

الأمن والشبكات: ما هي الشبكة؟ أنواع الشبكات. مكونات الشبكة الأساسية:

شبكة الحاسوب هو الاندماج بين تكنولوجيا الاتصالات وتكنولوجيا الحاسبات باستخدام مجموعة من الحاسبات والجهزة الأخرى المتصلة مع بعضها البعض حيث يكون لها القدرة على مشاركة عدد كبير من المستخدمين للبيانات Data والبرمجيات Software والجهزة Hardware كما تعتبر الشبكة وسيلة اتصال إلكتروني بين الأفراد والتي تمكنهم من:

- 1- إرسال رسالة مكونة من عدة صفحات وصور وأصوات ورسومات متحركة إلى مجموعة أشخاص في أي مكان دفعة واحدة وفي دقائق معدودة.
- 2- يتصل من حاسوب المنزل أو العمل ببنوك المعلومات والشركات والمكتبات العالمية للحصول على المعلومات التي تهتمه
- 3- عقد المؤتمرات والندوات التفاعلية لأطراف متباعدة عبر شبكة الإنترنت
- 4- التعليم عن بعد والتجارة الإلكترونية والحكومة الإلكترونية.

أنواع شبكات الحاسوب

أولاً : تصنيف الشبكات من حيث الحجم size

- 1- الشبكة المحلية LAN – Local Area Network
- 2- الشبكة الواسعة WAN – Wide Area Network
- 3- شبكة الإنترنت
- 4- شبكة الإكسترنانت
- 5- شبكة الإنترنت
- 6- الإكسترنانت
- 7- شبكة الإنترنت

ثانياً : تصنيف الشبكات من حيث طريقة التوصيل Topology:

- 1- شبكة المسار الخطي Bus Network
- 2- الشبكة الحلقية Token Ring Network

3- الشبكة النجمية Star Network

مكونات الشبكة:

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

- 1- الحاسوب الرئيسي – الخادم Server
- 2- محطات العمل Work Stations
- 3- خطوط الاتصال Communication Lines
- 4- بطاقات الشبكة Network Interface Card
- 5- المودم Modem
- 6- الأجهزة الملحقة
- 7- محولات الشبكة Communication Switches
- 8- برامج الشبكة

فوائد الشبكات:

- 1- المشاركة في استخدام الأجهزة Hardware اي استفادة أي مستخدم للشبكة من إمكانيات الحاسوب الرئيسي بدل من اقتناء حاسوب مستقل، كذلك الاستفادة من جميع الاجهزة الملحقة بالشبكة مثل الطابعات>
- 2- المشاركة في البرمجيات Software اي استفادة أي مستخدم للشبكة من البرمجيات المخزنة في الحاسوب الرئيسي أو أي حاسوب آخر متصل بالشبكة مثل مشاركة الملفات واستخدام البريد الالكتروني .
- 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 وفي منافذ الحدود.
- 4- سهولة تحديث (تطوير Update) البرامج والبيانات نظرا لاجراء عملية التطوير مرة واحدة على الحاسوب الرئيسي وليس على كل محطة عمل.
- 5- شراء نسخة واحدة من البرامج وتحميلها على الحاسوب الرئيسي بالشبكة يكون أرخص ثمناً من شراء عدة نسخ فردية User-Single وتحميل كل منها على محطة عمل .

- 6- استخدام الانترنت Internet في البحث عن المعلومات واستخدام البريد الالكتروني Electronic Mail-E Mail وتبادل المعلومات والملفات بين المشاركين.
- 7- إمداد متخذي القرار من الإدارة العليا بالبيانات والمعلومات الحديثة بسرعة وبصورة شاملة.
- 8- إمكانية شراء وبيع السلع والخدمات والتسويق والقيام بالاعمال التجارية من خلال الشبكة e-commerce .
- 9- تقديم الخدمات للمواطنين بسرعة وسهولة وبأقل تكلفة كما هو متبع عند دفع فاتورة الهاتف وتجديد البطاقة المدنية وظهور ما يسمى بالحكومة الإلكترونية.. e-government
- 10- اعتماد العديد من الشركات على الشبكات في عملها بشكل أساسي كشركات الطيران والبنوك وغيرها.

امن الشبكات:

هي مجموعة من الإجراءات التي يمكن خلالها توفير الحماية القصوى للمعلومات والبيانات في الشبكات من كافة المخاطر التي تهددها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية.

تصنيف جرائم المعلومات:

1. جرائم تهدف لنشر معلومات: يتم نشر معلومات سرية تم الحصول عليها بطرق غير مشروعة عن طريق الاختراقات لشبكات المعلومات ونشر هذه المعلومات
2. جرائم تهدف لترويج الإشاعات. وهنا يتم نشر معلومات مغلوطة وغير صحيحة تتعلق بالأشخاص أو المعتقدات أو الدول بهدف تكدير السلم العام في البلدان، وكذلك نشر الإشاعات عن بعض الأشياء وإحداث البلبلة في المجتمعات.
3. جرائم التزوير الإلكترونية. وهنا يتم استخدام وسائل التكنولوجيا في عمليات التزوير بغرض تحقيق هدف معين، وكذلك يندرج تحتها عمليات التحويل المصرفي الوهمية من حسابات إلى أخرى عن طريق اختراق شبكات المصارف.
4. جرائم تقنية المعلومات. وأهم مثال لها هو عمليات القرصنة التي تحدث للبرامج الحاسوبية الأصلية والتي يتم عمل نسخ منها لتباع في الأسواق بدلاً من النسخ الأصلية.

