب الرئيسي. يستخدم هذا التوصيل في المؤسسات التي تتغير بياناتها بسرعة مثل البنوك وسوق الأوراق المالية وشركات الطيران وغيرها .

رابعاً: الشبكة المتداخلة MESH NETWORK

- في الشبكات المتداخلة، يكون كل كمبيوتر متصل بجميع الكمبيوترات الأخرى بواسطة سلك منفصل. وهذا التصميم يوفر طرقاً متكررة للاتصال خلال الشبكة حيث أنه إذا فشل أحد الأسلاك (انقطع) فإن سلكاً آخر سيؤدي وظيفته ويعمل بدلاً منه. ولكن هذه الشبكات تكون عالية التكاليف لأنها تستخدم أسلاكاً كثيرة.



امان الحاسوب والشبكات COMPUTER AND NETWORK SECURITY

المحاضرة الثالثة



Computer Networks

➤ امن الحواسيب

➤ اهداف امن الحواسيب

➤ الحل الامني

اعداد

د. وفاء حسن

د. حيدر عباس

م. صباح محمد

يوضح تقرير معهد أمن الحاسب الآلي (Computer Security Institute-CSI) لعام ٢٠١٠/٢٠١١م^١ أن (٨, ١٦٪) من الجهات التي أجريت الدراسة المسحية عليها (شملت الدراسة جهات حكومية وشركات مختلفة ومعاهد مالية وطبية وجامعات) قد تعرّضت لهجوم تعطيل الخدمة (DoS)، وأن (٤, ١١٪) تعرّضت لسرقة كلمات المرور، وأن (٥, ٣٣٪) تعرّضت لسرقة الأجهزة المحمولة، وأن (٧, ٨٪) تعرّضت لاحتيال مالي، وأن (٤, ٧٪) تعرّضت لاستغلال الشبكات اللاسلكية، وأن (١, ٦٧٪) تعرّضت لهجمات البرامج الخبيثة.

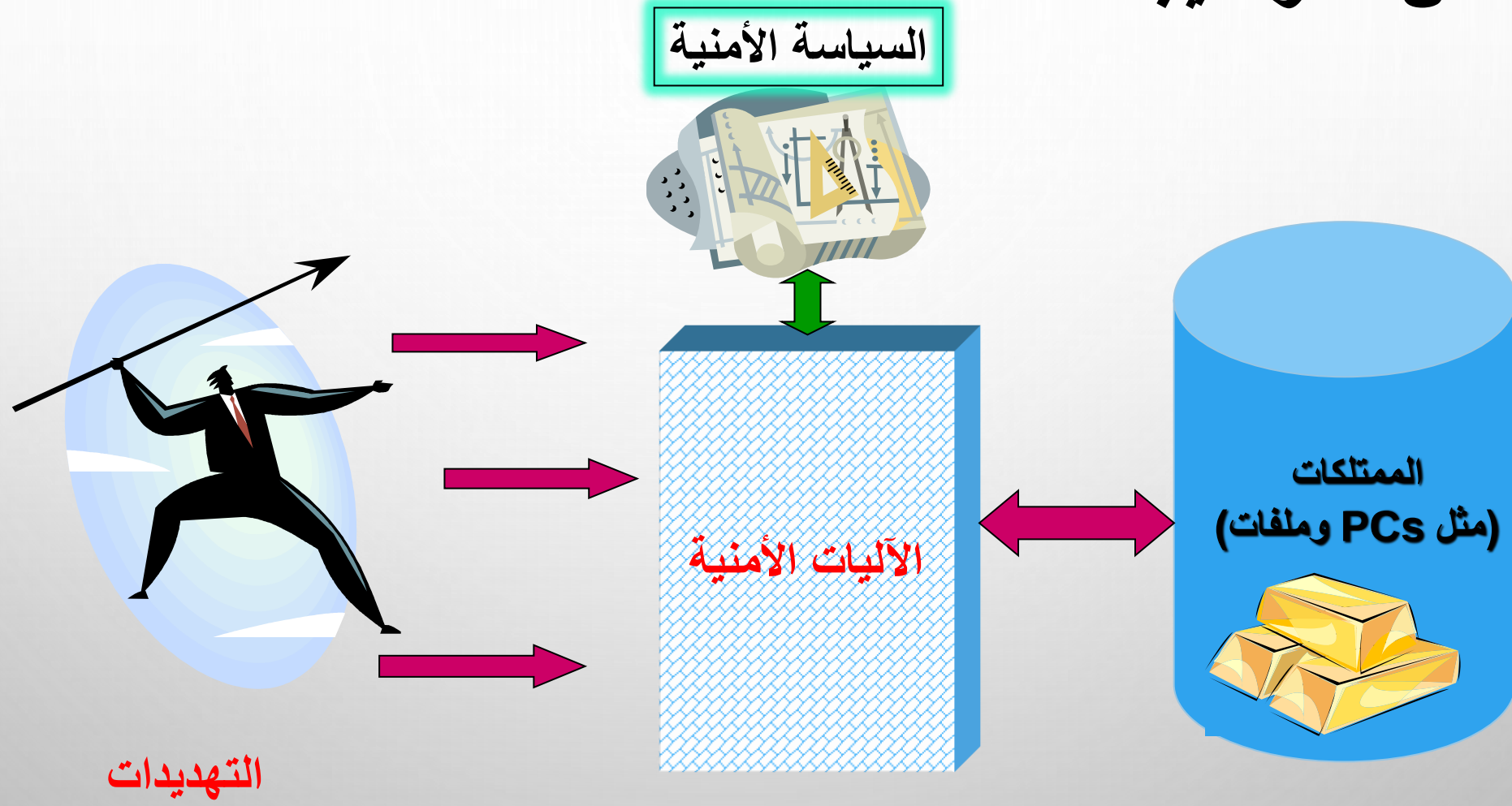
1. أمن الحواسيب

- **الأمن** هو حماية الثروات أو الممتلكات (ASSETS) من السرقة والتخريب.
- للأمن عدة فروع، منها:
 - الأمن القومي
 - والأمن الاقتصادي
 - ...
 - وأمن الحواسيب
- أمن الحواسيب: حماية **الممتلكات** داخل الحاسب:
 - أي حماية المعلومات والخدمات التي يقدمها الحاسب.
 - أي حماية المعلومات المعالجة والمخزنة والمنقولة.

• أمن الحواسيب:

- ماذا نريد أن نحمي؟
- أي الممتلكات التي نريد أن نحميها؟
- لماذا نحتاج لأن نحمي الممتلكات؟
- أي ما هي **المتطلبات الأمنية** لهذه الممتلكات؟
- مما يجب أن نحمي الممتلكات؟
- أي ما هي **التحديات ونقاط الضعف** أو الثغرات الأمنية **والأخطار**؟
- كيف يمكن أن نحمي الممتلكات؟
- أي ما هي **الإجراءات الأمنية** (Security Countermeasures) أو **الآليات الأمنية** (Security Mechanisms)؟
- عادةً تطبيق الإجراءات الأمنية وفقاً **للسياسة الأمنية**.

أمن الحواسيب



أمن الحواسيب – التهديد والهجوم

- **نقطة الضعف أو الهشاشة:** هي حالة ضعف في تصميم النظام أو تنفيذه أو في استثماره، وقد يكون في البرمجيات أو في الأجهزة المادية، أمثلة:
 - لا يوجد مضاد فيروس
 - وجود BUG في البرنامج
- **التهديد:** هي مجموعة الظروف أو الأفعال أو الأحداث التي توفر القدرة على إحداث إختراق أمني من خلال استغلال هشاشة النظام، أمثلة:
 - شخص لديه القدرة على إحداث عمل غير مرغوب به.
 - أو حادثة طبيعية قد تحدث ضرراً ما.
- **الخطر:** هو إمكانية التعرض للضرر أو الخسارة.
- **الهجوم (ATTACK):** هو تحقيق أو تنفيذ لتهديد ما.
- **المهاجم (ATTACKER):** هو الشخص أو الكيان (ENTITY) الذي يقوم بالهجوم، أي استغلال هشاشة نظام بدافع معين.
- مرادفات:
 - العدو (ENEMY)
 - والخصم (ADVERSARY)
 - والدخيل (INTRUDER)
 - و المتنصت (EAVESDROPPER).

- **المتسلل (HACKER):** هو شخص لديه خبرة معمقة في أنظمة التشغيل والبرمجيات ولغات البرمجة ويبذل جهد كبير لاكتشاف نقاط الضعف في أنظمة المعلوماتية ويشارك معلوماته مع الآخرين، ولكن لا يلحق الأذى بشكلٍ مباشر أو عن قصد.
- **المخرب (CRACKER):** هو الشخص الذي يقوم بانتهاك الأنظمة بسوء نية، أي ينفذ إلى الأنظمة بشكلٍ غير قانوني من أجل تحقيق أهداف مختلفة مثل محو المعلومات أو تعديلها.
- **المقاطعة (INTERRUPTION):** تأخير أو رفض خدمة ليصبح النظام خارج الاستخدام.
- **الاعتراض (INTERCEPTION):** قراءة معلومات بطريقة غير شرعية.
- **التعديل (MODIFICATION):** تعديل المعلومات بطريقة غير شرعية .
- **انتحال الشخصية (MASQUERADE):** إدخال أو تخزين معلومات إلى النظام أو الشبكة لتظهر كأنها قادمة من مستخدم مخول.
- **النكران (REPUDIATION):** ادعاء عدم القيام بإرسال شيء.
- **تحليل المرور (TRAFFIC ANALYSIS):** مراقبة الاتصال الشبكي بهدف استخلاص معلومات حول الاتصال.
- **إعادة الإرسال (REPLAY):** إعادة إرسال رسالة تم اعتراضها سابقاً على الشبكة.

2. أهداف أمن الحواسيب (CIA)

- السرية (CONFIDENTIALITY) أو الخصوصية (PRIVACY)

- السلامة أو التكاملية (INTEGRITY)

- التوافرية أو الإتاحة (AVAILABILITY)



1. السرية (CONFIDENTIALITY):

- السماح للأشخاص المخولين فقط بالإطلاع على المعطيات أو المعلومات.
- تضمن الثقة عدم تعرض البيانات للاختراق.
- أنواع اختراقات السرية:
 - اختراقات مقصودة (تعتمد على هجوم مباشر متعمد)
 - أمثلة:
 - التقاط حركة المرور على الشبكة
 - سرقة ملف كلمات المرور
 - مسح البوابات (PORT SCANNING)
 - الهندسة الاجتماعية (SOCIAL ENGINEERING)
 - اختراقات غير مقصودة (أخطاء بشرية، إهمال، سوء تصرف).
 - أمثلة:
 - عدم تشفير البيانات المتبادلة بشكل تام و صحيح.
 - ترك نقاط دخول أمنية مفتوحة.
 - اختراقات بسبب أنشطة المستخدمين، أو مدير النظام.
 - عدم تطبيق السياسة الأمنية بشكل جيد.
 - حماية السرية:
 - التشفير.
 - استخدام الحشو في حركة المرور على الشبكة.
 - التحكم بالنفاذية او السماح.
 - توعية المستخدمين.

2. التكاملية (INTEGRITY):

- السماح للأشخاص المخولين فقط بتعديل المعطيات أو المعلومات.
- تضمن الثقة أن البيانات لم تعدل عن حالتها الأصلية المحمية.
- التكاملية هي:
 - منع الكيانات غير المخولة من إجراء تعديلات.
 - منع الكيانات المخولة من إجراء تعديلات غير مرخص لهم إجرائها.
 - بقاء العلاقة بين المعلومات صحيحة و مترابطة ومحققة.
- اختراقات التكاملية:
 - اختراقات مقصودة (تعتمد على هجوم مباشر متعمد).
 - مثل: الفيروسات والنفاذ غير المرخص بهدف الكتابة أو المحو، إلخ
 - اختراقات غير مقصودة (أخطاء بشرية، إهمال، سوء تصرف)
 - مثل: حذف ملفات خطأ و إدخال بيانات غير صحيحة وتعديل وأخطاء في الأوامر، إلخ.
- حماية التكاملية:
 - التحكم بالنفاذ او السماحية،
 - نظم كشف الاقتحام،
 - اختبار وظائف الإدخال،
 - إلخ

3. التوافرية/الإتاحة (AVAILABILITY):

- توفر إمكانية نفاذ المخولين إلى المعلومات وقت الحاجة.
- أنواع الاختراقات التوافرية:
 - اختراقات مقصودة (تعتمد على هجوم مباشر متعمد)
 - مثل: هجمات رفض الخدمة (DOS) وتدمير البيانات ومقاطعة الاتصالات.
 - اختراقات غير مقصودة (أخطاء بشرية، إهمال، سوء تصرف)
 - مثل: حذف ملفات خطأ واستخدام الأجزاء المادية أو البرامج بشكل مبالغ فيه.

• حماية التوافرية

- تصميم أنظمة تسليم وسيطة ملائمة
- تقنيات ضبط نفاذ فعالة
- مراقبة الأداء و حركة مرور الشبكة
- استخدام الجدران النارية Firewalls
- اعتماد مبدأ الوفرة (**Redundancy**) في الأنظمة الحساسة
- صيانة واختبار نظم التخزين الاحتياطي.

أهداف أخرى

- **الوثوقية (Authentication):** التحقق من هوية الجهة المرسلة للرسالة.
- وثوقية كيان (Entity authentication): التأكد من هوية الكيان وترتبط بوصلة منطقية (Logical connection).
- وثوقية رسالة (Message authentication): التأكد من مصدر الرسالة.
- **عدم الإنكار (Non-Repudiation):** الحماية من إنكار الكيانات المشاركة في الاتصال. يمكن أن ينكر المصدر إرسال رسالة أو أن ينكر المستقبل استقبال رسالة.

3. الحل الأمني

• مراحل تطبيق حل أمني

1. السياسة الأمنية (SECURITY POLICY): هي مجموعة القواعد التي تحدد ما هو مسموح وما هو

مرفوض، أي تحديد الأهداف/الأمنية المطلوبة

• مثال: في النظم المُشاركة لا نسمح إلا للأشخاص المرخص لهم النفاذ إلى النظام.

• مثال: النفاذ إلى الخادم لا نسمح إلا للأشخاص المخولين.

• مثال: يسمح للأشخاص المخولين النفاذ إلى جداول الرواتب.

2. الآليات الأمنية (Security mechanisms):

• اختيار الأدوات التي تساعد على تحقيق الأهداف

• مثال: الاعتماد على كلمات المرور في ضبط النفاذ إلى النظام المُشارك.

• مثال: استخدام بروتوكول الدفع (Payment protocol) للتأكد من أن الزبون دفع رسم الدخول إلى خدمة الويب.

3. نقاط الضعف: البحث عن نقاط الضعف الممكنة في النظام والتي يمكن أن تترك النظام معرض للهجمات.

• مثال: كلمات المرور المرسله غير محمية.

• مثال: كلمات المرور مخزنة في ملفات مفتوحة.

4. آليات صيانة:

• تحسين الحل عن طريق معالجة نقاط الضعف .

• واقتراح آليات جديدة .

تقرير معهد الامن السيبراني CSI عن الأخطاء غير المقصودة

- فيما يتعلق بالتهديدات الداخلية المتعمدة، قد يُجبر الموظفون أو يُهددون بالكشف عن معلومات حساسة أو نشر معلومات سرية، أو قد يفعل العاملون المتعاقدون الشيء نفسه لضمان استمرارهم في العمل. وقد وجدت تحقيقات فيريزون (VERIZON) لاختراقات البيانات لعام 2019 أن 34% من جميع الاختراقات في عام 2018 كانت من قبل الموظفين أنفسهم، وهي زيادة تدريجية، وإن كانت كبيرة، مقارنةً بـ 25% في عام 2016 و 28% في عام 2017.
- ومن ناحية أخرى، يُعدّ الخطأ البشري غير المقصود من قبل موظفين غير متخصصين في تكنولوجيا المعلومات أمراً مروعاً بنفس القدر. فبعد شهرين من انتشار وباء فيروس الفدية WANNACRY على نطاق واسع، تم تصحيح الثغرات الأمنية بتحديث من مايكروسوفت؛ ولا يزال عدد كبير من الشركات حول العالم لم يُحدّث أنظمتها. ويتمثل الخطأ البشري غير المقصود بشكل أكبر في سوء استخدام المستخدم أو أخطائه.
- ومن المعروف أيضاً أن المتسللين والمجرمين الإلكترونيين يستخدمون وسائل الهندسة الاجتماعية من خلال خداع المستخدمين النهائيين للكشف عن معلومات حساسة، والتي حتى من خلال ساعات من التدريب والفكر، حتى الموظفين الأكثر خبرة يقعون ضحايا لها.

الهجمات السيبرانية الروسية على أوكرانيا- مقال لمعهد الامن السيبراني CSI

• في 24 فبراير 2022، شنت روسيا غزوًا واسع النطاق لأوكرانيا، لم يشهد المسرح الأوروبي مثيلاً له منذ عقود. قد يُذكرنا هذا الغزو، الذي نفذته الجيش الروسي، بحروب الماضي، ولكن ثمة تفصيلاً رئيسياً يجب مراعاته: **العنصر السيبراني**.

• العنصر السيبراني

• على عكس حروب القرن الماضي التي استلهم منها هذا النوع من الغزو العسكري البري الشامل، سبقه هجوم سيبراني روسي مُدبّر على البنية التحتية للدولة الأوكرانية. في عالمنا الحديث، يُمكن ربط أي شيء تقريباً بشبكة، من الهواتف المحمولة والساعات إلى إشارات المرور ومحطات الطاقة. لا توجد بنية تحتية حيوية بمنأى عن متناول جيش حديث أو منظمة إجرامية. نفت الدولة الروسية هجمات حجب الخدمة الموزعة (DDOS)، لكن نائب رئيس الوزراء الأوكراني يُصرّ على أنها عملية روسية. مع ذلك، من المهم الإشارة إلى أن الهجمات السيبرانية لا تسبق دائماً الهجمات المادية، بل تُشكّل صراعاً دائماً بين الدول. في عام ٢٠١٥، لوحظ بالفعل اختراق روسيا لشبكة الكهرباء الأوكرانية، والذي استُغلّ لاحقاً للتسبب في انقطاع التيار الكهربائي في جميع أنحاء البلاد. ومنذ نجاح روسيا في ضم شبه جزيرة القرم، ربما بدت فترة من السلام النسبي، لكن الحقيقة هي أنها دأبت على قصف أوكرانيا والدول المجاورة الأخرى بهجمات إلكترونية. وقد استهدفت الهجمات الأخيرة وزارة الدفاع الأوكرانية والعديد من البنوك الأوكرانية، مما تسبب في مشاكل اقتصادية ولوجستية متلاحقة.

