Vol-02,Iss-02 May 2018
ISSN : 2571-9858
(P:52-P:67)

دور الذكاء الاصطناعي في مواجهة الجرائم الالكترونية

د.دولي لخضر /ldouli@yahoo.fr-جامعة طاهري محمد بشار –الجزائر
د.ناصري نفيسة /nafissafine@yahoo.fr-جامعة طاهري محمد بشار –الجزائر

الملخص:

تعد التهديدات الأمنية الإلكترونية أكثر التحديات التي تواجهها الاقتصاديات العالمية، حيث يشكل استخدام أحدث تقنيات الحماية المعقدة وتعزيز أنظمة البنية التحتية لأمن المعلومات أزمة كبيرة على الاقتصاد لما تكلفه من مبالغ ضخمة، ويعتبر حجم الاستثمار في أمن المعلومات من أهم اولويات الحكومات والشركات في مختلف دول العالم، لذا يجب أن يكون هناك العديد من الاستراتيجيات لحماية الشركات ومختلف شبكاتها من التهديدات الحقيقية لأمن المعلومات.

ضف لذلك أن المخاطر الإلكترونية تتغير باستمرار والجرائم الإلكترونية تتسم بطابع دولي، من هنا تظهر الحاجة إلى بناء أنظمة ذكية لإدارة أمن المعلومات، مبنية على تقنيات الذكاء الاصطناعي و منهاجياتها لتدعم عمليات التحكم و المراقبة و اتخاذ القرارات الدقيقة من قبل الخبراء وأصحاب المعرفة و دعم عمليات إدارة أمن المعلومات و اكتشاف عمليات التلاعب و التجسس،

الكلمات المفتاحية: تقنيات الحماية ، الذكاء الاصطناعي، الجرائم الاقتصادية، أمن المعلومات.

ABSTRACT :

Security threats are one of the most pressing challenges facing global economies. The use of state-of-the-art complex protection technologies and the strengthening of information security infrastructure systems pose a major economic crisis for large sums. The investment in information security is a top priority for governments and companies around the world, So there must be many strategies to protect companies and their networks from real threats to information security.
n addition, electronic risks are constantly changing and cybercrime is international in nature, hence the need to build intelligent information security management systems based on artificial intelligence techniques and platforms to support control and control processes, accurate decision making by experts and knowledge owners, Information and detection of manipulations and espionage,

Keywords: protection techniques, artificial intelligence, economic crimes, information security.

مقدمة :

تعتبر أمن المعلومات من الأنظمة المعقدة التي يجب أخذها في الإعتبار في جميع مراحل تطوير أنظمة العمل وكيفية استخدامها من قِبل جميع العاملين عليها. ولهذا فإن المنشآت تحتاج إلى منهجية منظمة تدعم ثبات معايير الأمن خلال جميع المراحل، قائمة على أساس التنبؤ والتحليل (Reactive-based approach) وليس فقط على معالجة الثغرات أو نقاط الضعف المحسوسة في عمل المنشأة .

إن تكامل عدد من تقنيات الذكاء الاصطناعي(Artificial Intelligent) ، مثل تنقيب البيانات والشبكات العصبية الذكية (Intelligent Neural Network) و المنطق الضبابي (Fuzzy Logic) و الأنظمة الخبيرة، مع الإجراءات التقليدية والطرق الإحصائية قد تساعد في تحليل البيانات المخزنة لتدعم عمليات إدارة أمن المعلومات وإكتشاف عمليات التلاعب والتجسس. وتحسن هذه التقنيات قدرة أنظمة إدارة أمن المعلومات من ربط وتحليل الأحداث الناتجة من أنواع مختلفة من الأدوات الحديثة المستخدمة في إدارة الشبكات ومراقبتها.

فالجرائم الإلكترونية تُكلّف الاقتصاد العالمي حوالي 445 مليار دولار أمريكي سنوياً، وتُشكّل الجرائم الإلكترونية ثاني أكثر الجرائم الاقتصادية شيوعاً بنسبة 37% بعد اختلاس الأموال و الأصول في منطقة الشرق الأوسط بحسب ما ذكره استبيان PWC (Price water house Coopers) حول الجريمة الاقتصادية العالمية 2014.

و عليه فان الاشكال الذي نحن بصدد معالجته في هذه الورقة البحثية يتمثل فيما يلي:

كيف يمكن الاستعانة بتقنيات الذكاء الاصطناعي و الأنظمة الخبيرة في مواجهة الجرائم الالكترونية التي تهدد اقتصاد دول عديدة و بالتالي تنخر قوى الاقتصاد العالمي؟

و عليه سنحاول الاجابة عن اشكالية الدراسة بتقسيم الورقة البحثية الى ثلاثة أجزاء رئيسية:

- **الجرائم الاقتصادية في العالم الافتراضي**
- **الإجراءات والتدابير الواجب اتخاذها لمكافحة الجرائم الاقتصادية في العالم الافتراضي**
- **دور النظم الخبيرة و الذكاء الاصطناعي في تقوية أمن المعلومات**

أولا :الجرائم الاقتصادية في العالم الافتراضي:

هي الجريمة ذات الطابع المادي، التي تتمثل في كل سلوك غير قانوني من خلال استخدام الأجهزة الالكترونية ، ينتج منه حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة وغالبا ما يكون هدف هذه الجرائم هو القرصنة من اجل سرقة أو إتلاف المعلومات الموجودة في الأجهزة ومن ثم ابتزاز الأشخاص باستخدام تلك المعلومات.و بالتالي تظهر الحاجة إلى وجود جدار قوي لحماية الشركات من هذه المخاطر و الذي يتمثل في أمن المعلومات و الذي هو قضية تبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.

ومن زاوية تقنية، هي الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية . ومن زاوية قانونية ، فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى المعلومات ومكافحة

أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها جرائم الكمبيوتر والإنترنت.