مكونات أمن شبكات المعلومات:

ولاً: سرية المعلومات

[عدل]

(بالإنجليزية) Data Confidentiality : وهذا الجانب يشتمل على الإجراءات والتدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات التي يطبق عليها بند السرية أو المعلومات الحساسة، وهذا هو المقصود بأمن وسرية المعلومات، وطبعاً درجة هذه السرية ونوع المعلومات يختلف من مكان لآخر وفق السياسة المتبعة في المكان نفسه، ومن أمثلة هذه المعلومات التي يجب سريتها: المعلومات الشخصية للأفراد.

ثانياً: سلامة المعلومات

[عدل]

(بالإنجليزية) Data Integrity : في هذا الجانب لا يكون الهم الأكبر هو الحفاظ على سرية المعلومات وإنما يكون الحفاظ على سلامة هذه المعلومات من التزوير والتغيير بعد إعلانها على الملأ، فقد تقوم هيئة ما بالإعلان عن معلومات مالية أو غيرها تخص الهيئة وهنا يأتي دور الحفاظ على السلامة بأن تكون هذه المعلومات محمية من التغيير أو التزوير، ومن أمثلة ذلك مثلاً: إعلان الوزارات أو الجامعات عن أسماء المقبولين للعمل بها، تتمثل حماية هذه القوائم في أن تكون مؤمنة ضد التغيير والتزوير فيها بحذف أسماء ووضع أسماء غيرها مما يسبب الحرج والمشكلات القانونية للمؤسسات، وأيضاً بالنسبة للمعلومات المالية بتغيير مبلغ مالي من 100 إلى 1000000 وهذا هام جداً لما يترتب عليه من خسائر فادحة في الأموال.

ثالثاً: ضمان الوصول إلى المعلومات

[عدل]

(بالإنجليزية) Availability : لعله من المنطقي أن نعرف أن كل إجراءات وصناعة المعلومات في الأساس تهدف إلى هدف واحد وهو إيصال المعلومات والبيانات إلى الأشخاص المناسبين في الوقت المناسب، وبالتالي فإن الحفاظ على سرية المعلومات وضمن سلامتها وعدم التغيير فيها لا يعني شيئاً إذا لم يستطع الأشخاص المخولين أو المصرح لهم الوصول إليها، وهنا تأتي أهمية الجانب الثالث من جوانب أمن المعلومات وهو ضمان وصول المعلومات إلى الأشخاص المصرح لهم بالوصول إليها من خلال توفير القنوات والوسائل الآمنة والسريعة للحصول على تلك المعلومات، وفي هذا الجانب يعمل المخربون بوسائل شتى لحرمان ومنع المستفيدين من الوصول إلى المعلومات مثل حذف المعلومات قبل الوصول إليها أو حتى مهاجمة أجهزة تخزين المعلومات وتدميرها أو على الأقل تخريبها.

دوافع الهجوم على شبكات المعلومات

[عدل]

يمكن أن يتبادر إلى الذهن سؤال وهو لماذا يقوم المخربون أو المخترقون بعمليات مثل [اختراق شبكات المعلومات](#) وتهديد أمن المعلومات؟ وما هي الدوافع التي يمكن أن تكون لديهم لكي يقوموا بمثل هذه الأعمال؟ فلا بد لكل شخص من دوافع للقيام بعمل ما، وهنا سنتعرف على بعض الدوافع التي رصدها المختصون بمراقبة عمليات الاختراق وجرائم المعلومات لدى القائمون بهذه الهجمات.

الخدمات المصرفية الإلكترونية

تُعرف الخدمات المصرفية الإلكترونية بأنها إجراء المعاملات المصرفية المختلفة عبر استخدام أجهزة الحاسوب والاتصالات بدلاً من التفاعل البشري، إذ يتم من خلالها تحويل الأموال عبر تبادل الإشارات الإلكترونية بدلاً من تبادل النقد أو الشيكات أو المستندات الورقية الأخرى بين المؤسسات المالية المختلفة أو بين المؤسسات المالية والتجارية.

تعتمد الخدمات المصرفية الإلكترونية على أنظمة الحاسوب المعقدة والتي تتواصل معاً عبر خطوط الهاتف، إذ تسجل الأنظمة الحاسوبية التحويلات المالية كافة وملكية الأموال للأفراد، وتتحكم في الطرق التي يمكن للعملاء والمؤسسات التجارية الوصول من خلالها إلى الأموال، سواء من خلال أجهزة الصراف الآلي أو بطاقات الائتمان أو غيرها.

