1.1 المقدمة

مع تطور العلم وظهور أليات ومعدات وأساليب جديدة في تقنية المعلومات ظهرت الحوجة في إيجاد طرق ووسائل جديدة لتأمين المعلومات سواء كانت هذه المعلومات موجودة ومخزنة علي أجهزة ووحدات تخزين أم كانت هذه المعلومات منقوله عبر الشبكات الإلكترونية المختلفة [1]. وبالنظر إلي مكونات منظومة عمل الحواسيب نجد أن نظام التشغيل هو أحد أهم الأجزاء التي تحتاج إلي الأمن ولكن قبل التحدث عن أهمية حماية أنظمة التشغيل لابد لنا من تعريف نظام التشغيل حيث نجد أن نظام التشغيل بمفهوم مبسط للغاية هو مجموعة من البرمجيات المسؤولة عن إدارة موارد "عتاد" وبرمجيات الحاسوب، ويمثل وسيط بين المستخدم وعتاد الحاسوب، ويمكننا القول أنه مظلة لتشغيل برامج المستخدم، يقوم نظام التشغيل بالمهام الأساسية مثل إدارة وتخصيص مصادر الحاسوب (الذاكرة، القرص الصلب، الوصول للأجهزة الطرفية الملحقة..إلخ)، ترتيب أولوية التعامل مع الأوامر، التحكم في أجهزة الإدخال والإخراج، تسهيل عمل الشبكات، وإدارة الملفات.

ومن هذا التعريف يمكننا إستنتاج الأهمية الكبري لأنظمة التشغيل لذا كان لا بد من التمعن في هذه الجزئية المهمة لمنظومة عمل الحواسيب والنظر في طرق الحماية المتبعه لتأمين مستخدميها, ومحاولة إيجاد وسائل لسد الثغرات الموجوده بها.

تتمثل معايير الأمن من منظور أنظمة التشغيل في الية التعرف والتحقق من هوية المستخدمين وذلك لتحديد صلاحياتهم والمميزات الممنوحة لهم للإستفادة من موارد جهاز الحاسوب ومن هذا المنطلق بدأ الباحث في القيام بهذه الدراسة[2].

2.1 مشكلة البحث

يعتمد نظام التشغيل في طرق التأمين والحمايه للمعلومات بإعتماد مستخدمين يتم تسجيلهم للنظام ويتم منحهم كلمات مرور ولكن هذه المعلومات أي أسماء المستخدمين وكلمات مرورهم يتم تسجيلها في ملف داخل ملفات نظام التشغيل بطريقة مشفرة وقد ظهرت مؤخراً عدة طرق تمكنك من الوصول لهذه البيانات وحذفها او تعديلها كما هو موجود في ملف

(Security Accounts Manager – SAM) لنسخة الويندوز اكس بي ونسخة الويندو ان تي.

3.1 فرضيات البحث

تمثلت الفرضية الرئيسية لهذه الدراسة في أن الإعتماد علي تقنية كلمات المرور كوسيلة تحقق من هوية المستخدمين في أنظمة التشغيل باتت غير أمنة, هذا بالنسبة للفرضية الرئيسية ولكن هنالك فرضية فرعية تتمثل في أن التحقق من الهوية عبر معامل تحقق أحادي أصبح غير فعال في كثير من الحالات وخاصة تلك الحالات التي تحتاج قدر كبير من الأمن والسرية.

4.1 ألأهداف

- معالجة بعض العيوب الموجودة في في التحقق ذو العامل الواحد من خلال إضافة معامل تحقق أخر أكثر فعالية وبأقل تكاليف.
- إضافة مستوي حماية للمعلومات في نظام التشغيل يعتمد علي العتاد اي الهاردوير Hardwareوليس السوفت وير.

- إعتماد وسيلة اخري غير ملفات الريجيستري في تخزين معلومات المفتاح (Dongle Key) .
- معالجة السلبيات السابقه لإستخدام المفتاح (Dongle Key) المتمثلة في مشكلة المفتاح المحاكاة حيث يتم نقل معلومات التحقق إلي مفتاح أخر.
- إيجاد وسيلة لمعرفة محاولات الاختراق علي نظام التشغيل.

5.1 أهمية البحث

إبتكار وسيلة جديدة في تأمين أنظمة التشغيل وذلك دون التأثير علي التكلفة المالية بصورة كبيرة بإعتماد طريقة تحقق متعددة المعامل عبر إستخدام منهجية الأشياء الفيزيائية المملوكة مع إستخدام معامل أخر كإستخدام منهجية الأشياء المعروفة التي تمثلها تقنية كلمات المرور.

6.1 حدود البحث

تقتصر الحدود الموضوعية لهذه الدراسة في بناء تطبيق يعمل علي نظام التشغيل ويندوز 32 بت وذلك للقيام بالتحقق من هوية المستخدمين عبر إستخدام مفتاح دونقل, أما في ما يتعلق بالحدود

الزمانية والمكانية للبحث نجد أن هذا البحث لايقتصر علي زمان أو مكان محدد ولكن يشترط وجود منظومة عمل حواسيب تستخدم نظام التشغيل ويندوز ان تي 32 بت.

7.1 مصطلحات البحث

الدونقل كي: قطعة الكترونية صغيرة يتم تركيبها علي منفذ USB واحيانا يشار اليه بالمفتاح في هذا البحث.

جهاز التوكن Token: أي نوع من أنواع العتاد يتم إستخدامه في التحقق من الهوية يطلق عليه لفظ توكن Token مثل إستخدام الكارد او الجوال او المفاتيح USB ...الخ.

ويندوز: المقصود به نظام التشغيل ويندوز وهو نظام تشغيل خاص بالحاسبات الألية.

8.1 أسباب إختيار البحث

- الدور الكبير الذي باتت تلعبه الحواسيب في جميع نواحي الحياه المختلفه.

- أهمية نظم التشغيل وإعتبارها أحد الأعمده الرئيسيه التي

ترتكز عليها منظومة عمل الحواسيب.

- ظهور مراكز البيانات التي تعتمد علي المخدمات الإفتراضية التي تكون عبارة عن جهاز مخدم واحد يستخدم برمجيات محددة تقوم بعمل تقسيم افتراضي له حيث يصبح عدة مخدمات داخل مخدم فيزيائي واحد يتم إستغلاله من قبل عدة مؤسسات وعدة مستخدمين وهذا الوضع يستوجب الزيادة في التأمين.

9.1 منهج البحث

إتبعت الدراسة المنهج الوصفي التجريبي القائم علي جمع البيانات لتشخيص المشكلة موضوع البحث, ومن ثم الوصول إلي أهم الوسائل التي تفضي إلي معالجة المشكلة من خلال بناء تطبيق وتجربته. وسوف يتحصل الباحث علي المعلومات الخاصة بالدراسة من خلال المراجع والأطروحات العلمية السابقة.

10.1 هيكلية البحث

يحتوي البحث علي خمسة أبواب تبدأ بالباب الأول حيث يتناول المقدمة ومشكلة البحث والفرضيات وأهمية

البحث وأهدافه وحدوده والمنهجية المتبعة في البحث، أما الباب الثاني فيتناول الخلفية النظرية للبحث و الدراسات السابقة، والباب الثالث يتناول تحليل النظام، والباب الرابع التطبيق والنتائج، والباب الخامس يتناول الخاتمة وأخيراً التوصيات.

1.2 مفهوم أمن المعلومات

قبل التحدث عن مفهوم أمن المعلومات لا بد من استعراض السياق التاريخي لتطور هذا المفهوم. نجد أن هذا المجال من الأمن حتى أواخر السبعينيات كان معروفاً بإسم أمن الإتصالات Communication Security (COMSEC) والذي حددته توصيات أمن أنظمة المعلومات والإتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي:

(المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الإتصالات ولضمان أصالة وصحة هذه الإتصالات).

تضمنت النشاطات المحددة لأمن الإتصالات COMSEC أربعة أجزاء هي:

1. أمن التشفير Crypto security
2. أمن النقل Transmission Security

3. أمن الإشعاع Emission Security
4. والأمن الفيزيائي Physical Security.

