الآليات الداعمة للتنقيب عن المعطيات لإستخراج المعرفة في الأنظمة الأمنية المتكاملة[3]

* الدكتور المهندس نديم شاهين[1] المهندس معين قاسم[2]

الملخص

مع ازدياد المخاطر و التهديدات التي استهدفت الأفراد و الحكومات في السنوات الأخيرة، ازدادت أهمية إيجاد و بناء أنظمة أمن متكاملة قادرة على معالجة المعلومات المختلفة الناتجة عن مصادر المعلومات المتنوعة و معالجة التعارض الناتج عنها و دمجها في إطار متجانس لاتخاذ القرار على الرغم من هجانة هذه المعلومات (التي قد تكون اسمية، رقمية، ثنائية، احتمالية ..الخ) و على الرغم من تنوعها (صور، فيديو، صوت، نص، ... الخ). أمام هذا الكم الهائل من عناصر المعلومات، ازدادت أيضا حاجة الإنسان الذي أضحى غنيا بالمعطيات فقيرا بالمعرفة إلى إيجاد طرق فعالة لتبسيط هذه المعلومات و استخراج المعارف منها. في البحث التالي نقدم نموذجا رياضيا يعتمد بشكل أساسي على نظرية البيّنات Evidence Theory و نظرية الإمكانات Possibility Theory للتنقيب عن المعلومات واستنباط المعارف واتخاذ القرار الأمني الأكثر دقة . أن هذا النموذج سيكون قادرا على الإجابة عن أهم التحديات المطروحة في معالجة المعلومات المتباينة في النظم الأمنية المتكاملة والمعقدة .

الكلمات المفتاحية:

نظام أمني متكامل، نظرية البيّنات، و نظرية الإمكانات، التنقيب في المعطيات، اكتشاف المعارف، نمذجة التشابه إظهار التشابه، دمج المعلومات.

Abstract:

In this article we propose a mathematical model fundamentally based on evidence theory to combine and to process the information elements resulting from the different sources of information within a general integrated security system with the aim to extract the potential knowledge associated with the security events. Furthermore, we intend to simply materialize and visualize this knowledge by using different representational models. The proposed model is able to process the information and to extract the knowledge in spite of the heterogeneity of the information elements that could be qualitative, quantitative, ordinal, binary, .. etc, and in spite of their imperfection and uncertainty (imprecise, probabilistic, evidential, possibility, missing data.. etc.)

Key Words:

Integrated Security System, Evidence Theory, and Possibility Theory, Information Fusion, Data Mining, Knowledge discovery and Extraction, Similarity Modeling, Similarity Visualization.

١- الدكتور المهندس نديم شاهين : استاذ في كلية الهندسة الميكانيكية والكهربائية جامعة دمشق

٢- المهندس معين قاسم : طالب دكتوراة في قسم الهندسة الالكترونية والاتصالات بجامعة دمشق

٣- بحث مقدم ضمن اطار استنباط المعرفة في الانظمة الأمنية المتكاملة

١- مقدمة:

مع ازدياد التهديدات و المخاطر الإرهابية التي أخذت تهدد الأفراد و الحكومات، ازدادت الحاجة إلى بناء أنظمة متكاملة قادرة على اتخاذ القرارات المناسبة في الوقت المناسب و ذلك قبل حدوث الكارثة. و مع تقدم التكنولوجيا، ازدادت الحاجة للاستفادة منها في بناء هكذا أنظمة. فالتكنولوجيا متاحة في هذه الأيام لتزويدنا بكل مصادر المعلومات التي يمكن أن يتخيلها المرء (الحساسات، آلات التصوير، الليزر، ...الخ) و بكل الوسائط لتخزين هذه المعلومات (أقراص صلبة، ذواكر، ...الخ) و بشتى الوسائل لتبادل و نقل هذه المعلومات (ألياف بصرية، أنظمة الاتصالات الليزرية، ..الخ). لكن أمام هذا التطور الهائل، وقف الإنسان الذي أضحى غنيا بالمعطيات لكن فقيرا بالمعرفة حائرا مربكا أمام معالجة هذا الكم الهائل و إظهاره بشكل مناسب ومتماسك يغنينا بالمعارف. لذلك أطل علينا علم التنقيب عن المعطيات و كشف المعارف Data Mining and Knowledge Discovery بتقاناته المتعددة و خوارزمياته المتنوعة لكشف سبر هذه المعطيات و تمحيصها و استخراج القواعد المفيدة منها و تجسيد اللامنظور منها لتقريب فهمه لمالك هذه البيانات Data Owner ، مما دفعنا في هذا البحث لطرح و اقتراح تطبيق أهم النظريات الحديثة (نظرية البيّنات Evidence Theoryو نظرية الإمكانات Possibility Theory) عند التنقيب في المعطيات بقصد استخراج المعرفة في أنظمة الأمن المتكاملة. إن الطرق و الخوارزميات التي نقدمها ستطبق لأول مرة في هذا المجال و سنبين أهميتها في معالجة الأنواع المختلفة من البيانات الناتجة عن الحساسات و التي قد تكون اسمية Qualitative ، رقمية Quantitative ، احتمالية Probabilistic ، غير دقيقة Imprecise ، أو مفقودة Missing Data ..الخ .