ما أنواع الخدمات المصرفية الإلكترونية؟

يوجد العديد من الأنواع للخدمات المصرفية الإلكترونية التي توفرها المؤسسات المالية بكافة أشكالها، وفيما يلي أبرزها:

1. الخدمات المصرفية عبر الإنترنت

والتي يمكن للعملاء من خلالها إجراء العديد من المعاملات النقدية وغير النقدية باستخدام الإنترنت، وذلك عبر موقع البنك نفسه أو من خلال التطبيق الخاص به.

2. الخدمات المصرفية عبر الهاتف المحمول

والتي تتم بشكل أساسي من خلال التطبيق الخاص بالبنك، إذ وفرت معظم البنوك تطبيقات خاصة بها للهواتف المحمولة، والتي تمكن العملاء من إجراء معاملاتهم المصرفية المختلفة، كل ما يلزمهم هو هاتف محمول واتصال بالإنترنت وتطبيق البنك وإتاحة الخدمات المصرفية على الهاتف.

3. ماكينة الصراف الآلي (ATM)

تعد ماكينة الصراف الآلي من أكثر الخدمات المصرفية شيوعاً، وهي ليست مجرد آلة لسحب الأموال من خلالها، وإنما يمكن استخدامها لإجراء العديد من الخدمات المصرفية؛ كالتحقق من حالة الحساب، وتحويل الأموال، وإيداع الأموال، وتغيير المعلومات الخاصة بالعميل؛ كرقم هاتفه، ورقم التعريف الشخصي لبطاقته البنكية.

4. بطاقة الفيزا

وهي من أكثر البطاقات التي يستخدمها الأفراد في حياتهم اليومية، والتي ترتبط مباشرة بالحسابات المصرفية الخاصة بهم، بحيث يمكن للعميل من خلالها إجراء العديد من معاملات البيع والشراء؛ كالتسوق عبر الإنترنت، أو السحب من أجهزة الصراف الآلي، أو الدفع للمؤسسات التجارية، بحيث تخصم تلك المبالغ المسحوبة من حسابه مباشرة.

5. بطاقة الخصم الائتمان

بطاقات الخصم تساعدنا في سحب النقود بسهولة من أجهزة الصراف الآلي وماكينات نقاط البيع أما البطاقات الائتمانية هي بطاقات تصدرها البنوك لعملائها لغايات الدفع والشراء بناءً على طلبهم، والتي تمكنهم من اقتراض الأموال وفقاً لحد معين يضعه البنك، ولا يخصم المبلغ المسحوب من حساب العميل مباشرة، وإنما يبقى في ذمته على أن يدفعه للبنك في غضون فترة زمنية محددة مع بعض الرسوم الإضافية مقابل استخدام تلك البطاقة.

6. التحويل الإلكتروني للأموال

يتم من خلالها تحويل الأموال من حساب بنكي إلى آخر عبر الإنترنت للبنك نفسه أو لبنوك أخرى أو مؤسسات تجارية أخرى، وهي تغطي مجموعة من الخدمات الأخرى؛ كالودائع المباشرة للأموال.

ما أهمية الخدمات المصرفية الإلكترونية؟

تتمحور أهمية الخدمات المصرفية الإلكترونية حول عدة نقاط، وفيما يلي أبرزها:

1. توفير الوقت والجهد على العميل، نظراً لأنه لا يحتاج إلى زيارة فرع البنك لكل عملية مصرفية يقوم بها.
2. إمكانية إجراء المعاملات البنكية في أي وقت ومن أي مكان.
3. تقليل الأخطاء في التبادلات المالية، وذلك نتيجة حوسبة البيانات الخاصة بالعميل وحسابه المصرفي، مما يعني وجود الدقة في إجراء المعاملات البنكية.
4. التقليل من الأعمال المكتبية التي تحتاج إلى سجلات ورقية كثيرة خاصة ببيانات العملاء في البنوك.

سلبيات الخدمات المصرفية

- لمشاكل التقنية وصعوبة إجراء عمليات الإيداع.
- إجراء بعض المعاملات المعقدة قد يكون أمراً صعباً عند الاستعانة بالخدمات المصرفية عبر الإنترنت.
- المخاطر الأمنية بما في ذلك هجمات التصيد الاحتيالي، والبرامج الضارة، وسرقة الهوية، والمعاملات الاحتيالية التي يمكن أن تعرض بيانات العملاء والأصول المالية للخطر

الذكاء الاصطناعي (Artificial Intelligence - AI)

هو مجال من مجالات علوم الحاسوب يهدف إلى تطوير أنظمة قادرة على أداء مهام تتطلب عادةً ذكاءً بشريًا. تشمل هذه المهام التعلم، التفكير، حل المشكلات، الإدراك، فهم اللغة الطبيعية، والتفاعل مع البيئة.