كما تضمّن تعريف أمن الإتصالات خاصيتي السرية والتحقق من الهوية [3].

1.1.2 السرية

لتأكيد بأن المعلومات لم تصل لأشخاص، عمليات أو أجهزة غير مخولة بالحصول على هذه المعلومات (الحماية من إفشاء المعلومات غير المرخص لها) [3].

2.1.2 التحقق من الهوية

إجراء أمني للتأكد من صلاحية الإتصال، الرسالة أو المصدر أو وسيلة للتحقق من صلاحية شخص ما لاستقبال معلومات ذات تصنيف محدد (أو التحقق من مصدر هذه المعلومات).

بدأت في الثمانينات مع النمو المضطرد للحاسبات الشخصية حقبة جديدة من الأمن: أمن الحواسيب Computer Security (COMPUSEC) والتي حددتها توصيات أمن أنظمة المعلومات والإتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي:

(المعايير والإجراءات التي تضمن سرية، كمال وتوفر مكونات أنظمة المعلومات بما فيها التجهيزات، البرمجيات،

البرمجيات المدمجة firmware والمعلومات التي تتم معالجتها، تخزينها ونقلها).
كما تضمّن تعريف أمن الحواسيب خاصيتي السرية والتحقق من الهوية [3].

3.1.2 الكمال

تعكس جودة أي نظام للمعلومات مدى صحة ووثوقية نظام التشغيل، التكامل المنطقي للتجهيزات والبرمجيات التي توفر آليات الحماية ومدى تناغم بنى المعلومات مع البيانات المخزنة.

4.1.2 التوفر

الوصول الموثوق إلى البيانات وخدمات المعلومات عند الحاجة إليها من قبل الأشخاص المخولين بذلك.
لاحقاً وفي التسعينات من القرن الماضي تم دمج مفهومي الأمن (أمن الإتصالات وأمن الحواسيب) لتشكيل ما أصبح يعرف باسم أمن أنظمة المعلومات Information Systems Security –
ويتضمن مفهوم أمن أنظمة المعلومات الخصائص الأربعة المعرفة مسبقاً ضمن مفاهيم أمن الإتصالات وأمن الحواسيب: السرية، التحقق من الهوية، الكمال والتوفر، كما أضيف إليها خاصية جديدة: مكافحة الانكار [3].

5.1.2 مكافحة الإنكار

التأكيد بأن مرسل البيانات قد حصل على إثبات بوصول البيانات إلى المرسل إليه وبأن المستقبل قد حصل على إثبات لشخصية المرسل مما يمنع إحتمال إنكار أي من الطرفين بأنه قد عالج هذه البيانات.

2.2 وسائل تحقيق أمن المعلومات

هي مجموعة من الآليات والإجراءات والأدوات التي تستخدم للوقاية من المخاطر أو تقليل الخسائر بعد وقوع الحدث على المعلومات وأنظمتها. وتتعدد وسائل الحماية من حيث الطبيعة والغرض وفيما يلي بعض هذه الآليات:

1.2.2 نظام الإنذار المبكر

يستخدم في هذه الآلية أجهزة حساسة (Sensors) للإنذار المبكر ضد السرقة والحريق والكوارث الطبيعية مثل الزلازل والبراكين والفيضانات ,وأخرى أجهزة حساسة ضد المواد المشعة والمواد السامة كما تشمل كاميرات المراقبة الموصلة مع شاشات العرض (Monitors) ومع أنظمة الهاتف النقال.

2.2.2 التحقق من هوية المستخدمين

هنالك بعض التقنيات التي تستخدم في التحقق من شخصيات المستخدمين ولكن كل هذه الطرق والتقنيات تندرج تحت ثلاث منهجيات رئيسية :

أ- **التحقق بواسطة شئ تعرفه(Something you know)**

تعتبر هذه المنهجية هي الأكثر شيوعا وإستخداما بالرغم من ضعفها في كثير من الجوانب ومن الطرق المستخدمة في هذا النوع من التحقق طريقة إستخدام كلمة المرور Password وهي الطريقة المتبعة في أنظمة التشغيل, [4]والتي يتناولها الباحث من خلال البحث,ونجد أن كلمة المرور هي كلمة يتم تعريفها للنظام المراد تأمينه ويتم معرفتها من قبل المستخدم ليقوم بإدخالها متي ما طلب منه النظام ذلك.

ب- **التحقق بواسطة شئ تملكه (Something you have)**

تتمثل هذه المنهجية في استخدام شئ فيزيائي حقيقي يملكه المستخدم ويقوم بإستخدامه للتحقق من هويته,وهنالك عدة طرق وتقنيات تستخدم لهذه المنهجيه مثل(البطاقات الذكية -مفاتيح الدونقل)[4] . وهذه

المنهجية هي المنهجية التي تم طبيقها والإعتماد عليها من قبل الباحث في هذا البحث.

ت- **التحقق بواسطة شئ منك (Something you are)**

تعتبر هذه المنهجية ذات قوة تأمينية عالية ولكنها ايضا معقدة ومكلفة في نفس الوقت.تم الإعتماد علي هذه المنهجيه وفق قوانين مثبتة أن هنالك بعض من الأجزاء والخاصيات في جسم الإنسان لا تتكرر مطلقا مثل(قزحية العين-وعظام الوجه-ونبرة الصوت) وبناء علي هذه القوانين تم إستخدام هذه الأشياء في التحقق والتأكد من معرفة المستخدمين لدي الأنظمة التي يستخدمونها وذلك بعد قرائتها وتحليلها [4] .

3.2.2 التحكم في الوصول

عن طريق هذه الطريقة يتم تحديد مستخدمي النظام والموارد Resources المسموح لهم بها وغير المسموح لهم بها وإعطائهم صلاحيات الوصول إليها عن طريق نظام الترخيص Authorization. احد النماذج المستخدمة في تحديد عملية الوصول وتحديد الصلاحيات ما يعرف بمصفوفة

التحكم في الوصول Access Control Matrix والمعتمدة لتطبيق القواعد الأمنية في نظم التشغيل وقواعد البيانات.

4.2.2 تشفير البيانات

وهو تحويل النص العادي(Plaintext) من شكل مقروء, بواسطة خوارزميات التشفير ومفاتيح (Keys) إلى هيئة نص مرمز (Ciphertext) وغير مقروءة ,ثم إعادة فك الترميز(Decryption) وإعادة النص إلى أصله بواسطة الخوارزميات أيضا ومن قبل الأشخاص المسموح لهم بذلك (الذين يملكون أدوات فك التشفير) [5] .

5.2.2 برمجيات كشف ومقاومة الفيروسات

يقصد بها البرمجيات التي تستخدم لمكافحة البرامج المصممة خصيصاً للإضرار بنظام الحاسب الآلي وتسميتها بمضادات الفيروسات لا يجعلها قاصرة على مكافحة الفيروسات فقط بل هو اصطلاح يطلق على هذا النوع من البرمجيات. وفي كثير من الأحيان يطلق على كل البرامج الضارة إسم فيروس بغض النظر عما إذا كان فيروس فعلاً أو دودة أو Trojan Horse أو أي نوع آخر من أنواع البرمجيات الضارة .

6.2.2 أنظمة تأمين شبكات الإتصال

هي أنظمة تساعد في التأكد من أن الشبكة ومصادرها قد أستخدمت بطريقة مشروعة حيث تعمل على تحديد حقوق المستخدمين, أو قوائم المستخدمين، أو تحديد الميزات وأنواع الصلاحيات ومنع كافة أي شخص أو جهاز غير مسجل بقوائم المستخدمين من الوصول لموارد الشبكه أو المعلومات ومن أشهر هذه الأنظمة الجدار الناري Fire Wall [6] .

3.2 تعريف نظام التشغيل

هنالك تعريفات عديده لنظام التشغيل يمكن تلخيصها في أن نظام التشغيل هو الوسيط مابين المستخدم والعتاد وهذا الوسيط هو عبارة عن مجموعة برامج أساسية تقوم بإدارة جهاز الحاسب وتتحكم في كافة البرامج والتطبيقات و تيسر هذه البرمجيات على المستخدم الإستفادة من الأجهزة التي يتكون منها الحاسب والملحقات التابعة له. ويعد نظام التشغيل من أهم مكونات الحاسب لأن من خلاله يتم ترجمة الأوامر المطلوبة من قبل المستخدم الي لغة مفهومة للألة [7].