- على الرغم من هذه الهجمات الإلكترونية، يبدو للوهلة الأولى أن روسيا لم تُركز في الواقع على جانبها السيبراني في هذه الحرب. فقد اقتصرَت طبيعة هجماتها على هجمات حجب الخدمة الأساسية ومحاولات التصيد الاحتيالي، وهي هجمات لا تُقارن بما كان متوقعًا من دولة مُستعدة للحرب الإلكترونية مثل روسيا. قد يتوقع المرء هجومًا أقرب في طبيعته إلى دودة ستوكسنت (THE STUXNET WORM) التي أطلقها الإسرائيليون والأمريكيون ضد المنشآت النووية الإيرانية، مُسببةً أضرارًا جسيمة. ويمكن سرد الأسباب التالية كاحتمالات وراء أسلوب الهجوم الروسي.
- أولاً، أهملت الدولة الروسية جهودها في الحرب السيبرانية، ولا تمتلك القدرات التي كان يُعتقد أنها تمتلكها، مما أجبرها على الاعتماد بشكل أكبر على عملياتها العسكرية المادية القديمة.
- ثانياً، اختارت الدولة الروسية عدم شنّ الهجمات السيبرانية المدمرة التي كان يُعتقد أنها قادرة على شنّها على أوكرانيا، لأنها تحتاج البنية التحتية هناك لأغراضها الخاصة، ولا تريد إلحاق الضرر بها أثناء احتلالها. بدلاً من ذلك، وربما بالتزامن مع النظرية الثانية، فإن الدولة الروسية لم تُظهر كامل استعدادها، ولديها خطط حرب سيبرانية جاهزة للانطلاق في أي لحظة. هذا، بلا شك، هو الأكثر إثارة للقلق، لأنه يوحي بأن أوكرانيا ليست هدفهم الوحيد، أو على الأقل أنهم ينوون إلحاق أضرار أكبر من الكوارث التي شهدناها بالفعل. ومع ذلك، في نهاية المطاف، هذه النظريات ليست أكثر من مجرد تخمينات، ومن المرعب والمثير للاهتمام في آن واحد توقع عواقب هذه الهجمات السيبرانية على العالم في المستقبل، وخاصة في مجال الحرب. لسوء الحظ، كل ما يمكننا فعله الآن هو المراقبة والانتظار لمعرفة كيف تتطور هذه الحرب الساخنة على الجبهة السيبرانية وما هي العواقب التي ستترتب على ذلك بالنسبة لأوكرانيا وبقية العالم.

أمن شبكات الحاسوب

Network Security

المحاضرة الرابعة



- ما المقصود بأمن الشبكات؟
- لماذا أمن الشبكات مهم؟
- أفضل أساليب أمن الشبكات
- أنواع حلول أمن الشبكات
- تحديات أمان الشبكات
- أمثلة عن الهجمات

اعداد

د. وفاء حسن

د. حيدر عباس

م. صباح محمد

ما المقصود بأمن الشبكات؟

- يشمل أمن الشبكات جميع الخطوات المتخذة لحماية سلامة شبكة الحاسوب والبيانات الموجودة فيها. ويشمل ذلك مجموعة من الأدوات والسياسات والبروتوكولات والوسائل المصممة لمنع الوصول غير المصرح به، أو إساءة الاستخدام، أو التعديل، أو منع الوصول إلى الشبكة ومواردها.
- تستخدم استراتيجيات أمن الشبكات الناجحة أساليب أمنية متعددة لحماية المستخدمين والمؤسسات من البرامج الضارة والهجمات الإلكترونية، مثل هجمات حجب الخدمة الموزعة (DDoS).
- تتكون الشبكة من أجهزة مترابطة، مثل أجهزة الكمبيوتر والخوادم والشبكات اللاسلكية. العديد من هذه الأجهزة عرضة للمهاجمين.
- يتضمن أمن الشبكات استخدام أدوات برمجية وأجهزة على الشبكة أو استخدام البرمجيات كخدمة (SaaS).
- يزداد الأمن أهمية مع ازدياد تعقيد الشبكات، واعتماد الشركات بشكل أكبر على شبكاتها وبياناتها لإدارة أعمالها. يجب أن تتطور أساليب الأمن مع ابتكار الجهات المعادية أساليب هجومية جديدة على هذه الشبكات المتزايدة التعقيد.



لماذا امن الشبكات مهم؟

- نظرًا لأن المؤسسات تتبنى تقنيات جديدة مثل الحوسبة السحابية والذكاء الاصطناعي (AI) وإنترنت الأشياء (IoT) ، فإنها تزيد من حجم سطح الهجوم الذي يمكن للمخترقين استغلاله. في كل عام، تتسبب الهجمات الإلكترونية المعقدة التي تنطوي على برمجيات خبيثة (أحصنة طروادة)، والتصيد الاحتيالي، وبرامج الفدية، وهجمات الهندسة الاجتماعية وهجمات هجوم موزع لحجب الخدمة في تكبيد الشركات الملايين.
- يتم تصميم أفضل اساليب وحلول أمن الشبكات عادةً مع وضع ثلاثة أهداف أساسية في الاعتبار:
 1. منع الوصول غير المصرّح به إلى موارد الشبكة.
 2. الكشف عن الهجمات الإلكترونية الجارية ووقفها.
 3. تأكد من أن المستخدمين المصرح لهم لديهم إمكانية الوصول الآمن إلى موارد الشبكة التي يحتاجون إليها.



أفضل اساليب أمن الشبكات

1. اسلوب تجزئة الشبكة

يسمح اسلوب تجزئة الشبكة (وهي اسلوب تقسيم الشبكة إلى أجزاء أصغر) للمؤسسات بتنفيذ المزيد من التحكم في البيانات والمستخدمين على الشبكة. يقلل تجزئة الشبكة من حجم سطح الهجوم وعدد الطرق التي يمكن للقراصنة من خلالها الوصول غير المصرح به.

2. فرض المصادقة متعددة العوامل (MFA)

المصادقة متعددة العوامل (MFA) هي طريقة للتحقق من هوية المستخدم من خلال شكلين مختلفين على الأقل من الإثبات، مثل كلمة المرور ومعرف الوجه. في أمان الشبكة ، توفر المصادقة متعددة العوامل طبقة إضافية من الحماية بالإضافة إلى كلمة مرور المستخدم التي يمكن أن تمنع الجهات الفاعلة السيئة من الوصول إلى البيانات الحساسة.



3. استخدام الشبكات الخاصة الافتراضية (VPNs)

الشبكات الخاصة الافتراضية (VPNs) هي خدمات تنشئ اتصالات آمنة ومشفرة لتبادل البيانات والموارد عبر الإنترنت. يعتمد أمن الشبكة على الشبكات الخاصة الافتراضية (VPNs) لتغطية العنوان، وموقع الجهاز في الشبكة بحيث يصعب تتبع نشاط المستخدم. لعبت الشبكات الخاصة الافتراضية (VPNs) دوراً مهماً في تطوير العمل عن بعد، حيث مكّنت المستخدمين من الوصول إلى معلومات الشركة ومواردها من أي مكان في العالم. يتضمن هذا الوصول العمل عبر شبكات WiFi العامة في أماكن مثل المقاهي أو المكاتب التي تعتمد على الأقمار الصناعية.

4. بناء إطار عمل الثقة الصفريّة

الثقة الصفريّة: هي استراتيجية أمنية حديثة مصممة للسحابة، تركز على تأمين الاتصالات الفردية للمستخدمين بالشبكة بدلاً من منح الثقة ضمناً لجميع الأعضاء. قبل انتشار الحوسبة السحابية، ركّز أمن الشبكات على تأمين نقاط النهاية -الأجهزة التي تتصل بالشبكات وتتبادل المعلومات- ولكن هذا النهج لم يكن فعالاً في البيئة السحابية.

5. تدريب الموظفين واختبارهم بانتظام

إن أفضل حلول وأنظمة أمن الشبكات تكون فعّالة فقط إذا تم تدريب الفرق المسؤولة عن تنفيذها بشكل منتظم وخضعت لاختبارات صارمة. يجب على المؤسسات التأكد من أن مستخدمي الشبكة على دراية بسياساتها الأمنية، والمعروفة أيضاً باسم بروتوكولات الأمان. يجب عليها أيضاً فهم الخطوات التي يجب اتخاذها عندما يشتبهون في حدوث اختراق لأمن البيانات.



أنواع حلول أمن الشبكات

1. جدران الحماية

يُعدّ جدار الحماية برنامجًا أو جهازًا يمنع حركة المرور المريبة من الدخول إلى الشبكة أو الخروج منها، والسماح لبقية حركة المرور المشروعة بالدخول والخروج. يمكن نشر جدران الحماية على حواف الشبكة أو استخدامها داخليًا لتقسيم شبكة أكبر إلى شبكات فرعية أصغر. إذا ما حدث اختراق لجزء واحد من الشبكة، فسيظل المخترقون ممنوعين من الوصول إلى بقية الأجزاء.

2. حلول التحكم في الوصول إلى الشبكة (NAC)

تعمل حلول التحكم في الوصول إلى الشبكة على التحقق من هوية المستخدمين وترخيصهم لتحديد من يُسمح له بالدخول إلى الشبكة وما يمكنهم فعله عندما يكونون بالداخل. يُشير مصطلح "المصادقة" إلى تأكيد هوية المستخدم والتأكد من حصوله على الأدونات المناسبة للوصول إلى موارد الشبكة المحددة. غالبًا ما يتم استخدام حلول التحكم في الوصول إلى الشبكة (NAC) لفرض سياسات التحكم في الوصول المستند إلى الأدوار (RBAC) ، حيث تعتمد امتيازات المستخدمين على وظائفهم.

3. الأمن السحابي Cloud Security

تعمل حلول أمن السحابة على حماية مراكز البيانات والتطبيقات والأصول السحابية الأخرى من الهجمات الإلكترونية. معظم حلول أمن السحابة هي ببساطة عبارة عن تدابير أمنية قياسية للشبكة (على سبيل المثال، جدار الحماية و NACs والشبكات الخاصة الافتراضية) المطبقة على بيئات السحابة. يقوم العديد من موفري الخدمات السحابية بإنشاء عناصر تحكم أمنية في خدماتهم أو يقدمونها كوظائف إضافية.



4. أنظمة كشف التسلل والوقاية منه (IDPSs)

يقوم نظام كشف التسلل والوقاية منه (IDPS) ، والذي يُطلق عليه أحياناً اسم نظام منع التطفل، بفحص حركة المرور الواردة بحثاً عن التهديدات الأمنية. تطورت أدوات الأمن هذه من أنظمة كشف التسلل (IDSs) ، والتي كانت فقط تقوم برصد الأنشطة المشبوهة من أجل المراجعة. تتمتع أنظمة كشف التسلل والوقاية منه (IDPSs) بالقدرة الإضافية على الاستجابة تلقائياً للانتهاكات المحتملة عن طريق حظر حركة المرور أو إعادة تعيين الاتصال.

5. إجراءات أمن التطبيقات

يشير أمن التطبيق (AppSec) إلى الأنظمة والعمليات التي تعتمد عليها فرق الأمن لحماية التطبيقات من الهجمات الإلكترونية. نظراً لأن معظم الشركات الحديثة تستخدم التطبيقات لتنفيذ وظائف الأعمال الرئيسية أو معالجة البيانات الحساسة، فإن هذه التطبيقات كثيراً ما تصبح أهدافاً رئيسية للهجمات الإلكترونية. ونظراً لاستضافة العديد من التطبيقات في السحابة العامة، يمكن للمخترقين استغلال نقاط ضعفها لاقتحام شبكات الشركات الخاصة. بعض الأمثلة الشائعة لأدوات أمن التطبيقات هي جدران حماية التطبيقات والحماية الذاتية لتطبيقات وقت التشغيل واختبار أمن التطبيقات الثابت واختبار أمن التطبيقات الديناميكي.

6. أمان البريد الإلكتروني

يعد التصيد الاحتيالي، وهو نوع من الهجمات الإلكترونية التي تستخدم رسائل البريد الإلكتروني الاحتيالية لخداع الأشخاص لمشاركة البيانات الحساسة، أحد أكثر التهديدات الإلكترونية شيوعاً وفعالية. تساعد مجموعة واسعة من أدوات وأنظمة أمن البريد الإلكتروني (مثل مرشحات البريد العشوائي وتشفير الرسائل) المؤسسات على إحباط محاولات التصيد الشائعة. حتى أن بعض أدوات أمن البريد الإلكتروني الأكثر تقدماً تتميز بميزة آلية تحديد الوصول، وهي بيئات معزولة حيث يمكن لمحترفي الأمن فحص مرفقات البريد الإلكتروني دون تعريض الشبكة بأكملها لمحتوياتها.



تحديات امان الشبكات

يتضمن الحفاظ على أمن الشبكات عددًا من التحديات، منها ما يلي:

1. تطور أساليب هجمات الشبكات: يتمثل التحدي الأكبر لأمن الشبكات في معدل تطور الهجمات الإلكترونية. تتغير الجهات الفاعلة في مجال التهديد وأساليبها باستمرار مع تطور التكنولوجيا. على سبيل المثال، أدت التقنيات الجديدة، مثل تقنية البلوك تشين (Blockchain) إلى أنواع جديدة من هجمات البرامج الضارة، مثل سرقة العملات المشفرة. ونتيجة لذلك، يجب أن تتكيف استراتيجيات الدفاع عن أمن الشبكات مع هذه التهديدات الجديدة.
2. التزام المستخدم: كما ذكرنا، فإن الأمن مسؤولية كل مستخدم للشبكة. قد يكون من الصعب على المؤسسات ضمان التزام الجميع بأفضل ممارسات أمن الشبكات مع تطوير هذه الاستراتيجيات في الوقت نفسه لمواجهة أحدث التهديدات.
3. الوصول عن بُعد ومن خلال الهاتف المحمول: تتبنى المزيد من الشركات سياسات "إحضار جهازك الخاص"، مما يعني شبكة أجهزة أكثر توزيعًا وتعقيدًا على المؤسسات لحمايتها. كما أن العمل عن بُعد أكثر انتشارًا. وهذا يزيد من أهمية أمن الشبكات اللاسلكية، حيث من المرجح أن يستخدم المستخدمون شبكة شخصية أو عامة عند الوصول إلى شبكات الشركة.
4. شركاء الطرف الثالث: غالبًا ما يتمكن مزودو الخدمات السحابية وخدمات الأمن المُدارة وبائعو منتجات الأمن من الوصول إلى شبكة المؤسسة، مما يفتح الباب أمام ثغرات أمنية جديدة.
5. التهديدات الداخلية: تنشأ هذه المشاكل من أفراد لديهم بالفعل وصول مُصرَّح به إلى الأنظمة والبيانات داخل المؤسسة. سواءً كان موظفًا ساخطًا يتصرف بسوء نية أو موظفًا حسن النية يرتكب خطأً فادحًا، فإن التهديدات الداخلية غالبًا ما تتجاوز ضوابط الأمن التقليدية. يتطلب اكتشاف المخاطر الداخلية والتخفيف منها نهجًا دقيقًا يجمع بين مراقبة السلوك وضوابط الوصول الصارمة وثقافة الوعي الأمني في جميع أنحاء المؤسسة.

6. ميزانيات الأمن المحدودة: يمكن لقيود الميزانية أن تعيق بشكل كبير قدرة المؤسسة على الحفاظ على أمن شبكي قوي. عندما تكون الموارد المالية محدودة، فغالبًا ما يعني ذلك تأخير التحسينات المهمة، أو التأخر في إدارة اصلاح المشاكل، أو العمل دون توفر كامل الكادر اللازم للكشف عن التهديدات والاستجابة للحوادث. تخلق هذه القيود ثغرات يمكن للمهاجمين استغلالها، مما يجعل من المهم للمؤسسات إعطاء الأولوية لاستثمارات الأمن بشكل استراتيجي، حتى في البيئات المالية الصعبة.

7. سوء ضبط اعدادات الشبكة والخطأ البشري: لا تزال اعدادات الضبط الخاطئة والخطأ البشري من بين الأسباب الرئيسية للاختراقات الأمنية. سواءً كان ذلك منفذًا معطلًا عن طريق الخطأ، أو قواعد جدار حماية شديدة التساهل، أو تصحيحًا برمجياً مفقودًا، فإن حتى أصغر الإغفالات يمكن أن يكون لها عواقب وخيمة. مع توسع الشبكات وتطورها، يصبح الحفاظ على دقة التكوينات أكثر صعوبة، مما يجعل من الضروري تطبيق أدوات تحقق آلية، وتطبيق إجراءات صارمة لإدارة التغيير، وغرس عقلية تضع الأمن في المقام الأول بين الفرق.

8. إرهاق الانذارات وزيادة عبء العمل على وسائل الأمان: تعاني العديد من المؤسسات من إرهاق التحذيرات والانذارات وزيادة تحميل استخدام وسائل الأمان، مما قد يقوض حتى أفضل جهود الأمن تمويلًا. عندما تُنتج أدوات الأمن المتباينة سيلاً من التنبيهات دون سياق أو ارتباط، تُترك فرق الأمن لتبحث في ضوضاء المعلومات لتحديد التهديدات الحقيقية. هذا لا يُبطئ أوقات الاستجابة فحسب، بل يزيد أيضاً من خطر إغفال مؤشرات الاختراق المهمة. يمكن أن يُساعد دمج الاستجابات وأتمتتها من خلال منصات مثل SOAR أو XDR في تبسيط العمليات وتقليل الإرهاق.



امثلة عن الهجمات

1. **هجوم رفض الخدمة (DoS):** يهدف هجوم (Denial of Service DoS) إلى تعطيل عمل النظام أو الشبكة بالكامل من خلال تعريضه لعبء من حركة المرور أو الطلبات أو البيانات. وهذا يمنع المستخدمين المشروعين من الوصول إلى المورد أو الخدمة المستهدفة. تشمل هجمات رفض الخدمة الموزعة (DDoS) عدة أنظمة مخترقة (Botnet) تتكاثف لتنفيذ الهجوم.
2. **البرمجيات الضارة (Malware):** تتضمن هجمات برمجيات الضارة توزيع وتنفيذ برمجيات ضارة مثل الفيروسات والديدان وبرامج التجسس وبرامج الفدية. يمكن لبرامج الضارة أن تصيب الأنظمة وتسرق المعلومات الحساسة وتفسد الملفات أو تمنح الوصول غير المصرح به للمهاجمين.
3. **الصيد الاحتيالي (Phishing):** تستخدم هجمات الصيد الاحتيالي رسائل البريد الإلكتروني أو الرسائل أو المواقع الإلكترونية المضللة لخداع الأفراد وإقناعهم بالكشف عن معلومات حساسة مثل كلمات المرور أو أرقام بطاقات الائتمان أو التفاصيل الشخصية. يُستخدم الصيد الاحتيالي غالبًا لسرقة بيانات الاعتماد على الدخول أو ارتكاب سرقة الهوية أو توزيع برمجيات الضارة.
4. **هجوم الرجل في الوسط (MitM):** يقوم المهاجم بالتقاط وربما تعديل الاتصال بين طرفين دون علمهما. وهذا يتيح للمهاجم سماع المعلومات الحساسة مثل بيانات الاعتماد أو المعاملات المالية التي تم نقلها عبر الشبكة.
5. **الحقن الخلوي (SQL Injection):** تستغل هجمات الحقن الخلوية الثغرات في تطبيقات الويب أو قواعد البيانات لحقن استعلامات SQL ضارة. ويمكن أن يؤدي ذلك إلى الوصول غير المصرح به إلى قواعد البيانات أو الكشف عن معلومات حساسة أو التلاعب بالبيانات.