يعرف خبراء القانون الجرائم الإلكترونية بأنها :كل من ضبط داخل نظام المعالجة الآلية للبيانات أو جزء منه وترتب على هذه الطريقة أحد **العناصر** التالية :محو بيانات أو تعديل بيانات أو تعطيل تشغيل النظام[1] .

كما يعرف أمن المعلومات بأنه " توفير الوسائل والإجراءات التي تحقق الحماية من الأحداث المستقبلية غير المرغوب فيها، وهذه جزئيات النظام[2]."

-دوافع ارتكاب الجرائم الالكترونية :توجد عدة دوافع لارتكاب هذه الجرائم، نذكر منها ما يلي:

أ .الدافع السياسي والعسكري :مما لا شك فيه أن التطور العلمي والتقني أديا إلى الاعتماد بشكل شبه كامل على أنظمة الكمبيوتر في أغلب الاحتياجات التقنية والمعلوماتية .فمنذ نهاية الحرب الباردة والصراع المعلوماتي بين الاتحاد السوفياتي – سابقا – والولايات المتحدة الأمريكية، ومع بروز مناطق جديدة للصراع في العالم وتغير الطبيعة المعلوماتية للأنظمة والدول، أصبح الاعتماد كليا على الحاسب الآلي وبذلك أصبح الاختراق من أجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية؛

ب.الدافع التجاري :من المعروف أن الشركات التجارية الكبرى تعيش هي أيضا فيما بينها حربا مستعرة .وإن عددا من كبريات الشركات التجارية يجري عليها كثيرا من محاولات الاختراق لشبكاتها كل يوم؛

ج.الدافع الفردي :بدأت أولى محاولات الاختراق الفردية بين طلبة الجامعات بالولايات المتحدة الأمريكية كنوع من التباهي بالنجاح في اختراق أجهزة شخصية لأصدقائهم ومعارفهم وما لبثت أن تحولت تلك الظاهرة إلى تحدي فيما بينهم في اختراق الأنظمة بالشركات ثم بمواقع الانترنت .ولا يقتصر الدافع على الأفراد فقط بل توجد مجموعات ونقابات أشبه ما تكون بالأندية وليست بذات أهداف تجارية.

-جرائم الأموال في نطاق التجارة الالكترونية[3]:

وهي من المخاطر الجسيمة التي تواجه هذه الحكومة، ومن الجرائم التي يمكن أن تتم في هذا النطاق هي:

---

[1] د .مكاوي محمد محمود ، **البيئة الرقمية بين سلبيات الواقع وآمال مجلة إلكترونية**، عدد3 ، سبتمبر Cybrarians journal المستقبل، مجلة 2004، متاحة على الموقع:
http://www.cybrarians.info/journal/no9/info-secuirty.htm

[2] د .ديريه سعيد، أمن المعلومات، 2004 ، متاح على الموقع: http://www.saidder.jeeran.com/amn.htm

[3] مجلة البحوث والدراسات العلمية، جامعة الدكتور يحي فارس، **مخاطر القرصنة المعلوماتية على الحكومة الالكترونية**، الأستاذ يحياوي محمد.ص258-260، العدد الخامس-جويلية 2011.

–سرقة المعلومات من طرف القراصنة والتجسس على حسابات العملاء في البنوك؛

–العبث بالبطاقات الممغنطة واستعمالها في التلاعب بحسابات العملاء أو تحويل مبالغ من أموالهم إلى حسابات القراصنة أنفسهم؛

–إتلاف الشبكات أو الأجهزة الالكترونية إما بطريقة مادية كسكب سوائل باردة أو ساخنة على الدعامات الالكترونية المخزن عليها البيانات أو المعلومات، أو من خلال زرع فيروسات) القنابل المنطقية، القنابل الموقوتة، باب المصيدة، الدودة الالكترونية، أحصنة طروادة (تعمل على التعطيل الكلي أو الجزئي لعمل الشبكات أو لتشويه المعلومات التي تقدمها الحكومة الالكترونية للأفراد.

جرائم السطو على أرقام البطاقات الائتمانية[4] :

مع بداية استخدام البطاقات الائتمانية خلال شبكة الانترنت واكبت ظهور الكثير من المتسللين للسطو عليها بلا هوادة، فالبطاقات الائتمانية تعد نقوداً الكترونية والاستيلاء عليها يعد استيلاء على مال الغير .ومع وضع تفعيل مفهوم التجارة الالكترونية قامت العديد من شركات الأعمال إلى استخدام الانترنت والاستفادة من مزايا التجارة الالكترونية.

إن الاستيلاء على بطاقات الائتمان أمراً ليس بصعوبة مكان، فلصوص بطاقات الائتمان مثلاً يستطيعون الآن سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنت ومن ثم بيع هذه المعلومات للآخرين.ويتعدى الأمر المخاطر الأمنية التي يمكن أن تتعرض لها البطاقات الائتمانية الحالية فنحن الآن في بداية ثورة نقدية يطلق عليها اسم النقود الالكترونية والتي يتنبأ لها بأن تكون مكملة للنقود الورقية أو البلاستيكية ومن المتوقع أيضاً أن يزداد الاعتماد على هذا النوع الجديد والحديث من النقود أن تحوز الثقة التي تحوزها النقود التقليدية.