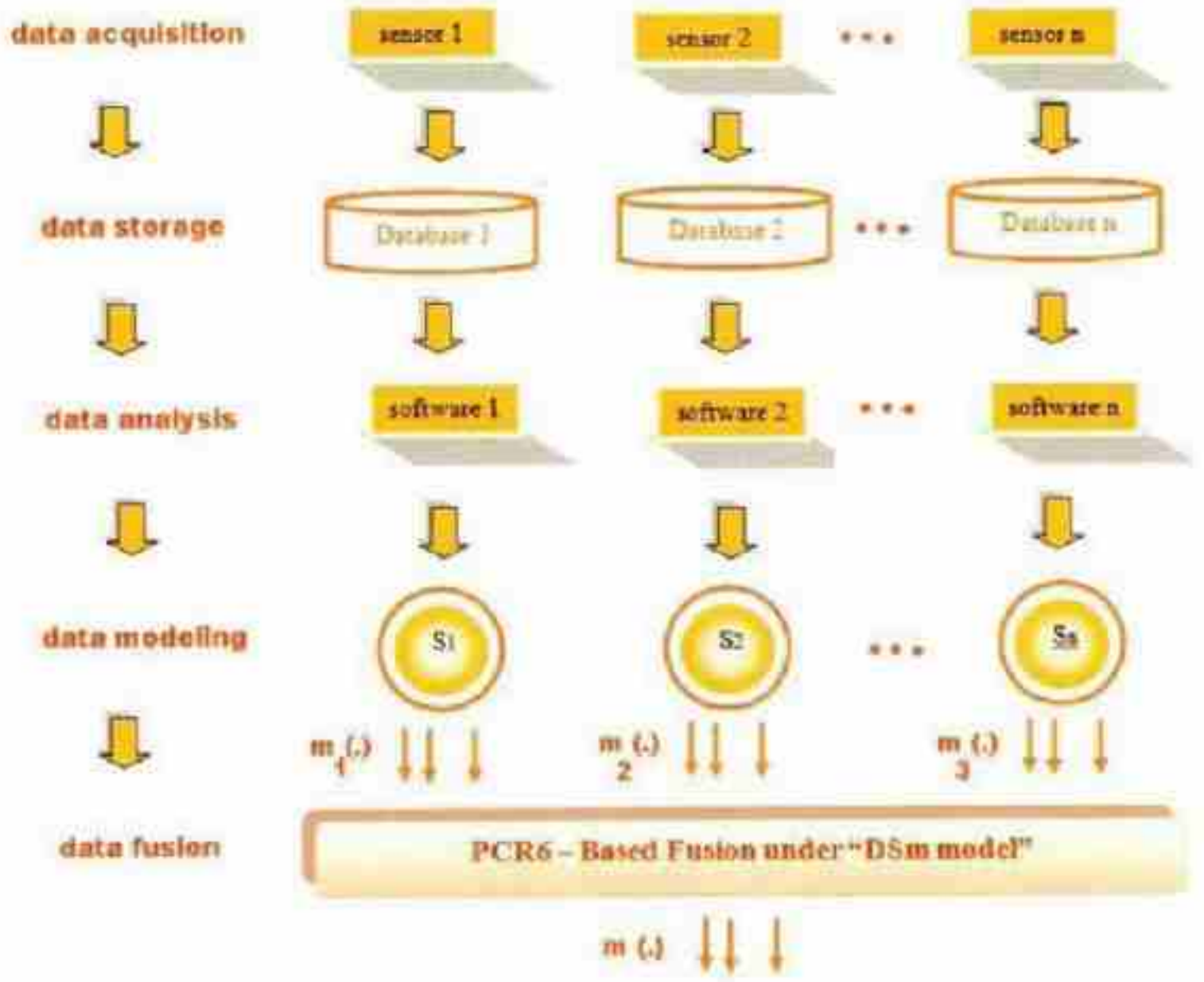
٢- تصميم النظام الأمني المتكامل:

يتألف النظام الأمني المتكامل المصمم من قبلنا كما هو مبين في الشكل ١ من:

١- وحدات التقاط المعطيات Data : المؤلف من مصادر المعلومات المختلفة (حساسات، عناصر الأمن، ...الخ) و التي تزودنا بالمعطيات المختلفة و التي تكون هجينة من جهة نوعها (صور، فيديو، صوت بارامترات، ... الخ) أو من جهة قياسها (قيم اسمية، رقمية، ثنائية، احتمالية ...الخ).

٢- نظام نقل المعلومات: و هو عبارة عن نظام الاتصالات الموثوق الذي سيتم من خلاله نقل المعلومات مع الحفاظ قدر الإمكان على جودتها و نقاوتها و أمنها.

٣- نظام تخزين و تحليل المعطيات: يتم تخزين المعطيات الملتقطة على وسائط تخزين مناسبة فمثلا يتم تخزين المعطيات الملتقطة في كاميرات الـ CCTV على مسجلات الفيديو الرقمية DVRs (Digital Video Recorders) بنما يتم تخزين معطيات الكاميرا IP Cam على مسجلات الفيديو الشبكية NVRs (Network Video Recorders



شكل (١) تصميم الهيكلية الأساسية للنظام الأمني المتكامل

٤- استنباط المعرفة :

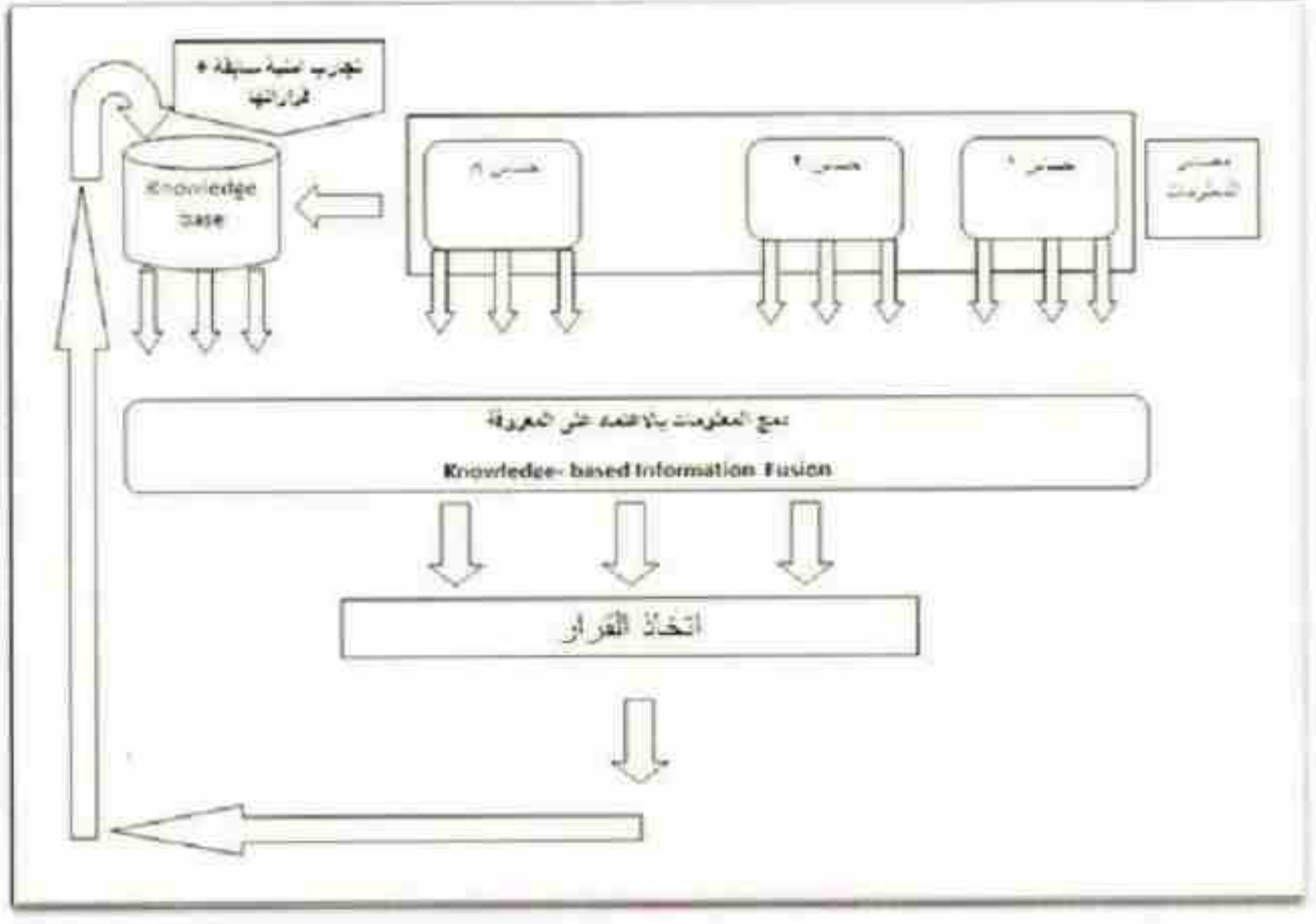
بعد أن يتم التقاط المعطيات بواسطة الحساسات المختلفة والمتنوعة في النظام الأمني المتكامل " Data Acquisition" ونقلها بواسطة نظام اتصالي موثوق وآمن وسريع "Data Transmission" ومن ثم تخزينها على وسائط مناسبة "Data Storage" وتحليلها بواسطة البرمجيات المتنوعة المتواجدة في هذه الوسائط " Data Analysis" يتم دمذجتها وتمثيلها بواسطة موديل رياضي مناسب متكامل يؤمن معالجة المعلومات الهجينة (اسمية ، رقمية ، ترتيبية ، ...الخ) بأنواعها المختلفة (معلومات احتمالية ، غير دقيقة ، مفقودة ، ..الخ) ودمجها في إطار واحد وحيد متكامل قادر على الأخذ بزمام الأمور عند إجراء المهام الأمنية المختلفة (التعرف على الأوجه، تصنيف العناصر، كشف الاختلال ..الخ)

