1. **عنوان البحث باللغة العربية:**

التقنيات والأساليب الفنية للإدارة والتحكم بقواعد البيانات ومنع الاختراق.

1. **عنوان البحث باللغة الأنكليزية:**

Techniques for managing and controlling access to databases and preventing breaches.

1. **المشكلة العلمية ومبررات مشروع البحث:**

**1.3. المشكلة العلمية في مشروع البحث:**

تعتمد جميع المؤسسات أنظمة قواعد البيانات لتخزين وحماية المعلومات الحساسة حيث سهل الاستخدام الواسع للإنترنت إمكانية الوصول إلى البيانات من أي مكان في العالم. إن سهولة الوصول هذه مفيدة للغاية للمستخدمين المصرح لهم، لكنها جعلت قاعدة البيانات هدفًا ضعيفًا للمتسللين. يؤدي الوصول غير المصرح به إلى البيانات الحساسة إلى فقدان ثقة العميل في المؤسسة. لذلك، أصبح أمن البيانات من أكثر المجالات أهمية والتي تخضع للتدقيق المستمر من قبل الباحثين. وقد ثبت أن التدابير السائدة لأمان الشبكة ونظام التشغيل غير كافية لحماية قاعدة البيانات، حيث تمكنت العديد من عمليات الاقتحام تجاوز تدابير الأمان هذه والوصول إلى بيانات قاعدة المعطيات. إذن تكمن المشكلة العلمية في الضعف الأمني الذي تعاني منه البيانات المخزنة في قاعدة بيانات غير محمية على مستوى قاعدة البيانات لعدم كفاية الحماية على مستوى الشبكة ونظام التشغيل.

**2.3. مبررات مشروع البحث:**

تتعرض أنظمة قواعد البيانات لهجمات أمنية من قبل مهاجمين خارجيين أو داخليين في مؤسسة أو شركة. المهاجمون من الداخل هم أشخاص داخل المنظمة مرخص لهم بالوصول إلى البيانات من قِبل المنظمة، ولكن يتصرفون بنوايا خبيثة. المهاجمون الخارجيون هم أشخاص خارج المنظمة حصلوا على وصول غير مصرح به إلى قاعدة البيانات من خلال استغلال الثغرات الأمنية. تركز تقنيات أمان قاعدة البيانات التقليدية – كالتحكم بالوصول access control- بشكل أساسي على منع الهجمات من الخارج؛ وقد ثبت أن هذه التقنيات التقليدية بالكاد تساعد في تحديد التهديدات الداخلية ومواجهتها. لذلك، كان لا بد من التوجه نحو حلول أكثر دقة وفعالية في التعرف على الهجمات الناشئة من الداخل ومواجهتها.

تعتمد الحلول الأكثر نجاعة في مواجهة التهديدات الداخلية على أنظمة كشف التسلل Intrusion Detection Systems (IDS). يوجد عدة وجهات نظر وتقنيات لتنفيذ أنظمة كشف التسلل نذكر منها:

1. أنظمة كشف التسلل القائمة على التحليل الزمني temporal analysis
2. أنظمة كشف التسلل القائمة على تحليل العلاقات والتبعيات بين أوامر المستخدم Dependency and relation analysis
3. أنظمة كشف التسلل القائمة على تحليل محاذاة السلاسل Sequence Alignment
4. أنظمة كشف التسلل القائمة على دمج تحليل التبعية وتحليل محاذاة السلاسل Integrating Dependency with Sequence Alignment
5. أنظمة كشف التسلل القائمة على التحليل الإحصائي Statistical analysis
6. أنظمة كشف التسلسل القائمة على نظرية المعلومات Information-Theoretic Analysis
7. أنظمة كشف التسلسل القائمة على تحليل قوالب الأوامر Command Template Analysis
8. أنظمة كشف التسلل القائمة على تحليل نتائج الاستعلامات data-centric approach

إن جميع المقاربات السابقة لتنفيذ أنظمة كشف التسلل تتضمن بشكل أساسي بناء نموذج لسلوك المستخدم الطبيعي في مرحلة التدريب، ثم مقارنة سلوك المستخدمين في مرحلة الكشف مع ذلك النموذج الطبيعي بحيث يصنف السلوك على أنه شاذ إذا تباين بشكل كبير عن النموذج الطبيعي.