القمار عبر الانترنت:

في الماضي كان لعب القمار يستلزم وجود اللاعبين معاً على طاولة واحدة ليتمكنوا من لعب القمار ، أما الآن ومع انتشار شبكة الانترنت على مستوى العالم فقد أصبح لعب القمار أسهل وغدا التفاف اللاعبين على صفحة واحدة من صفحات الانترنت على مستوى العالم ومن أماكن متفرقة أسهل من ذي قبل . كما تنافست كثير من المواقع المتخصصة في ألعاب القمار لتزويد صفحات مواقعهم بكثير من البرامج نظراً لان اللاعبين بات بإمكانهم اللعب وكل في مسكنه وكثير ما تتداخل عملية غسيل الأموال في شكل يتم على شبكة الانترنت ولتكن مثلا مع

[4] المستشار الدكتور محمد ياسر أبو الفتوح، **خصائص وتصنيفات الجريمة المعلوماتية**، محكمة استئناف القاهرة، مستشار مركز المعلومات ودعم واتخاذ القرار : http://www.F-law.netبرئاسة مجلس الوزراء،2008

أندية القمار المنتشرة ، الأمر الذي جعل مواقع الكازينوهات الافتراضية على الانترنت محل اشتباه ومراقبة من قبل السلطات الأمريكية ، وبالرغم من مشروعية أندية القمار في أمريكا ، إلا أن المشكلة القانونية التي تواجه أصحاب مواقع القمار الافتراضية على الانترنت أنها غير مصرح لها حتى الآن في أمريكا بعكس المنتشرة في لاس فيجاس[5].

تزوير البيانات:

تعتبر جرائم تزوير البيانات من أكثر الجرائم شيوعاً من بين كافة أنواع الجرائم التي ترتكب سواء على شبكة الانترنت أو ضمن جرائم الحاسب الآلي نظرا لأنه لا تخلو جريمة من الجرائم إلا ويكون من بين تفاصيلها جريمة تزوير البيانات بشكل أو بأخر ، وتزوير البيانات يكون بالدخول على قاعدة البيانات الموجودة وتعديل تلك البيانات سواء بإلغاء بيانات موجودة بالفعل أو بإضافة بيانات لم تكن موجودة من قبل.[6]

ووفقاً لدراسة برايسووترها وسكوبرز تتمثل أكثر التهديدات الإلكترونية الأكثر شيوعاً في المنطقة بالتطبيقات والأنظمة والشبكات إضافة إلى المخاطر التي تتعرض لها الأجهزة المحمولة وأجهزة التخزين والبيانات المتنقلة الموجودة لدى الطرف الثالث. ومن بين الأمثلة الحديثة التي شهدتها منطقة الشرق الأوسط على صعيد التهديدات الإلكترونية على نطاق واسع ما حصل في **عام 2012** عندما تعرضت اثنتان من كبرى شركات النفط والغاز لهجمات إلكترونية تسببت بتعطيل عمل عشرات الآلاف من الكمبيوترات بشكل كبير.

ووفقاً لـ **آلين بينيل**، نائب الرئيس الإقليمي، الشرق الأوسط، في شركة فورتينت، فإن التهديدات تزداد تعقيداً وأن شركات الخدمات المالية باتت عرضاً للكثير من الهجمات المتطورة، لافتاً إلى أن الكثير من شركات أمن تقنية المعلومات في المنطقة باتت تعيد التفكير لما يتعلق باستراتيجية أمن المعلومات وعمدت إلى استبدال برمجيات الحماية التقليدية للوفاء بمتطلبات البيانات والمعلومات المتزايدة والتصدي في الوقت ذاته للعدد المتزايد من التهديدات المعقدة. وأضاف: ''نحن في فورتينت ننصح العملاء باعتماد التقنيات التي لها أقل تأثير على سرعة أداء الشبكات من خلال السماح لعمليات فحص عميقة وإجراءات تحليلات دقيقة للمحتويات وتفادي استخدام المنتجات التي تعمل على نقاط متعددة، ولدينا المنتجات التي تتميز بأدائها العالي والكفاءة والتكاليف المعتدلة التي باتت مستخدمة على نطاق واسع لدى أبرز البنوك والمؤسسات المالية في المنطقة''.

[5] رصاع فتيحة،**الحماية الجنائية للمعلومات على شبكة الانترنت**، مذكرة لنيل شهادة الماجستير في القانون العام،جامعة ابي بكر بلقايد تلمسان، 2011-2012، ص81

[6] رصاع فتيحة، **نفس المرجع السابق** ، ص 89.

ويقول **جواكين سندبيرج**، مصمم الحلول الأمنية في أف فايف،"بات على المؤسسات المالية على صعيد الشرق الأوسط والعالم مؤخراً التعامل مع مختلف التهديدات ذات التأثير المدمر، الأمر الذي فرض عملية إعادة تفكير لإجراءات حماية الشبكات. وبموازاة ذلك، طورت أف فايف بنية تحتية مرجعية للحماية ضد مختلف التهديدات، والتي تمثل استراتيجية لمستويات عديدة توفر المرونة والقدرة على إدارة المخاطر لتخفيف أكثر هجمات DDoS تأثيراً."

ويشار إلى إن الإمارات قد عمدت إلى التشديد على شبكة الأمن الإلكتروني فأصبحت الرائدة على صعيد المنطقة والعالم. وقد أولت الإمارات جدية كبيرة للغاية للأمن الالكتروني بحيث تبوأت المركز الأول على صعيد دول مجلس التعاون الخليجي والرابع عالمياً عام 2012 وفقاً لتقرير المعهد الدولي للتطوير الإداري، سويسرا، والذي أظهر إن الإمارات قفزت في الترتيب من المركز 35 عالمياً عام 2011 إلى المركز الرابع[7].