لقد وجدنا بأن الموديل الرياضي المؤسس على نظرية البيّنات "Evidence Theory" ، وفقا لما يطلق عليه نظرية توابع التصديق "Belief Theory" و المبنية على إعادة توزيع التعارض بشكل متناسب وفق طريقة آرنو مارتا [1] المطبقة في ظل الموديل الرياضي المقترح من ديزيرت وسمارندش [2] ، هو القالب الرياضي الصحيح الذي يستجيب إلى متطلبات نظامنا والمقتضيات الأمنية الواجب اتخاذها في النظام الأمني المدروس . كذلك فأن الأدوات الرياضية الفعّالة كتابع المصداقية "Credibility function" وتابع المعقولية "Plausibility Function" واحتمال المراهنة "Pegnistic Probolility" وغيرها في هذا الموديل الرياضي

تساعدنا على اتخاذ القرار ، اما درجة الارتياب (uncertainty degree) والمتمثلة بالفرق بين المصداقية والمعقولة بإضافة إلى محتوى المعلومات الاحتمالي (Probabilistic Information Content) وغيرها تمكننا من تحليل النظام وفهمه [3] [4] لمعرفة مصادر المعلومات التي تؤدي إلى التعارض مع المصادر الأخرى وبالتالي الواجب إصلاحها أو إخراجها من النظام وتمييزها عن تلك التي تغني النظام بعناصر المعلومات المفيدة .

مجموعة الأطوار السابقة (التقاط + تخزين + تحليل + دمج + مراجعة المعلومات) لكل حادثة "event" تشكل ما يسمى بالتجربة الأمنية أو بما يسمى حالة أمنية "case " .

لتحسين أداء النظام من جهة والحس الإدراكي والفهمي لمديري النظام والمسؤولين الأمنيين من جهة أخرى لابد من الاستفادة القصوى من الحالات الأمنية لحوادث مسبقة والتي تمت معالجتها واتخاذ الحلول الملائمة لها في اتخاذ القرار لحادثة مشابهة في اللحظة الراهنة on- line وهذا ما يسمى بالـ case- based Reasoning . بكلمات أخرى ، بناء قاعدة معرفة "Knowledge Base" مؤلفة من الحالات الأمنية المدروسة السابقة واستثمارها جنباً إلى جنب مع الحساسات ومصادر المعلومات الأخرى كمصدر معلومات مباشر يساعد على اتخاذ الحلول والقرارات المناسبة لحالة امنية في موقع محدد [5] ، بعدها يتم تحديث قاعدة المعرفة هذه على ضوء القرار المتخذ للتجربة قيد التحليل كما في الشكل (٢) :



الشكل (٢) آلية دمج المعلومات بالاعتماد على المعرفة المسبقة لاستنباط معرفة جديدة واتخاذ القرار

٣- تطبيق نموذجي لبناء قواعد معطيات للنظام الأمني المتكامل المصمم :

إذا فرضنا أن مجموعة المحتوى المعلوماتي (مجموعة القرارات التي نريد اتخاذها في تجربة أمنية معينة) تتألف من مجموعة من الوحدات الفرعية في النظام الأمني (كوحدة الشرطة ، وحدة الأطباء ، وحدة الصيانة ...الخ) ، فيمكن أن تكون المعرفة المستخرجة والمخزنة في قاعدة المعرفة على الشكل التالي :

[" إذا تم كشف حريق ، دخان ، او ماشابه ، فأن رد الفعل الطبيعي او الحل يكون بطلب وحدة الإسعاف مع وحدة الشرطة مع وحدة الأطباء "]

لبناء هكذا نوع من القواعد أو لدراسة النظام وتحليله بشكل بياني أو فراغي أو غيره لابد من تطبيق التقانات و الخوارزميات المتنوعة في مجال التنقيب عن المعطيات (Data Mining) من أجل استكشاف واستنباط المعارف من الحوادث الأمنية السابقة (Knowledge Discovery) بما يمكننا من زيادة الخبرة لدى المسؤولين الأمنيين و تدريب المسؤولين الحديثي العهد في العمل وبالتالي زيادة وثوقية النظام الآلي لاتخاذ القرارات.

وفيما يلي نقدم طريقة عامة و مبسطة للمساعدة على بناء هذة القواعد المساهمة في استنباط المعارف للنظام الأمني التطبيقي .