وخلال السنوات الأخيرة، قفز التطور في تقنية الذكاء الاصطناعي قفزات كبيرة، وتعد تقنية "التعلم العميق" أبرز مظاهره، وهي تركز على تطوير شبكات عصبية صناعية تحاكي في طريقة عملها أسلوب الدماغ البشري، أي أنها قادرة على التجريب والتعلم وتطوير نفسها ذاتيًا دون تدخل الإنسان

أنواع الذكاء الاصطناعي

1. الذكاء الاصطناعي الضيق (weak AI): مصمم لأداء مهام محددة، مثل التعرف على الصور أو الترجمة الآلية.

2. الذكاء الاصطناعي العام (Strong AI): يهدف إلى امتلاك قدرات ذكاء مشابهة للإنسان، قادر على أداء أي مهمة فكرية.

الذكاء الاصطناعي (AI) يشمل مجموعة واسعة من التقنيات والأساليب التي تمكن الآلات من محاكاة الذكاء البشري. فيما يلي بعض أهم التقنيات والأساليب المستخدمة في هذا المجال:

1. *التعلم الآلي Machine Learning

- القدرة على تحليل البيانات والتعلم منها دون برمجة صريحة.
- تحسين الأداء مع مرور الوقت من خلال التجربة والخبرة.

2. *التعلم العميق Deep Learning

- استخدام الشبكات العصبية الاصطناعية لمحاكاة عمل الدماغ البشري.
- فعال في معالجة البيانات المعقدة مثل الصور والفيديو والنصوص.

3. *معالجة اللغة الطبيعية Natural Language Processing - NLP

- فهم وتوليد اللغة البشرية بشكل طبيعي.
- تطبيقات مثل الترجمة الآلية، المساعدات الصوتية، وتحليل المشاعر.

4. *الرؤية الحاسوبية Computer Vision

- القدرة على تحليل وفهم الصور والفيديوهات.
- تطبيقات مثل التعرف على الوجوه، السيارات ذاتية القيادة، والتحليل الطبي.

5. *التفكير والاستدلال Reasoning and Problem Solving

- القدرة على حل المشكلات المعقدة واتخاذ القرارات بناءً على البيانات.
- تطبيقات في التخطيط، التحليل الاستراتيجي، والألعاب.

6. *التكيف Adaptability

- القدرة على التكيف مع الظروف الجديدة والبيئات المتغيرة.
- تحسين الأداء في مواجهة التحديات غير المتوقعة.

7. *الأتمتة Automation

- تنفيذ المهام الروتينية والمتكررة بدقة وسرعة.
- تقليل الحاجة للتدخل البشري في العمليات اليومية.

8. *التفاعل مع البشر Human Interaction

- القدرة على التفاعل مع البشر بشكل طبيعي وفعال.
- تطبيقات مثل الروبوتات الاجتماعية وواجهات المستخدم الذكية.

9. *التحليل التنبؤي Predictive Analytics

- استخدام البيانات التاريخية للتنبؤ بالأحداث المستقبلية.
- تطبيقات في التمويل، التسويق، والصحة.

10. *التخصيص Personalization

- توفير تجارب مخصصة بناءً على تفضيلات المستخدم وسلوكه.
- تطبيقات في التسويق، الترفيه، والتعليم.

11. *الاستقلالية Autonomy

- القدرة على العمل بشكل مستقل دون تدخل بشري مستمر.

- تطبيقات في الروبوتات والأنظمة الذكية.

12. *التكامل مع التقنيات الأخرى*:

- القدرة على العمل مع تقنيات مثل إنترنت الأشياء (IoT)، البلوك تشين، والحوسبة السحابية).

إيجابيات الذكاء الاصطناعي

1. معالجة خالية من الأخطاء

2. يساعد في الوظائف المتكررة

3. متاح دائما

4. اتخاذ القرارات الصحيحة

5. المساعدة الرقمية

6. سرعة اتخاذ القرارات

7. الاستخدام في الحالات الخطرة

8. ظهور اختراعات جديدة

سلبيات وعيوب الذكاء الاصطناعي

1. ارتفاع التكاليف

2. زيادة البطالة

3. ضعف الابداع

4. الافتقار الى التحسن

5. مخاطر الأمان والخصوصية

6. زيادة الكسل بين الافراد

تكنولوجيا الهاتف المحمول مع الذكاء الاصطناعي

تكنولوجيا الهاتف المحمول مع الذكاء الاصطناعي تشهد تطورا سريعا ومتزايدا حيث يتم دمج تقنيات الذكاء الاصطناعي في الهواتف الذكية لتحسين تجربة المستخدم وتقديم ميزات متقدمة مثل:

1. *المساعدات الذكية*

* -المساعدات الافتراضية*: مثل Google Assistant و Siri و Bixby، التي تستخدم الذكاء الاصطناعي لفهم الأوامر الصوتية وتنفيذ المهام مثل إرسال الرسائل النصية، أو البحث على الإنترنت، أو التحكم في الأجهزة الذكية.

التفاعل الطبيعي: تحسين فهم اللغة الطبيعية (NLP) للتفاعل بشكل أكثر طبيعية مع المستخدمين.