ثانيا :الإجراءات والتدابير الواجب اتخاذها لمكافحة الجرائم الاقتصادية في العالم الافتراضي:

هناك مجموعة من الإجراءات الإدارية والفنية التي يمكن استعمالها في هذا الصدد لتحقيق أمن المعلومات، وهي كالآتي:

1.الإجراءات الإدارية لأمن المعلومات :على الحكومات التي تتبنى تقديم خدماتها الكترونية للمواطنين القيام بعدة مهام تجاه أمن المعلومات كالرقابة والإشراف على أمن المعلومات، وسوف يتم استعراض مهام رئيسية يجب عليها القيام بها، وهي كالتالي:

أ .**توفير أمن الأجهزة** :لتأمين الأجهزة لابد من تأمين المبنى كعدم السماح لغير المصرح لهم بالدخول إلى غرفة الحاسب الآلي، ومخزن وسائط التخزين .ويفضل استخدام التكنولوجيا الحديثة للدخول على الأنظمة مثل: بصمة الأصبع، بصمة العين، البطاقة الممغنطة ... إلخ.[8]

ب .**توفير أمن البيانات** :يتوجب على الإدارة توزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي بما يضمن رفع المستوى الأمني، وتقليص الجرائم، ووضع آلية يتم تنفيذها للقيام بالنسخ الاحتياطي وتأمين وسائط الحفظ

[7] http://www.n1t1.com/gisec-2014-banking-sector/

[8] د .الشدي طارق عبد الله، **الآلية البناء الأمني لنظم المعلومات**، دار الوطن للطباعة والنشر، الرياض، المملكة العربية السعودية، 2000 ، ص 182.

الخارجية بما يكفل أمنها وتحديثها، ويجب صياغة الضوابط المنظمة لعمليات التشغيل، ولمبرمجي قواعد البيانات ومدرائها، ولإدارة الشبكات وخطوط الاتصال، ولعمليات الإدخال والإخراج، والضوابط الأمنية لبناء وتشغيل البرامج التطبيقية.

ج .**توفير أمن الأفراد** :عندما تريد الإدارة حماية معلوماتها عليها إتباع)الإجراءات الإدارية في مجال أمن الأفراد على النحو التالي[9]:

-منع التوظيف المؤقت نهائيا، ومراعاة إجراءات إنهاء خدمة الموظف بطلب تسليم كل ما كان بحوزته كالمفاتيح والبطاقات الممغنطة، وتغيير كلمة المرور قبل مغادرته؛

-متابعة العاملين ونقلهم إجباريا بين الأقسام المختلفة في الإدارة، وملاحظة الذين لا يطلبون إجازة بإجبارهم على الإجازة ومراقبة النظام بعد ذلك للتأكد من عدم وجود خلل كانوا يتفادونه بوجودهم؛

-عقد ندوات ومؤتمرات ومحاضرات بشكل دوري في مجال أمن المعلومات، وعرض النشرات الداخلية وتعليمات الإدارة التي تتضمن إطلاع الأفراد على المعلومات المهمة في مجال الأمن، لإلزام العاملين بالنظم الإدارية المحددة؛

-دفع العاملين لحضور المعارض العالمية للأجهزة والبرامج، وإرسالهم إلى الدورات المتخصصة بأمن المعلومات، ليكون لديهم خلفية قوية بما يكفل تحقيق أمن المعلومات؛

-منح الحوافز وربط الترقية والدورات بمدى التقيد بأمن المعلومات.

د.**توفير قسم متخصص بأمن المعلومات** :تقوم المؤسسة الكبيرة بتعيين مدير أمن نظم المعلومات يرتبط بالإدارة العليا مباشرة لأهمية التقارير التي يعدها.

ويرأس مدير الأمن قسما مستقلا من المتخصصين في مجال أمن المعلومات ومن ذوي الخبرة الفنية والأمنية في معالجة البيانات والبرمجة حسب نظم التشغيل ولغات البرمجة وقواعد البيانات المستخدمة في المؤسسة، ومدربين على التنسيق الأمني ولديهم المقدرة الكافية للتعامل مع جرائم نظم المعلومات والحالات الطارئة.

.**2الإجراءات الفنية لأمن المعلومات** :هناك مجموعة من الإجراءات الفنية التي ينبغي على المؤسسات توفيرها لحماية معلوماتها، نذكر منها:

أ .**توفير الحماية الإلكترونية** :تخضع الحماية الإلكترونية للإعدادات الخاصة بالحاسب الآلي، والأجهزة الملحقة به، ويمكن بيانها على النحو التالي:

[9] BARMAN S, Writing Information Security Policies, New Riders Publishing, Available http://Safari.informit.com November 2001 .

-حذف الملفات غير الهامة ولو كانت المعلومات التي تحويها ضئيلة وعديمة الفائدة، والتأكد من عدم إبقائها في سلة المحذوفات.

-الكشف على الحاسب الآلي بعد الغياب عن طريق المستكشف، وتركيب برامج تمنع مسح المعلومات من المستكشف، أو استخدام برامج تحتفظ بالعمليات التي تم إجراؤها؛ لعدد كثير من Password كنظام حماية مرور.

- استغلال برنامج الملفات المراد حمايتها .وضغط الملفات وحمايتها بكلمة مرور؛

-التأكد من عدم وجود برامج تجسس من فئة أحصنة طروادة في حالة الارتباط بشبكات في الحاسب الآلي؛

-عند استخدام الإنترنت يجب عدم حفظ كلمة المرور الخاصة بالمستخدم وقت الدخول للإنترنت، وغلق المتصفح حال الابتعاد عن الجهاز لتعطيل خاصية الرجوع للخلف في المتصفح، وعدم استخدام خاصية تذكر اسم المستخدم وكلمة المرور؛

-عند استخدام البريد الإلكتروني يجب عدم فتح الملفات المرفقة إلا بعد التأكد منها؛

-من الضروري تركيب البرامج المضادة للفيروسات على الجهاز وتشغيلها طوال فترة استخدام الجهاز، ومن الضروري أيضا تحديث برامج مستكشف الفيروسات بصورة دورية.

ب .**تأمين جميع مكونات الشبكة** :في حالة استخدام الشبكات، فإن الحماية في هذه الحالة تعتمد على التحقق من الشخصية، للدخول إلى الشبكة، وعلى وسائل أمن الشبكة والتي يجب فحصها بالكامل وتقييم إمكانية اختراق نظام الحماية وتحديد تلك المخاطر المتعلقة بالتصميم والإدارة.