4.2 مراحل تطور أنظمة التشغيل

تطور الحاسوب من خلال عدة مراحل وفترات زمنية ولكن نجد أن أنظمة التشغيل بمعناها الواضح وبمفهومها الحالي بدأت مابعد الجيل الثالث للحاسوب في فترة السبعينات وذلك بعد تطوير الحواسيب ذات التكامل الواسع النطاق Large Scale Integration واستخدام الشرائح الرقيقة Chips في بناء الحواسيب حيث أصبح نظام التشغيل داخل الحاسوب نفسه. ولكن بالرغم من ظهور أنظمة التشغيل في فترة السبعينات ولكن نظام التشغيل بدأت فكرته منذ الستينات وذلك بعد ظهور الباتش PATCH وتقوم فكرة الباتش بإستخدام حاسوب للتحكم بالأوامر وإعطائها لجهاز أخر ليقوم بتنفيذها مثل البطاقات للتحكم بالأوامر وكان هذا أول ظهور لما يشبه بسطر الأوامر في أنظمة التشغيل الحالية, نجد أن في هذه الفترة إنقسمت صناعة الحاسب الآلي إلى قسمين الأول الأجهزة العلمية القوية العملاقة, والثاني الأجهزة التجارية الأقل قوة. ولكن هذا أثر جدا على تصنيع الحاسب الآلي لأن بناء جهازين منفصلين قد يؤثر على خط سير الانتاج, والشركات تحتاج إلى أجهزة بحيث تضمن

أنه يمكن في المستقبل تطويرها مع امكانية تنفيذ البرامج الحالية وبكفائة أعلى لذلك لجئت IBM إلى حل هذا الموضوع بانتاج الجهاز الأول من نوعه الذي يسمى ب software-compatible machine. هذه السلسة من الأجهزة سمتها IBM بسلسلة 360. حيث أنتجت IBM العديد من الأجهزة المعتمدة على نفس التقنية والتي تختلف فيما بينها فقط في السعر والكفائة ولكن البرامج التي تعمل على أحدها تعمل على الأخرى نظريا. هذه الأجهزة إعتمدت على تقنية الدارات المتكاملة المستخدمة حاليا, هذا ما أدى إلى زيادة كفائتها عن أجهزة الجيل الثاني المعتمدة فقط على الترانزستور في عملها. وايضا انتقلت هذه الفكرة في التوافقية إلى الشركات الأخرى وبدأت معظم الشركات في تصنيع أجهزة متوافقة وكانت الأجهزة التي انتجتها IBM تعمل في عدة مجالات مختلفة من الأمور العلمية حتى الأعمال التجارية لذا كانت النتيجة هو نظام تشغيل ضخم جدا ومعقد إلى درجة غير معقولة حيث يحتوي على ملايين من أسطر الأسمبلي كتبت عن طريق آلاف المبرمجين ولكنه احتوى على آلاف

الآلاف من الأخطاء bugs و كلما يتم تصحيح مجموعة من الأخطاء في الاصدارات المتتالية يتم انشاء أخطاء أخرى وبالتالي الأخطاء موجودة في أعداد ثابتة تقريبا. بعد هذا النظام ظهرت أول الأنظمة القوية التي تدعم التشارك واسمه CTSS تم تطويره في MIT على أجهزة IBM 7094 المعدلة, بعد ذلك قررت MIT و Bell Labs و General Electric تطوير نظام يدعم المئات من المشاركات في نفس الوقت ، سمي هذا النظام ب MULTICS وهو على درجة عالية جدا من التعقيد أيضا ولكن هذا النظام توقف لاحقا بسبب تعقيده وبعد أن توقفت General Electric عن تطوير الحاسبات الآلية .

في هذه الحقبة أيضا توالي ظهور سلسة من الأجهزة الصغيرة المطورة من الجهاز DEC PDP-1 حتي وصلت احدثها وأفضلها DEC PDP-11 .[7]

5.2 وظائف نظم التشغيل

من أهم الوظائف لنظم التشغيل هي التعرف علي المكونات المادية للجهاز ومن ثم بعد تعريفها يقوم نظام التشغيل بالتحكم في طريقة عمل أي مكون من هذه المكونات وربطها ببعضها

البعض كما يقوم بإدارة كافة المهام التي يجب تأديتها بواسطة هذه المكونات والتأكد من عدم تداخلها.

6.2 أهداف نظام التشغيل

توجد أهداف عديدة لنظام التشغيل ولكن الهدف الرئيسي يتمثل في تسهيل الإتصال بين المستخدم والحاسب وذلك من خلال توفير البرامج المساعدة وواجهات الإستخدام ومن خلال تمكين المستخدم من الاستفادة القصوي من كافة الموارد سواء كانت هذه الموارد لجهاز حاسوب منفرد او مجموعة أجهزة متصلة ببعضها البعض ومن ثم توفير الحماية الكاملة لهذه الموارد سواء كانت موارد عتاد او برمجيات أو بيانات وهذا الجانب يمثل المحور الرئيسي للبحث.

7.2 أنواع نظم التشغيل

هنالك عدة مفاهيم يمكن من خلالها تصنيف أنظمة التشغيل فيمكن تصنيف أنظمة التشغيل من حيث القدرة علي أداء المهام إلي أنظمة تشغيل وحيدة المهام وأنظمة تشغيل متعددة المهام, أما من ناحية الإستخدام تصنف أنظمة التشغيل إلي متعددة المستخدمين ووحيدة المستخدم ونجد أن أنواع أنظمة التشغيل

قد إشتقت من خلال هذه المفاهيم أو التصنيفات الرئيسيه وهي كالأتي:

1.7.2 المستخدم الواحد والمهمه الواحدة

هذا النوع من أنظمة التشغيل يسمح لمستخدم واحد تشغيل تطبيق أو أداء مهمة واحدة فقط ولايمكن تشغيل تطبيق أو أداء مهمة ثانية إلا بعد نهاية المهمة الأولي ومن أمثلة هذا النوع من أنظمة التشغيل نظام التشغيل دوس MS-DOS [8].

2.7.2 المستخدم الواحد متعدد المهام

هذا النوع من أنظمة التشغيل يسمح لمستخدم واحد تشغيل عدة تطبيقات أو أداء مهام مختلفة في وقت واحد كما يمكن لهذا المستخدم التنقل بين هذه التطبيقات علي حسب الحوجه ومن أمثلة هذا النوع من أنظمة التشغيل نظام التشغيل مايكروسوفت ويندوز Microsoft Windows الذي تمثل إحدي إصداراته الحالة التطبيقيه التي تم تناولها من خلال هذا البحث.

3.7.2 المتعدد المستخدمين المنفرد المهمة

هذا النوع من أنظمة التشغيل يسمح لأكثر من مستخدم من العمل حيث

ينفذ كل مستخدم برنامج واحد, بحيث يزود كل مستخدم بوحدة إدخال وإخراج مكونة من لوحة مفاتيح وشاشة عرض تتصل مع الحاسب المركزي ومن أمثلة هذا النوع ويندوز ان تي Windows NT.

وهنالك أيضا تسمية أخري لهذا النوع من أنظمة التشغيل حيث يسميه البعض نظام المشاركه الزمنية لانه يعطي المستخدمين فترات زمنيه ثابته لاستخدام المعالج [8].

4.7.2 متعدد المستخدمين ومتعدد المهام

هذا النوع من أنظمة التشغيل يسمح لعدة مستخدمين بإستغلال موارد الجهاز والقيام بعدة مهام مختلفه في وقت واحد لكل مستخدم مع وجود إدارة من قبل النظام لتنظيم أداء المهام وترتيبها ليمنع بذلك تداخلها ومن أمثلة هذا النوع نظام التشغيل لينيكس ويونيكس Linux & Unix.