٣-١- حساب استنباط المعرفة للنظام :

لاستخراج المعارف أو لتمثيلها بواسطة واجهات بسيطة للمستخدمين(Friendly User Interfaces) اعتباراً من قاعدة بيانات تحتوي على حالات و تجارب أمنية مسبقة مع حلولها (القرارات المتخذة) نتبع التالي:

١- حساب التشابه بين كل حالة أمنية و حالة أخرى (Similarity Measuring)

٢- تجزئة القاعدة إلى مجموعات من العناصر المتشابهة باستخدام طرق التجزئة (Segmentation) أو العنقدة (Clustering) .

٣- تجسيد وإظهار الترابط و التشابه بين الحالات باستخدام الرسم (Graphic) أو الطريقة الفراغية (Spatial) أو الهندسية (Geometric) أو غيرها .

٤- دراسة الصفات المشتركة لتوصيفات الحالات التي تنتمي إلى نفس المجموعة والتي تمايزها عن صفات حالات المجموعات الأخرى . هذا يسمى في علم التنقيب عن المعطيات "باستخراج القواعد" (Rule Extraction) [6] (استخدم في الأبحاث التجارية لدراسة فواتير المستهلكين في السوبر ماركت لمعرفة السلع التي تشترى في نفس الوقت لوضعها على رفوف متقاربة و الإيحاء للمستهلك بشرائها ، كما طبق في الطب لدراسة العناصر المفتاحية التي تميز مرضى مرض معين عن غيرهم باستخراج قواعد غير معروفة مسبقاً للأطباء)

٣-١-١- حساب التشابه بين المصادر الأمنية (Similarity Measuring) :

لحساب التشابه بين حالات أمنية وأخرى يجب أولاً دراسة التشابه بين كل توصيف من الحالة الأولى مع التوصيف المقابل في الحالة الأخرى وحساب التشابه الموضعي Local Similarity وبعدها يجب حساب التشابه الكلي Global Similarity بين الحالات بتجميع وأخذ متوسط جميع قيم التشابهات الموضعية المحسوبة بين توصيفات الحالات .

فمثلاً فإذا كانت الحالة موصوفة بأربع توصيفات Attributes or characteristics مثل x4,x3,x2,x1 والتي يسمى كلاً منها عنصر معلومات .

اولا : يتم حساب التشابه بين قيمة x1 في الحالة الأولى وقيمتها في الحالة الثانية ويسمى هذا بالتشابه الموضعي (Local Similarity)

ثانيا : تعاد الخطوة السابقة لـــ x4,x3,x2 ويتم من بعدها حساب التشابهية الكلية بين الحالتين (Inter-Cases) بأخذ متوسط التشابهات الموضعية الأربعة السابقة.

ثالثا : توصيفات القيم الناتجة وفقا للمفهوم التالي :

١) قيم اسمية "qualitative" مثل (high) .
   أو رقمية "quamitative" مثل ("200")
   أو ثنائية "Rinary" مثل (Yes or No)
٢) قيم معطاة أو مفقودة بسبب خروج الحساس عن العمل "missing data" والتي تسمى في إطار نظرية البيّنات بحالة الجهل المطلق (total ignorance)
٣) قيم دقيقة ("200") أو غير دقيقة "imprecise" (مثل بين 150 و 250 أو حوالي الـــ 200)
٤) مصرح بها مثل "200" أو معطاة بواسطة تابع توزيع احتمالي أو بيني أو امكاني أو باستخدام توابع العضوية Membership Functions المستخدمة في تطبيقات المجموعات العائمة Fuzzy Sets Theory .

رابعا : يتم إيجاد مقياس متكامل للتشابه قادرا على معالجة جميع الحالات السابقة للمعلومات في إطار واحد متجانس (within an integrated framework) .

من أجل ذلك قمنا باستخدام نمذجة التشابهية المعتمدة حديثا (٢٠١٠) في [8-7] والتي تعتمد على نظرية الإمكانات "Possibility Theory " لحل جميع الحالات السابقة في أطار متكامل ، ولاسيما أن هذه النظرية هي اقتباس مباشر لنظرية البيّنات Evidence Theory .

في هذا الموديل الرياضي التطبيقي يُنمذج التشابه بواسطة قياسين نمطين عائمين (two monotone fuzzy measures) هما درجة الإمكانية "Possibility" والمرمزة بـــ "Π" ودرجة الضرورة "Necessity" والمرمزة "N" وهما شبيهان بمقياسي المعقولية والمصداقية ،ولا سيما أنه في كلا الحالتين يقع احتمال حدوث أي حدث بين هذه القيم وفقا للتالي :

* في حالة نظرية البيّنات "Evidence Theory" :

$$Bel(A) \leq Pr(A) \leq pl(A)$$

حيث ان :

Bel(A) : stands for belief.

Pr (A) : stands for Probability

pl(A) : stands for Plausibility

* وفي حالة نظرية الإمكانات "Possibility Theory"