2. *التصوير الذكي*

تحسين الصور

التعرف على الوجوه

3. *الترجمة الفورية*

4. *الامان والخصوصية*

5. *تحسين الأداء*

6. *الواقع المعزز*

7. *الصحة واللياقة*

8. *التعلم الآلي على الجهاز*

9. *التحكم الصوتي*

10. *التخصيص الذكي*

11. *الذكاء الاصطناعي في الألعاب*

12. *الذكاء الاصطناعي في الاتصالات*

13. *التنبؤات والاقتراحات*

14. *الذكاء الاصطناعي في التصوير الطبي*

15. *الذكاء الاصطناعي في التسوق*

16. *الذكاء الاصطناعي في التعليم*

17. *الذكاء الاصطناعي في السيارات الذكية*

18. *الذكاء الاصطناعي في الترفيه*

19. *الذكاء الاصطناعي في الإنتاجية*

20. *الذكاء الاصطناعي في الخدمات المصرفية

باختصار، الذكاء الاصطناعي يعيد تشكيل طريقة تفاعلنا مع الهواتف الذكية، مما يجعلها أكثر ذكاءً وفعالية في تلبية احتياجاتنا اليومية

*** Alexa ***

هو مساعد افتراضي ذكي يعتمد على الذكاء الاصطناعي، طورته شركة *أمازون*. يعمل Alexa من خلال الأوامر الصوتية، ويمكن استخدامه لإداء مجموعة واسعة من المهام، مثل:

- *التحكم بالأجهزة الذكية*: مثل الإضاءة، الكاميرات، الثلاجات، وأجهزة التلفاز الذكية.
 - *تشغيل الموسيقى*: من خلال خدمات مثل Spotify أو Amazon Music.
 - *تقديم المعلومات*: مثل الطقس، الأخبار، المواعيد، والرد على الأسئلة العامة.
 - *إدارة المهام اليومية*: مثل ضبط المنبهات، إعداد قوائم التسوق، وتذكيرك بالمواعيد.
 - *التفاعل مع التطبيقات والخدمات*: مثل طلب الطعام أو حجز سيارة أجرة.
- يعمل Alexa من خلال أجهزة مثل مكبرات صوت ذكية أو التطبيقات على الهواتف الذكية. يتم تنشيطه عادةً بكلمة "Alexa"، ثم يمكنك إعطاء الأوامر أو طرح الأسئلة.
- يتميز Alexa بقدرته على التكامل مع العديد من الأجهزة والخدمات، مما يجعله جزءًا من نظام المنزل الذكي Smart Home

*** سيري (Siri) ***

هو مساعد افتراضي ذكي يعمل بالذكاء الاصطناعي، طورته شركة Apple. يتوفر سيري على أجهزة ابل مثل iPhone و iPad و Mac و Apple Watch و Home Pod يمكن للمستخدمين التفاعل مع سيري عبر الأوامر الصوتية أو الكتابية لإداء مهام مختلفة، مثل إرسال الرسائل، وأجراء المكالمات، وتعيين التذكيرات، والحصول على الاتجاهات، والبحث عن المعلومات على الإنترنت، والتحكم في الأجهزة الذكية المنزلية، وغير ذلك.

سيري يدعم العديد من اللغات، بما في ذلك العربية، ويتكامل مع تطبيقات وخدمات أبل الأخرى لتقديم تجربة مستخدم سلسة. يتميز سيري بقدرته على فهم السياق والتعلم من تفاعلات المستخدم لتحسين تجربة المساعدة بمرور الوقت.

Google Assistant

هو مساعد رقمي ذكي تم تطويره بواسطة شركة **جوجل**، ويستخدم الذكاء الاصطناعي لفهم الأوامر الصوتية والنصية وتنفيذ المهام المختلفة. يمكنه مساعدتك في إجراء المكالمات، إرسال الرسائل، تشغيل الموسيقى، البحث في الإنترنت، التحكم في الأجهزة الذكية، تقديم التذكيرات، الإجابة على الأسئلة، وحتى إجراء المحادثات الطبيعية.

يمكن استخدام Google Assistant على مجموعة واسعة من الأجهزة، مثل الهواتف الذكية (أندرويد و iOS) وأجهزة مثل Google Home، الساعات الذكية، وأجهزة التلفاز الذكية، وحتى في بعض السيارات.

يمكن تفعيله بقول "ok Google" أو "ok Google"

الذكاء الاصطناعي وتأثيراته

الذكاء الاصطناعي أصبح جزءاً أساسياً من حياتنا، وله تأثيرات عميقة على العلاقات الاجتماعية والدولية، وكذلك على مستقبل البشرية ككل. يمكننا تقسيم تأثيراته إلى عدة محاور رئيسية:

1. الذكاء الاصطناعي والعلاقات الاجتماعية

- تغيير طبيعة التواصل: أصبحت تقنيات الذكاء الاصطناعي مثل الروبوتات والردشة الذكية مثل (ChatGPT) تؤثر على كيفية تواصل الأفراد، حيث تقلل الحاجة إلى التواصل المباشر وتزيد من الاعتماد على التكنولوجيا.
- تأثير على سوق العمل: يُحدث الذكاء الاصطناعي تحولاً كبيراً في فرص العمل، مما قد يزيد من البطالة في بعض المجالات، لكنه أيضاً يخلق فرصاً جديدة في مجالات أخرى مثل البرمجة وتحليل البيانات.
- تعزيز العزلة الاجتماعية: مع انتشار الروبوتات والمساعدات الذكية، قد يقلل ذلك من التفاعل البشري المباشر، مما قد يؤثر على العلاقات الأسرية والاجتماعية.
- تحسين جودة الحياة: من خلال تقديم حلول في مجالات الصحة، التعليم، والخدمات اليومية، مثل التشخيص الطبي الذكي والتعليم المخصص.

2. الذكاء الاصطناعي والعلاقات الدولية

- التأثير على السياسات الدولية: تتسابق الدول في تطوير أنظمة الذكاء الاصطناعي لأغراض عسكرية وتجارية، مما يزيد من المنافسة الجيوسياسية بين القوى الكبرى مثل الولايات المتحدة والصين.
- حروب سيبرانية وتجسس رقمي: أصبح الذكاء الاصطناعي يُستخدم في الهجمات السيبرانية، مما يزيد من التحديات الأمنية بين الدول.
- تحسين الدبلوماسية والتعاون الدولي: يمكن للذكاء الاصطناعي أن يساهم في تحليل البيانات السياسية، وتحسين عمليات التفاوض، والتنبؤ بالأزمات الدولية قبل وقوعها.

3. الذكاء الاصطناعي ومستقبل البشرية

- تهديد الوظائف التقليدية: من المتوقع أن يحل الذكاء الاصطناعي محل العديد من الوظائف، لكن يمكن أن يؤدي ذلك أيضاً إلى خلق فرص جديدة تتطلب مهارات مختلفة.
- المخاطر الأخلاقية: هناك مخاوف من أن يتم استخدام الذكاء الاصطناعي بطرق غير أخلاقية، مثل التحيز في القرارات أو انتهاك الخصوصية.
- هناك جدل حول مستقبل الذكاء الاصطناعي إذا تجاوز الذكاء البشري، (Super AI) تطوير الذكاء الفائق وهل سيكون ذلك خطراً على البشرية أم سيسهم في تقدمها؟
- التكامل مع البشر: قد نشهد في المستقبل اندماجاً أكبر بين البشر والذكاء الاصطناعي من خلال واجهات دماغ-حاسوب، مما قد يغير مفهومنا عن الهوية البشرية.
- الذكاء الاصطناعي يغيّر العالم بسرعة، ومع ذلك فإن كيفية استخدامه ستحدد ما إذا كان سيصبح قوة إيجابية أو سلبية. من الضروري وضع تشريعات وأطر أخلاقية لضمان استخدامه بطريقة تخدم البشرية وتعزز القيم الإنسانية.

التحديات الأخلاقية في الذكاء الاصطناعي (AI)

هي من أهم القضايا التي تُناقش حالياً، بسبب التوسع الكبير في استخدام هذه التقنية في مجالات متعددة. إليك أبرز هذه التحديات:

1. التحيز والتمييز

نُظم الذكاء الاصطناعي تتعلم من البيانات، وإذا كانت البيانات منحازة (مثلاً بسبب التمييز العرقي أو الجنسي أو الاجتماعي)، فإن النتائج ستكون كذلك. وهذا قد يؤدي إلى قرارات غير عادلة، خصوصاً في التوظيف، والعدالة الجنائية، والقروض البنكية.

2. الخصوصية

الذكاء الاصطناعي يتطلب كميات ضخمة من البيانات للتعلم، وغالباً ما تكون هذه البيانات شخصية. السؤال الأخلاقي هنا هو: كيف نحمي خصوصية الأفراد من التعدي؟

3. المساءلة

عند ارتكاب خطأ بواسطة نظام ذكاء اصطناعي (مثل حادث سيارة ذاتية القيادة)، من المسؤول؟ المطور؟ الشركة؟ المستخدم؟ هذه مسألة لم تُحسم بعد قانونياً وأخلاقياً.

4. فقدان الوظائف

أتمتة الوظائف باستخدام الذكاء الاصطناعي قد يؤدي إلى فقدان عدد كبير من الناس لوظائفهم، ما يثير تساؤلات أخلاقية حول العدالة الاجتماعية وتوزيع الثروة.

5. استخدامات عسكرية وأمنية

استخدام الذكاء الاصطناعي في تطوير الأسلحة أو في المراقبة الجماعية يُثير قضايا أخلاقية خطيرة حول الحق في الحياة، والحريات الفردية.

6. الشفافية والتفسير

الكثير من أنظمة الذكاء الاصطناعي (خاصة الشبكات العصبية العميقة) تُعتبر "صندوقاً أسوداً" يصعب تفسير كيفية اتخاذها للقرارات. هذا يعيق فهم ما إذا كانت القرارات عادلة أو سليمة.