6. البرمجيات النصية عبر المواقع المتقاطعة (XSS): تقوم هجمات (Cross-site scripting XSS) بحقن نصوص خبيثة في صفحات الويب التي يشاهدها المستخدمون الآخرون. يمكن لهذه النصوص سرقة ملفات تعريف الارتباط أو الرموز الخاصة بالجلسة أو معلومات أخرى حساسة من متصفحات المستخدمين، مما يؤدي إلى اختراق الحساب أو سرقة الهوية.
7. استغلال الثغرات المجهولة (Zero-Day Exploits): تستهدف هجمات استغلال الثغرات اليوم الصفري الثغرات في البرمجيات أو الأجهزة التي لا تعرف للبائع أو التي لم يتم إصلاحها بعد. يستغل المهاجمون هذه الثغرات للوصول غير المصرح به إلى الأنظمة أو تنفيذ الشيفرة التعسفية أو سرقة البيانات الحساسة.
8. التهديدات الداخلية: تشمل التهديدات الداخلية الأفعال الخبيثة أو اللامبالاة من قبل الأفراد الذين لديهم وصول مصرح به إلى الأنظمة أو الشبكات أو البيانات. قد تشمل هذه الموظفين أو المتعاقدين أو الشركاء التجاريين الذين يسيئون استخدام الامتيازات الخاصة بهم لسرقة البيانات أو تخريب الأنظمة أو المساس بالأمان.



المحاضرة الخامسة

الذكاء الاصطناعي

ARTIFICIAL INTELLIGENCE (AI)

اعداد

د. وفاء حسن
د. حيدر عباس
م. صباح محمد

- مفهوم الذكاء الاصطناعي
- تاريخ الذكاء الاصطناعي
- تقنيات الذكاء الاصطناعي
- أهمية الذكاء الاصطناعي
- أنواع الذكاء الاصطناعي
- سلبيات الذكاء الاصطناعي
- تطبيقات الذكاء الاصطناعي
- الروبوت Robot

مفهوم الذكاء الاصطناعي



يُعرف الذكاء الاصطناعي ويمكن تعريفه بأنه فرع من علوم الحاسوب يركز على تطوير أنظمة ومعدات وبرامج تحاكي القدرات الذهنية للبشر وبخصائص متعددة: التعلم، الاستنتاج، التفكير، رد الفعل، اتخاذ القرارات والإدراك والقدرة على حل المشكلات.



كما أنّ الذكاء الاصطناعي يتميز بقدرته على اختيار أفضل الإجراءات لتحقيق هدف معين بأفضل فرصة مُمكنة، كما يمتلك خاصية التعلّم الآلي، إذ يُمكن للبرامج داخل أجهزة الكمبيوتر التعلّم من البيانات الجديدة المُدخلة إليها وهي عبارة عن كميات كبيرة جداً من البيانات غير المُهيكلّة مثل: النص أو الصور أو الفيديو، ثمّ تتكيّف مع هذه البيانات تلقائياً دون مساعدة الإنسان.

تاريخ الذكاء الاصطناعي

يشهد تطوير الذكاء الاصطناعي دورات من التقدم وانخفاض الاهتمام به. تشمل الفترات الرئيسية ما يلي:

1. أربعينيات وخمسينيات القرن الماضي: ظهرت الحواسيب القابلة للبرمجة، واقترح آلان تورينج "اختبار تورينج" عام ١٩٥٠ كمقياس لذكاء الآلة.
١٩٥٦: صُنِع مصطلح "الذكاء الاصطناعي"، ومثّل مشروع بحثي رئيسي البداية الرسمية للذكاء الاصطناعي.
2. ستينيات وسبعينيات القرن الماضي: طُوّرت برامج ذكاء اصطناعي مبكرة مثل ELIZA و Shakey the Robot. أدت محدودية القدرة الحاسوبية إلى ما يُعرف بـ "شتاء الذكاء الاصطناعي".
3. ثمانينيات القرن الماضي: أعادت أنظمة الخبراء، التي تحاكي الخبرة البشرية بقواعد، إحياء هذا المجال.
4. تسعينيات وألفينيات القرن الماضي: تحوّل التركيز إلى التعلم الآلي، حيث تتعلم الحواسيب من البيانات. وكان هزيمة غاري كاسباروف، باستخدام حاسوب Deep Blue من IBM، عام ١٩٩٧ حدثًا بارزًا.
5. من العقد الأول من القرن الحادي والعشرين حتى الوقت الحاضر: أدت التطورات في البيانات الضخمة، وقوة الحوسبة، والتعلم العميق إلى تقدم سريع. وأنتجت هذه الحقبة تقنيات مثل المساعدين الصوتيين، والسيارات ذاتية القيادة، ونماذج الذكاء الاصطناعي التوليدية.

تقنيات الذكاء الاصطناعي

يشمل الذكاء الاصطناعي عدة تقنيات أساسية:

1. التعلم الآلي (ML): تتعلم الأنظمة من البيانات دون برمجة صريحة. وتشمل أنواعه:-
 - التعلم الموجه: يستخدم بيانات مُصنفة لربط المدخلات بالمخرجات.
 - التعلم غير الموجه: يكتشف أنماطاً في البيانات غير المُصنفة.
 - التعلم المُعزز: يتعلم العامل من خلال التجربة والخطأ مع المكافآت والعقوبات.
 - التعلم العميق (DL): مجموعة فرعية من التعلم الآلي تستخدم شبكات عصبية متعددة الطبقات للأنماط المعقدة، وهي ناجحة في التعرف على الصور والكلام.
2. معالجة اللغة الطبيعية (NLP): تُمكن أجهزة الكمبيوتر من فهم وتوليد اللغة البشرية لتطبيقات مثل الترجمة وروبوتات الدردشة.
3. الرؤية الحاسوبية: تسمح لأجهزة الكمبيوتر بتفسير المعلومات المرئية لاستخدامات مثل التعرف على الوجه والسيارات ذاتية القيادة.
4. أنظمة الخبراء: برامج تُحاكي عملية اتخاذ القرارات البشرية بالخبرة باستخدام التعليمات (القواعد) وقاعدة معرفية.
5. حل المشكلات والتفكير المنطقي: أساليب مثل تحليل الوسائل والغايات لتحقيق الأهداف من خلال تقليل الفروق بين الوضعين الحالي والمرغوب فيه.
6. الروبوتات: تشمل تصميم وبناء وتشغيل وتطبيق الروبوتات، والتي يمكن تشغيلها بالذكاء الاصطناعي.
7. الأساليب الاحتمالية: تُستخدم تقنيات مثل الشبكات البايزية (Bayesian) وعمليات اتخاذ القرار لماركوف في المهام التي تنطوي على عدم اليقين واتخاذ القرارات والتخطيط وفقاً للتقارير الأخيرة لجامعة أوصلو.

أهمية الذكاء الاصطناعي

1- تحسين عملية اتخاذ القرارات

يُعد اتخاذ القرارات المُمكن بالذكاء الاصطناعي أسرع وأذكى لأنه يُوفر البيانات التي يحتاجها قادة الأعمال في الوقت الفعلي.

2- زيادة الكفاءة

من خلال أتمتة المهام المتكررة، يُعزز الذكاء الاصطناعي كفاءة أعلى عبر مجموعة من عمليات الأعمال.

3- تحسين خدمة العملاء

يتوقع العملاء أن تكون الشركات متاحةً على مدار الساعة طوال أيام الأسبوع، بغض النظر عن طبيعة استفساراتهم. ومع ذلك، ليس من الممكن دائمًا الرد على كل استفسار فورًا. وهنا يأتي دور الذكاء الاصطناعي. بفضل معالجة اللغة الطبيعية (NLP) وتوليد اللغة الطبيعية (NLG)، يمكن لروبوتات الدردشة ورسائل البريد الإلكتروني الآلية التعامل مع العديد من استفسارات العملاء.

4- خفض التكاليف

تُعد إدارة الميزانية إحدى العمليات التجارية التي تتطلب اهتمامًا كبيرًا. فمن خلال تسريع العمليات التجارية وتقليل الحاجة إلى التدخل البشري، يمكن للذكاء الاصطناعي المساعدة في خفض التكاليف بشكل كبير.

5- إدارة المخاطر

يستخدم الذكاء الاصطناعي البيانات التاريخية للتنبؤ بالمستقبل. وتُصبح إدارة المخاطر أسهل بفضل قدرته على تقديم توصيات مبنية فقط على البيانات دون أي تحيز تقريبيًا. كما يُمكن للذكاء الاصطناعي تقييم كميات أكبر بكثير من البيانات مقارنةً بالإنسان، مما يضمن استخدام جميع التوصيات لمعلومات من مصادر متعددة

6- الابتكار

يُعد الذكاء الاصطناعي المؤلّد ممتازًا للعصف الذهني وابتكار أفكار جديدة تُساعد المُبتكرين على تبادل الأفكار. ومع ذلك، يُمكن للذكاء الاصطناعي التحليلي أن يكون أيضًا قوة إبداعية. ففهم الاتجاهات الحالية والمستقبلية، المدعومة بملايين الوحدات الخزنّية من البيانات، يُساعد أقسام البحث والتطوير.

7- التحليلات التنبؤية

التحليلات التنبؤية فرع من التحليلات المتقدمة، يستخدم البيانات التاريخية والخوارزميات الإحصائية وتقنيات التعلم الآلي لتحديد احتمالية النتائج المستقبلية بناءً على البيانات التاريخية. يُحسّن الذكاء الاصطناعي التحليلات التنبؤية من خلال تمكين تحليل مجموعات البيانات الضخمة بسرعة ودقة، وتحديد الأنماط المعقدة التي قد يغفلها المحللون البشريون.

أنواع الذكاء الاصطناعي:

يمكن تصنيف الذكاء الاصطناعي بشكل عام إلى نوعين:

1. **الذكاء الاصطناعي المحدد أو الضعيف:** صُمم الذكاء الاصطناعي المحدد لأداء مهام محددة أو حل مشكلات محددة، مثل التعرف على الصور أو ترجمة اللغات. ويعتمد على خوارزميات التعلم الآلي المُدربة على مجموعات بيانات كبيرة للتعرف على الأنماط والتنبؤ بناءً عليها.

2. **الذكاء الاصطناعي العام أو القوي:** بينما صمم الذكاء الاصطناعي العام، ليهدف إلى محاكاة الذكاء البشري في مجموعة واسعة من المجالات، مثل التفكير والإدراك والإبداع.

وبينما حقق الذكاء الاصطناعي المحدد تقدمًا كبيرًا في السنوات الأخيرة، إلا أنه لا يزال هدفًا طويل الأجل. يعمل الذكاء الاصطناعي من خلال معالجة كميات هائلة من البيانات، وتحديد الأنماط والعلاقات بينها، واستخدام تلك المعلومات لاتخاذ القرارات أو اتخاذ الإجراءات اللازمة.

تُتاح هذه العملية بفضل خوارزميات مصممة للتعلم من البيانات التي تُغذى بها. تُعد الشبكات العصبية من أكثر أنواع خوارزميات الذكاء الاصطناعي شيوعًا، وهي مصممة على غرار بنية ووظيفة الدماغ البشري. تتكون هذه الشبكات من طبقات من العقد المترابطة التي تعالج المعلومات وتنقلها إلى الطبقة التالية، مما يسمح للخوارزمية بتحديد الأنماط والعلاقات في البيانات.

الاعتبارات الأخلاقية لآثاره السلبية :

على الرغم من فوائده المحتملة العديدة، إلا أن الذكاء الاصطناعي يثير أيضاً العديد من المخاوف الأخلاقية والمجتمعية. ومن أكبر هذه المخاوف تأثيره المحتمل على التوظيف. فمع تطوره، قد يتمكن من أداء العديد من المهام التي يقوم بها البشر حالياً، مما يؤدي إلى فقدان وظائف كبيرة.

وهناك أيضاً مخاوف بشأن إساءة استخدام الذكاء الاصطناعي المحتملة، مثل استخدام تقنية التعرف على الوجه لأغراض المراقبة.

بالإضافة إلى ذلك، هناك مخاوف بشأن التحيز الذي قد يكون مُدمجاً في خوارزميات الذكاء الاصطناعي، حيث أن حياديتها لا تتعدى البيانات التي تُدرَّب عليها. وبالنظر إلى المستقبل، من المرجح أن يلعب الذكاء الاصطناعي دوراً متزايد الأهمية في حياتنا. ومع تطوره، سيتمكن من أداء مهام أكثر تعقيداً واتخاذ قرارات أكثر دقة. وسيكون لذلك آثار على جميع جوانب المجتمع تقريباً، من الرعاية الصحية والمالية إلى النقل والتعليم. وسيكون من المهم لصانعي السياسات والمجتمع ككل التعامل مع الآثار الأخلاقية والمجتمعية لهذه التطورات وضمان استخدام الذكاء الاصطناعي لصالح الجميع. في الختام، يُعدّ الذكاء الاصطناعي مجالاً سريع التطور، ولديه القدرة على إحداث ثورة في جوانب عديدة من حياتنا. فهو يعتمد على خوارزميات مصممة لتعلم من البيانات وتحديد الأنماط، وله تطبيقات واسعة في مختلف الصناعات والمجالات. ورغم أنه يثير العديد من المخاوف الأخلاقية والمجتمعية، إلا أنه يمتلك أيضاً القدرة على تحقيق فوائد كبيرة للمجتمع. ومع استمرار تقدم الذكاء الاصطناعي، سيكون من المهم للمجتمع أن يتعامل مع هذه القضايا، وأن يضمن أن يكون تطويره مسترشداً بالمبادئ الأخلاقية، وأن يُستخدم لمصلحة الجميع.

سلبيات الذكاء الاصطناعي



- **تكلفة تنفيذه باهظة جداً :** عملية تطوير البرمجيات التي تقوم بتطبيق الذكاء الاصطناعي تكلفتها العالية.
- **سبباً من أسباب البطالة :** وذلك بسبب الروبوتات التي تقوم بأداء الوظائف والتي تُعدّ إحدى تطبيقات الذكاء الاصطناعي.
- **سبباً في خطر كبير على الإنسان :** في حال استخدامها بشكل خاطئ أو وضع إحدى آلاتها في الأيدي غير الكفؤ.
- **استخدام الذكاء الاصطناعي بطريقة خطيرة :** لتحقيق هدف معين، ويحدث هذا عندما لا يتطابق عمل الذكاء الاصطناعي مع هدف الإنسان، إذ إنّ هذه التطبيقات لا تُنفذ ما يريده الإنسان بل تُطبّق ما يطلبه منها حرفياً.

تطبيقات الذكاء الاصطناعي

التصنيع

يُستخدم في تطوير الأنظمة التقنية المُستخدمة لجعلها قابلة للتكيف، ومرنة، وقادرة على اتخاذ القرارات الذكية في المواقف غير المتوقعة والاستجابة لها، ويمكن تطبيقها في مجال الهندسة، وإدارة سلسلة التوريد، والإنتاج والصيانة، وضمان الجودة، والتخزين في المستودعات.

الطاقة

يُستخدم لموازنة الطاقة بكفاءة وتخزينها في أنظمة الطاقة المتجددة، كما يتضمن ذلك استخدام عدادات ذكية لتحسين القدرة على تحمل تكاليف الطاقة الشمسية.

علم الروبوتات

والتي تستخدم في العديد من الصناعات مثل الرعاية الصحية، والتمويل، والتسويق. استكشاف الفضاء الخارجي مثل الآلات المرسلة إلى الفضاء؛ الأقمار الصناعية، وبناء الخرائط، وتكنولوجيا تتبع المواقع.

الرعاية الصحية

يُستخدم الذكاء الاصطناعي في مجال الرعاية الصحية في المناطق التي تفتقر إلى نظام رعاية صحية مُتقدم، حيث يتم من خلال التطبيقات التي تعتمد على الذكاء الاصطناعي التعرف على الأوبئة المحتملة مُبكراً، وتشخيصها من خلال التصوير، وعلاجها.

الزراعة

يستخدم في مراقبة صحة المحاصيل والتربة، الكشف عن الحشرات وأمراض النباتات، مراقبة صحة الماشية، الرش الذكي للمبيدات، إزالة الأعشاب الضارة تلقائياً، تصنيف المنتجات الزراعية وفرزها.

وسائل الإعلام الرقمية

بحيث تعرض الإعلانات التي تهم الشخص المستهدف من خلال تحليل بياناته وفهم توجهاته من عمليات بحثه على الإنترنت.

خدمة العملاء

مثل الروبوتات التي تستخدم في عمليات الرد على دردشات العملاء، والروبوتات التي تقوم بوظائف خدمة العملاء والتسويق الإلكتروني.

سوق الأوراق المالية

مثل الخوارزميات التي تستخدم في تحليل الأسهم في السوق المالية، وتحليل الأرباح والخسائر والتنبؤ بها.

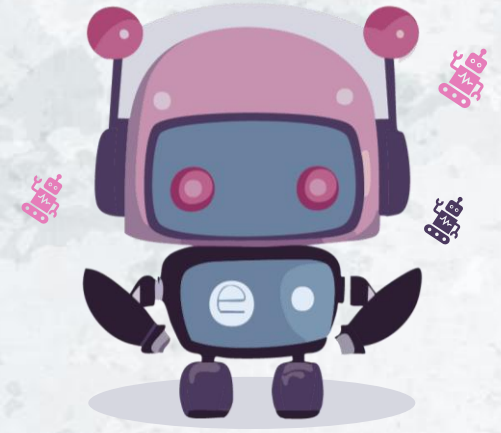
نماذج من تطبيقات الذكاء الاصطناعي :

اليوم يُعدّ الذكاء الاصطناعي مجالاً سريع النمو يُغيّر طريقة حياتنا وعملنا. من المساعدين الافتراضيين مثل سيري وأليكسا إلى السيارات ذاتية القيادة وأنظمة التصوير الطبي المتطورة، يلعب الذكاء الاصطناعي دورًا متزايد الأهمية في حياتنا اليومية. من أبرز التطورات في مجال الذكاء الاصطناعي اليوم تطوير الروبوتات المتقدمة، وابتكار أدوات تشخيص طبي مدعومة بالذكاء الاصطناعي، واستخدام خوارزميات التعلم الآلي لتحليل كميات هائلة من البيانات وتحديد الأنماط.

في الختام، يُجسّد تاريخ الذكاء الاصطناعي قصة بحث علمي، وابتكار تكنولوجي، وتطور الفكر البشري حول معنى الذكاء. من الأعمال المبكرة لتورينج ونيويل إلى الإنجازات التي حققها الذكاء الاصطناعي في عصرنا الحالي، قطع شوطاً طويلاً في غضون عقود قليلة. وبينما نتطلع إلى المستقبل، يتضح جلياً أن الذكاء الاصطناعي سيواصل لعب دور متزايد الأهمية في تشكيل العالم من حولنا، ولا يسعنا إلا أن نتخيل ما يحمله المستقبل من إنجازات وابتكارات جديدة. الذكاء الاصطناعي (AI) هو مصطلح يشير إلى قدرة الآلات أو برامج الحاسوب على أداء مهام تتطلب عادةً ذكاءً بشرياً، مثل التعلم وحل المشكلات واتخاذ القرارات. تواجد مجال الذكاء الاصطناعي لعقود عديدة، إلا أن التطورات الحديثة في التكنولوجيا أدت إلى زيادة سريعة في قدراته وتطبيقاته. في هذا الفصل، سنستكشف ماهية الذكاء الاصطناعي، وكيفية عمله، وتطبيقاته الحالية والمستقبلية المحتملة.

(الروبوت)

الروبوت يُعد من إحدى المجالات التي دخل فيها الذكاء الاصطناعي، حيث إنّ الروبوت هو جهاز ميكانيكيّ مصمّم ومبرمج لأداء الأعمال التي يقوم بها الإنسان بشكل عام، وقد أدّى اختراع الروبوتات الحديثة إلى ظهور الأجهزة والآلات التي لا حصر لها، والتي تحلّ محلّ عمل الأفراد.



من الجدير بالذكر أنّ معظم الروبوتات مبنية على برمجيات للعمل بشكل مستقل عن السيطرة البشرية المباشرة، ويُستخدم المصطلح أيضاً للمركبات وغيرها من الآلات التي يتمّ التحكم بها عن بعد من قبل المشغلّ البشري.