ج .**استخدام التشفير** :إرسال البيانات عبر الشبكة يجعل من السهل التصنت عليها، والطريقة الوحيدة لمنع هذا التصنت هي استخدام التشفير. بأنه عملية تحويل المعلومات إلى شفرات غير Encryption يعرف التشفير مفهومة تبدو غير ذات معنى لمنع الأشخاص غير المرخص لهم من الإطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مشفرة .وتشكل الإنترنت الوسط الأضخم لنقل المعلومات الحساسة، وقصد الحفاظ على سلامتها وأمنها فلابد من تشفيرها.

ويمكن استخدام ثلاث طرق للتشفير كالتالي:

-**الشهادات الرقمية** :تصدر الشهادات الرقمية المانحة الموثوق بها التي توقع عليها وتستخدم هذه الشهادات للتحقق من موثوقية المفاتيح العامة التي أصدرت؛

-**البصمة الإلكترونية** :وهي بصمة رقمية يتم اشتقاقها وفقا لخوارزميات معينة تدعى دوال أو اقتران التمويه .

-**التوقيع الرقمي** :يستخدم التوقيع الرقمي الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل ويمكن للمرسل استخدام المفتاح الخاص لتوقيع الوثيقة إلكترونيا .أما في طرف المستقبل فيتم التحقق من صحة التوقيع عن طريق استخدام المفتاح العام المناسب .و باستخدام التوقيع الرقمي يتم تأمين سلامة الرسالة والتحقق من صحتها، ومن فوائد هذا التوقيع أنه يمنع المرسل من التنكر للمعلومات التي أرسلها.

-استخدام كلمات المرور :يتطلب أمان نظم المعلومات استخدام كلمات مرور معقدة لتسجيل الدخول إلى شبكة أو حاسب الآلي ، وتكون كلمات المرور القوية هامة على اعتبار أن أدوات اكتشاف كلمات المرور مستمرة في التحسن وعلى اعتبار أن أجهزة الحاسب الآلي المستخدمة لاكتشافها أصبحت أكثر فعالية من ذي قبل، وأصبح بالإمكان الآن كسر كلمات مرور الشبكة بكل يسر.

ثالثا :دور الأنظمة الخبيرة و الذكاء الاصطناعي في تفعيل حماية الشركات:

إن الهدف من استخدام الأنظمة الخبيرة[10] المعززة بتقنيات الذكاء الاصطناعي هو تطوير وتحسين عمليات المراقبة وإتخاذ القرارات بحجم تأثيري أكبر من قدرة خبراء أمن المعلومات. بالإضافة إلى تحسين عملية إنشاء قاعدة المعرفة بخصوص التهديدات و السياسات و الإجراءات و المخاطر المتعلقة بأمن المعلومات. و إمكانية تكيف النموذج ودعمه لمعالجة الأحداث والبيانات وتصنيفهما والتي تقود إلى إمكانية التنبؤ بالهجمات و تحديد طرق المعالجة المناسبة من قبل وقوعها. و تعد أحد أهم مكونات صميم النظام حسب آراء الخبراء هو القدرة على تطوير نموذج ذكي يقوم بتحليل و ربط الأحداث والبيانات فورياً (أي في وقت الحدوث) وذلك لزيادة إمكانيات الإكتشاف والمنع (Detection and Prevention) في تقنيات الأمن: أنظمة كشف الخداع (Intrusion Detection System)و برامج مكافحة الفيروسات و ترشيح الرسائل الدعائية وأنظمة تقييم نقاط الضعف. فعلى سبيل المثال: النماذج الضبابية (fuzzy models) يجب أن تستخدم في إدارة المخاطر (Risk Management) والتي تعتبر إحدى أهم مراحل إدارة أمن المعلومات.

مجالات الذكاء الاصطناعي:

مع التقدم السريع لتكنولوجيا الحاسبات وبفضل كون الحواسب مصممة أصلا لتحصيل وتخزين ومعاملة واستخدام المعلومات، من المتوقع أن تصبح تقنيات وتطبيقات الذكاء الاصطناعي جزءًا هامًا من حياتنا.

[10] **النظم الخبيرة**: عبارة عن تطبيق حاسوبي لصنع القرارات في المجالات الحقيقية للحياة، معتمد على قاعدة معرفة تمثل خبرة إنسان خبير في المجال المحدد، وتستخدم عادة في حقول الطب، التعليم، القانون ، البيولوجيا،...

الشبكات العصبونية ، Expert Systems إلى عدة أجزاء منها : النظم الخبيرة AI يمكن تقسيم مجالات تمثيل القدرات الحسية للإنسان ، Natural Languagesفهم اللغات الطبيعية ،Neural Network ، Fuzzy logic المنطق العائم ، Robotic الروبوتيك ، Computer Vision وخاصة الرؤية الحاسوبية وغالبًا ما تتقاطع هذه الأجزاء فيما بينها.. .، Agent العميل ، Computer gamesألعاب الحاسب

–الشبكات العصبونية[11]:

وهي عبارة عن نظم تقوم بتمثيل " الذكاء " بواسطة مجموعة من عناصر المعالجة تشابه العصبونات في الدماغ، وتتصل هذه العناصر مع بعضها البعض من خلال شبكة من الوصلات الموزونة بحيث تتم(neurons) معايرة هذه الأوزان من خلال التعليم كما يحدث عادة مع الإنسان .وهذه الوصلات في التقنيات الحالية قليلة جدًا مقارنة مع ما هو متوفر في الدماغ) حيث يوجد بلايين الموصلات .(تطبق نظم الشبكات العصبونية في مجال محدد مثل التعرف على الأشكال.

–المنطق العائم[12]:

وهو منطق يستخدم ــ بالإضافة إلى المستويين المنطقيين المعروفين :صح /نعم أو خطأ/لا – مستويات وسيطة مستمرة بينهما مثلا أكثر حرارة، بارد نوعًا ما، ..وهو بذلك محاولة لتطبيق طريقة تفكير أكثر شبهًا بالإنسان في برمجة الحواسب.