7. الاعتماد الزائد

الاعتماد المفرط على الذكاء الاصطناعي قد يضعف من قدرة الإنسان على التفكير النقدي واتخاذ القرار، ويخلق علاقة تبعية غير صحية.

أخلاقيات الذكاء الاصطناعي :

هي مجموعة المبادئ والقيم التي تهدف إلى توجيه تطوير واستخدام تقنيات الذكاء الاصطناعي بطريقة تحترم الإنسان وتخدم الصالح العام. هذه الأخلاقيات تُعد ضرورية لتقليل المخاطر وتعزيز الفوائد. وهنا أبرز المبادئ الأخلاقية المتعلقة بالذكاء الاصطناعي:

1. العدالة

يجب أن تكون أنظمة الذكاء الاصطناعي عادلة وغير متحيزة. لا يجوز أن تميز بين الناس على أساس العرق أو الجنس أو الدين أو الخلفية الاجتماعية.

2. الشفافية

من الضروري أن تكون عمليات اتخاذ القرار في أنظمة الذكاء الاصطناعي واضحة ومفهومة للمستخدمين. يجب أن يتمكن الناس من فهم كيف ولماذا يتخذ النظام قرارات معينة.

3. الخصوصية

يجب احترام خصوصية الأفراد وحماية بياناتهم. ينبغي استخدام البيانات الشخصية فقط بإذن واضح ومحدد.

4. السلامة والأمان

يجب أن تكون أنظمة الذكاء الاصطناعي آمنة ولا تسبب ضررًا للناس. من المهم أن تكون مقاومة للهجمات السيبرانية ولا تُستخدم لأغراض ضارة.

5. المساواة

يجب تحديد من هو المسؤول عن نتائج استخدام الذكاء الاصطناعي. لا ينبغي أن تُستخدم الأنظمة الذكية كـ"عذر" للتخلص من المسؤولية.

6. احترام الكرامة الإنسانية

يجب أن يُستخدم الذكاء الاصطناعي لتعزيز قدرات الإنسان وليس للسيطرة عليه أو تقليله. لا يجوز استغلال الذكاء الاصطناعي في تهمة أو إذلال الأفراد.

7. الاستدامة الاجتماعية والبيئية

يجب أن يساهم الذكاء الاصطناعي في دعم التنمية المستدامة وليس الإضرار بالبيئة أو المجتمعات الضعيفة.

تأثير الذكاء الاصطناعي على سوق العمل هو موضوع كبير ويثير جدلاً واسعاً، لأنه يحمل فرصاً كبيرة لكنه في نفس الوقت يأتي بتحديات حقيقية :

أولاً: التأثيرات الإيجابية

1. خلق وظائف جديدة

ظهور تخصصات ووظائف جديدة مثل: محللي بيانات، مهندسي تعلم آلي، مطوري أنظمة ذكية، مدققي أخلاقيات الذكاء الاصطناعي. ازدياد الطلب على المهارات التكنولوجية والتحليلية.

2. زيادة الإنتاجية

أنظمة الذكاء الاصطناعي تساعد الشركات على أتمتة المهام المتكررة، مما يسرّع الإنجاز ويقلل الأخطاء.

تحسين اتخاذ القرار في الأعمال من خلال التحليلات الذكية والتنبؤات.

3. دعم الأعمال الصغيرة

أدوات الذكاء الاصطناعي أصبحت متاحة أكثر، وتساعد المشاريع الصغيرة في التسويق، وخدمة العملاء، وإدارة الموارد.

ثانياً: التأثيرات السلبية

1. فقدان الوظائف التقليدية

المهن التي تعتمد على المهام الروتينية مثل: موظفي الاستقبال، إدخال البيانات، وخدمة العملاء، تواجه خطر الأتمتة. يُتوقع أن تستبدل بعض الوظائف البشرية بالكامل بالآلات الذكية.

2. توسيع فجوة المهارات

العمال الذين لا يمتلكون مهارات رقمية أو تقنية قد يجدون صعوبة في مواكبة التحولات. تزايد الحاجة لإعادة تأهيل القوى العاملة لتتلاءم مع العصر الجديد.

3. زيادة اللا مساواة

الدول أو الأفراد الذين يمتلكون التقنية والمهارات سيجنون الفوائد، بينما قد تُهمش الفئات الأقل قدرة على التكيف.

كيف يمكن التعامل مع التأثير؟

تحديث أنظمة التعليم والتدريب المهني لتشمل المهارات الرقمية.

دعم سياسات التحول العادل لضمان ألا يُترك أحد خلف الركب.

تشجيع ريادة الأعمال في مجالات تكميلية للذكاء الاصطناعي.

حماية أمن الشبكات الإلكترونية

تُعدُّ أمرًا بالغ الأهمية في عصر التكنولوجيا الحديثة، حيث تزداد التهديدات الإلكترونية تعقيدًا يوميًا بعد يوم.