المحاضرة السادسة

الذكاء الاصطناعي ARTIFICIAL INTELLIGENCE (AI)

اعداد

د. وفاء حسن
د. حيدر عباس
م. صباح محمد

- أدوات الذكاء الاصطناعي وأطر العمل
- أنواع أدوات الذكاء الاصطناعي وأطر العمل
- كيف تدعم أطر عمل الذكاء الاصطناعي تطوير تطبيقات الذكاء الاصطناعي؟
- اختيار إطار عمل الذكاء الاصطناعي المناسب
- التطبيقات الواقعية لأدوات وأطر عمل الذكاء الاصطناعي

ما هي أدوات الذكاء الاصطناعي وأطر العمل؟

تُعدّ أدوات وأطر عمل الذكاء الاصطناعي بمثابة ركائز أساسية في تطوير الذكاء الاصطناعي، إذ تُمكن من تطوير نماذج ذكاء اصطناعي تُحاكي القدرات البشرية وتقوم بتدريبها ونشرها، بل وتحسّنها ايضاً.

فهي مجموعة من الأدوات المُصممة خصيصاً لتبسيط المهام التي يُمكن للآلات تعلمها، بدءاً من التعرّف على الكلام ووصولاً إلى التنبؤ بالاتجاهات، وتتضمن:

1. بيئات برمجية متكاملة تُساعد في كل مرحلة من مراحل تطوير نماذج الذكاء الاصطناعي،
2. مكاتب متخصصة تُركز على مهام مُحددة.

تُعنى هذه الأطر بالعمل الشاق وتمنع البدء بالبرمجة من الصفر فهي عبارة عن هياكل مُعدّة مسبقاً للشبكات العصبية ومجموعات البيانات، تحقق اهداف عدة منها تحسين منتج باستخدام خاصية التعرف على الصور، أو التنبؤ بالاتجاهات المالية، أو تحسين تفاعلات العملاء من خلال التحليلات التنبؤية، وهي باختصار، تُساعد المبرمجين على بناء أنظمة ذكاء اصطناعي مُعقدة بكفاءة أكبر.

أمثلة على أطر عمل الذكاء الاصطناعي الرائدة

► يُعدّ TensorFlow ،الذي طورته جوجل و PyTorch الذي صمم في مختبر الذكاء الاصطناعي التابع لفيسبوك، من أطر عمل الذكاء الاصطناعي الرئيسية والشائعة وهما يعتبران مفتوحا المصدر والذي يجعلهما مجانيين للاستخدام وبالتالي يسمحان بالتحديث المستمر من خلال مساهمات المستخدمين عبر العالم.

► يشتهر TensorFlow ببيئته الغنية بالأدوات والمكتبات والموارد، مما يُتيح أبحاثًا مكثفة في مجال التعلم الآلي وتطويرًا سهلًا لتطبيقات الذكاء الاصطناعي.

► على العكس من ذلك، يوفر PyTorch واجهة استخدام أبسط وأكثر سهولة، وهو مفضل بفضل رسوماته الحسابية الديناميكية التي تسمح بالتعديلات أثناء التشغيل. وهو مفيد للباحثين والمطورين الذين يحتاجون إلى مرونة في تصميم نماذجهم.

أنواع أدوات الذكاء الاصطناعي وأطر العمل

ان فهم هذه الأدوات يُساعد في اختيار الأداة المناسبة، سواءً لتحليل البيانات الضخمة، أو بناء أنظمة ذاتية التشغيل، أو تحسين تفاعل العملاء. ومن هذه الأنواع:

1. أطر التعلم الآلي

تُعدّ أطر عمل التعلم الآلي بمثابة محركات لتطوير نماذج الذكاء الاصطناعي التي تتعلم وتتخذ القرارات بناءً على البيانات. تُعد أدوات مثل Scikit-learn و TensorFlow و PyTorch رائدة في هذا المجال.

► تُناسب Scikit-learn المبتدئين والمحترفين على حد سواء، حيث تُوفر أدوات لاستخراج البيانات وتحليلها، وهي مثالية لخوارزميات التعلم الآلي التقليدية.

► أما TensorFlow و PyTorch، فتُوفر بيئات أكثر تعقيدًا للتعلم العميق، مما يُمكن النماذج من تنفيذ مهام مثل التنبؤ بالأسهم، والتشخيص الطبي، والقيادة الذاتية.

2. أدوات معالجة اللغة الطبيعية (NLP)

تُحسّن أدوات معالجة اللغة الطبيعية (NLP) التفاعل بين الحواسيب والبشر باستخدام اللغة. تُوفّر مكتبات مثل NLTK و SpaCy ميزات فعّالة لمهام معالجة اللغة، مثل تحليل المشاعر، وتجزئة المواضيع، وترجمة اللغات. على سبيل المثال، تستخدم SpaCy لبناء التطبيقات التي تتطلب فهمًا لغويًا، مثل برامج الدردشة الآلية أو أنظمة أتمتة خدمة العملاء.

3. أدوات الرؤية الحاسوبية

تساعد أدوات مثل TensorFlow و OpenCV الآلات على تفسير محيطها. تُسهم هذه الأطر في مهام متنوعة، من التعرف على الصور إلى تحليل الفيديو المعقدة. وهي بالغة الأهمية في المراقبة الآلية، والروبوتات المتقدمة، وتشخيص الصور الطبية.

4. أدوات معالجة البيانات وتحليلها

قبل أن يُحقق الذكاء الاصطناعي أهدافه، يجب أن تكون البيانات نظيفة ومنظمة. تستخدم أدوات معالجة البيانات المسبقة، مثل Pandas و NumPy و TensorFlow ، حيث تُبسّط Pandas و NumPy معالجة البيانات وتحليلها، مما يُسهّل تنظيفها وتحويلها. سواءً كان ذلك من خلال فرز مراجعات المستخدمين أو إعداد بيانات السلاسل الزمنية للتنبؤ.

كيف تدعم أطر عمل الذكاء الاصطناعي تطوير تطبيقات الذكاء الاصطناعي؟

1. TensorFlow: يُعد TensorFlow ، الذي طورته جوجل، يتميز بكفاءته في العمليات الحسابية الرقمية واسعة النطاق فهو ضروري لتدريب نماذج التعلم العميق.

تتيح بنية TensorFlow المرنة إجراء العمليات الحسابية على وحدات معالجة مركزية (CPU) أو وحدات معالجة رسومية (GPU) متعددة، مما يُسرّع تدريب النماذج. بالإضافة، تتميز أداة TensorBoard بميزات صورية قوية تستخدم لمراقبة تقدم التدريب وتحليله.

2. PyTorch: يتميز PyTorch ، الذي طورته مختبر أبحاث الذكاء الاصطناعي التابع لفيسبوك، برسم بياني حسابي ديناميكي يسمح بالتغييرات في وقت العمل الفعلي. يُعد هذا مفيداً للمشاريع التي تتطلب تعديلات متكررة على النموذج أثناء التشغيل.

يُشاد بـ PyTorch لسهولة استخدامه، وسهولة تصحيح أخطائه، ودعمه الكامل للتنفيذ السريع. وهو شائع الاستخدام بين الباحثين والمطورين الذين يُعطون الأولوية للمرونة والسرعة في تطوير الذكاء الاصطناعي.

3. Scikit-learn: على الرغم من تركيز كلٍّ من TensorFlow و PyTorch على التعلم العميق، إلا أن Scikit-learn يتفوق في مجال التعلم الآلي التقليدي.

يتميز Scikit-learn بسهولة الوصول إليه وبساطته، ويوفر خوارزميات تعلم متنوعة موجهة وغير موجهة عبر واجهة واحدة. وهو مثالي للمطورين الذين يحتاجون إلى حلول تعلم آلي سريعة وموثوقة دون تعقيدات التعلم العميق.

4. Keras: Keras هي واجهة برمجة تطبيقات (API) للشبكات العصبية عالية المستوى، مكتوبة بلغة بايثون، وتعمل على TensorFlow و CNTK و Theano صُممت أساسًا للتجارب السريعة، مما يجعلها مثالية للمبتدئين والباحثين على حد سواء.

تتيح بساطة Keras وتعدد وحداتها للمستخدمين التركيز على المفاهيم بدلًا من البرمجة المعقدة. كما أنها تُلخص العديد من تفاصيل برمجة الشبكات العصبية العميقة، مما يجعلها سهلة الاستخدام وفعّالة في الوقت نفسه.

5. أدوات مايكروسوفت المعرفية (CNTK): تتميز بكفاءتها العالية في تدريب خوارزميات التعلم العميق، وتوفر مكتبة شاملة تدعم أنواعًا مختلفة من الشبكات العصبية.

يُعدّ CNTK مفيدًا خصوصًا في البيئات التي تتضمن مجموعات بيانات ضخمة، حيث تُعد الكفاءة الحسابية أمرًا بالغ الأهمية.

اختيار إطار عمل الذكاء الاصطناعي المناسب

1. متطلبات المشروع وأهدافه

تعالج أطر عمل الذكاء الاصطناعي مشاكل مختلفة بناءً على احتياجات المشروع، بالنسبة لنماذج التعلم العميق المعقدة، يُعدّ TensorFlow وPyTorch خيارين مثاليين بفضل دعمهما للتخصصات الشاملة وقابلية التوسع. أما بالنسبة لحلول التعلم الآلي السريعة على مجموعات البيانات الأصغر، فإن بساطة Scikit-learn تُوفر الوقت والجهد. إن فهم أهداف المشروع - مثل معالجة اللغة الطبيعية، والتعرف على الصور، والتحليلات التنبؤية - يُساعدك على تضيق نطاق خيارات الأطر.

2. منحني التعلم ودعم المجتمع

تتميز أطر العمل مثل PyTorch بسهولة الاستخدام وسرعة التعلم، مما يجعلها مثالية للمبتدئين. أما TensorFlow ، فرغم قوته، أكثر تعقيدًا ويتطلب وقتًا أطول لإتقانه.

توفر أطر عمل مثل TensorFlow وPyTorch الموارد والدعم اللازمين للمجتمع عند مواجهة التحديات.

3. احتياجات الأداء وقابلية التوسع

تتطلب المشاريع المختلفة مستويات متفاوتة من القدرة الحسابية. بالنسبة لمشاريع البحث التي تتطلب نماذج أولية سريعة، تُعد قدرات PyTorch الديناميكية للرسوم البيانية مثالية. أما بالنسبة للتطبيقات واسعة النطاق، مثل الخدمات السحابية أو الذكاء الاصطناعي التوليدي، تتميز TensorFlow بقابلية التوسع والمتانة.

يُعد CNTK من Microsoft ممتازًا للمعالجة عالية الأداء عبر وحدات معالجة رسومية متعددة، بفضل معالجته للبيانات المتعددة الأبعاد.

4. متطلبات التكامل والنشر

بالنسبة للنماذج التي تتطلب تكاملاً سهلاً، يجب اختيار أطر عمل تتميز بدعم قوي لواجهات برمجة التطبيقات (API) وتوافقية بين المنصات. في حين يدعم TensorFlow منصات سحابية مثل Google Cloud و AWS و Azure، مما يُسهّل استخدامه على مستوى المؤسسات. يُعد TensorFlow Lite مناسباً لنشر النماذج على أجهزة الطرفية مثل الهواتف الذكية.

5. قابلية التوسع والدعم للمشروع في المستقبل

يتلقى كل من PyTorch و TensorFlow تحديثات منتظمة ودعمًا قويًا، مما يضمن استمرارهما في التطور. اختيار إطار عمل يتماشى مع الاتجاهات المستقبلية يضمن استثمارك مع تطور التكنولوجيا.

التطبيقات الواقعية لأدوات وأطر عمل الذكاء الاصطناعي

1. الرعاية الصحية: ثورة في التشخيص والعلاج

تُحسّن أطر عمل الذكاء الاصطناعي، مثل TensorFlow وPyTorch، تشخيص الأمراض للحصول على نتائج أدق وأسرع. يُستخدم الذكاء الاصطناعي في التصوير الطبي، ويستخدم الرؤية الحاسوبية لتحليل صور الأشعة السينية والرنين المغناطيسي والتصوير المقطعي المحوسب. ويحدد الذكاء الاصطناعي التشوهات، مثل الأورام أو الكسور، وتُحلل الخوارزميات بيانات المرضى لتخصيص العلاجات بناءً على السمات الجينية الفردية.

2. التجزئة (البيع بالمفرد): تحسين تجربة العملاء من خلال التخصيص

لقد أثّرت أدوات الذكاء الاصطناعي بشكل كبير على تجارة التجزئة، حيث خصّصت تجارب التسوق، وحسّنت سلاسل الدعم. تتنبأ نماذج الذكاء الاصطناعي، التي تستخدم أطر عمل مثل PyTorch، بتفضيلات العملاء من خلال سجلّ التصفح والمشتريات السابقة. يتيح ذلك تقديم توصيات فورية بالمنتجات، مما يعزز المبيعات ويرفع مستوى رضا العملاء. على الصعيد التشغيلي، تُدير أدوات الكشف الحاسوبية المخزون من خلال مراقبة مستوياته بالكاميرات، وضمان توافره، وتقليل عمليات الفحص اليدوي.

3. المالية: أتمتة تقييم المخاطر والكشف عن الاحتيال

في مجال التمويل، تُعزز أطر عمل الذكاء الاصطناعي أمن وكفاءة البنوك والمؤسسات المالية.

تُنشئ أطر عمل التعلم الآلي، مثل Scikit-learn ، نماذج تنبؤية لتقييم مخاطر مقدمي طلبات القروض من بياناتهم المخزنة مسبقاً. تتنبأ هذه النماذج باحتمالية التخلف عن السداد، مما يُساعد البنوك على اتخاذ قرارات إقراض مدروسة.

تُحسن أدوات الذكاء الاصطناعي التفاعلية خدمة العملاء بشكل ملحوظ من خلال أتمتة الردود عبر روبوتات الدردشة المُدعمة بالذكاء الاصطناعي. بالإضافة إلى ذلك، تقوم TensorFlow والأطر المماثلة بإنشاء خوارزميات للكشف عن المعاملات الاحتيالية من خلال تحديد الأنماط التي غير مرئية للبشر.

4. التسويق: قيادة الحملات القائمة على البيانات

تُحسن أدوات الذكاء الاصطناعي الحملات التسويقية وتجعلها أكثر تركيزاً على البيانات. تتيح أطر عمل مثل TensorFlow و PyTorch للمسوقين تحليل بيانات العملاء الشاملة للتنبؤ بسلوكياتهم وتفضيلاتهم. بل يمكنهم أيضاً التنبؤ بنجاح الحملة قبل إطلاقها. إضافةً إلى ذلك، تُنتج أدوات معالجة اللغة الطبيعية (NLP) نصوصاً تلبي احتياجات العملاء المحددة، مما يضمن مواد تسويقية مُخصصة وفعّالة وذات صلة.

5. التأثير على الابتكار وحل المشكلات

تُمكن أطر العمل المطورين من إنشاء نماذج أولية واختبارها بسرعة ، مما يُختصر رحلة التصميم من الفكرة إلى التنفيذ. وهذا يُسرّع الابتكار في مجالات مثل الرعاية الصحية والمالية. ومن خلال أتمتة تحليل البيانات، والتعرف على الصور، والتفاعلات الحوارية.

توفر أدوات الذكاء الاصطناعي الموارد البشرية، مما يُتيح التركيز على العمل الاستراتيجي، ودفع عجلة الابتكار بطرق غير مسبوقة.

المحاضرة السابعة

الذكاء الاصطناعي ARTIFICIAL INTELLIGENCE (AI)

- دور الذكاء الاصطناعي في الهواتف الذكية
- كيف يعزز الذكاء الاصطناعي دور
المساعدين الافتراضيين في الهواتف الذكية
- كيف يُعزز الذكاء الاصطناعي في الأجهزة
المحمولة الكفاءة ورضا المستخدم؟

اعداد

د. وفاء حسن
د. حيدر عباس
م. صباح محمد

دور الذكاء الاصطناعي في الهواتف الذكية

برز الذكاء الاصطناعي كقوة ثورية في عالم الهواتف المحمولة، محوّلًا هذه الأجهزة من أدوات تواصل بسيطة إلى رفيق ذكي من خلال محاكاة الذكاء البشري عبر تقنيات مثل التعلم الآلي، ومعالجة اللغة الطبيعية، والرؤية الحاسوبية.

مكّن الذكاء الاصطناعي الهواتف الذكية من أداء مهام كانت تتطلب تقليدياً تدخلاً بشرياً.

من الوظائف الأساسية إلى الميزات المتقدمة مثل التعرف على الوجه والواقع المعزز، يتغلغل الذكاء الاصطناعي بعمق في أنظمة تشغيل الهواتف المحمولة، مما يُشكّل طريقة تفاعلنا مع هواتفنا الذكية واعتمادنا عليها.

كيف يعزز الذكاء الاصطناعي دور المساعدين الافتراضيين في الهواتف الذكية

لقد غير صعود الذكاء الاصطناعي (AI) طريقة حياتنا وعملنا، ويُعدّ المساعدون الافتراضيون أحد أبرز الأمثلة على هذا التحوّل. فقد أصبح المساعدون الافتراضيون، المدعومون بالذكاء الاصطناعي، جزءًا لا يتجزأ من حياتنا اليومية، مما يُسهّل علينا إدارة وقتنا، والوصول إلى المعلومات، والتحكم في أجهزتنا الذكية. في هذه المحاضرة، سنستكشف المساعدين الافتراضيين الثلاثة الأكثر شيوعًا والمدعومين بالذكاء الاصطناعي: سيري ((Siri، وأليكسا ((Alexa، ومساعد جوجل (Google Assistant)، وكيف يُحدثون ثورة في طريقة حياتنا وعملنا. كما سنتناول فوائد وتحديات المساعدين الافتراضيين المدعومين بالذكاء الاصطناعي، وتطبيقاتهم المُحتملة في مختلف القطاعات.

1. سيري (Siri)

كان سيري (Siri)، الذي طورته شركة آبل، أول مساعد افتراضي يُطرح للعالم عام ٢٠١١. كان سيري متاحًا في البداية على هاتف iPhone 4S، ومنذ ذلك الحين تم دمج في أجهزة آبل الأخرى مثل iPad، وApple Watch، وMacBooks. يستخدم سيري خوارزميات معالجة اللغة الطبيعية (NLP) وتعلم الآلة لفهم الأوامر الصوتية والاستجابة لها.

لقد شهدت قدرات سيري Siri تطورًا مستمرًا على مر السنين، وأصبحت الآن قادرة على أداء مجموعة واسعة من المهام، بما في ذلك:



- الإجابة على أسئلة المعرفة العامة
- ضبط التذكيرات والتنبيهات
- إرسال الرسائل والبريد الإلكتروني
- إجراء المكالمات الهاتفية
- توفير الاتجاهات والملاحة
- التحكم في أجهزة المنزل الذكي
- تشغيل الموسيقى والبودكاست

يُعدّ تكامل سيري Siri مع أجهزة وخدمات Apple الأخرى أداةً فعّالة لمستخدمي Apple على سبيل المثال، يُمكن لـ Siri إرسال الرسائل والبريد الإلكتروني باستخدام تطبيقاتي الرسائل والبريد، وإجراء المكالمات الهاتفية باستخدام تطبيق الهاتف، وتوفير الاتجاهات والملاحة باستخدام تطبيق الخرائط.