$$\Pi(A) \leq Pr(A) \leq N(A)$$

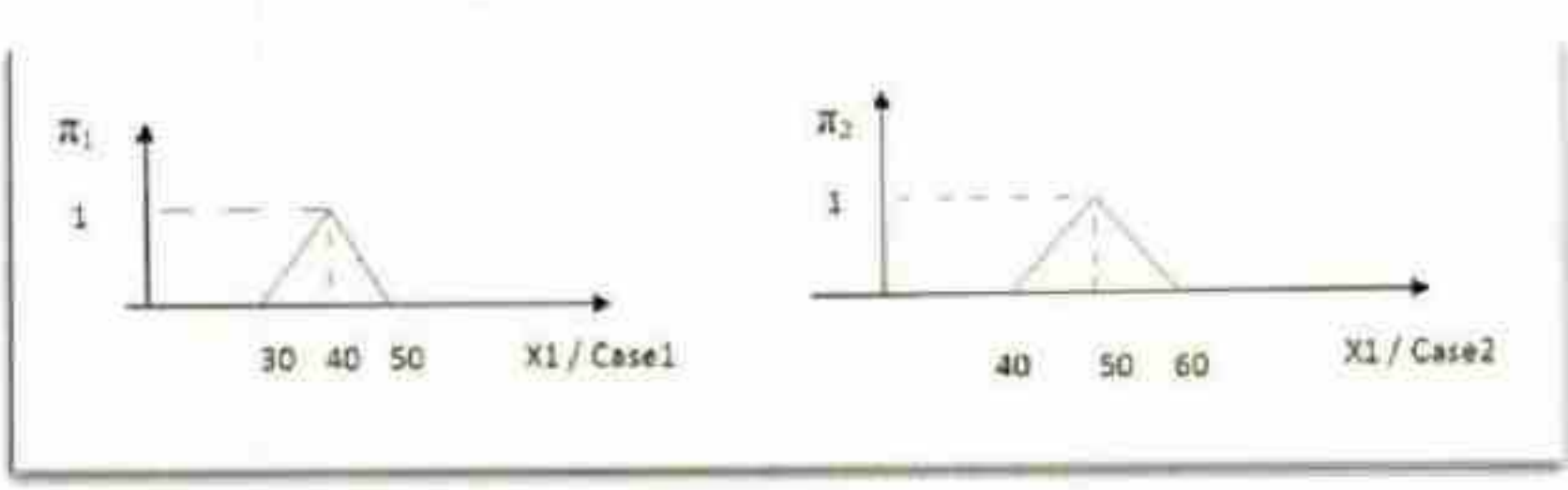
Π (A): stands for Possibility

N(A): stands for Necessity

Pr (A): stands for Probability

في مثالنا للحالات المذكورة كل منها مكون من أربع توصيفات نبدأ بـــ x1. فبفرض أن قيمته في الحالة الأولى ممذجة بواسطة تابع توزع إمكاني " π_1 " Possibility distribution. وقيمته في الحالة الثانية ممذجة بواسطة تابع إمكاني " π_2 "

(مثلاً قيمة x1 في الحالة الأولى قريبة من الرقم 40 وفي الحالة الثانية حوالي خمسين ، يمكن نمذجة القيمتين close to 40 و close to 50 باستخدام مثلثات عائمة كما هو موضح في الشكل ٣) .

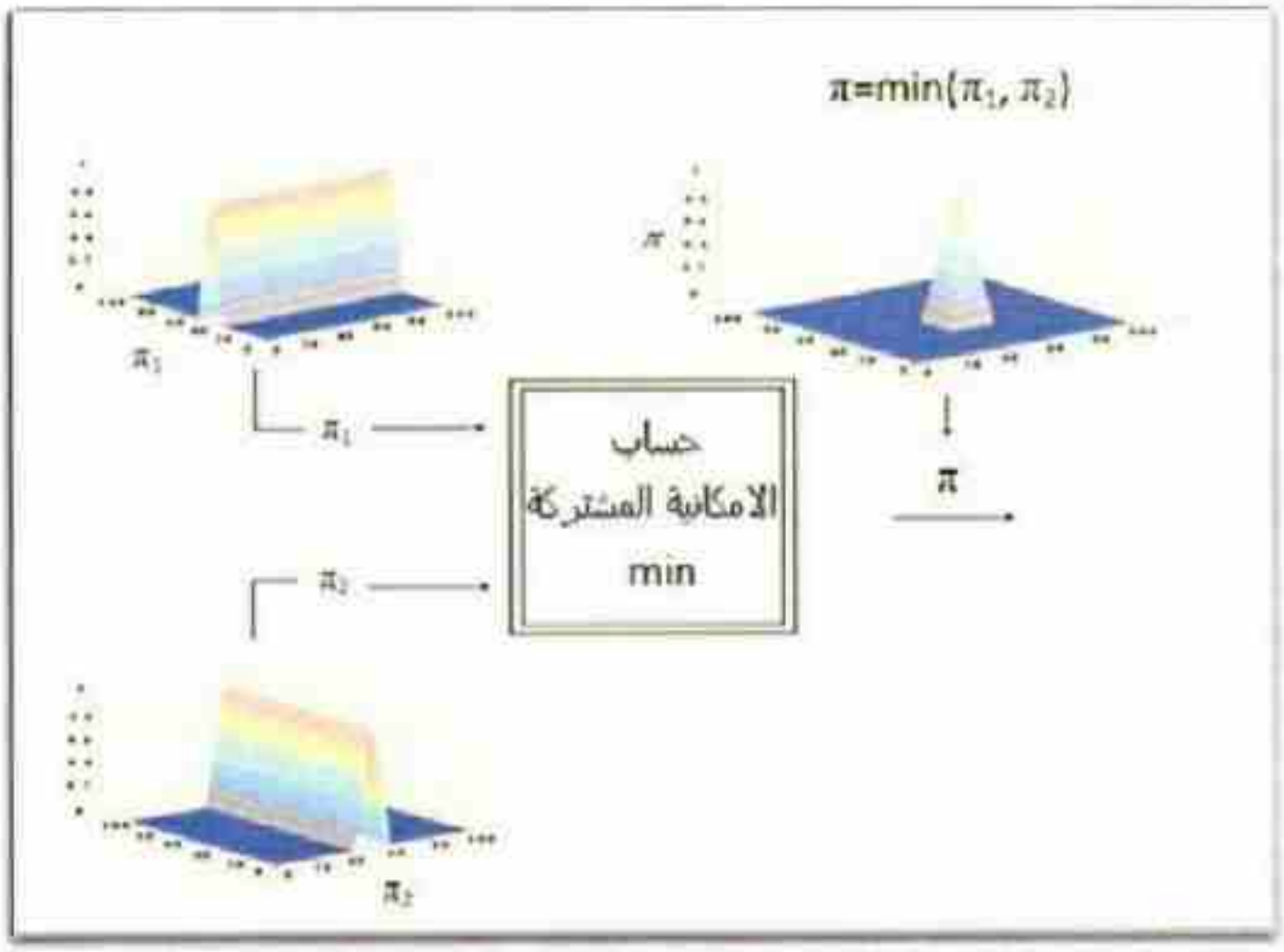


شكل (٣) نمذجة قيم x1 في كل من الحالتين الافتراضيتين (مثال عددي)

الأن لحساب التشابهية الموضعية Local Similarity باعتبار أن القيمتين لا تعد متشابهتين اذا تجاوز اختلافهما درجة التسامحية المفروضه من قبلنا ولتكن $\Delta = 10$ (Tolerance Degree)

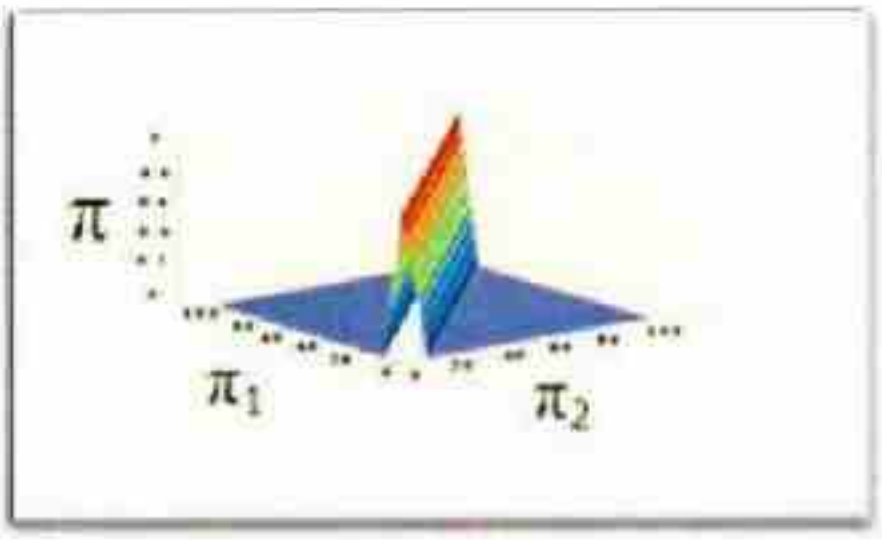
يتم الحساب وفقاً للطرقة المقترح في [8-7] وفقا للتالي :