5.7.2 أنظمة تشغيل الوقت الحقيقي Real Time OS

هذه النوعية من أنظمة التشغيل صممت للتحكم في ألألات وألادوات العلمية والنظم الصناعية وهذه ألأنظمة لاتتعامل مع المستخدم بشكل كبير لأنها لاتقدم له الكثير من الخدمات وهذه

الانظمة تحتوي على ميكانيكيه عالية في التوقيت مثل أجهزة تخطيط القلب [9].

6.7.2 أنظمة تشغيل متعددة المعالجه

هذا النوع من أنظمة التشغيل ينفذ تعليمات عديدة بشكل متواز في نظام حاسوب واحد يمتلك وحدات معالجة مركزية عديدة والأنظمة متعددة المعالجة تنفذ الوظائف بشكل متوافق زمنيا اي في نفس اللحظة كما تتميز بالسرعة ومن أمثلتها نظام التشغيل صن Sun OS .

8.2 المكونات الرئيسية لنظام التشغيل

يتكون نظام التشغيل من عدة مكونات يمكن تعريفها وتقسيمها علي حسب وظيفتها مثل مكونات الإدخال والإخراج والوظائف, ولكن نجد أن أنظمة التشغيل الحديثة تعتمد بشكل أساسي علي مكونات تعتبر أساسية يمكن تقسيمها إلي:

1.8.2 إدارة العمليات Process Management

نظام التشغيل هو نظام مسؤول عن تنظيم عمل الحاسب، ومن مسؤوليات هذا النظام إدارة العمليات حيث تعتبر إدارة العمليات واحدة من أهم مهام

نظام التشغيل وذلك نسبة لأن نظام التشغيل يهدف الي تشغيل أكثر من عملية في نفس الوقت ولكن هذه العملية أي عملية تنفيذ المهام المتعددة تحتاج الي طريقة أو عملية تنظيمية لهذه المهام لتنفيذها عبر وحدة معالجة مركزية وهنا يكمن دور إدارة العمليات حيث تقوم بتنظيم تنفيذ العمليات في المعالج وطريقة للتعامل مع العمليات العديدة التي في حالة نشاط في الحاسب [10].

2.8.2 إدارة الذاكرة Memory Management

إحدي وظائف نظام التشغيل إدارة موارد الحاسب والتي من أهمها الذاكرة الرئيسية وذلك لأنها المكان الوحيد الذي منه تستدعي وحدة المعالجة المركزية البرامج والبيانات المراد تنفيذها ويسمي الجزء من النظام الذي يتولي إدارة الذاكرة بمدير الذاكرة Manager Memory والذي من أهم مهامه مراقبة جميع مواقع الذاكرة من حيث الفراغ وذلك لتسكين العمليات المراد تنفيذها أو الإمتلاء من أجل تفريغ المواقع بعد إنتهاء العمليات من التنفيذ, كما يقوم مدير الذاكرة

بتحديد الطريقة التي من خلالها يتم توزيع المواقع الفارغة من الذاكرة للعمليات المراد تنفيذها مع تحديد الأولويات[11].

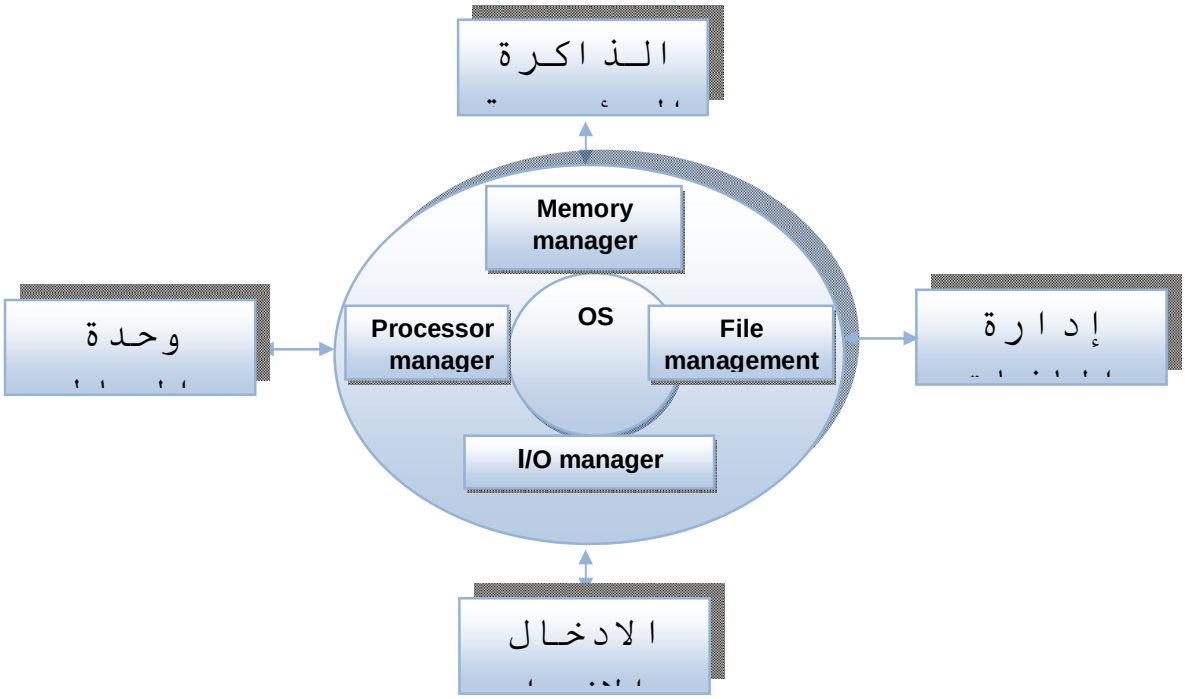
3.8.2 إدارة الملفات File Management

إدارة الملفات مهمة يقوم بها مدير الملفات وهو عبارة عن مجموعة من البرمجيات تكون مسؤولة عن إنشاء الملفات، حذفها، تعديلها والتحكم في العمليات التي تحدث للملفات - بمعنى أنها مسؤولة عن إدارة جميع الموارد التي تستخدم من قبل الملفات ومن أهم هذه المسؤوليات هي عملية تخزين الملفات ومعرفة الطرق والسياسات المتبعة في ذلك وبالتمعن في عملية التخزين نجد أن عملية التخزين تتم بصورة فيزيائية في وحدات مختلفة مثل القرص الصلب او القرص المرن ولكن نظام التشغيل يقوم بعمل مستخلص او خريطة منطقية غير محسوسة Logical تشير للكائن الفيزيائي الذي تم حفظه في وحدات التخزين المختلفة[12].

4.8.2 إدارة عملية الإدخال والإخراج I/O System Management

تعتبر إدارة عملية الإدخال والإخراج من أهم المكونات في أنظمة

التشغيل خاصة أن أجهزة الحاسوب الحديثه أصبحت تستوعب أعداد كبيرة من الأطراف التي يمكن أن تتصل بها مثل الشاشات ولوحات المفاتيح والماسحات الضوئية والطابعات وغيره لذا نجد أن هذه الأعداد من الأجهزة المتصلة تحتاج لعملية تنظيمية وتنسيقية, ويمكن تلخيص المهام الأساسية لمكون إدارة عملية الإدخال والإخراج في عملية ربط المعالج بوحدات الإدخال والإخراج المختلفة وتحديد كيفية إستقبال المعالج للبيانات من هذه الوحدات ومن ثم تحديد الطريقة المستخدمة في عملية الإدخال والإخراج[12].



شكل رقم (1.2) شكل يوضح المكونات الرئيسية لنظام التشغيل

9.2 تعريف نظام التشغيل ويندوز

نظام التشغيل ويندوز أو نظام النوافذ هو نظام تشغيل رسومي يعتمد مستخدميه علي واجهات إستخدام رسومية لتنفيذ كافة المهام دون الحاجة الي كتابة أوامر, تم إنتاج ويندوز من قبل شركة مايكروسوفت الأمريكية في خطوة منها للإستجابة علي الإهتمام المتزايد من قبل المستخدمين للإعتماد علي واجهات الإستخدام الرسومية. ويعتبر نظام التشغيل ويندوز منذ إنتاجه يمثل أحد أكثر أنظمة التشغيل إستخداما في العالم.