2. أليكسا (Alexa)

أطلقت أليكسا، التي طورتها أمازون، عام ٢٠١٤، وأصبحت من أشهر المساعدين الافتراضيين في العالم. أليكسا مُدمجة في مكبرات صوت أمازون إيكو الذكية وغيرها من الأجهزة، وتُمكنها من أداء مجموعة واسعة من المهام، بما في ذلك:

- الإجابة على أسئلة المعرفة العامة
- تشغيل الموسيقى والاستماع إلى البودكاست
- ضبط المنبهات والمؤقتات
- التحكم في أجهزة المنزل الذكي
- توفير تحديثات الأخبار وتوقعات الطقس
- طلب المنتجات من أمازون



يُضفي تكامل أليكسا مع خدمات وأجهزة أمازون الأخرى عليها أداة فعّالة لمستخدمي أمازون. على سبيل المثال، يُمكن لأليكسا طلب المنتجات من أمازون باستخدام تطبيق أمازون للتسوق، والتحكم في أجهزة المنزل الذكي باستخدام مهارة أمازون للمنزل الذكي، وتوفير تحديثات الأخبار وتوقعات الطقس باستخدام مهارة أمازون للأخبار والطقس.

3. مساعد جوجل (Google Assistance)

طُرح مساعد جوجل، الذي طورته جوجل، عام ٢٠١٦ وأصبح منافسًا قويًا لسيري وأليكسا. يُدمج مساعد جوجل في مكبرات صوت جوجل هوم الذكية وغيرها من الأجهزة، ويُمكنه أداء مجموعة واسعة من المهام، بما في ذلك:



- الإجابة على أسئلة المعرفة العامة
- ضبط التذكيرات والتنبيهات
- إرسال الرسائل والبريد الإلكتروني
- إجراء المكالمات الهاتفية
- توفير الاتجاهات والملاحة
- التحكم في أجهزة المنزل الذكي
- تشغيل الموسيقى والبودكاست

تُكامل مساعد جوجل مع خدمات وأجهزة جوجل الأخرى يجعله أداة فعّالة لمستخدمي جوجل. على سبيل المثال، يُمكن لمساعد جوجل إرسال الرسائل والبريد الإلكتروني باستخدام تطبيق Gmail، وإجراء المكالمات الهاتفية باستخدام تطبيق Google Phone، وتوفير الاتجاهات والملاحة باستخدام تطبيق خرائط جوجل.

Siri VS Alexa VS Google Assistance

الأفضل في الإجابة على الأسئلة



كيف يُعزز الذكاء الاصطناعي في الأجهزة المحمولة الكفاءة ورضا المستخدم؟

يُعدّ دمج الذكاء الاصطناعي في الأجهزة المحمولة حافزًا يُمهّد الطريق لتحسينات جذرية تُعزز رضا المستخدم وتُحسّن الكفاءة العامة. يُعزز هذا التكامل السلس من قوة الهواتف الذكية ويُمهّد الطريق لوظائف مبتكرة مُصممة خصيصًا لتلبية احتياجات المستخدم.

1. تحسينات الكاميرا

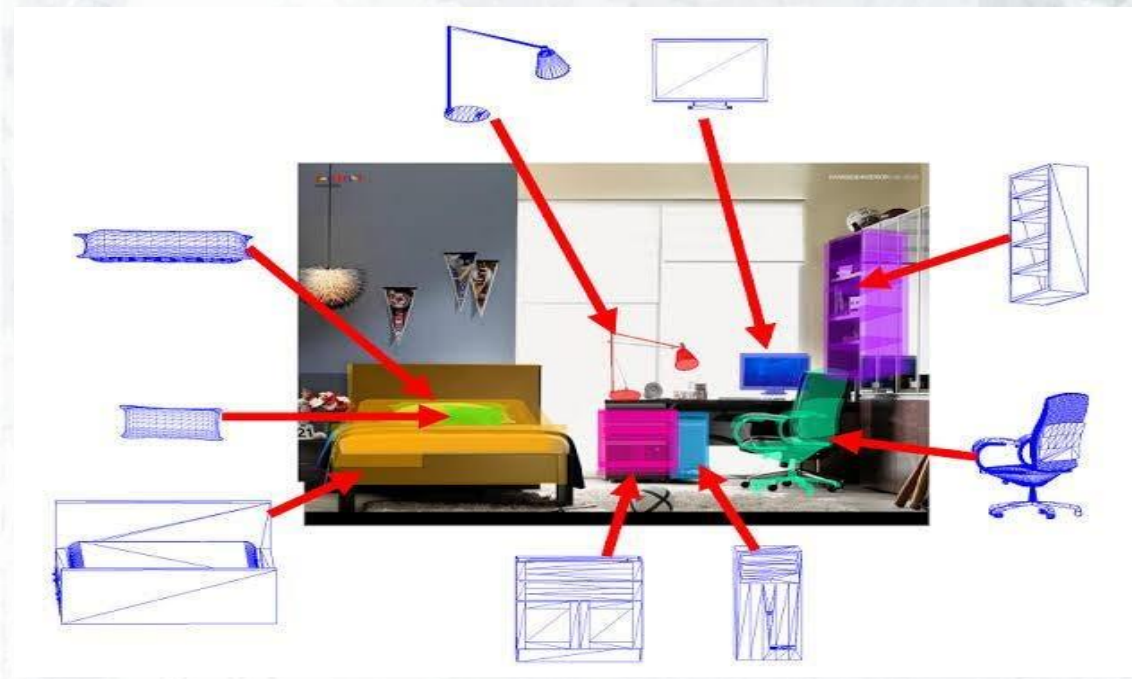
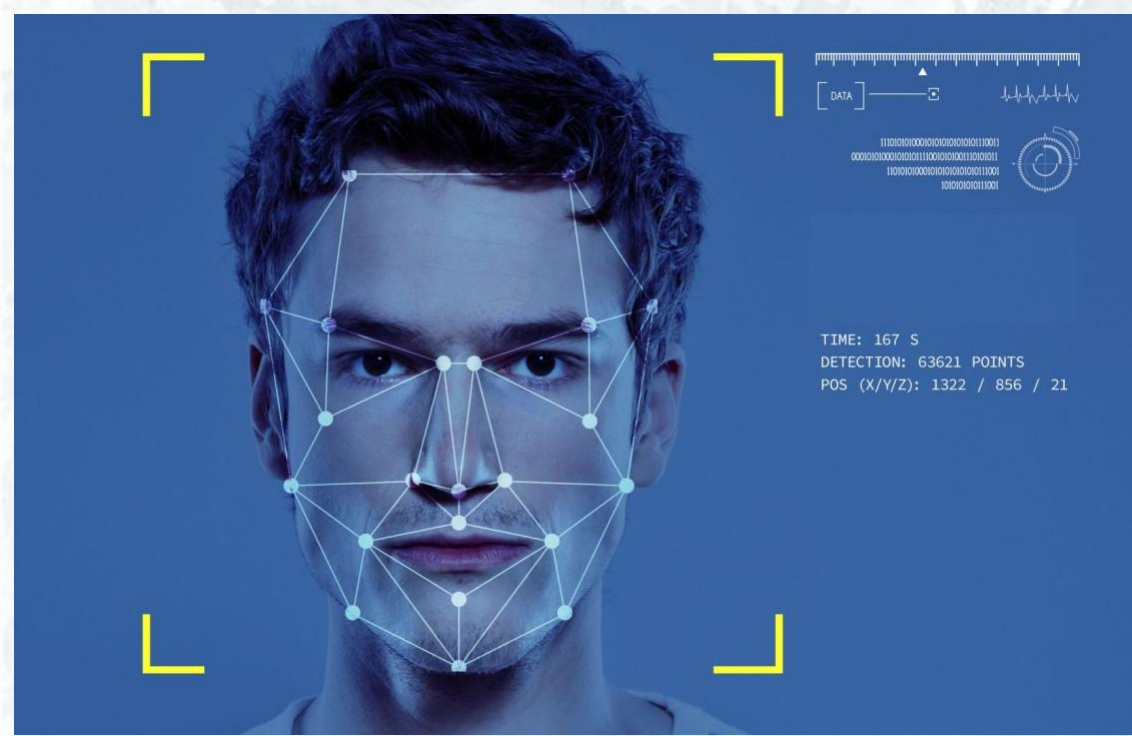
أثر الذكاء الاصطناعي بشكل كبير على قدرات الكاميرا في الأجهزة المحمولة الحديثة. فمن خلال التعرّف على الصور ومعالجتها المُتقدّمة، تُحسّن خوارزميات الذكاء الاصطناعي إعدادات الكاميرا بناءً على المشهد وظروف الإضاءة والموضوع، مما يُنتج جودة صورة فائقة. تُحسّن ميزات مثل التعرّف على المشهد القائم على الذكاء الاصطناعي، والتعرّف على الوجه، والتصوير الحاسوبي تجربة التصوير الشاملة للمستخدمين، مما يسمح لهم بالتقاط صور مذهلة بسهولة. بالإضافة إلى ذلك، تُمكن أدوات تحرير الصور المُدعّمة بالذكاء الاصطناعي المستخدمين من تحسين صورهم وتخصيصها مباشرةً على هواتفهم الذكية، مما يُسهّم في تجربة مستخدم أكثر إرضاءً وإبداعًا.

1.1 اكتشاف الوجه

شهدت تقنية اكتشاف الوجه المدعومة بالذكاء الاصطناعي في التصوير الفوتوغرافي بالهواتف المحمولة تطورًا ملحوظًا. تضمن هذه التقنية تركيزًا دقيقًا على الأجسام، مما يجعل صور البورتريه واضحة ونقية. علاوة على ذلك، تُمكن من وضع علامات تلقائية على الوجوه في معارض الصور، مما يُسهّل على المستخدمين تنظيم صورهم وتحديد مواقعها. بالإضافة إلى ذلك، تُوظف ميزات التجميل المدعومة بالذكاء الاصطناعي تقنية اكتشاف الوجه لتحسين ملامح الوجه، مما يُتيح للمستخدمين القدرة على تحسين صورهم وإتقانها بسهولة.

1.2 التعرف على الأشياء

يُعدّ التعرف على الأشياء نقلة نوعية في التصوير الفوتوغرافي بالهواتف المحمولة، إذ يتجاوز مجرد الوجوه البشرية ليحدّد مجموعة واسعة من الأشياء داخل المشهد. تُحلّل خوارزميات الذكاء الاصطناعي تركيب الصورة، مُتعرّفةً على عناصر مثل النباتات والحيوانات، أو حتى معالم مُحدّدة. تُتيح هذه القدرة على التعرّف للهواتف الذكية ضبط الإعدادات بذكاء، مثل توازن اللون والتعريض الضوئي، بناءً على الأشياء المُحدّدة. نتيجةً لذلك، يمكن للمستخدمين التقاط صور متوازنة وجذابة بصريًا، خاصةً في المشاهد المعقدة التي تتضمن عناصر متعددة.



1.3 وضع البورتريه

أحدث وضع البورتريه، المدعوم بالذكاء الاصطناعي، ثورةً في كيفية التقاط المستخدمين لصور بورتريه احترافية باستخدام هواتفهم الذكية. فمن خلال خوارزميات متقدمة لاستشعار العمق، يُمكن الذكاء الاصطناعي من محاكاة عمق مجال ضحل، مما يُطمس الخلفية مع الحفاظ على تركيز الجسم. وهذا يُنتج تأثير بوكيه مذهلاً بصرياً، يُشبه ما تُحققه كاميرات DSLR المتطورة. لا يُتيح وضع البورتريه المدعوم بالذكاء الاصطناعي للمستخدمين القدرة على التقاط صور بورتريه فنية فحسب، بل يُوفر أيضاً مستوى من التحكم في جماليات الخلفية، مما يسمح بتصوير أكثر إبداعاً وشخصية.



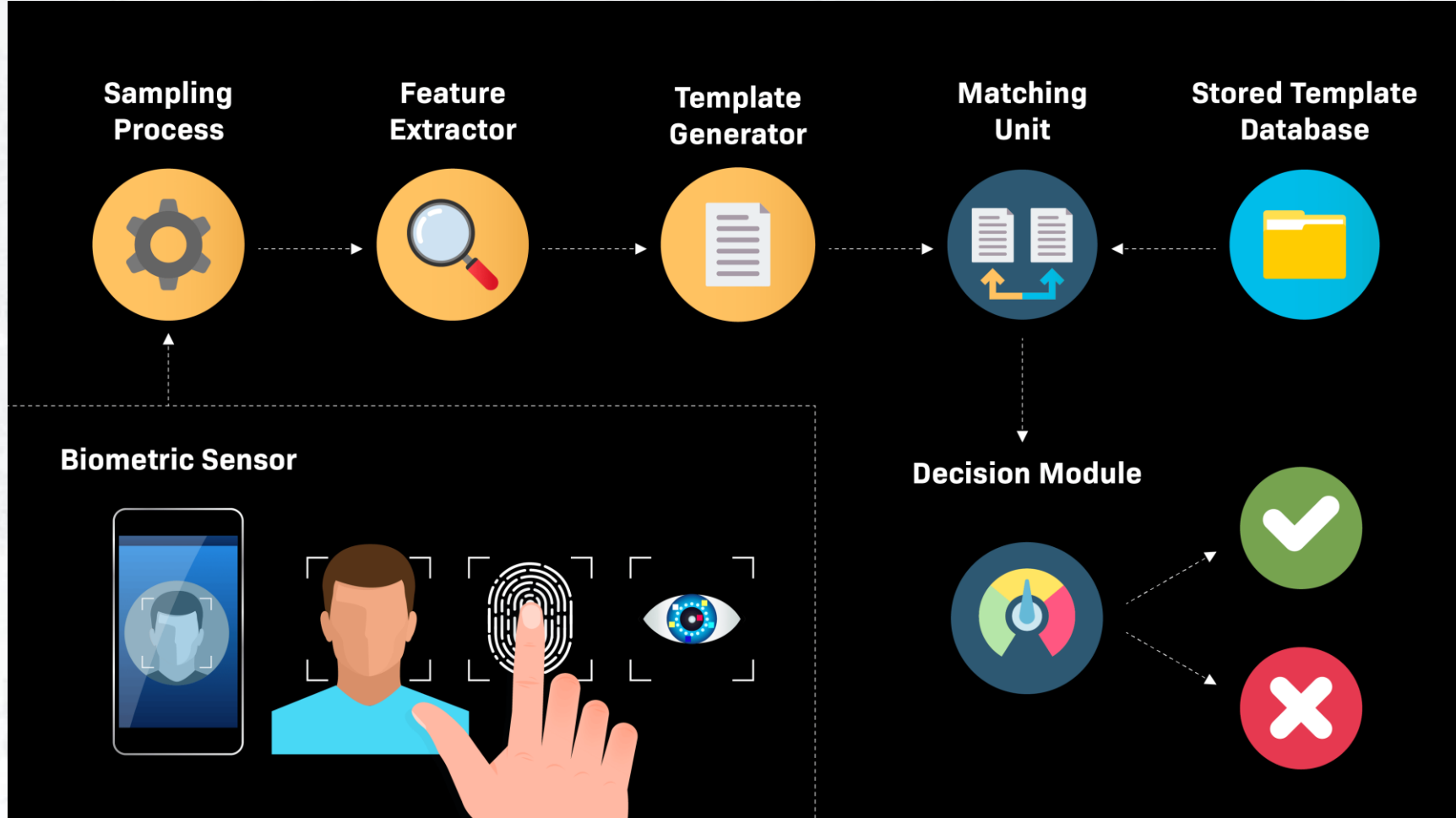
1.4 الوضع الليلي

يُحسّن الوضع الليلي إعدادات الكاميرا المختلفة لتحسين رؤية الأجسام، وتقليل الضوضاء، وتحسين جودة الصورة بشكل عام. تُحلل خوارزميات الذكاء الاصطناعي الضوء المتاح وتُضبط أوقات التعرض، مما يضمن للمستخدمين التقاط صور ساطعة ومفصلة حتى في ظروف الإضاءة الليلية الصعبة. أصبحت هذه الميزة عنصراً أساسياً في الهواتف الذكية الحديثة، مما يسمح للمستخدمين بتوثيق تجاربهم الليلية بوضوح وتفصيل غير مسبوقة.



2. الأمان والقياسات الحيوية

يلعب الذكاء الاصطناعي دورًا حاسمًا في تعزيز ميزات الأمان في الأجهزة المحمولة. توفر تقنيات التعرف على الوجه ومسح بصمات الأصابع، المدعومة بخوارزميات الذكاء الاصطناعي، طرقًا آمنة ومريحة لفتح الهواتف والتحقق من هوية المستخدمين. ولا تقتصر موثوقية هذه الطرق على كونها أكثر موثوقية فحسب، بل تتكيف وتتحسن بمرور الوقت، مما يعزز الوضع الأمني العام للأجهزة المحمولة.



ويتعلم الذكاء الاصطناعي ويُحدِّث نماذجَه باستمرار للتعرف على المستخدمين الحقيقيين والتهديدات الأمنية المحتملة والتمييز بينها، مما يضمن حماية قوية ضد الوصول غير المصرح به.

3. تحسين عمر البطارية

غالبًا ما تواجه الأجهزة المحمولة تحديات في إدارة عمر البطارية بكفاءة. ويأتي الذكاء الاصطناعي لإنقاذ الموقف من خلال تحسين استهلاك الطاقة بناءً على سلوك المستخدم وأنماط استخدامه. وتتعلم الخوارزميات التكيفية متى وكيف يُستخدم الجهاز، مع تعديل عمليات الخلفية والتطبيقات المستهلكة للطاقة للحفاظ على الطاقة. ويؤدي ذلك إلى إطالة عمر البطارية وتحسين موثوقية الجهاز بشكل عام. كما يساعد الذكاء الاصطناعي في التنبؤ بحالة البطارية، موفرًا للمستخدمين رؤى وتوصيات للحفاظ على الأداء الأمثل للبطارية مع مرور الوقت.

4. تتبع الصحة والسلامة

في عصر المستهلكين المهتمين بصحتهم، تُسهم الأجهزة المحمولة المجهزة بالذكاء الاصطناعي في تحسين صحة المستخدمين. تستخدم تطبيقات تتبع الصحة واللياقة البدنية الذكاء الاصطناعي لتحليل البيانات من المستشعرات، وتقديم رؤى شخصية حول النشاط البدني، وأنماط النوم، والصحة العامة. تُمكن هذه الميزات المستخدمين من اتخاذ قرارات مدروسة بشأن صحتهم، مما يعزز نهجًا شاملاً للصحة. تستطيع خوارزميات الذكاء الاصطناعي اكتشاف أي شذوذ أو أنماط تشير إلى مشاكل صحية، مما يُقدم للمستخدمين اقتراحات استباقية لأسلوب حياة أكثر صحة.