أ ــ حساب وتمثيل الإمكانية المشتركة $\pi=\min(\pi_1, \pi_2)$ (شكل ٤) كما يلي :



شكل ٤ حساب الإمكانية المشتركة باستخدام ال min

ب ــ إيجاد تابع التسامح Tolerance Function أخذ قيمة Δ بعين الاعتبار سنعتبر في هذا المثال أنه يمكن نمذجته بمثلث عائم (نرمزه ب μ) (شكل ٥ــ ٤) كما هو الحال في قيمتي x1 في كلا الحالتين:



(شكل ٥) تابع التسامح Tolerance Function

جـ ـ حساب إمكانية التشابه (Π وَ N)

Possibility of resemblance وَ Necessity of resemblance

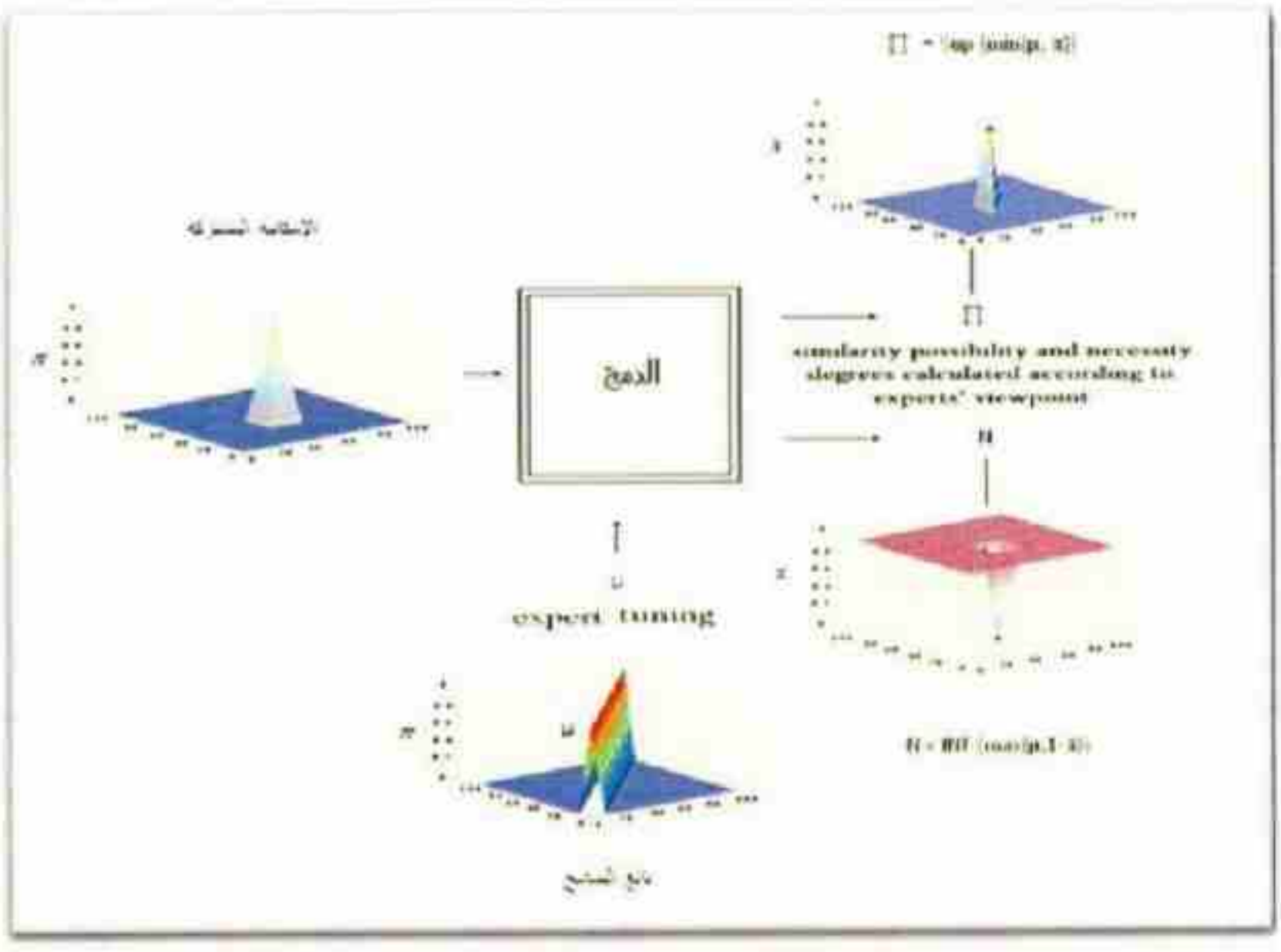
باستخدام قوانين نظرية الإمكانات كما يلي :

$$\Pi = \text{Sup}\ \{\min(\mu, \pi)\}$$

$$N = \text{INF}\ \{\max(\mu, 1-\pi)\}$$

الأشكال المبينة في (٦) :

نجد أن Π=1 وَ N=0.30 .



الشكل ٦ حساب درجات إمكانية و التشابه بين القيمتين

بشكل مماثل يتم حساب التشابه لـ x2 وَ x3 و x4 ويتم إيجاد التشابه الكلي بين الحالتين بأخذ المتوسط للتشابهات المحلية لهذه التوصيفات .

٣-١-٢-التجزئة والعنقدة segmentation & clustering

بالاعتماد على التشابهية المحسوبة في الفقرة السابقة يمكن تقسيم الحالات الأمنية المدروسة إلى مجموعات متجانسة ، وكل منها يمثل صنف معين بحيث تكون العناصر المنتمية إلى نفس الصنف class متشابهة فيما بينها أكثر من العناصر المنتمية للأصناف الأخرى.