10.2 تاريخ نظام التشغيل ويندوز

في سبتمبر من العام 1981م بدأت شركة مايكروسوفت في تطوير نظام يسمى Interface Manager بهدف تطوير واجهة عمل رسومية تقدم طريقة متطورة وبسيطة للتعامل مع أجهزة الكمبيوتر الشخصية, ولم يكن وقتها قد مر على إصدار النسخة الأولى من نظام MS DOS سوى ثلاثة عشر شهرا فقط، وإستمرت عملية التطوير تلك نحو 25 شهرا في ظل منافسة قوية من جانب أنظمة أخرى كانت قد بدأت في الظهور تباعا مثل XEROX Starو Vision و Apple Lisa حتى أعلنت شركة مايكروسوفت عن نظامها الجديد في شهر نوفمبر من العام 1983 والذي عرف وقتها بإسم **Windows 1.0** ولكن هذا النظام لم يطرح رسميا في الأسواق إلا في شهر نوفمبر من العام 1985م [7].

11.2 إصدارات نظام التشغيل ويندوز

تنتج شركة مايكروسوفت أنواع عديدة من أنظمة التشغيل يمكن تقسيمها حسب بيئة عملها إلي:

- أنظمة تشغيل .

- أنظمة تشغيل المخدمات.
- أنظمة تشغيل أجهزة الكمبيوتر الكفي.
- أنظمة تشغيل أجهزة الهواتف النقالة.

12.2 الدراسات السابقة

هنالك إهتمامات بدأت تظهر مع تزايد إستخدامات الحاسب الألي وظهور أجيال جديدة ومتقدمة أصبحت تشكل عنصر أساسي في جميع مناحي الحياة, حيث كانت مثل هذه الإهتمامات في السابق لا أهمية لها ومن هذه الإهتمامات أخذ أمن المعلومات حيزاً أساسياً نظرا لظهور بعض المهددات لسلامة الحواسيب او المعلومات المخزنة بها وظهرت العديد من الدراسات في أمن وسلامة المعلومات وبالنظر للدراسات التي تناولت تأمين المعلومات من منظور التحقق من المستخدمين ومنع الوصول الغير مصرح به وهو ذات المنظور الذي تناولته هذه الدراسة وجد الباحث أن هنالك العديد

من الدراسات مثل الورقة العلمية المقدمة من قبل روبرت موريس وكين تومسون في العام 1979 والتي إستعرضا من خلالها عملية التحليل التجريبي لكلمات مرور المستخدمين عن طريق إجراء هجوم القواميس Dictionary Attack علي نظام التشغيل يونكس, ومن ثم قاما بتصميم Crypt Function لتشفير كلمات مرور المستخدمين [13].

في العام1990م قدم David C. Feldmeie , Philip R. Karan دراسة تناولت بعض الثغرات في مقدرة نظام التشغيل يونكس علي مواجهة الهجمات التي تستهدف كشف كلمات المرور الخاصة بالمستخدمين مؤكدين علي أن التطور الذي طرأ علي عالم الحواسيب وزيادة السرعات والسعات التخزينية للأجهزة جعل تطوير الأدوات التي تمكن من الوصول لكلمات المرور بصورة سريعه وسهلة [14]. يمكننا القول أن الدراستين السابقتين هما بمثابة سرد تاريخي للدراسات والأبحاث التي تناولت قضايا أمن وسلامة المعلومات بصورة عامة وفي التحقق من هوية المستخدمين في أنظمة التشغيل بصورة خاصة ولكن لايمكن مناقشتها وتقييمها نظراً للتغيرات

الكبيرة التي حدثت في مجال أجهزة الحاسوب وظهور حقبة جديدة من العتاد والبرمجيات جعلت من هذه الدراسات مرجعيات تحفظ لأصحابها مساهماتهم التي تعتبر مرتكزات أساسية في تطور هذا المجال. بعد تناول الباحث لعدة دراسات وجد الباحث أن هنالك دراسات حديثة ذات إرتباط وثيق وأخري ذات إرتباط جزئي بمجال البحث وفيما يلي إستعراض لأهم الدراسات ذات الإرتباط الوثيق :

1.12.2 دراسة Anu Varghese, Deepthy Mathews (2014م)

قدمت هذه الدراسة إستعراض للمنهجيات المختلفة المتبعة في طرق التحقق من هوية المستخدمين والتقنيات المستخدمه في ذلك مثل إستخدام كلمات المرور وإستخدام الخصائص الحيوية والبطاقات الإلكترونية مبينة بعض المشاكل الناتجة من إستخدام كل طريقة علي حدة. هدفت الدراسة الي تقديم نظام للتحقق من هوية المستخدمين ويعتمد هذا النظام علي ثلاث عناصر أساسية جهاز خادم وهاتف نقال للمستخدمين وجهاز

GSM Modem لتبدأ بعد ذلك عملية التحقق من المستخدم بإرسال رسالة نصية من الهاتف الجوال من قبل المستخدم بصورة مشفرة وتحتوي هذه الرسالة علي بعض المعلومات مثل إسم المستخدم وكلمة المرور والرقم المتسلسل للوحة الجوال يقوم بإستلامها جهاز الخادم عن طريق جهاز المودم ويعمل علي فك شفرتها لمقارنتها وبعد ذلك توليد كلمة مرور لمرة واحدة فقط ومن ثم إرسالها في رسالة نصية لهاتف جوال المستخدم[15].

خلصت الدراسة الي أن إستخدام طريقة أو منهجية واحدة للتحقق من هوية المستخدمين بات أمر قليل الفعالية خاصة في بيئات العمل التي تتطلب طبيعتها قدر عال من السرية خاصة أن معظم المستخدمين يستخدمون كلمات مرور سهلة ولها علاقة إجتماعية بهم مثل تواريخ الميلاد وأسماء الأبناء وخلافه من الكلمات التي يمكن الوصول لها بطريقة سهلة وسريعه كما أن مفهوم التحقق عبر طريقتين مثل إستخدام كلمة المرور والبطاقات في أن واحد بات من الضروريات الملحة من قبل المؤسسات ويوفر قدر كبير من الأمن للأنظمة التي تستخدم هذا النوع من التحقق, ولكن

رأي الباحثان أن إستخدام الأشياء الملموسة التي تكون بحوزة المستخدمين في التحقق قد يمثل عبأ إضافي علي المستخدمين في حملها كما يمثل عبأ مالي علي المؤسسات في شرائها وتوفيرها وصيانتها. لذلك يجب إستخدام أشياء أساسية يمكن أن يستخدمها المستخدم بصورة مباشرة كإستخدام الهاتف النقال وغيره من الأدوات التي بحوزة المستخدمين.

رأي الباحث ونقد الدراسة

بعد تناول الباحث لهذه الدراسة والتمعن فيها يري الباحث أن هنالك إرتباط وثيق بين ما تناولته هذه الدراسة وما تناوله الباحث ويكمن هذا الإرتباط في مشكلة الدراستين المتمثلة في إيجاد طريقة فعالة تحد من الثغرات الموجودة في إستخدام كلمات المرور كوسيلة للتحقق من هوية المستخدمين بالرغم من إختلافهم في المصادر المراد تأمينها إذ يتناول الباحث الموضوع من منظور أنظمة تشغيل الحاسب الألي بينما تتناول الدراسة الموضوع بصورة عامة. يقول الباحث أن هنالك نقاط عديدة يتفق فيها مع ما خلصت له الدراسة وتتمثل في أن الإعتماد علي طريقة واحدة علي التحقق

من هوية المستخدمين أصبح أقل فعالية ولابد من إستخدام أكثر من طريقة خاصة في المصادر ذات القيمة المعلوماتية الكبيره , هنالك أيضا إتفاق في أن إستخدام الأشياء المحسوسة Token المستخدمة كألية لعملية التحقق يحد من مشاكل الاختراق التي يمكن أن تتعرض لها كلمات المرور من مشاكل هندسة إجتماعية وهجوم القواميس وغيره. أما فيما يتعلق بجوانب القصور في هذه الدراسة يري الباحث أن التطبيق العملي لهذه الدراسة يمكن أن يكون ملائما وعمليا في بعض الحالات مثل الأنظمة التي لاتكون عملية التحقق فيها تجري بصورة مستمرة وذلك نسبة لأن عملية التحقق المطبقة في الدراسة المعنية تعتمد علي خدمة رسائل الجوال القصيرة التي عادة ما تكون مدفوعة القيمة مما يشكل تكلفة ذات قيمة مالية مؤثرة خاصة إذا ما كان عنصر التكلفة من العناصر المؤثرة علي الجهة التي تريد تطبيق هذه الطريقة.