–العميل:

تتصرف لصالح شخصيات أخرى) غالبًا Computational Entity وهو عبارة عن شخصية حاسوبية بشرية (بشكل مستقل .مثلا يمكن لشخص أن يملك عميله الخاص الذي يراقب له المقالات الحديثة على وينتخب له المقالات المفضلة لديهUsenet .

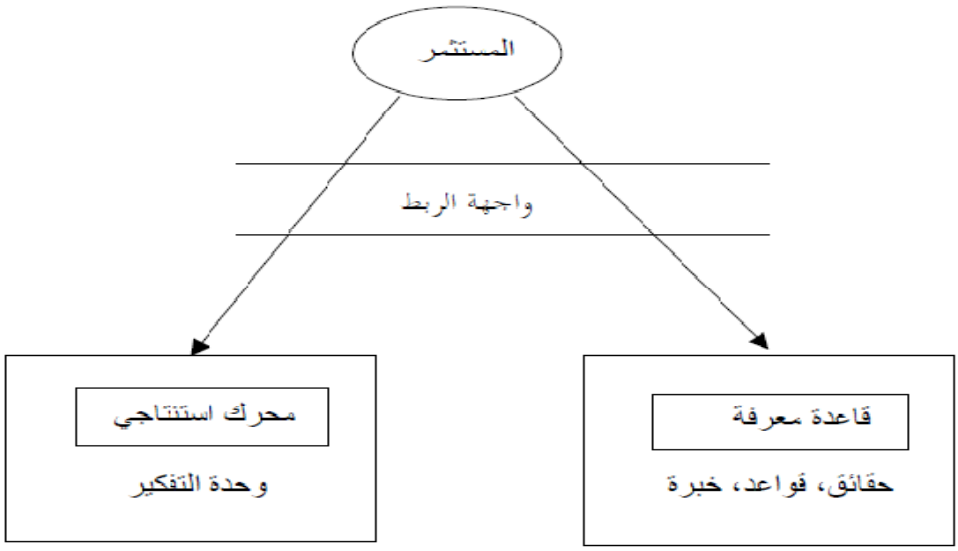
- **مكونات النظم الخبيرة**

يتألف النظام الخبير عادة من:

[11] Kate A. Smith!,*, Jatinder N.D. Gupta" !School of Business Systems, Monash University, Clayton, VIC 3168, Australia "Department of Management, Ball State University, Muncie, IN 47306, USA, **Neural networks in business**: **techniques and applications for the operations researcher**, Computers & Operations Research 27 (2000) 1023}1044.

[12] George Bojadziev, Simon Fraser University, Canada Maria Bojadziev British Columbia Institute of Technology, Canada **Fuzzy Logic for Business**, **Finance**, **and Management 2nd Edition**, **Advances in Fuzzy Systems – Applications and Theory – Vol**. **23**, World Scientific .

1- End User Interface .واجهة ربط مع المستثمر : معلومات، حقائق، قواعد، خبرة، ..
يقوم المستثمر باستشارة النظام من خلال واجهة الربط والتي تحدد الطلبات واللغة المطلوب استخدامها، ويقوم النظام بالاستفسار من المستثمر بواسطة نفس الواجهة ليحصل على المعلومات اللازمة لأخذ القرار.
2- Knowledge Base قاعدة معرفة: تحتوي قاعدة المعرفة على كل" المعارف "التي يستخدمها الخبير البشري لحل مشاكل المجال المحدد .
3- Inference Engine .محرك استنتاجي: يقوم المحرك الاستنتاجي باستخدام الاستنتاجات اللازمة وباستخدام قاعدة المعرفة حتى يصل إلى القرار بالنسبة للمسألة المطروحة.



شكل – 1 – مكونات النظام الخبير

بطريقة أخرى يمكن القول أن قاعدة المعرفة والمحرك الاستنتاجي يمثلان المعرفة المخزنة في ذاكرة الخبير البشري والقدرات الاستنتاجية التفكيرية له . يحتوي المحرك الاستنتاجي على مجموعة من العلاقات المنطقية والتي يمكن أن تشبه أو لا تشبه أحياناً طريقة التفكير التي يستخدمها الإنسان ، تتميز بعض النظم الخبيرة بإمكانية استخدامها لمعطيات غير كاملة حيث تتضمن قاعدة المعرفة درجة التأكد عند تصميم النظام الخبير Degree of Certainty .

تتكون الأنظمة الذكية من جزئين أساسيين هما:

1-**الجزء الداخلي – الحسابي** :**Computational** والذي يمكن تصنيفه إلى أربع أنظمة جزئية:

– المعالجة الحسية – (Sensory processing) تستخدم الحساسات كأداة إدخال في الأنظمة الذكية وكأداة لمراقبة العالم الخارجي للنظام والنظام نفسه.

– نمذجة العالم أو البيئة – (World Modeling) تتضمن قواعد بيانات معرفية عن عالم النظام و وحدة محاكاة، تقوم ببناء حالة مستقبلية لعالم النظام.

– إنشاء السلوك – (Behavior Generation) وحدة صنع القرار، تقوم بإختيار الأهداف والخطط وتنفيذ المهام.

– التقييم الذاتي – (Value Judgment) تقييم الحالة المدركة للنظام و الحالة المتنبأة.

2-الجزء الخارجي التفاعلي :**Interfacing** المدخلات والمخرجات من و إلى النظام الذكي تكون إما عن طريق حساسات أو مشغلا(actuators) ، والتي تعتبر الأجزاء الخارجية للنظام.