المحاضرة الثامنة

الذكاء الاصطناعي ARTIFICIAL INTELLIGENCE (AI)

اعداد

د. وفاء حسن
د. حيدر عباس
م. صباح محمد

- تأثير الذكاء الاصطناعي على تجربة المستخدم
- فكيف يُحسّن الذكاء الاصطناعي تفاعل المستخدم؟
- الذكاء الاصطناعي وتجربة الهاتف الذكي المخصصة
- الذكاء الاصطناعي المتقدم: إعادة تصور الهواتف الذكية اليوم
- الآفاق المستقبلية للذكاء الاصطناعي في الهواتف الذكية
- الاتجاهات الناشئة في الذكاء الاصطناعي لتكنولوجيا الهاتف المحمول
- تحديات الذكاء الاصطناعي

تأثير الذكاء الاصطناعي على تجربة المستخدم

- أن فهم الذكاء الاصطناعي يشير الى أساسيات التكامل المبكر للهواتف الذكية فهو يشير إلى محاكاة الذكاء البشري في الآلات المبرمجة للتفكير والتعلم.
- هو مجال واسع يبدأ من خوارزميات التعلم الآلي التي تتكيف وتتعلم من البيانات الجديدة، وصولاً إلى معالجة اللغة الطبيعية التي تُمكن الأجهزة من فهم الكلام البشري والاستجابة له.
- يهدف الذكاء الاصطناعي إلى تحسين وظائف الآلات، وتمكينها من أداء مهام معقدة بدرجة من الاستقلالية.
- الذكاء الاصطناعي ليس إضافة جديدة في مجال الهواتف الذكية. فقد كانت ميزات مثل أدوات التصوير، والمساعدين الصوتيين، والنص التنبؤي، بالإضافة إلى الموسيقى والتعرف على الوجه، أساسيةً لسنوات. وقد غيّر Siri، مساعد آبل الصوتي، الذي أُطلق عام ٢٠١١، طريقة تفاعل المستخدمين مع أجهزتهم. وبالمثل، يُعزز الذكاء الاصطناعي من جوجل ميزات التنبؤ بالنص والتعرف على الصوت في هواتف أندرويد، مما يجعلها أكثر ذكاءً وسهولة في الاستخدام.
- مع ظهور الذكاء الاصطناعي، أصبحت الهواتف الذكية أكثر من مجرد أدوات اتصال، بل أصبحت رفيقًا ذكيًا يفهم احتياجات مستخدميه ويتكيف معها.

فكيف يُحسّن الذكاء الاصطناعي تفاعل المستخدم؟

► لقد حسّن الذكاء الاصطناعي تفاعل المستخدمين مع الهواتف الذكية بشكل كبير من خلال تمكين تقنيات متقدمة مثل معالجة اللغة الطبيعية والتعرف على الصوت. مهدت هذه التطورات الطريق للمساعدين الافتراضيين، المدعومين بالذكاء الاصطناعي، لفهم الأوامر الصوتية والاستجابة لها.

► تخيل أنك قادر على إنجاز مهام على هاتفك الذكي دون لمسّه. بفضل الذكاء الاصطناعي، أصبح هذا واقعًا ملموسًا بفضل المساعدين الافتراضيين مثل سيري ومساعد جوجل وأليكسا. أصبح بإمكان المستخدمين الآن التحدث إلى هواتفهم الذكية وتنفيذ الأوامر، سواءً كانت إرسال رسالة نصية أو إجراء مكالمة هاتفية أو تشغيل موسيقاهم المفضلة.

► لا يُعزز هذا التفاعل بدون استخدام اليدين الراحة فحسب، بل يفتح أيضًا آفاقًا جديدة للأشخاص ذوي الإعاقة. إذ أصبح بإمكان الأشخاص الذين يجدون صعوبة في استخدام أيديهم أو محدودي الحركة الوصول إلى كامل وظائف الهواتف الذكية، مما يُمكنهم من البقاء على اتصال دائم بالعالم الرقمي.

الذكاء الاصطناعي وتجربة الهاتف الذكي المخصصة

► من أهم مزايا دمج الذكاء الاصطناعي في الهواتف الذكية القدرة على توفير تجارب شخصية حيث تُحلل خوارزميات الذكاء الاصطناعي كميات هائلة من بيانات المستخدم، بما في ذلك سجل التصفح وأنماط استخدام التطبيقات والتفضيلات، لتخصيص تجربة الهاتف الذكي لكل مستخدم على حدة.

► تستطيع هذه الخوارزميات التنبؤ باحتياجات المستخدم، واقتراح محتوى ذي صلة، بل وتوقع الإجراءات قبل طلبها صراحةً. على سبيل المثال، إذا كان المستخدم يستخدم تطبيقًا معينًا بشكل متكرر في وقت محدد من اليوم، يعرض الهاتف الذكي اختصارًا لهذا التطبيق بشكل استباقي خلال ذلك الوقت، مما يسهل الوصول إليه.

► علاوة على ذلك، تستطيع الهواتف الذكية المدعومة بالذكاء الاصطناعي التعلّم من سلوك المستخدم وتكييف توصياتها مع مرور الوقت. فمع تفاعل المستخدمين مع أجهزتهم، تُحسّن خوارزميات الذكاء الاصطناعي فهمهم للتفضيلات الفردية باستمرار، مما يضمن تخصيص تجربة الهاتف الذكي بشكل متزايد وتخصيصها لتلبية احتياجات كل مستخدم الفريدة.

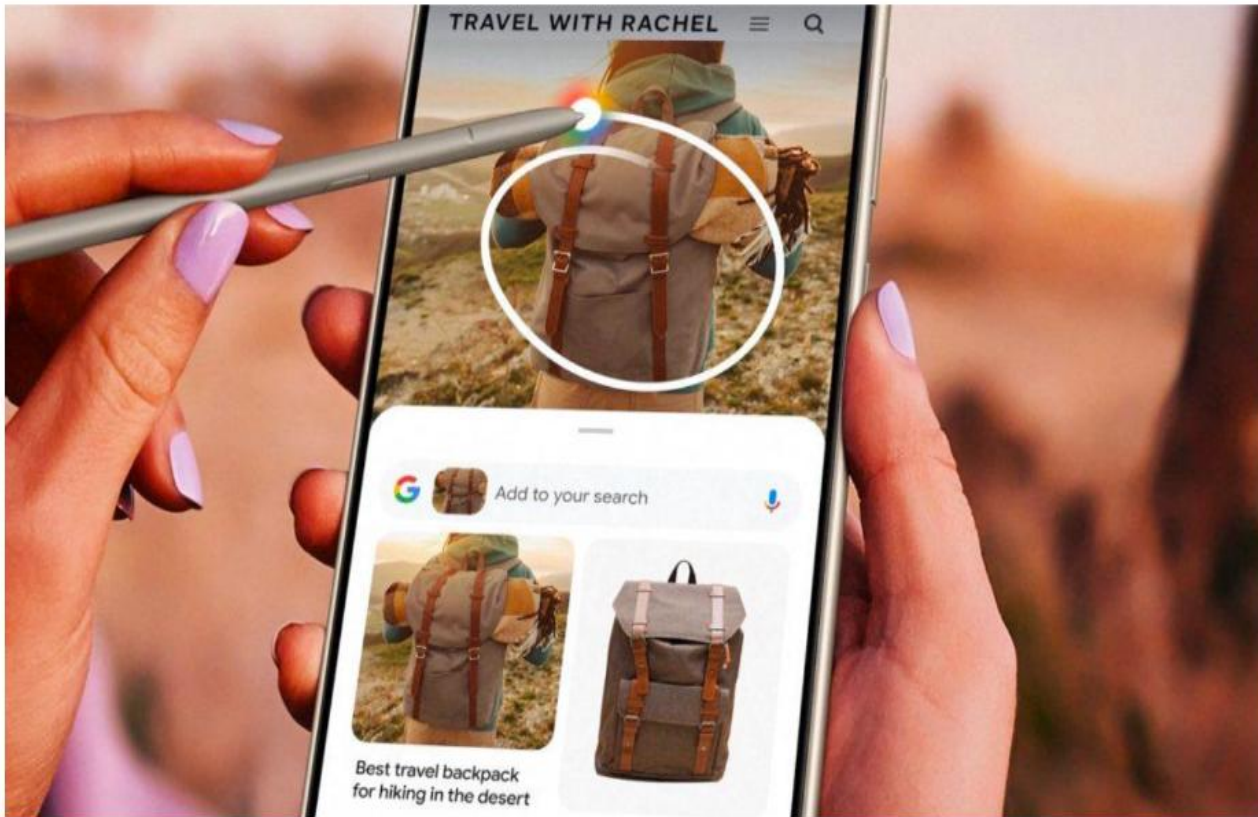
► هذا المستوى من التخصيص لا يعزز رضا المستخدم فحسب، بل يُعزز أيضًا ارتباطًا أعمق بين المستخدمين وهواتفهم الذكية. فمن خلال تقديم محتوى ذي صلة وفي الوقت المناسب، تصبح الهواتف الذكية المدعومة بالذكاء الاصطناعي أدوات لا غنى عنها تتكامل بسلاسة مع الحياة اليومية للمستخدمين.

► في الختام، للذكاء الاصطناعي تأثير عميق على تجربة مستخدم الهواتف الذكية. فمن تمكين التفاعل بدون استخدام اليدين إلى توفير تجارب شخصية، حوّل الذكاء الاصطناعي الهواتف الذكية إلى رفيق ذكي يفهم احتياجات مستخدميه ويتكيف معها. ومع استمرار تطور الذكاء الاصطناعي، يمكننا توقع المزيد من التطورات المثيرة في المستقبل، مما يُحسّن تجربة المستخدم ويجعل الهواتف الذكية جزءًا أساسيًا من حياتنا.

الذكاء الاصطناعي المتقدم: إعادة تصور الهواتف الذكية اليوم

ومع ذلك، فإن الجديد هو إدخال الذكاء الاصطناعي التوليدي في الهواتف الذكية، حيث سيتم شحن أكثر من مليار هاتف ذكي مزود بالذكاء الاصطناعي التوليدي بحلول عام 2027. وبعيدًا عن الاعتماد على السحابة، تتيح التطورات في شرائح المعالجة، مثل معالج Dimensity 9300 من MediaTek ومعالج Snapdragon 8 Gen3 من Qualcomm، المزيد من الذكاء الاصطناعي للعمل مباشرةً على الأجهزة، مما يُسرّع المعالجة ويُحسّن تجربة المستخدم. وهناك العديد من الأمثلة على كيفية استخدام الذكاء الاصطناعي التوليدي بالفعل في أحدث الهواتف الذكية:

Google's 'circle to search' feature



1. تحسين البحث: كشفت جوجل عن ميزة "البحث الدائري" لهواتف أندرويد، وهي ميزة تُمكن المستخدمين من البحث من أي مكان على أجهزتهم باستخدام إيماءات مثل التدوير أو التظليل أو الكتابة أو النقر.

2. تحرير الصور: في سلسلة Pixel 8، أطلقت جوجل إمكانيات مدعومة بالذكاء الاصطناعي، مثل Magic Editor لملء الخلفية وتعديل العناصر، وBest Take، الذي يدمج عدة صور لإنتاج صورة جماعية مثالية. بالإضافة إلى ذلك، تتضمن هواتف سامسونج جالاكسي الذكية وظيفة Object Eraser، المصممة لإزالة العناصر من الصور.
3. المساعدة الافتراضية: قدمت OnePlus أداة AI Summarizer لتلخيص المكالمات الهاتفية بإيجاز. وفي الوقت نفسه، يُلخص Android Auto AI الرسائل والمستندات ومحتوى الويب بسرعة. علاوة على ذلك، يُمكن لمساعد الدردشة من سامسونج و Magic Compose من جوجل ضبط نغمات الرسائل قبل إرسالها.
4. إمكانية الوصول: يُكسر الذكاء الاصطناعي حواجز اللغة من خلال ميزات الترجمة الفورية، ويُمكنه مساعدة المستخدمين ذوي الإعاقة من خلال الأوامر الصوتية وقارئ الشاشة، مما يجعل الهواتف الذكية أكثر تنوعًا وشمولاً.

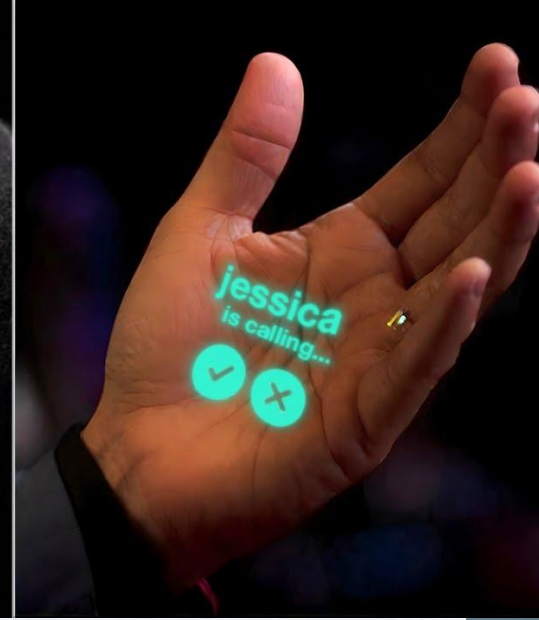
الآفاق المستقبلية للذكاء الاصطناعي في الهواتف الذكية

يحمل مستقبل الذكاء الاصطناعي في تطوير الهواتف الذكية إمكانات هائلة لمزيد من الابتكار والتطوير. من المرجح أن تُشغل هواتف الجيل التالي الذكية المزودة بالذكاء الاصطناعي شرائح أكثر تطورًا، مثل معالج Snapdragon 8 Gen4 القادم، والذي يهدف إلى تعزيز الأداء، وتطوير الميزات الحالية، وإدخال ميزات جديدة، مما يُعزز ابتكارات الهواتف المحمولة. ومع ذلك، في حين أن تفاصيل هذه الميزات القادمة لم تُكشف بعد، إلا أنها قد تشمل قدرات اتصال مُحسّنة، مثل مساعد رد آلي مُدعم بالذكاء الاصطناعي يُجيب على المكالمات بصوتك، أو تجارب ألعاب أكثر تخصيصًا. بالإضافة إلى ذلك، هناك تكهنات حول فرض رسوم على العملاء مقابل ميزات الذكاء الاصطناعي هذه، إما من خلال رسوم فتح لمرة واحدة، أو، وهو الأرجح، من خلال نموذج اشتراك.

ومع ذلك، فإن الشراكات المبتكرة، مثل تلك التي عقدتها Qualcomm ، Deutsche Telekom وBrain.ai، هي التي تُمهّد الطريق لتطورات رائدة مثل "T-phone"، وهو مفهوم هاتف ذكي بدون تطبيقات. باستخدام الذكاء الاصطناعي، يعمل هذا الجهاز كبواب رقمي، يفهم أهدافك ويدير مهامك نيابةً عنك، مُغنيًا عن الحاجة إلى العديد من التطبيقات.

تُطوّر شركات أخرى أجهزة قابلة للارتداء ومحمولة لدعم الهواتف الذكية، مثل جهاز AI Pin من Humane، ونظارات Meta الذكية، وجهاز Rabbit R1، مما يُمثّل مرحلة جديدة في دمج الذكاء الاصطناعي مع التكنولوجيا الشخصية. تُقدّم هذه الأجهزة أشكالاً جديدة من المساعدة المُدعّمة بالذكاء الاصطناعي، وتندمج بسلاسة في الروتين اليومي. ومع ذلك، ورغم أنها ليست بدائل مباشرة للهواتف الذكية حتى الآن، إلا أنها تُشير إلى مستقبل قد يتحول فيه تفاعلنا الأساسي مع العالم الرقمي بعيداً عن الشاشات التقليدية.

Rabbit R1



AI Meta Glasses



الاتجاهات الناشئة في الذكاء الاصطناعي لتكنولوجيا الهاتف المحمول

► من المتوقع أن يشهد الذكاء الاصطناعي في الهواتف الذكية اتجاهات ناشئة، مثل تحسين معالجة اللغة الطبيعية، وتحسين فهم السياق، وتحسين القدرات التنبؤية. بالإضافة الى ذلك، من المتوقع أن يحدث دمج الذكاء الاصطناعي مع الواقع المعزز (AR) والواقع الافتراضي (VR) ثورة في طريقة تفاعلنا مع الهواتف الذكية وتجربة المحتوى الرقمي.



تحديات الذكاء الاصطناعي

1. مخاوف الخصوصية والأمان: غالبًا ما تتطلب أنظمة الذكاء الاصطناعي الوصول إلى كمية هائلة من البيانات الشخصية للتعلم والتنبؤ، مما يُثير مخاوف بشأن كيفية استخدام هذه البيانات وحماية أمنها والتحيز. قد تُصبح أنظمة الذكاء الاصطناعي المتطورة أهدافًا للمُخترقين، مما يُشكّل تهديدًا لبيانات المستخدم وخصوصيته. فمن الضروري ضمان التعامل مع معلومات المستخدم بمسؤولية وشفافية وأمان. بالإضافة إلى ذلك، يجب معالجة التحيزات المحتملة في خوارزميات الذكاء الاصطناعي لضمان نتائج عادلة وغير متحيزة لجميع المستخدمين .
2. قيود الأجهزة: هناك تحديات تقنية مثل تلك التي واجهتها أجهزة Gemini Nano من Google. كان هذا النموذج من الذكاء الاصطناعي يهدف في البداية إلى تعزيز هاتف Pixel 8 بميزات مُتقدّمة، ولكنه واجه مشاكل في التكامل بسبب قيود الأجهزة. يُؤكد هذا على الصراع بين الوعود النظرية للذكاء الاصطناعي والواقع العملي لأجهزة الهواتف الذكية.
3. العوائق الاقتصادية: تُشكل التكاليف المرتفعة المرتبطة بتطوير الذكاء الاصطناعي خطرًا يُصعّب الوصول إلى هذه الابتكارات، خاصةً لأصحاب الميزانيات المحدودة. ومع ذلك، يهدف إصدار معالج Snapdragon 8s Gen3 في عام 2024 إلى جلب ميزات رائدة إلى هواتف ذكية بأسعار معقولة، مما يُحسن إمكانية الوصول إليها.
4. النفائات الإلكترونية: قد يؤدي دمج الذكاء الاصطناعي في الهواتف الذكية إلى زيادة مبيعاتها، حيث يسعى المستهلكون إلى مواكبة أحدث التقنيات، مما يؤدي إلى زيادة النفائات الإلكترونية.

5. الاعتماد على الأجهزة: مع ازدياد ذكاء الهواتف الذكية، قد يجد المستخدمون أنفسهم معتمدين بشكل مفرط على هذه الأجهزة في المهام اليومية، مما قد يؤثر على قدرتهم على أداء هذه المهام بشكل مستقل.
6. نقص القوى العاملة الماهرة للتنمية: يتطلب تطوير ميزات الذكاء الاصطناعي المتقدمة قوة عاملة متخصصة في التعلم الآلي وعلوم البيانات وهندسة الأجهزة. ويؤدي النقص العالمي في هذه الكفاءات إلى إبطاء الابتكار، كما أنه يزيد من تكلفة تطوير الذكاء الاصطناعي، مما يُشكل عقبة كبيرة أمام المُصنّعين الذين يسعون إلى دمج أحدث قدرات الذكاء الاصطناعي في الهواتف الذكية.
7. زيادة استهلاك الطاقة: مع أن الذكاء الاصطناعي يُحسّن الأداء، إلا أنه قد يُرهق بطاريات الأجهزة بسبب متطلبات معالجة البيانات المكثفة. لذا، يجب تطوير أنظمة فعّالة لإدارة الطاقة لتجنب أي اختلال في الأداء وضمان عدم تعرض المستخدمين لانخفاض في عمر البطارية نتيجة دمج الذكاء الاصطناعي.
8. التحديات التنظيمية والقانونية: يخضع تطبيق الذكاء الاصطناعي للوائح وأطر قانونية متفاوتة في مختلف المناطق. ويمثل استيفاء هذه المتطلبات، مع ضمان الامتثال لقوانين حماية البيانات والمعايير الأخلاقية للذكاء الاصطناعي، تحديًا معقدًا لمصنعي الهواتف الذكية العالميين. ومع ذلك، يمكن لشركة رائدة في تطوير الذكاء الاصطناعي مساعدتك في التغلب على التحديات التنظيمية والقانونية.