2.12.2 دراسة Vekram Verma, Shilpi Sharma (2013م)

تناولت هذه الدراسة إستخدام كلمات المرور كوسيلة للتحقق من هوية

المستخدمين مبينة نقاط الضعف والمهددات المترتبة علي ذلك والتي من خلالها قدمت الدراسة طريقة تهدف لإيجاد حلول ومعالجة لهذه المهددات. إعتمد الباحثان في الطريقة الجديدة علي إستخدام أكثر من وسيلة للتحقق من الهوية وتمثلت هذه الوسائل في إستخدام كلمات المرور الرسومية بدلا عن كلمات المرور النصية وإستخدام ملف صوتي يتم تحديده من قبل المستخدم مع كلمة مرور رسومية ومن ثم تخزينها في قاعدة بيانات ليتم مقارنتها بعد ذلك [16].

خلصت الدراسة الي أن إستخدام كلمات المرور الرسومية يساعد المستخدمين في تكوين كلمات مرور معقدة, نسبة لأن العقل البشري يستطيع حفظ الأشكال بصورة أفضل من النصوص ومع إضافة الملف الصوتي تصبح عملية الإختراق أو الوصول لمعلومات المستخدمين أمر صعب. كما أشارت الدراسة إلي أن هذا النظام يمكن تطبيقه علي كافة التطبيقات والمصادر التي تحتاج الي حماية بصورة أكبر.

رأي الباحث ونقد الدراسة

بالنظر لمشكلة الدراسة نجدها هي ذات المشكلة التي يتناولها البحث ولكن هنالك جانب أساسي لم تتناوله الدراسة في ما يخص الجزء التطبيقي حيث ذكرت الدراسة أن إستخدام كلمات المرور الرسومية يمثل حل عملي لمشاكل إستخدام كلمات المرور النصية ولكن من وجهة نظر الباحث الحل هو حل جزئي يمكن حصره في صعوبة إستخدام كلمات مرور نصية من قبل المستخدمين ولكن لإستخدام هذا النوع من كلمات المرور أوجه قصور أهمها إمكانية التجسس والمتابعه أثناء دخول المستخدمين. كما أن إستخدام الملفات الصوتية يمثل إهدار لموارد تخزين الأجهزه خاصة إذا كانت أعداد المستخدمين كبيرة لأن ملفات الصوت غالبا ما تكون كبيرة الحجم .

3.12.2 دراسة التحقق ثنائي المعامل عبر تقنية البلوتوث, (2013م)

أجرى كل من أحمد محمد موسي، وجهاد العطاء، وعبد الماجد جعفر, دراسة بعنوان التحقق ثنائي المعامل عبر تقنية البلوتوث في مشروع مقدم كأحد متطلبات الحصول على بكالوريوس الشرف في نظم الحاسوب والشبكات من

كلية علوم الحاسوب وتقانة المعلومات بجامعة السودان في العام 2013م, وقدم الباحثون عبر هذه الدراسة ألية للتحقق من هوية المستخدمين وذلك من خلال معاملين للتحقق إذ تمثل تقنية كلمات المرور المعامل الأول بينما تمثل تقنية البلوتوث الموجودة علي الهاتف النقال معامل التحقق الثاني.

هدفت هذه الدراسة الي تقليل المخاطر المتعلقة بأليات التحقق الأحادي المعامل والتحقق عبر تقنية كلمات المرور, وذلك من خلال بناء تطبيق بلغة السي شارب ويعمل من خلال عدة طبقات إذ تمثل الطبقة الأولي في جهاز خادم به قاعدة بيانات مخزن بها معلومات عن المستخدم مثل إسم المستخدم, كلمة المرور, ورقم MAC الخاص بجهاز الهاتف النقال. أما الطبقة الثانية متمثلة في جهاز عميل به واجهات إستخدام للنظام المراد حمايته وتم تمثيله هنا بنظام حسابات بنكية, أما الطبقة الأخيرة هي الهاتف النقال وهو المعامل الثاني المقترح من قبل فريق البحث, نجد أن سيناريو عملية التحقق يبدأ بعد أن يقوم المستخدم بإدخال بيانات الدخول من خلال الجهاز العميل الذي

يقوم بدوره بإرسالها للجهاز الخادم للتحقق من وجودها في قاعدة البيانات ليقوم الجهاز الخادم بدوره بإرسال MAC Address الخاص بالهاتف النقال ليقوم جهاز العميل بالبحث عن البلوتوث المتوفرة في النطاق للتأكد من MAC المرسل.

خلصت هذه الدراسة الإ أن التحقق عبر أكثر من معامل يمكن أن يؤدي إلي تعزيز الجوانب الأمنية في تطبيقات الحاسوب كما أن إستخدام البلوتوث الموجود علي أجهزة الهواتف النقالة الخاصة بالمستخدمين يمكن أن يستخدم كألية للتحقق من الهوية دون إضافة أعباء مالية علي النظام [17].

رأي الباحث ونقد الدراسة

هنالك أوجه شبه بين الدراستين إذ يكمن الشبه في تناول الدراستين لمشاكل إستخدام تقنية كلمات المرور كمعامل أحادي للتحقق من الهوية هذا من جانب أما الجانب الأخر هو إتفاقهما علي أن الإعتماد علي معامل تحقق أحادي أصبح ضعيف الفعالية في كثير من الأحيان.

بالنسبة للإختلافات بين الدراستين ونقد الدراسة يقول الباحث تختلف الدراستين في إطار العمل إذ تتناول هذه الدراسة

التأمين من منظور تطبيقات الحاسوب أما الباحث قد تناول الموضوع من منظور أنظمة التشغيل ويري الباحث أن هنالك بعض الثغرات في الجانب التطبيقي لهذه الدراسة وتتمثل هذه الثغرات في عدم إستخدام أي وسيلة لتشفير MAC Address الخاص بالهاتف النقال قبل تخزينه في قاعدة البيانات مما يساعد في الوصول إليه وتغييره بأخر يكون غير مصرح له بالدخول من قبل إدارة النظام.

4.12.2 دراسة A. Alnajjar , H. Janicke (2012م)

وصف الباحثان في هذه الدراسة بأن الإعتماد علي كلمات المرور في التحقق من المستخدمين يعتبر مشكلة وثغرة أمنية تحتاج إلي حلول عملية يمكن تطبيقها بشكل سهل.

هدفت هذه الدراسة الي تقديم طريقة مزدوجة أو متعددة الطرق في التحقق يمكن من خلالها سد كافة الثغرات المتعلقه بالمشكلة المذكورة. تمثلت هذه الطريقة في تطبيق ألية للتحقق من الهوية عبر معاملين أساسيين هما إستخدام العتاد بدلا عن كلمة المرور وإستخدام تقنيات تحليل نمط الإستخدام للمستخدمين.