إليك بعض الخطوات الأساسية التي يمكن اتباعها لتأمين الشبكات الإلكترونية

1*تحديث البرمجيات والأجهزة بانتظام

التأكد من تثبيت آخر التحديثات الأمنية لأنظمة التشغيل والبرامج المستخدمة على الشبكة

2* (Firewalls) استخدام جدران الحماية

تثبيت جدران الحماية على الشبكة لمراقبة حركة المرور الواردة والصادرة ومنع الوصول غير المصرح به والتأكد

من تكوين جدار الحماية بشكل صحيح ليكون فعالاً في حماية الشبكة

3*تشفير البيانات

تشفير البيانات الحساسة المخزنة على الخوادم أو أثناء نقلها عبر الشبكة

4* إدارة الهويات والوصول

قلل من صلاحيات المستخدمين إلى الحد الأدنى لأداء مهامهم (مبدأ الامتياز الأقل)

5* تقسيم الشبكة

تقسيم الشبكة إلى أجزاء منفصلة لتقليل تأثير الهجمات.

6*مراقبة الشبكة باستمرار

استخدم أدوات مراقبة الشبكة لاكتشاف أي نشاط غير عادي أو مشبوه وبانتظام لتحديد أي محاولات اختراق أو انتهاكات أمنية

7*توعية الموظفين

تدريب الموظفين على أفضل الممارسات الأمنية، مثل تجنب فتح رسائل البريد الإلكتروني المشبوهة أو النقر على الروابط غير المعروفة

تشجيع الموظفين على استخدام كلمات مرور قوية وتغييرها بانتظام

8*نسخ احتياطي منتظم

إجراء نسخ احتياطي منتظم للبيانات المهمة وتخزينها في مكان آمن والتأكد من إمكانية استعادة البيانات بسرعة في حالة حدوث هجوم إلكتروني أو فقدان البيانات

9*استخدام أنظمة منع التسلل (IDS) واستخدام أنظمة كشف التسلل

تثبيت أنظمة كشف التسلل لاكتشاف ومنع الهجمات في الوقت الفعلي

10* تقييم الأمن بشكل دوري

إجراء اختبارات بشكل دوري لتقييم نقاط الضعف في الشبكة.

11*تطبيق سياسات أمنية واضحة

وضع سياسات أمنية واضحة للشبكة وتأكد من أن جميع المستخدمين يلتزمون بها

12* حماية الأجهزة الطرفية

تثبيت برامج مكافحة الفيروسات وبرامج الحماية من البرامج الضارة على جميع الأجهزة المتصلة بالشبكات والتأكد من تحديث هذه البرامج بانتظام

استكشاف أخطاء الكمبيوتر وإصلاحها

استكشاف أخطاء الكمبيوتر وإصلاحها يعتمد على نوع المشكلة التي تواجهها، وهذه أبرز المشاكل الشائعة وحلولها:

1. الجهاز لا يعمل أو لا يشتغل

الأسباب المحتملة:

- ❖ مشكلة في مصدر الطاقة أو البطارية.
- ❖ زر التشغيل لا يعمل.
- ❖ عطل في مجهز الطاقة (power supply).

الحلول:

- ❖ تأكد من توصيل الكهرياء أو شحن البطارية.
- ❖ جرب تغيير السلك أو مجهز الطاقة.
- ❖ افصل كل شيء وأعد التوصيل.

2. بطء الجهاز

الأسباب:

- ❖ برامج كثيرة تشتغل في الخلفية.
- ❖ فيروسات أو برمجيات خبيثة.
- ❖ قرص صلب ممتلئ أو قديم.

الحلول:

- ❖ افتح "مدير المهام" (Task Manager) واغلق البرامج غير الضرورية.
- ❖ شغل فحص فيروسات.
- ❖ احذف الملفات المؤقتة وملفات النظام غير المهمة.
- ❖ فكر في ترقية الـ RAM أو استخدام SSD.

3. شاشة سوداء عند التشغيل

الأسباب:

- ❖ كرت الشاشة فيه مشكلة.
- ❖ نظام التشغيل ما يطلع.
- ❖ الشاشة نفسها فيها عطل.

الحلول:

- ❖ تأكد من توصيل الشاشة بشكل صحيح.
- ❖ جرب شاشة أخرى.
- ❖ شغل الجهاز في "الوضع الآمن" Safe Mode.
- ❖ أعد تثبيت تعريف كرت الشاشة.

4. الجهاز يطفى فجأة

الأسباب:

- ارتفاع حرارة المعالج.
- مشاكل كهربائية.
- عطل في الهاردوير.

الحلول:

- نظف مروحة التبريد.
- استخدم برامج لمراقبة درجة الحرارة.
- تأكد من سلامة مزود الطاقة.

5. الانترنت لا يعمل

الأسباب:

- مشكلة في الراوتر.
- إعدادات الشبكة.
- تعريف كرت الشبكة.

الحلول:

- أعد تشغيل الراوتر.
- شغل مستكشف الأخطاء التلقائي في ويندوز.
- جرب الاتصال من جهاز آخر للتأكد إذا المشكلة عامة.
- أعد تثبيت تعريف كرت الشبكة.