التجارة الإلكترونية E _ Commerce

المحاضرة التاسعة

■ التجارة الإلكترونية

■ تاريخ التجارة الإلكترونية

■ مزايا وعيوب التجارة الإلكترونية

■ أنواع التجارة الإلكترونية

■ خدمات بطاقات الصراف الآلي والخصم

■ ماهي بطاقة الخصم

■ الخدمات المصرفية عبر الهاتف المحمول

■ مزايا وعيوب الخدمات المصرفية عبر الهاتف المحمول

■ الخدمات المصرفية عبر الرسائل النصية القصيرة

■ التنبيه الإلكتروني (الاشعارات)

(E_C)

اعداد

د. وفاء حسن

د. حيدر عباس

م. صباح محمد



التجارة الإلكترونية

التجارة الإلكترونية هي عملية شراء وبيع السلع والخدمات عبر الإنترنت. يمكن ممارسة التجارة الإلكترونية عبر أجهزة الكمبيوتر، والأجهزة اللوحية، والهواتف الذكية، وغيرها من الأجهزة الذكية. أصبح كل منتج وخدمة تقريبًا متاحًا الآن من خلال التجارة الإلكترونية. لكنها لا تقتصر على مجرد وجود مشترٍ وبائع، بل تعتمد على بنية تحتية واسعة، غالبًا ما تكون غير مرئية، لضمان استمراريتها.

Ecommerce

[ˈē kă-()mɑrs]

Companies and individuals that buy and sell goods and services over the Internet.



- ساعدت التجارة الإلكترونية الشركات (وخاصةً تلك ذات النطاق الضيق، مثل الشركات المحلية الصغيرة) على الوصول إلى سوق أوسع من خلال توفير قنوات بيع وتوزيع أرخص وأكثر كفاءة لمنتجاتها أو خدماتها.
- في حين أن بعض الشركات تعمل بالكامل عبر الإنترنت، فإن بعضها الآخر يتنقل بين العالمين الحقيقي والافتراضي.

على سبيل المثال، تُعد شركة تارجت (TGT) واحدة من العديد من شركات التجزئة العملاقة التي استكملت حضورها التقليدي بمتجر إلكتروني يتيح للعملاء شراء كل شيء، من الملابس وآلات صنع القهوة إلى معجون الأسنان ودمى الحركة، دون مغادرة منازلهم. في المقابل، يتزايد إقبال البائعين الأفراد على إجراء معاملات التجارة الإلكترونية عبر مواقعهم الإلكترونية الشخصية. وتُعدّ الأسواق الرقمية مثل eBay وEtsy بمثابة منصاتٍ لتبادل المنتجات، حيث يجتمع عددٌ كبيرٌ من المشترين والبائعين لإجراء معاملاتهم التجارية.

تاريخ التجارة الإلكترونية

يعود تاريخ التجارة الإلكترونية إلى ستينيات القرن الماضي، عندما استخدمت الشركات نظامًا إلكترونيًا يُسمى التبادل الإلكتروني للبيانات لتسهيل نقل المستندات. ولم تُجرَ أول معاملة تجارية إلا عام ١٩٩٤، حيث شملت بيع قرص مدمج بين صديقين عبر موقع بيع بالتجزئة عبر الإنترنت يُسمى NetMarket.

مزايا وعيوب التجارة الإلكترونية

المزايا:

تُقدم التجارة الإلكترونية للمشتريين والبائعين عددًا من المزايا:

1. الراحة: يُمكن ممارسة التجارة الإلكترونية على مدار الساعة طوال أيام الأسبوع. يُمكن للمستهلكين الشراء في أي وقت يناسبهم، ويُمكن لأصحاب الأعمال إجراء عمليات البيع وهم نائمون.
2. تنوع أكبر: تُقدم العديد من المتاجر مجموعة واسعة من المنتجات عبر الإنترنت مقارنةً بالمتاجر التقليدية. كما تُقدم العديد من المتاجر التي تعمل حصريًا عبر الإنترنت للمستهلكين مخزونًا حصريًا غير متوفر في أي مكان آخر.
3. تكاليف بدء تشغيل منخفضة محتملة: قد تحتاج شركات التجارة الإلكترونية إلى موقع إلكتروني أو موقع تصنيع، لكنها عادةً لا تحتاج إلى واجهة عرض فعلية. غالبًا ما تكون تكلفة التشغيل الرقمي أقل من تكلفة دفع الإيجار والتأمين وصيانة المبنى وضرائب العقارات.
4. المبيعات الدولية: طالما أن متجر التجارة الإلكترونية قادر على إيجاد طريقة لشحن منتجاته إلى عملائه، فإنه يستطيع البيع لأي شخص في العالم دون قيود جغرافية.

العيوب:

خدمة عملاء محدودة: إذا كنت تتسوق عبر الإنترنت لشراء جهاز كمبيوتر، فلن تتمكن ببساطة من طلب عرض ميزات طراز معين شخصيًا من الموظف. وعلى الرغم من أن بعض المواقع الإلكترونية تتيح لك الدردشة عبر الإنترنت مع أحد الموظفين، إلا أن هذه الممارسة ليست شائعة. على الرغم من أنها ميزة للمتسوقين، إلا أنها قد توفر المال لتجار التجزئة.

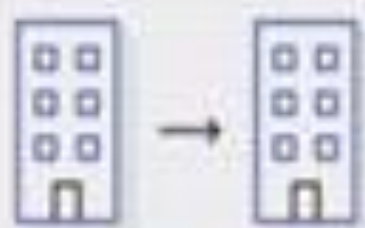
1. عدم الرضا الفوري: عند شراء منتج عبر الإنترنت، عليك انتظار شحنه إلى منزلك أو مكتبك.
2. عدم القدرة على لمس المنتجات: لا تعكس الصور المعروضة على الإنترنت بالضرورة الصورة الكاملة للمنتج، وقد تكون عمليات الشراء عبر التجارة الإلكترونية مخيبة للآمال عندما لا ترقى المنتجات إلى مستوى توقعات المشتري. على سبيل المثال: قد تكون قطعة ملابس مصنوعة من قماش رديء الجودة مما تشير إليه صورتها على الإنترنت.
3. الاعتماد على التكنولوجيا: في حال تعطل موقع إلكتروني أو إجباره على الإغلاق مؤقتًا لأي سبب، يُغلق العمل فعليًا حتى تعود الأمور إلى طبيعتها.
4. منافسة أكبر: على الرغم من أن انخفاض تكلفة بدء مشروع تجارة إلكترونية قد يكون ميزة، إلا أنه يعني أيضًا إمكانية دخول المنافسين إلى السوق بسهولة.

أنواع التجارة الإلكترونية

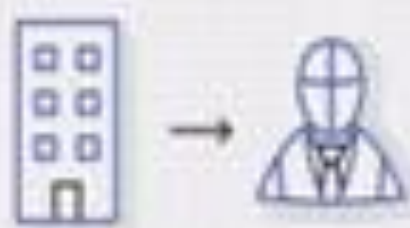
تستخدم شركات التجارة الإلكترونية نماذج أعمال مختلفة.

1. من شركة إلى مستهلك (B2C): تباع شركات التجارة الإلكترونية من شركة إلى مستهلك مباشرةً للمستخدم النهائي للمنتج بدلاً من توزيعه عبر وسيط مثل بائع تجزئة آخر.
2. من شركة إلى شركة (B2B): على غرار نموذج B2C، يمكن لشركة التجارة الإلكترونية بيع السلع لشركة أخرى.
3. من شركة إلى حكومة (B2G): تعمل بعض شركات التجارة الإلكترونية كمتعاقدين حكوميين، حيث توفر السلع أو الخدمات للوكالات الحكومية والجهات الأخرى.
4. من مستهلك إلى مستهلك (C2C): يمكن للأفراد بيع سلع لأفراد آخرين عبر مواقعهم الإلكترونية الخاصة أو من خلال منصات التجارة الإلكترونية التي تُسهّل العملية. ومن الأمثلة على هذه المنصات: eBay و Etsy وغيرها الكثير.
5. التعاملات بين المستهلكين والشركات (C2B): تتيح بعض المنصات للأفراد التواصل بسهولة أكبر مع الشركات وتقديم خدماتهم، خاصةً فيما يتعلق بالعقود قصيرة الأجل، أو الأعمال المؤقتة، أو فرص العمل الحر. Upwork مثال على ذلك.
6. التعاملات بين المستهلكين والحكومة (C2G): على الرغم من أنها ليست علاقة تجارة إلكترونية بالمعنى التقليدي، إلا أن التعاملات بين المستهلكين والحكومة تُعدّ وسيلةً للأفراد للتفاعل مع الحكومة. على سبيل المثال، يُمكن اعتبار تحميل إقرارات الضريبي الفيدرالي على موقع دائرة الإيرادات الداخلية ((Internal Revenue Service (IRS) معاملة تجارة إلكترونية نظرًا لتبادل المعلومات. كما يُمكن لدافعي الضرائب سداد ما عليهم أو طلب استرداد المبلغ الزائد الذي قد يكون دفعوه.

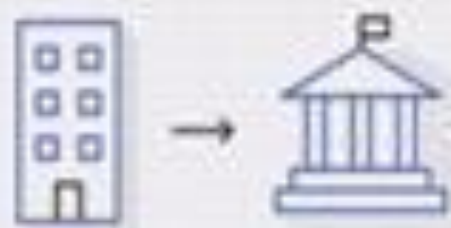
Types of E-Commerce



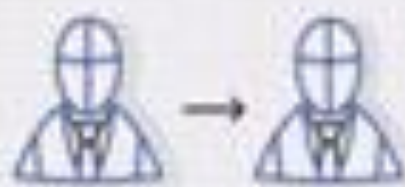
Business to business



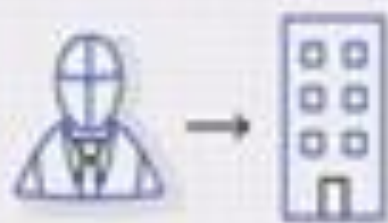
Business to consumer



Business to Government



Consumer to consumer



Consumer to business



Consumer to Government

خدمات بطاقات الصراف الآلي والخصم

تتيح لك بطاقة الصراف الآلي سحب النقود من هذه الأجهزة حتى حدود سحب محددة، وتحويل الأموال بين الحسابات المصرفية. ومع ذلك، فإن وظائف البطاقة محدودة. لا يمكنك استخدامها لإجراء عمليات شراء شخصية أو عبر الإنترنت كما هو الحال مع بطاقة الخصم. يربط البنك بطاقة الصراف الآلي بحسابك. عند استخدام جهاز الصراف الآلي، تُدخل رقم التعريف الشخصي (PIN) المكون من أربعة أرقام للوصول إلى حسابك.

ما هي بطاقة الخصم؟

مثل بطاقة الصراف الآلي، ترتبط بطاقة الخصم بحسابك المصرفي، وتتيح لك سحب النقود وإدارة حسابك الجاري. ومع ذلك، تتمتع بطاقات الخصم بحدود سحب أعلى، مما يعني أنه يمكنك الوصول إلى المزيد من النقود يوميًا مقارنةً ببطاقة الصراف الآلي. عادةً ما تُمنح البنوك بطاقات الخصم المباشر للعملاء الذين لديهم حسابات جارية. تُعدّ بطاقة الخصم المباشر أيضًا بطاقة دفع. بمعنى آخر، يمكنك استخدام بطاقة الخصم المباشر في المتاجر لشراء السلع والخدمات. كما تُمكنك بطاقتك من إجراء عمليات شراء عبر الإنترنت. مع ذلك، لبطاقات الخصم المباشر حدود شراء، ما يعني أنه لا يُمكنك إجراء سوى معاملات بقيمة عدة دولارات يوميًا. عادةً، تتراوح حدود الشراء بين بضع مئات من الدولارات وبضعة آلاف من الدولارات. يعتمد حدك على البنك أو الاتحاد الائتماني الذي يُدير حسابك.

الخدمات المصرفية عبر الهاتف المحمول

تشير الخدمات المصرفية عبر الهاتف المحمول إلى استخدام جهاز محمول للوصول إلى الخدمات المصرفية والمالية التي تقدمها البنوك. يُمكن هذا التطبيق العملاء من التحقق من رصيد حساباتهم المصرفية، وإجراء المعاملات الإلكترونية، وتحويل الأموال، ودفع الفواتير، وغيرها، دون الحاجة لزيارة البنوك. كما يمكن للعميل تحويل الأموال بين الحسابات باستخدام الخدمات المصرفية الهاتفية من أمثلة هذه الخدمات:

✚ سحب وإيداع النقود

✚ معلومات عن رصيد الحساب وسجل المعاملات

✚ دفع الفواتير إلكترونياً

✚ تحويل الأموال بين الحسابات

✚ طلبات القروض

✚ طلب دفاتر الشيكات

✚ استبدال بطاقات الخصم

مزايا وعيوب الخدمات المصرفية عبر الهاتف المحمول

العيوب

1. يسبب إزعاجًا لأصحاب الحسابات الأقل خبرة في التكنولوجيا
2. يزيل اللمسة الإنسانية من الخدمات المصرفية
3. يثير مخاوف أمنية وعمليات احتيال عبر الإنترنت
4. يؤدي إلى تأخير أو خسائر في المعاملات بسبب الأخطاء البشرية
5. يثير مشاكل في الفهم بسبب واجهة التطبيق المعقدة
6. يجعل متابعة تقارير الاحتيال أمرًا صعبًا.
7. يؤخر طلبات الخدمة في حالة حدوث مشكلات في الإنترنت .



المزايا

1. يوفر إمكانية الوصول إلى الخدمات المصرفية على مدار الساعة.
2. يوفر الوقت في إدارة الحسابات المصرفية.
3. يوفر طريقة مريحة لتحويل الأموال والدفع.
4. يتيح تتبع ومراقبة الحسابات المصرفية بسهولة.
5. يسهل الإبلاغ السريع عن أي معاملة غير قانونية أو نشاط احتيالي.
6. يسمح بمعالجة سريعة لشكاوى المستهلكين.
7. يزيد من سرعة معالجة الطلبات.
8. يتيح التسوق عبر الإنترنت.
9. يسمح بإدارة الاستثمارات دون مشاكل.
10. يرسل إشعارات بمدفوعات الفواتير أو القروض.
11. يشجع العملاء على البقاء في منازلهم أثناء الجائحة.
12. يلغي الحاجة إلى حمل النقود طوال الوقت.
13. يقلل من فرص السرقة .

الخدمات المصرفية عبر الرسائل النصية القصيرة

بعض استخدامات الرسائل النصية القصيرة في الخدمات المصرفية والمالية

1. إشعارات بحالة الدفع: يحتاج العملاء إلى التأكد من إرسال واستلام أموالهم بأمان، أو إيداع الأموال المتوقعة في حساباتهم.
2. تأكيد الدفع: يحرص أي بنك أو مؤسسة مالية حسنة السمعة على التواصل مع العميل دائمًا في حال وجود أي شك في أي دفعة. تستخدم معظم المؤسسات المالية والبنوك خدمات الرسائل القصيرة (SMS) للحد من الاحتيال وتزويد العملاء بإشعارات فورية حول أي نشاط مشبوه.
3. تحديثات الحالة: يرغب العملاء في معرفة حالة طلب الرهن العقاري أو مطالبة التأمين. في العصر الرقمي، السرعة هي المعيار. تُعد المعلومات الفورية المتعلقة بالمعاملات المصرفية، وتغييرات العناوين، وما إلى ذلك، بالغة الأهمية.
4. تذكيرات التجديد: رسالة نصية قصيرة بسيطة تلفت انتباه العميل عندما يحين وقت تحديث خطة التأمين أو إجراء دفعة.
5. التحقق من هوية المستخدمين: هل تحتاج إلى التحقق من هوية العميل للتأكد من هويته؟ هناك طريقة بسيطة وآمنة للسماح له بالوصول وهي إصدار رمز مصادقة فريد أو كلمة مرور لمرة واحدة.
6. استطلاعات الرأي: للحصول على تعليقات ورؤى وفهم أعمق للعملاء.
7. تحديث البيانات الشخصية: يساعد استخدام الرسائل النصية القصيرة على تسريع عملية تقديم خدمة العملاء.
8. العروض الخاصة والخصومات: تستخدم البنوك والمؤسسات المالية الرسائل النصية القصيرة لإعلام العملاء المحتملين المهتمين بالبرامج والسلع والخدمات الجديدة والاحتفاظ بهم، مع توفير رابط مباشر للصفحة ذات الصلة أحيانًا.

التنبية الإلكترونية (الإشعارات)

إعداد التنبيهات في الخدمات المصرفية عبر الإنترنت أو تطبيق الهاتف المحمول لتلقي إشعارات الحساب عبر الرسائل النصية أو البريد الإلكتروني. فيما يلي بعض الأمثلة على كيفية استخدام مختلف القطاعات للإشعارات الإلكترونية الآلية لتبسيط الاتصالات وتحليل البيانات.

1. الخدمات المالية: يمكن لشركات بطاقات الائتمان إرسال تنبيهات فورية بالاحتيال إلى عملائها عند أول بادرة استخدام للبطاقة أو عمليات شراء كبيرة. يمكن للبنوك إخطار العملاء عندما يكون حسابهم على وشك السحب على المكشوف.
2. التسويق: يمكن لشركات التسويق الوصول إلى جمهور أوسع من خلال استطلاع آراء العملاء عبر منصات مختلفة. يمكنهم تتبع الحملات الترويجية لتحليل فعاليتها.
3. التعليم: يمكن للطلاب والأساتذة تلقي تنبيهات فورية بإلغاء الفصول الدراسية. في حالة الطوارئ يمكن إرسال تحذيرات حاسمة إلى جميع أعضاء هيئة التدريس والموظفين والطلاب عبر جميع المنصات المتاحة في آنٍ واحد.
4. السفر والسياحة: لشركات الطيران إرسال إشعارات فورية بتأخير الرحلات أو تحذيرات سفر مهمة إلى العملاء. ويمكن للمسافرين الدائمين استلام رسائل بريد إلكتروني خاصة بعروض الرحلات. الإشعار الإلكتروني هو أي اتصال آلي يتم استلامه عبر البريد الإلكتروني أو الهاتف أو الرسائل النصية أو الفاكس ومنها:

✚ تنبيهات الأخبار والطقس التي يتم استلامها كرسائل نصية على هاتفك المحمول.

✚ عروض السفر التي يتم استلامها عبر البريد الإلكتروني كجزء من برنامج المسافر الدائم.

✚ استطلاعات الرأي السياسية الآلية التي يتم إجراؤها عبر الهاتف.

✚ حملات تسويقية مستهدفة يتم إرسالها عبر الفاكس.

اكتشاف الأخطاء وإصلاحها TROUBLESHOOT

- ▶ تقنيات كشف الأخطاء وإصلاحها الأساسية
- ▶ أولاً: تشخيص وإصلاح الأخطاء البرمجية (Software Troubleshooting)
- ▶ ثانياً: تشخيص وإصلاح الأخطاء المادية (Hardware Troubleshooting)
- ▶ كيفية التعامل مع مشاكل الكمبيوتر

اعداد
د. وفاء حسن
د. حيدر عباس
م. صباح محمد

تقنيات كشف الأخطاء وإصلاحها الأساسية

► إذا كنت تستخدم جهاز كمبيوتر للعمل أو للترفيه، فمن المرجح أنك واجهت رسائل خطأ أو أعطالاً غير متوقعة. هذه المشاكل شائعة، وكلما زاد وقت استخدامك للجهاز، زاد احتمال استخدامك لتقنيات استكشاف الأخطاء وإصلاحها. استكشاف أخطاء الكمبيوتر وإصلاحها ليس حكرًا على متخصصي تكنولوجيا المعلومات. فمع المعرفة والأدوات والمنهجية الصحيحة، يمكن لأي شخص التغلب على مشاكل الكمبيوتر.