في الوقع يوجد أنواع عديدة من الخوارزميات والتقانات المستخدمة لهذا الغرض كالعنقدة الهرمية Hierarchical Clustering والعنقدة المسماة بـــ k-mean ونسخته العقدية c-mean وغيرها مما شاع استخدامه بشكل كبير والذي تم تطويره بشكل كامل ، لهذا السبب لن نغص هنا في تفاصيل أو تطوير هذه التقانات ، وإنما نريد فقط أن نقترح استخدام العنقدة البينية الإمكانية Possibilistic Evidential clustering التي تم اقتراحها من قبل العالم الفرنسي تيري دنو في [9] وتوسيعها لتشمل المصفوفات المعتمدة على نظرية الإمكانات في [7] وسنعتمد هذه النظرية في أنظمة الأمن المتكامل للحفاظ على الإطار المتجانس المصمم من قبلنا والمعتمد بشكل أساسي وواسع على نظرية البيّنات Evidence Theory مما يحفظ لنا حجم في وسائط التخزين ويضمن سرعة في الأداء وسهولة في إدارة البرمجيات وإصلاح أخطائها أو تحديثها كونها تعتمد جميعها على نفس الموديل الرياضي .

٣-١-٣- اظهار التشابهية Similarity Visualization

لفهم العلاقة والترابط بين الحالات والتجارب الأمنية السابقة لا بد من إظهار وتجسيد قيم التشابه المحسوبة في الفقره ٣-١-١- خلال إيجاد النموذج الأمثل للتمثيل (The Best Representational Model) وهذا يختص به فرع كامل منبثق عن علم التنقيب عن المعطيات (Data Mining) والمسمى بتحليل المعطيات الاستكشافي (Exploratory Data Analysis) .

لقد تم تجميع و تقسيم وسائل إظهار التشابه في [8] إلى ٣ أقسام رئيسية هي :

١ـ إظهار فراغي وهندسي Geometric & Models Spatial : وذلك إما بإظهار الحالات والتجارب الأمنية (cases or objects) كنقاط على مستقيم بحيث تعبر المسافة فيما بينها عن التشابه وتسمى بالتقييس وحيد البعد الخطي (Linear Unidimensional Scaling LVS) أو كنقاط على دائرة ثنائي الأبعاد بحيث تتجمع الحالات المتشابهة في أماكن محددة من الدائرة ويسمى ذلك بالتقييس الدائري (Circular Scaling) أو كنقاط في فراغ من بعدين أو أكثر باستخدام التقييس متعدد الأبعاد (Multidimensional Scaling MDS) بحيث يتم تجزيء الفراغ الإقليدي إلى مجموعات متجانسة من الحالات .

٢ـ إظهار رسمي أو بياني Graphical Models : فيه يتم تمثيل الحالات باستخدام طرق شجرية مثلاً كالشجرة الجمعية (Additive Trees) أو الشجرة الأولترامترية (Ultrametric Trees)

وفي هذه الأنماط من التمثيل تتعلق جميع الحالات المتشابهة بنفس الغصن بحيث يكون الطول الواصل بين الحالة الناشئة و أقرب عقدة ناشئة عن الغصن ممثلاً للمسافة بين الحالتين والتي تتناسب عكساً مع التشابه .

٣ـ إظهار تركيبي Structural Models : وهي الطرق المعتمدة على بعض تقانات العنقدة لإظهار المعلومات ونستخدم هنا العنقدة الجمعية (Additive Clustering) لإظهار انتماء الحالات على شكل

مجموعات sets وأوزان ربط مشابهة لأوزان الشبكات العصبونية Neural Networks أو باستخدام العنقدة الهرمية (Hierarchical Clustering) لإظهار الحالات باستخدام الأشجار الأولتراسترية .

أو العنقدة باستخدام شبكات كوهنن ذاتية التنظيم (Self – Organizing Kohonen Maps) لإظهار الحالات باستخدام كرت وخلايا وغيرها من الطرق المفيدة حسب الاستخدام المطلوب

٣-١-٤-استنباط القواعد Rules Extraction :

تعتبر هذه الخطوة من أهم الخطوات إذ فيها تدرس العلاقة بين الحالات المختلفة والعلاقة بين توصيفات كل حالة وذلك بهدف استنتاج قواعد هامة غير معروفة للمستخدم (Valuable Potential Rules) لمعرفة الروابط الخفية التي تقف خلف الكواليس في قاعدة البيانات المدروسة بهدف خلق وبناء قاعدة جديدة من القواعد والإظهارات المفيدة والتي تسمى بقاعد المعارف "Knowledge Base" .

تم إيجاد تقانات وخوارزميات شتى في هذا المجال بدءاً من تحليل السلة Basket Analysis وحتى التحاليل المعقدة التي تعتمد على المنطق العام والشبكات العصبونية .

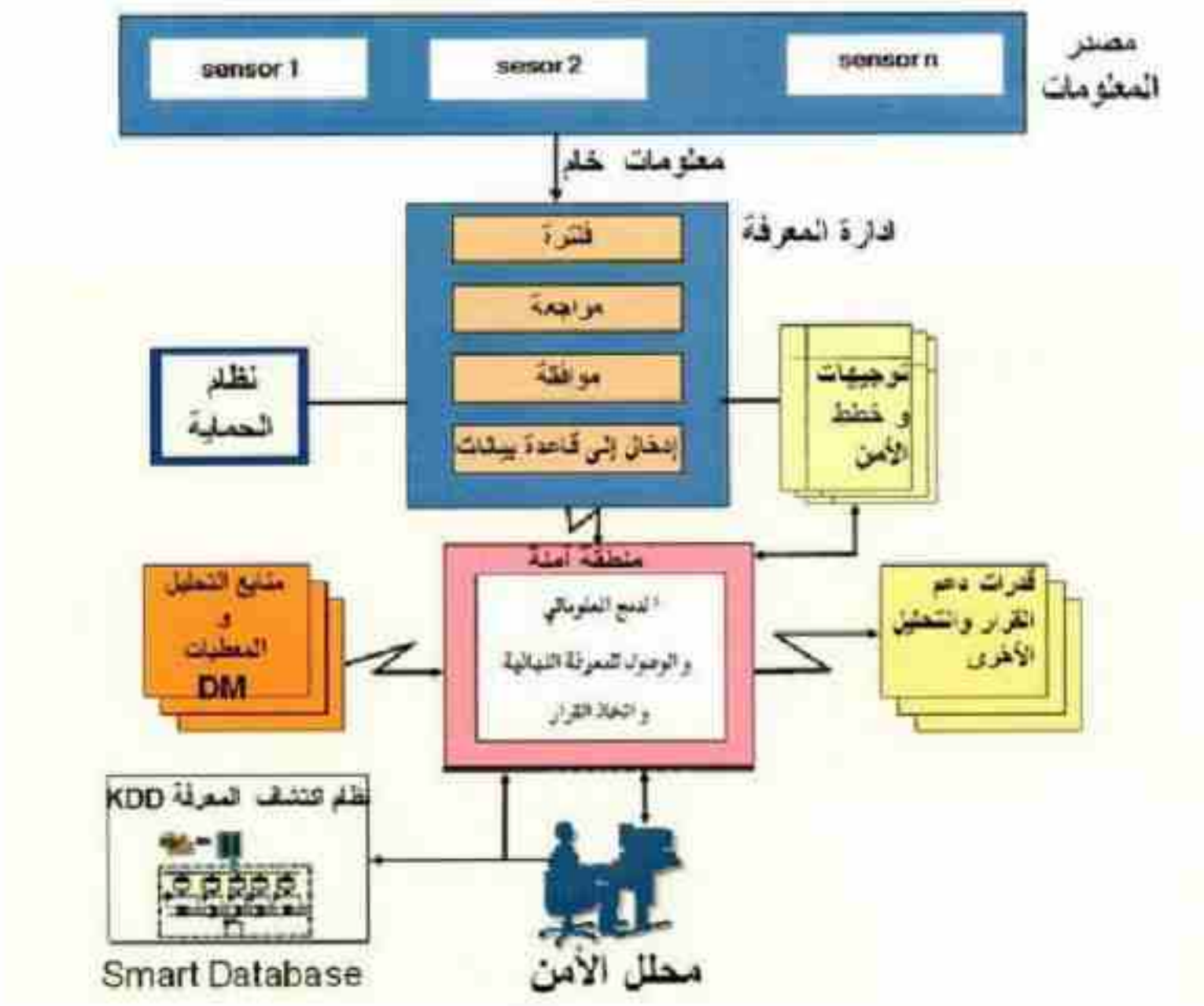
الشيء المهم في جميع هذه الخطوات هو الانطلاق من مصفوفة تشابه صحيحة ناظمة لجميع الحالات المدروسة.