طريقة العمل: تقوم المعالجة الحسية بمعالجة البيانات المسجلة من الحساسات للحصول على النموذج الداخلي لعالم النظام وحفظها، ثم يقوم نظام إنشاء السلوك بإختيار سياق التصرفات (actions) لتحقيق الأهداف وتتحكم بالمشغلات لمتابعة الأهداف السلوكية ضمن سياق النموذجِ العالميِ المحسوس. البيانات الناتجة من الحساسات تعتبر الأساس لبناء قواعد المعرفة و إكتشاف الهجمات على النظام وتوقعها قبل حصولها وكذلك القيام بإتخاذ القرارات الزمنية الفورية.من الأمثلة على بيانات الحساسات تتضمن قياسات مرتبطة بأداء و أمن و حالة ما يلي:

-الأجهزة مثل أداء وحدة المعالجة المركزية (CPU) و استخدام الذاكرة و مساحة القرص المستخدمة و عدد الملفات المستخدمة في الاتصالات النشطة و عدد محاولات الدخول إلى النظام الفاشلة و عدد العمليات (من استعلامات و تحديثات و حذف) و زمن الاستجابة للطلبات و عدد المستخدمين ذوي الامتيازات الداخلين إلى النظام في نفس الوقت و عدد التغييرات في إعدادات النظام و عدد الاتصالات المنتظِرة ونسبة استخدام ملفات النظام و مراقبة ساعة النظام (System Clock) و بروتوكولات تزامن ساعة النظام و حجم ملفات سجل النظام (Log Files)وغيرها.

-الشبكة مثل سعة الاتصال المتاحة (available band width) و التأخير وطلبات الدخول إلى الشبكة و عدد المصادر الغير متاحة للإستخدام لبعض الوقت و عدد المنافذ المفتوحة و عدد العمليات على شبكة الانترنت والتغييرات في إعدادات الشبكة و عدد الحزم (Packets) الساقطة و عدد رسائل البريد الالكتروني و إستخدام بروتوكولات الاتصال وغيرها.

-الواجهات مثل إحصاءات الإستخدام

-البيئة المحيطة بالنظام مثل درجة الحرارة والإنذارات.

-ضمانات الأمن) Security Safeguards – جدار الحماية و أنظمة إكتشاف التدخل و برمجيات الحماية من الفيروسات و الشبكات الشخصية الإفتراضية و التشفير) مثل عدد الاتصالات المرفوضة و عدد التحذيرات و أوقات الصيانة و عدد تحديثات البرمجيات و عدد المفاتيح المستخدمة في عملية التشفير وفكها و الدخول عن بعد (Remote Access)وغيرها.

-سياسات الأمن.

-خطط حالات الطوارئ و الاسترداد.

-نشاطات مدراء الأمن والشبكات (الدخول و التغييرات في الإعدادات و تثبيت البرمجيات و تحديثها و عدد رسائل التبليغ (Notification Messages) وغيرها.

العميل (Agent) هي وحدات حاسوبية تتكرر عدة مرات (عقد) في النظام الذكي خلال عدة مراحل. في كل عقدة (loop) تُعالج حساسات الأمن وتحفظ المعلومات في قاعدة البيانات المعرفية للنظام. في كل مرحلة تبنى خطط وتُحدث بأفاق تخطيطية أخرى. على سبيل المثال: متغيرات التحكم قد تكون سعة الإرسال للشبكة. هذا النموذج المبني على تدرج هرمي لمتعدد قرارات (multi-resolutional hierarchy) من العقد الحاسوبية ينتج القدرة على تحليل ظواهر التصرف والفهم والإدراك وحل مشاكل النظام وقدرته على التعلم الذاتي. إن تركيبة النظام المقترحة قائمة على بناء إطار عمل (framework) من العملاء الحاسوبيين، بحيث يكون لكل عميل خصائصه وتركيبته الخاصة به والتي تستخدم واحدة أو أكثر من تقنيات الذكاء الاصطناعي، مثل معالجة اللغات الطبيعية والشبكات العصبية الذكية و المنطق الضبابي وكذلك تقنيات تنقيب البيانات. بالإضافة إلى الاستفادة من تقنيات البرمجة التقليدية وحزم الحلول الإحصائية لبناء تركيبة هجينة للنظام، إن الفكرة الأساسية من بناء هذا النظام الهجين هو تمكين النظام من القيام بمهام وظيفية مختلفة مستقلة بمعايير ومقاييس مختلفة عن الوظائف الأخرى، بالإضافة إلى تكملة نقاط الضعف في أحد النماذج بنقاط القوة في النماذج الأخرى. فعلى سبيل المثال: قد تستخدم الشبكات العصبية الذكية Intelligent neural (network في تصنيف أنماط إستطلاعات العملاء الحاسوبيين ولكن تمرر المؤشرات الناتجة إلى أنظمة المنطق الضبابي الخبيرة (Fuzzy Logic Expert System) والتي يمكنها ترجمة المخرجات إلى شكل يدركه المستخدم العادي بسهولة.

خصائص النظم الخبيرة – المزايا والعيوب

–المزايا:

النظام الخبير غير معرض للنسيان بينما الخبير البشري لا يتمتع بهذه الميزة .

يمكن نسخ عدة نسخ من النظام الخبير بسرعة، بينما يشكل تدريب شخص خبير من قبل آخر عملية طويلة ومجهدة. قد يكون بناء نظام خبير بحد ذاته مكلفًا غير أن كلفة التطوير والصيانة له يمكن توزيعها على عدة مستثمرين، وبالتالي تكون الكلفة العامة مقبولة مقارنة مع كلفة الإنسان الخبير. يعامل النظام الخبير المسائل المتشابهة بنفس الطريقة، بينما يمكن للإنسان الخبير أن يتأثر بشكل أكبر بعدة عوامل منها:

–أحدث المعلومات.

–أول المعلومات التي حصل عليها.

–يمكن للنظام الخبير أن يوثق قراراته بشكل دائم .

– إمكانية تجميع خبرة أكثر من شخص في نظام واحد .