► استكشاف أخطاء الكمبيوتر وإصلاحها هو عملية تحديد وتشخيص وحل المشكلات التي تحدث في أنظمة الكمبيوتر، أو تطبيقات البرامج، أو مكونات الأجهزة ذات الصلة.

► قبل البدء في فك الجهاز أو إعادة تثبيت النظام، يعتمد الخبراء منهجية تسمى "عزل المشكلة" (Problem Isolation):

1. تحديد الأعراض: هل الجهاز لا يعمل مطلقاً؟ أم يعمل ببطء؟ أم تظهر رسائل خطأ؟
2. التغييرات الأخيرة: هل تم تثبيت برنامج جديد أو قطعة جديدة مؤخراً؟
3. النسخ الاحتياطي: قبل أي إجراء، يجب ضمان سلامة البيانات.

► أولاً: تشخيص وإصلاح الأخطاء البرمجية (Software Troubleshooting)

تعتبر المشاكل البرمجية هي الأكثر شيوعاً وعادة ما تكون أقل تكلفة في الإصلاح.

1. مشاكل نظام التشغيل (OS Issues)

- الأعراض: بطء شديد، تجمد النظام (Freezing)، أو الشاشة الزرقاء (BSOD).

- التشخيص والإصلاح:

- o الوضع الآمن (Safe Mode) تشغيل الجهاز بالحد الأدنى من البرامج والتعريفات. إذا اختفت المشكلة، فالسبب برنامج تم تثبيته مؤخراً.

- o أداة SFC: استخدام موجه الأوامر (CMD) كمسؤول وتشغيل الأمر `sfc /scannow` لإصلاح ملفات النظام التالفة.

- o استعادة النظام (System Restore) إعادة الحاسوب إلى نقطة زمنية سابقة كان يعمل فيها بشكل جيد.

2. مشاكل التعريفات (Drivers)

- الأعراض: توقف الصوت، دقة شاشة سيئة، أو توقف الطابعة.

- الحل: الذهاب إلى "إدارة الأجهزة" (Device Manager) إذا وجدت علامة صفراء، يعني أن التعريف مفقود أو معطوب. الحل يكون

بـ (Update Driver) أو حذفه وإعادة تشغيل الجهاز.

3. البرمجيات الخبيثة (Malware & Viruses)

- الأعراض: نوافذ منبثقة، ملفات تختفي، استخدام عالي للمعالج (CPU) دون مبرر.

- الحل: استخدام برامج موثوقة مثل Malwarebytes أو Windows Defender لإجراء فحص كامل (Full Scan).

ثانياً: تشخيص وإصلاح الأخطاء المادية (Hardware Troubleshooting)

هذا النوع يتطلب حذراً أكبر وأدوات فحص.

1. مرحلة الإقلاع (POST - Power On Self Test)

عند الضغط على زر التشغيل، يقوم الحاسوب بفحص أولي.

• التشخيص: الاستماع إلى "الصافرات" (Beep Codes).

• صافرة واحدة قصيرة: الجهاز سليم.

• صافرات متكررة وطويلة: غالباً مشكلة في الذاكرة (RAM).

• سلسلة صافرات (طويلة ثم قصيرة): غالباً كرت الشاشة (GPU).

ملاحظة: تختلف دلالات الصافرات حسب نوع اللوحة الأم (Motherboard).

2. مشاكل الذاكرة العشوائية (RAM)

• الأعراض: إعادة تشغيل مفاجئة، شاشة زرقاء، فشل في فتح البرامج الكبيرة.

• الحل:

1. تنظيف "أسنان" الذاكرة بممحاة ناعمة لإزالة الأكسدة.

2. تجربة قطعة ذاكرة واحدة في كل مرة لتحديد القطعة التالفة.

3. استخدام برنامج (MemTest86) للفحص الدقيق.

3. مشاكل القرص الصلب (Hard Drive / SSD)

• **الأعراض:** بطء في فتح الملفات، أصوات "طقطقة" (في HDD)، أو رسالة "No Boot Device".

• **الحل:** قراءة بيانات الـ S.M.A.R.T التي تخبرك بحالة القرص الصحية باستخدام برامج مثل (CrystalDiskInfo). إذا كانت الحالة "Bad" أو "Caution"، يجب استبدال القرص فوراً.

4. ارتفاع الحرارة (Overheating)

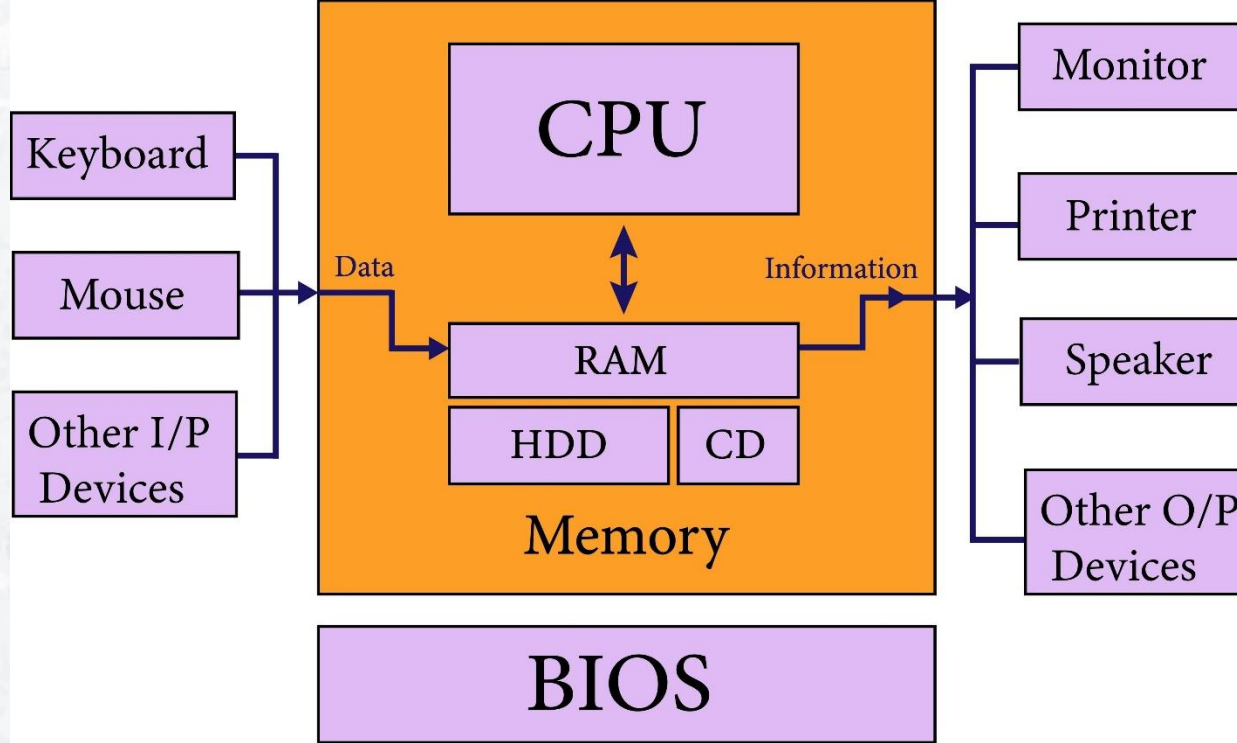
• **الأعراض:** الجهاز ينطفئ فجأة بعد مدة من التشغيل، صوت المراوح عالي جداً.

• **الحل:** تنظيف المراوح من الغبار، وتغيير المعجون الحراري (Thermal Paste) للمعالج.

5. وحدة تزويد الطاقة (Power Supply - PSU)

• **الأعراض:** الجهاز لا يستجيب لزر التشغيل، أو رائحة حرق.

• **الحل:** اختبار الـ PSU باستخدام جهاز (Multimeter) أو تجربة وحدة أخرى سليمة.



نوع العطل (Category)	العرض الظاهر (Symptom)	التشخيص / السبب المحتمل (Diagnosis)	إجراء الحل والإصلاح (Solution)
برمجي (Software)	بطء شديد في النظام	كثرة برامج بدء التشغيل، أو وجود برمجيات خبيثة.	1. تعطيل برامج الـ Startup من مدير المهام. 2. تنظيف القرص (Disk Cleanup). 3. فحص الفيروسات.
برمجي (Software)	الشاشة الزرقاء (BSOD)	تعارض في التعريفات (Drivers) أو تلف في ملفات النظام.	1. الدخول في الوضع الآمن (Safe Mode). 2. استخدام أمر sfc /scannow. 3. تحديث أو استعادة التعريفات السابقة.
برمجي (Software)	توقف خدمة الإنترنت	خطأ في إعدادات IP أو تعريف كرت الشبكة.	1. استخدام أداة Windows Troubleshoot. 2. إعادة تشغيل الراوتر. 3. إعادة تثبيت تعريف الشبكة.
مادي (Hardware)	الجهاز لا يعمل (شاشة سوداء دون صوت)	انقطاع التيار، أو تلف وحدة تزويد الطاقة (PSU).	1. التأكد من كابلات الكهرباء. 2. فحص المزود (Power Supply) بجهاز قياس. 3. التأكد من زر التشغيل باللوحة الأم.
مادي (Hardware)	صافرات متكررة عند التشغيل (Beeps)	خطأ في الذاكرة العشوائية (RAM) أو كرت الشاشة.	1. تحديد نوع الصافرة (طويلة/قصيرة) حسب كتيب اللوحة الأم. 2. فك الذاكرة وتنظيفها وإعادة تركيبها. 3. تجربة الذاكرة في منفذ آخر.
مادي (Hardware)	انطفاء مفاجئ للجهاز (Restart)	ارتفاع حرارة المعالج (Overheating).	1. التأكد من عمل المراوح. 2. تنظيف المشتت الحراري من الغبار. 3. تغيير المعجون الحراري (Thermal Paste).
مادي (Hardware)	أصوات ضجيج أو طقطقة	تلف ميكانيكي في القرص الصلب (HDD) أو المراوح.	1. إذا كان الصوت من القرص: انسخ بياناتك فوراً واستبدله. 2. إذا كان من المراوح: يتم تنظيفها أو تزييتها أو استبدالها.

نوع العطل (Category)	العرض الظاهر (Symptom)	التشخيص / السبب المحتمل (Diagnosis)	إجراء الحل والإصلاح (Solution)
برمجي (Software)	تعطل البرنامج أو توقفه عن العمل	تطبيقات بها أخطاء، أو موارد نظام غير كافية، أو تعارضات بين البرامج.	1. محاولة تحديث البرنامج، أو إعادة تثبيته. 2. إغلاق التطبيقات الأخرى التي تستهلك موارد النظام.
برمجي او مادي (HW او SW)	مشاكل الطابعة	قد يكون سبب فشل الطابعة مشاكل في الاتصال، أو برامج تشغيل قديمة، أو انحشار الورق.	1. التحقق من اتصالات الطابعة. 2. تحديث برامج التشغيل. 3. إزالة أي انحشار ورق.
برمجي (Software)	توجد مشاكل في الصوت	مشاكل في إخراج الصوت بسبب إعدادات كتم الصوت، أو عطل في مكبرات الصوت، أو تعارضات في برامج التشغيل.	1. التحقق من إعدادات الصوت. 2. اختبار مكبرات صوت مختلفة. 3. تحديث برامج تشغيل الصوت.
مادي (Hardware)	عدم استجابة الأجهزة الطرفية	مشاكل مع الأجهزة الخارجية، مثل محركات أقراص USB أو الفأرة أو لوحات المفاتيح، بسبب ضعف التوصيلات، أو مشاكل في برامج التشغيل، أو خلل في الأجهزة.	1. اختبار الأخطاء الأجهزة على منافذ أو أجهزة كمبيوتر أخرى . 2. تحديث برامج التشغيل.
برمجي (Software)	أخطاء خاصة بالتطبيقات	تعرض بعض البرامج رسائل خطأ محددة أو لا تعمل بشكل صحيح.	1. البحث عن رسالة الخطأ عبر الإنترنت للعثور على حلول محتملة. 2. تحديث التطبيق.
برمجي (Software)	الملفات المفقودة أو التالفة	قد تفقد ملفات النظام المهمة أو تتلف، مما يؤدي إلى مشاكل مختلفة.	1. تشغيل برامج فحص ملفات النظام. 2. استعادة البيانات من النسخ الاحتياطية.
برمجي (Software)	مشاكل متعلقة بكلمات المرور	ينسى المستخدمون كلمات مرورهم أو يواجهون مشاكل في إعادة تعيينها.	1. استخدام عمليات استرداد كلمة المرور. 2. الاتصال بالدعم. 3. حفظ كلمات المرور في ملف واحد وحفظها في مكان امن.

نوع العطل (Category)	العرض الظاهر (Symptom)	التشخيص / السبب المحتمل (Diagnosis)	إجراء الحل والإصلاح (Solution)
أمني (Security)	بطء شديد واستهلاك عالٍ للمعالج (High CPU Usage)	وجود برمجيات تعدين (Cryptojacking) أو برامج تعمل في الخلفية دون علم المستخدم.	1. فصل الإنترنت فوراً. 2. مراقبة العمليات في (Task Manager). 3. فحص كامل (Full Scan) ببرنامج متخصص مثل Malwarebytes.
أمني (Security)	ظهور نوافذ منبثقة (Pop-ups) وتغير محرك البحث	الإصابة ببرمجيات إعلانية (Adware) أو اختطاف المتصفح (Browser Hijacker).	1. إزالة الإضافات (Extensions) الغريبة من المتصفح. 2. إعادة تعيين إعدادات المتصفح الافتراضية. 3. استخدام أداة (AdwCleaner).
أمني (Security)	تشفير الملفات وتغير امتدادها (مثل locked.)	الإصابة بفيروس الفدية (Ransomware). (وهو الأخطر)	1. عزل الجهاز عن الشبكة فوراً لمنع الانتشار. 2. عدم دفع الفدية نهائياً. 3. فرمته الجهاز واستعادة البيانات من نسخة احتياطية خارجية (Backup).
أمني (Security)	تعطل أدوات النظام (Task Manager/Antivirus)	إصابة ببرمجيات خبيثة متقدمة تحاول حماية نفسها (Rootkits) عن طريق تعطيل دفاعات النظام.	1. عدم تشغيل الجهاز من النظام المصاب. 2. استخدام "قرص إنقاذ" (Rescue Disk) خارجي (USB) من شركات مثل Kaspersky أو Bitdefender للإقلاع والفحص.
أمني (Security)	اختفاء الملفات أو تحويلها لاختصارات (Shortcuts)	فيروسات الاختصارات (Shortcut Virus) وغالباً تنتقل عبر الـ USB.	1. إظهار الملفات المخفية من إعدادات المجلد. 2. استخدام أمر CMD :X /d /s -r -h attrib *.* (مع استبدال X بحرف القرص). 3. تنظيف القرص بمضاد فيروسات.

كيفية التعامل مع مشاكل الكمبيوتر

كما ذكرنا، وحسب نوع المشكلة، لا حاجة لخبير تكنولوجيا معلومات. بمساعدة دروس يوتيوب، ومنتديات الدعم، أو غيرها من الموارد، قد تتمكن من استكشاف الأخطاء وإصلاحها بنفسك. إليك بعض الخطوات التي يمكنك اتخاذها لإيجاد حل فعال لمشاكل الكمبيوتر الشائعة:

1. التزم الهدوء والصبر : قد يكون استكشاف الأخطاء وإصلاحها أمرًا محبطًا، لكن الحفاظ على الهدوء والصبر سيساعدك على التفكير بوضوح أكبر واتخاذ قرارات أفضل. هذه نصيحة قيّمة لأي مشكلة قد تواجهها. مع ذلك، عندما يتعلق الأمر بأجهزة الكمبيوتر، قد يؤدي عدم التفكير بوضوح إلى المزيد من المشاكل والإحباط. من الأفضل بكثير البحث عن مصدر المشكلة بدلًا من تجربة حلول متعددة دون جدوى.

2. تحديد المشكلة : راقب الأعراض أو رسائل الخطأ بعناية لفهم المشكلة التي تواجهها. باستخدام قائمة المشاكل الشائعة التي ذكرناها أعلاه، قد تتمكن من تحديد سبب مشكلتك والبحث عن حلول محتملة.

3. إجراء فحوصات أساسية : ابدأ بفحوصات بسيطة، مثل التأكد من توصيل جميع الكابلات بشكل صحيح، ومصدر الطاقة يعمل بشكل صحيح، وأن الكمبيوتر نظيف من الغبار والأوساخ.

4. **البحث عن المشكلة :** استخدم محركات البحث للبحث عن رسالة الخطأ أو الأعراض. غالبًا ما واجه آخرون مشاكل مماثلة وشاركوا حلولًا عبر الإنترنت.
5. **مراجعة التغييرات الأخيرة :** فكّر في أي تثبيتات أو تحديثات أو تغييرات حديثة في الأجهزة قد تكون سبب المشكلة. يمكن أن يساعد التراجع عن التغييرات في تحديد المشكلة.
6. **استخدام الوضع الآمن :** شغل جهاز الكمبيوتر في الوضع الآمن، والذي يُحمّل مجموعة أساسية من برامج التشغيل والإعدادات. يمكن أن يساعدك هذا في تحديد ما إذا كانت المشكلة ناتجة عن برنامج أو برامج تشغيل تابعة لجهات خارجية.
7. **فحص مكونات الأجهزة :** إذا كنت تشك في وجود مشاكل في الأجهزة، فاختر المكونات بشكل فردي (مثل ذاكرة الوصول العشوائي (RAM) والقرص الصلب) أو جرّبها على جهاز كمبيوتر آخر لمعرفة ما إذا كانت المشكلة لا تزال قائمة.
8. **تحديث برامج التشغيل والبرامج :** تأكد من تحديث نظام التشغيل وبرامج التشغيل والبرامج. يمكن أن تُسبب المكونات القديمة مشاكل في التوافق وعدم الاستقرار.

9. **شغل برامج مكافحة الفيروسات والبرامج الضارة :** أجرِ فحصًا شاملاً للنظام باستخدام برنامج مكافحة فيروسات موثوق للتحقق من أي إصابة محتملة بالبرامج الضارة وإزالتها.
10. **أنشئ نسخًا احتياطية :** قبل محاولة إجراء تغييرات أو إصلاحات رئيسية، أنشئ نسخًا احتياطية للبيانات المهمة لتجنب فقدانها في حال حدوث أي خطأ.
11. **استخدم استعادة النظام أو إعادة تعيينه :** إذا كان جهاز الكمبيوتر لديك مزودًا بنقاط استعادة النظام أو خيار إعادة تعيين، ففكر في استخدامها لإعادة النظام إلى حالة مستقرة.
12. **استخدم أدوات التشخيص :** تحتوي العديد من أنظمة التشغيل على أدوات تشخيص مدمجة تساعد في تحديد وحل مشكلات محددة. ابحث في إعدادات نظام التشغيل لديك عن هذه الأدوات.