٣-٢- اتخاذ القرار

بعد تطبيق كافة المعالجات المعلوماتية المشروحة في هذا البحث بدءا من المعطيات الخام بكافة أشكالها و هجائنها و تعقيدات وجودها نحصل على قاعدة المعرفة Knowledge Base و التي تحتوي على القواعد اللازمة لاتخاذ القرار حيث أن المعرفة بالتعريف هي المعلومة التي يمكن فهمها و اتخاذ رد الفعل المناسب بالاعتماد عليها مفردة أو بالشراك مع المعلومات الأخرى المستنبطة.

هنا يبدأ تدخل صاحب القرار (المسؤول الأمني) ليشرك خبرته و خلفيته المعرفية و ذكائه و المعرفة المستخلصة في قاعدة المعرفة بهدف ايجاد الحل الأمثل للمشكلة المدروسة أو المطروحة باقل مايمكن من اخطاء او باكبر ميمكن من احتمالية النجاح .

الشكل ٧ يلخص السيناريو الاجمالي للعملية ككل بشكلها العام لآلية اتخاذ القرار في النظام الأمني المتكامل



الشكل ٧. السيناريو الاجمالي لمعالجة المعلومات بهدف استنباط المعرفة و اتخاذ القرار

٤- مناقشة واستنتاجات :

في هذا البحث تم استعراض أهم التقانات والخوارزميات الواجب تطبيقها في نظام أمني متكامل وذلك بهدف استنباط المعرفة لاتخاذ القرار السليم المبني على المعرفة والخبرة.

نركز في جميع هذه الطرق على نظرية البيّنات التي اقترحناها سابقاً لمعالجة معلومات النظام ودمجها واتخاذ القرار المناسب وتقييم العمل ، لكي تضمن العمل في بيئة متكاملة تكفل لنا اقتصادية التخزين و سرعة زمن التطبيق ومرونة عالية في تعقب أخطاء البرمجيات وتحديثها وفهمها

بما أن المعرفة غالباً تتمثل في القواعد Rules والإظهارات Displays فقد تم تبيان طرق بناءة في إيجاد القواعد الخفية المفيدة وإظهار الترابط بين المعلومات من خلال نماذج الإظهار التي اقترحناها.

ان هذا يعد اساسا يسهم في بناء قاعدة معارف بالاعتماد على الحالات والتجارب الأمنية المرجعية التي حدثت سابقا .

تشكل هذة القاعدة فيما بعد مصدراً جديداً للمعلومات يمكن دمجه مع المعلومات المزودة من الحساسات بشكل مباشر on line يساهم في تقديم المعرفة لإتخاذ القرار الأمني بأفضل احتمال لسلامة هذا القرار .

وستشكل المعلومات الجديدة مع القرارات المتخذة ونتائجها مصدرا مرجعيا يستفاد منه في تحديث قاعدة المعرفة المعتمدة سابقا وهذا يسمى بالمحاكمة بالاعتماد على الحالة Case – Based Reasoning .

References:

[1] Martin A., Osswald C., *Une Nouvelle Règle de Combinaison Répartissant le Conflit - Applications en Imagerie Sonar et Classification de cibles Radar.* Revue Traitement de Signal. 24 (2), (2007), 71-82.

[2] Smarandache F., Dezert J., *Advances and Applications of DSmT for Information Fusion*, American Research Press Rehoboth, 1, (2004), Chapters 1-6.

[3] Sudano, J., The system probability information content (PIC) relationship to contributing components, combining independent multi-source beliefs, hybrid and pedigree pignistic probabilities, Proc. of Fusion 2002, Vol.2, pp. 1277-1283, Annapolis, MD, USA, July 2002.

[4] Dezert, J., Threat assessment of a possible Vehicle-Born Improvised Explosive Device using DSmT. 26 pages. Fusion'10 Conference, (2010).

[5] Liu, W.Z., White, A.P., Thompson S.G., Techniques for Dealing with Missing Values in Classification, LNCS Springer, 1280, (1997), 527- 536.

[6] Fayyad, U., Piatetsky-Shapiro, G., Smyth, P., From data mining to knowledge discovery in databases, AI magazine, 17(3), (1996), 37–54.

[7] Multi-Sensor Data Fusion with Mathlab.

[8] DAHABIAH A., PUENTES John, SOLAIMAN Basel, Fusion of Possibilistic Sources of Evidences for Pattern Recognition, International Journal of Integrated Computer-Aided Engineering, IOS Press, April 2010, vol. 17, n° 2, pp. 117-130, ISSN: 1069-2509.

[9] Denoeux T., Masson M.H., *EVCLUS: Evidential Clustering of Proximity Data*, IEEE Transactions on Systems, Man and Cybernetics, 34 (1) (2004), 95-109.