–العيوب:

يتميز الشخص الخبير بالإدراك يمكن للإنسان الخبير أن يتجاوب مع حالة غير اعتيادية بينما يتعذر على النظام الخبير القيام بذلك، يتأقلم الشخص الخبير مع تغير الظروف بينما يحتاج النظام الخبير إلى تحديث الظروف. كما أن النظم الخبيرة قاصرة عند المشاكل الخارجة عن نطاق خبرتها .

كنتيجة يمكن القول أنه في بعض الحالات في برنامج – Bugs مثلا توقع الحالة الجوية أو البحث عن أعطال ما – يمكن للنظام الخبير أن يكون أسرع و/أو أدق من الإنسان، ولكن في مجالات أخرى كالطب يكون النظام الخبير مساعدًا فعالا – وليس بديلا –عن الخبير البشري.

الخاتمة:

يتسم الإجرام الالكتروني بالذكاء الخارق مقارنة بالإجرام التقليدي الذي يتسم بالعنف، لهذا يطلق عليه بإجرام الأذكياء، لأنه يعتمد على وسائل تكنولوجية متطورة في تدمير أو اختراق المواقع الحكومية أو قرصنة المعلومات الخاصة بالأفراد والاعتداء على خصوصياتهم . وبالتالي، نستطيع أن نؤكد أن نجاح أمن الملومات يعتمد كثيرا على نجاح نظام الحماية الذي تعتمده الشركات و المنشآت الاقتصادية والذي يجب أن تكون حماية مدنية، جنائية ومعلوماتية على نحو ذا فاعلية. وتتحقق الحماية المعلوماتية عن طريق تطوير الأبحاث العلمية للنظم الأمنية لكي تؤمن بياناتها ومعلوماتها من القرصنة وإساءة استعمالها، واكتشاف حالات القرصنة إن حدث ذلك.

يعتبر الذكاء الاصطناعي أحد المحاور الأساسية في البحوث العلمية المعاصرة، حيث يتمحور الاهتمام الكبير والمتنامي بشكل سريع به حول التوصل إلى نظم ذكية تكون قادرة على التصرف بشكل مشابه – ما أمكن– للتصرف الإنساني.

النتائج و التوصيات

- ✓ ستكون مثل هذه النظم ذات فائدة ملموسة للإنسان نظرًا للتطبيقات الواسعة لها في مجالات الحياة المختلفة على أن التعرف على النصوص المطبوعة أو المكتوبة أحد المواضيع الأساسية في هذا المجال.
- ✓ وتجدر الإشارة إلى أن التطور العلمي والتقني الذي شهدته العقود الأخيرة في مجال النظم الإلكترونية بشكل عام والمعالجات بشكل خاص، إضافة إلى البرمجيات الموافقة يجعل الخطى متسارعة في التوصل التدريجي لنظم ذكية يمكنها محاكاة التصرف الإنساني بشكل مناسب وذلك ضمن مجال محدد.
- ✓ إن محاكاة التصرف الإنساني بشكل مطلق هو مسألة في غاية التعقيد، مما يعتبر شاهدًا— من الشواهد الكثيرة _على عظمة الخالق سبحانه وتعالى في تكوين العقل البشري والقدرات الهائلة التي منحها له.
- ✓ إن تطور العلوم وانتشار تقنيات تكنولوجيا المعلومات لتسهيل حياة الفرد وتكامل بناء الدول ، تفاقم في نفس الوقت التيار المعاكس الذي يحاول وبنفس التقنيات تعكير الأجواء وتبديد الاحلام لأغراض واهداف تم شرحها تفصيلاً والوقوف عليها تخصيصا في وريقات بحثنا المتواضع هذا.

الاحالات و الهوامش:

- د .مكاوي محمد محمود ، **البيئة الرقمية بين سلبيات الواقع وآمال مجلة إلكترونية**، عدد3 ، سبتمبر Cybrarians journalالمستقبل، مجلة 2004، متاحة على الموقع:
http://www.cybrarians.info/journal/no9/info-secuirty.htm
- د .ديريه سعيد، أمن المعلومات، 2004 ، متاح على الموقع: http://www.saidder.jeeran.com/amn.htm
- مجلة البحوث والدراسات العلمية، جامعة الدكتور يحي فارس، **مخاطر القرصنة المعلوماتية على الحكومة الالكترونية**، الأستاذ يحياوي محمد.ص258-260، العدد الخامس-جويلية 2011.
- المستشار الدكتور محمد ياسر أبو الفتوح، **خصائص وتصنيفات الجريمة المعلوماتية**، محكمة استئناف القاهرة، مستشار مركز المعلومات ودعم واتخاذ القرار : http://www.F-law.netبرئاسة مجلس الوزراء،2008
- رصاع فتيحة،**الحماية الجنائية للمعلومات على شبكة الانترنت**، مذكرة لنيل شهادة الماجستير في القانون العام،جامعة ابي بكر بلقايد تلمسان، 2011-2012، ص81
- رصاع فتيحة، **نفس المرجع السابق** ، ص 89.

http://www.n1t1.com/gisec-2014-banking-sector/

- د .الشدي طارق عبد الله، **الآلية البناء الأمني لنظم المعلومات**، دار الوطن للطباعة والنشر، الرياض، المملكة العربية السعودية، 2000، ص182 .

- BARMAN S, Writing Information Security Policies, New Riders Publishing, . Available http://Safari.informit.com November 2001 .

- Kate A. Smith!,*, Jatinder N.D. Gupta" !School of Business Systems, Monash University, Clayton, VIC 3168, Australia "Department of Management, Ball State University, Muncie, IN 47306, USA, **Neural networks in business**: **techniques and applications for the operations researcher**, Computers & Operations Research 27 (2000) 1023}1044.

- George Bojadziev, Simon Fraser University, Canada Maria Bojadziev British Columbia Institute of Technology, Canada **Fuzzy Logic for Business**, **Finance**, **and Management 2nd Edition**, **Advances in Fuzzy Systems – Applications and Theory – Vol**. **23**, World Scientific .