تمثل الجانب التطبيقي لهذه الدراسة في بناء نظام بلغة الجافا يقوم بتحليل النمط الإستخدامي المتمثل في سرعة وإستجابة المستخدمين في كتابة كلمة المرور بحيث يصبح الوقت المستغرق من قبل المستخدم في الكتابة علي لوحة المفاتيح بمعاملي الضغط والرفع من المفتاح يمثل سمة معرفية للمستخدم.
يقوم النظام بالتحقق عبر ثلاث مستويات حيث يمثل مستوي إسم المستخدم وكلمة المرور المستوي الأول ليأتي بعد ذلك التأكد من مطابقة خصائص المستخدم في الكتابة علي لوحة المفاتيح ومن ثم تأتي مرحلة التحقق عبر العتاد بمقارنة خصائص العتاد المستخدم والمتمثلة في الرقم المتسلسل لقرص التخزين الصلب والرقم المتسلسل لشريحة Bios و MAC Address وتكمن المقارنة في التأكد من أن هذا المستخدم قد إستخدم هذا العتاد من قبل .
خلصت الدراسة الي أن إستخدام العتاد في عملية التحقق من هوية المستخدمين يمكن أن يؤدي إلي مزيد من القوة الأمنية للمصادر المراد تأمينها, كما يمكن تحليل وإستخدام بعض السمات النمطية مثل سرعة الكتابة وزمن

إستجابة المستخدم في التعامل مع لوحة المفاتيح كألية تحقق ذات خصائص حيوية دون الحوجة لإضافة عتاد إضافي من شأنه زيادة التكلفة المالية للأجهزة مثل أجهزة مقارنة بصمة العين وغيره من الأجهزة المستخدمة في عملية التحقق بالسمات الحيوية. هنالك رؤية مستقبلية قدمتها الدراسة تمثلت في صقل اليات التحقق بإستخدام السمات النمطية وتنفيذ تقنيات تعتمد علي الشبكات العصبية[18].

رأي الباحث ونقد الدراسة

يقول الباحث أن هذه الدراسة تعتبر من أهم الدراسات التي شكلت الملامح الأساسية للطريقة المتبعة من قبله ويتفق الباحث مع الدراسة لحد كبير في تناولتها خاصة فيما يتعلق بالمشكلة التي تناولتها الدراسة إذ تعتبر مشكلة إستخدام كلمات المرور هي القاسم المشترك بين كافة الدراسات السابقة, بالرجوع الي الحالة التطبيقية التي تناولتها هذه الدراسة يري الباحث أن طريقة التحقق التي تناولتها الدراسة يمكن أن تكون ذات فعالية في بيئات العمل ذات الأطراف المتعددة مثل الشبكات المحلية والشبكات

العنكبوتية والتي يتم فيها دخول المستخدمين عبر أجهزة طرفية أخري.
أما في ما يتعلق بما ذكر في خلاصة الدراسة يقول الباحث أن إستخدام السمات النمطية يمكن أن يكون ذو فعالية كبيرة وأقل كلفة من السمات الحيوية ولكن بالمقابل لا يمكن إعتماده كبديل للسمات الحيويه التي أكد العلم أنها لا تتكرر ولا تتطابق.

بعد أن تناول الباحث بعض الدراسات التي يري أن لديها إرتباط كبير بمجال البحث هنالك أيضا دراسات تناولت جوانب جزئية من البحث وفي ما يلي إستعراض لدراسة ذات إرتباط جزئي بمجال البحث:

5.12.2 دراسة البصمة الألية وعلاقتها بالبعد الأمني, محمد صالح عبد العزيز (2012م)

أجري الباحث دراسته في المملكة العربية السعودية في قطاع الجوازات

سعيا لإثبات مساهمة تقنية البصمة الألية وتأثيرها علي البعد الأمني خاصة بعد لجوء المنتحلين والخارجين عن القانون لإستخدام التقنيات الحديثة في في تزوير المستندات وإنتحال الشخصيات وقد تطرقت الدراسة للتقنيات المستخدمة في التحقق من الهوية بإستخدام الخصائص الحيوية , كما تناولت عرض لتحليل بيانات الدراسة ومناقشتها مستخدما الباحث المنهج الوصفي التحليلي، باستخدام الإحصائيات كأداة لجمع البيانات[19].

ومن أهم النتائج التي توصلت لها الدراسة أن بصمة الأصبع وبصمة العين الآلية هما أفضل تقنيتين في الوقت الراهن لتحديد هوية الشخص لأن كل شخص من المستحيل أن تتطابق بصمتة مع شخص أخر.

رأي الباحث ونقد الدراسة:

إرتبطت هذه الدراسة بجزئية محدده هي جزئية التحقق الإلكتروني من هوية المستخدمين ولكنها إختلفت في مجال التطبيق إذ تناولت الدراسة موضوع التحقق من منظور أمني بالمفهوم الجنائي. إتفق الباحث مع الدراسة في النتائج التي توصلت لها والمتمثلة في أن

إستخدام الخصائص أو السمات الحيوية بصورة عامة وإستخدام بصمة الأصبع وبصمة العين بصورة خاصة تعتبر من أفضل التقنيات المستخدمة لتحديد هوية الأشخاص ولكن يري الباحث أن هذه الدراسة لم تتطرق للمعوقات التي تحد من إستخدام هذه التقنيات والتي من أهمها التكلفة العالية جدا لتطبيق مثل هذا النوع من الوسائل , وأن هنالك بعض من الممارسات لتطبيق أنظمة الأمن تتطلب موازنة مابين الأمن والتكلفة أي توفير قدر عالي من الأمن بأقل التكاليف الممكنه.

1.3 التحليل

بالنظر لتعريف التحليل إصطلاحا نجده هو رد الشئ الي عناصره ومكوناته ألأساسية وإستنادا علي هذا التعريف يمكننا القول أن عملية التحليل تعتبر من أهم العمليات في كافة المجالات والتي من خلالها يمكن معرفة الخلل ومعالجته بغية الوصول الي نتائج صحيحة[20].

نجد أن في هذه الدراسة عملية التحليل شملت العديد من الأنظمة حتي يتمكن الباحث من الوصول إلي طريقة لمعالجة المشاكل المتعلقة بالبحث ومن هذه الأنظمة كان لابد من تحليل الوضع الحالي والمتمثل في الطريقة المتبعة للتحقق من هوية المستخدمين في نظام التشغيل ويندوز الذي يعتبر بمثابة إطار عمل للبحث, ونظرا لإعتماد الباحث علي منهجية تكامل المكونات القابلة للاستخدام Integration from reusable components في بناء النظام المراد تطبيقه كان لابد من تناول التحليل لطريقة التأمين بإستخدام مفاتيح Token التي تمثل أحد عناصر النظام المراد تطبيقه من قبل الباحث ومن ثم معرفة سلبياتها ومعالجتها عند إعادة إستخدامها. هنالك ايضا التنبيه عبر الرسائل القصيرة يمثل عنصر من عناصر النظام كان لابد من تحليله والتعرف علي خصائصه.

بعد دراسة وتحليل كافة المكونات المتعلقة بالحالة التطبيقية للبحث كانت مرحلة التحليل لطريقة التكامل لهذه المكونات مع بعضها البعض وتحديد المدخلات المطلوبة لبناء تطبيق يعمل

علي توفير مزيد من الحماية علي نظام التشغيل وتوفير خدمة للكشف الفوري لمحاولات الدخول الغير مصرح به حال حدوثه.

2.3 تحليل الوضع الحالي

لتناول التحليل للوضع الحالي لابد من أن يشمل التحليل ثلاث جوانب ترتبط بالوضع الحالي ويمكن تصنيف وسرد هذه الجوانب علي النحو التالي:

1.2.3 أولا الطريقة المتبعة حاليا للتحقق من الهوية في نظام التشغيل

غالبا ما تقوم عملية التأمين و التحقق من هوية المستخدمين في أنظمة التشغيل حاليا من خلال تسجيل المستخدمين ومن ثم منحهم الصلاحيات والإمتيازات الخاصة بالإستخدام مثل صلاحية المدراء Administrators وصلاحية المستخدمين Users بحيث أن المدراء لهم كافة الصلاحيات والإمتيازات بما فيها تسجيل المستخدمين ومنحهم الصلاحيات, هذا بالنسبة للمنهجية المتبعه في التأمين ولكن بالنسبة للطريقة المتبعة لتطبيق هذه المنهجية هي طريقة تعتمد علي تسجيل البيانات الخاصة بالمستخدمين عند منحهم الصلاحيات والإمتيازات في ملفات خاصة يتم تشفيرها من خلال خوارزميات تشفير ومن ثم حفظها داخل الملفات الخاصة بنظام التشغيل.