تعاني جميع المقاربات المذكورة من مشاكل ونقاط ضعف قد تمنعها من أداء وظيفتها بشكل فعال. تتمحور نقاط الضعف حول عدم قدرة هذه المقاربات على كشف التسلل خلال وقت يسمح بمنع الاختراق. لذلك، يجب دراسة بنية هذه المقاربات لمحاولة المكاملة بينها والحصول بالنتيجة على نظام يمكِّن من تفادي نقاط الضعف في المقاربات المنفردة المذكورة.

1. **هدف مشروع البحث:**

نهدف في هذا المشروع إلى دراسة التهديدات الأمنية التي تعاني منها قواعد البيانات، وتصنيف هذه التهديدات لتسهيل كشفها ومنعها. كما نهدف إلى دراسة كافة التقنيات المستخدمة على مستوى قاعدة البيانات لمواجهة هذه التهديدات كالتحكم في الوصول Access Control وأنظمة كشف التسلل IDS. سنبين من خلال الدراسة القصور الذي تعاني منه التقنيات التقليدية في حماية البيانات الحساسة في قواعد البيانات من التهديدات الداخلية. وسنتوجه إلى دراسة أنظمة كشف التسلل بشقيها المتمثلين بكشف سوء الاستخدام misuse detection والكشف عن الشذوذ anomaly detection. يبحث اكتشاف إساءة الاستخدام عن أنماط الهجوم الشائعة، وبالتالي فهو غير قادر على اكتشاف تصرفات المستخدم الضارة التي تبدو طبيعية. بينما يبحث اكتشاف الشذوذ عن الإجراءات التي تحيد عن سلوك المستخدم العادي لذلك فهو يستطيع التعرف على الهجمات الجديدة التي لا تتبع نمطا محددا. سنناقش خلال المشروع كافة المقاربات المستخدمة لتنفيذ أنظمة كشف التسلل والمذكورة آنفا في الفقرة السابقة، وسنبين من خلال هذه المناقشة البنى المختلفة لتلك المقاربات بالإضافة إلى نقاط ضعف كل مقاربة ونقاط قوتها بحيث نتمكن في النهاية من تنفيذ نظام كشف تسلل فعال يجمع بين نقاط القوة في المقاربات المختلفة ويتجنب نقاط الضعف فيها.

1. **النتائج التطبيقية المتوقعة من البحث والجهات المستفيدة منها:**

من المتوقع من هذا البحث أن يفضي إلى تحديد التقنيات الأكثر فعالية التي يجب استخدامها في أنظمة كشف التسلل وذلك عن طريق مقارنة أداء النظام من أجل تقنيات ومنهجيات مختلفة في التنقيب عن المعطيات. حيث سيتم تكميم الأداء باعتماد احتمال الإنذارات الكاذبة واحتمال الإنذارات الإيجابية الصحيحة. ومن المتوقع أن ننفذ نظام كشف تسلل مبني على مكاملة تقنيات مختلفة بحيث يجمع بين نقاط قوتها ويتجنب نقاط ضعفها. كما يمكن لأي مؤسسة تريد حماية بياناتها السرية استخدام هذا النظام و الاستفادة منه.

1. **مخطط المشروع**

دراسة تحليلية تبين نقاط ضعف وقوة مقاربات تنفيذ IDS

دراسة مقاربات تنفيذ أنظمة كشف التسلل IDS

مكاملة المقاربات المختلفة لتنفيذ نظام كشف تسلل فعال

Anomaly detection

Misuse detection

أنظمة كشف التسلل IDS

التحكم في الوصول Access Control

دراسة التقنيات المستخدمة على مستوى قاعدة البيانات لمواجهة التهديدات الأمنية

تصنيف التهديدات الأمنية

دراسة التهديدات الأمنية التي تعاني منها قواعد البيانات