عند بدأ عمل نظام التشغيل وبعد تحميل ملفات الإقلاع علي الذاكرة يطلب النظام من المستخدم إدخال إسم الدخول وكلمة المرور لتكتمل عملية الدخول من خلال خطوتين تبدأ بالكشف عن هوية المستخدم User Identification وهنا يتم التأكد من وجود إسم الدخول بملف بيانات المستخدمين المسجل مسبقا, أما الخطوة الثانية هي خطوة التحقق من المستخدم User Authentication وهي مطابقة كلمة المرور المدخلة بالكلمة المسجلة من ضمن بيانات المستخدم الذي تم الكشف عنه في الخطوة الأولي , وبهذه الخطوة تكون عملية دخول المستخدمين قد إكتملت إما بالدخول لنظام التشغيل أو بالرجوع الي نافذة إدخال بيانات الدخول في حال عدم مطابقة بيانات الدخول.

2.2.3 ثانيا طريقة التحقق بإستخدام العتاد

يعتبر التحقق من الهوية بإستخدام العتاد هي الطريقة المتبعة لتطبيق مفهوم التحقق عبر الأشياء المملوكة وتكون هذه الأشياء المملوكة في الغالب قطع الإلكترونية يتم تركيبها علي الجهاز مباشرة عبر المنافذ الموجودة مثل منفذ USB أو يتم توصيلها بطريقة غير مباشرة مثل إستخدام البلوتوث أو التوصيلات اللاسكية الأخري. بالنظر للتقنيات المستخدمة في هذه الطريقة هنالك تقنيات كثيرة مثل البطاقات الذكية ومفاتيح Dongle التي تسمي أحيانا مفاتيح Token.

3.2.3 ثالثا تقنية التحقق عبر مفاتيح Token

يعتمد التحقق بإستخدام مفتاح Token علي نوعين أساسيين هما:

- مفاتيح Active Token: يحتوي هذا النوع من المفاتيح علي وحدة معالجة تقوم بتوليد كلمة مرور عبر خوارزمية محددة تعتمد علي الزمن ومفتاح تشفير ومن ثم يقوم جهاز الحاسوب بالتأكد من القيمة التي تم

توليدها بإستخدام نفس الية التوليد وهو ما يعرف Time-synchronized one-time passwords, ويعتبر هذا النوع أكثر فعالية ولكن ذو تكلفة مالية عالية.

- مفاتيح Passive Token: يعتمد هذا النوع من المفاتيح علي قيم مسجلة بطريقة مشفرة ولايمكن مسحها أو إعادة الكتابة عليها إلا عبر الشركة المصنعة لذلك, ليقوم النظام المراد تأمينه عبر هذه المفاتيح بقراءة القيمة المسجلة ومقارنتها, ويعتبر هذا النوع أقل تكلفة ولكنه أيضا ذو كفاءة تأمينية متوسطة إذ يمكن للمخترق الوصول للمعلومات المسجله بسهولة وعمل مفتاح محاكي يحمل نفس المعلومات الموجودة بالمفتاح الحقيقي.

3.3 مخططات ونماذج وصف النظام الحالي

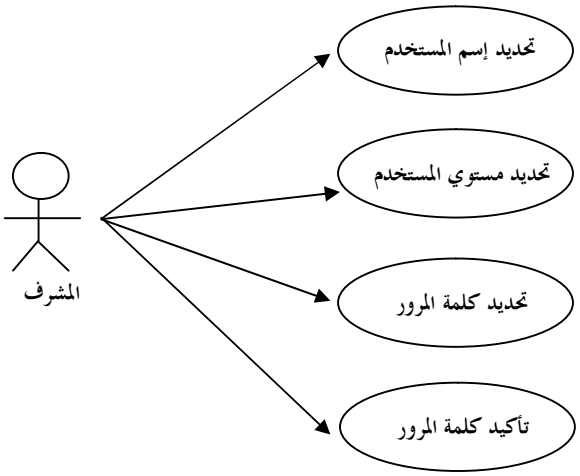
من خلال تحليل العملية المتبعة حاليا للتحقق من هوية المستخدمين في بيئة نظام التشغيل ويندوز وبإستخدام

لغة النمذجة الموحدة UML يمكننا تكوين النماذج و المخططات الأتية:

حالة الإستخدام	إضافة حساب مستخدم جديد لإستخدام نظام التشغيل
وصف مختصر	تمثل حالة الإستخدام هذه العملية الرئيسية التي يتم من خلالها منح المستخدمين صلاحيات لإستغلال موارد الجهاز من خلال إستخدام نظام التشغيل.
شروط سابقة	لابد من إمتلاك الشخص القائم بهذه المهمة علي حساب إستخدام مسبق لنظام التشغيل وصلاحية تمكنه من القيام بذلك
شروط لاحقة	بعد إنتهاء عملية تسجيل الحساب لابد من إعادة تشغيل النظام أو الخروج من حساب الشخص المنشأ للحساب للدخول بالحساب الجديد.
المجريات الأساسية	في حالة الإستخدام هذه لابد من إدخال إسم المستخدم وتحديد مستوي الإستخدام وإدخال كلمة

	المرور ومطابقتها.

شكل رقم (1.3) نموذج لتوصيف حالة الإستخدام لإضافة حساب مستخدم في ويندوز

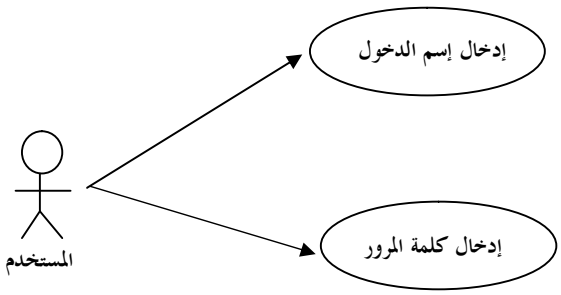


شكل رقم (2.3) مخطط حالة إستخدام يوضح إضافة مستخدم في ويندوز

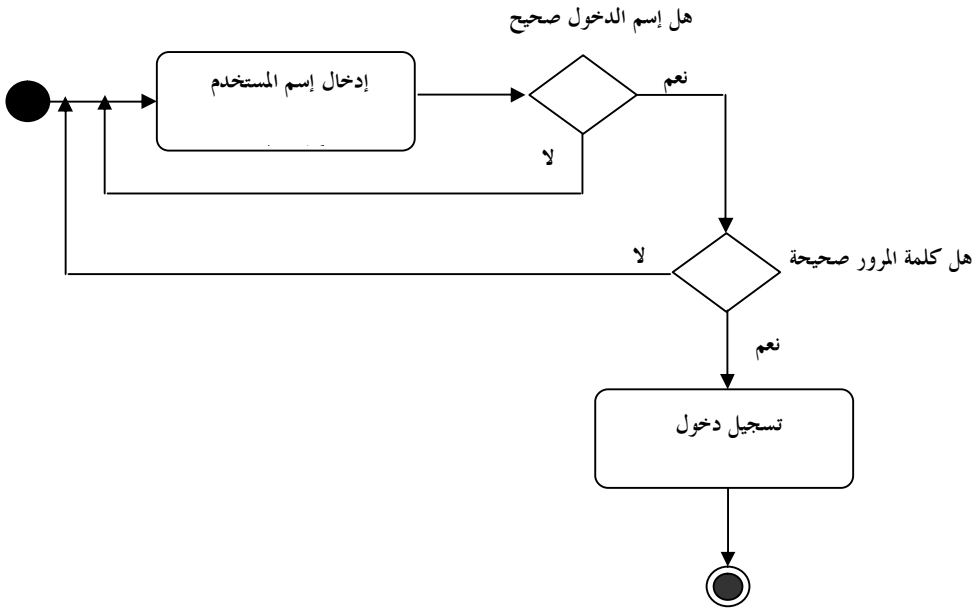
حالة الإستخدام	تسجيل دخول المستخدمين في نظام التشغيل ويندوز
وصف مختصر	تمثل حالة الإستخدام هذه العملية الرئيسية التي يتم من خلالها دخول المستخدمين علي نظام التشغيل.

شروط سابقة	لابد من إمتلاك المستخدم لحساب دخول مسبق كما هو موضح في الشكل رقم (1.3).
شروط لاحقة	لاتوجد شروط لاحقة إذا ما تمت عملية تسجيل الدخول بصورة صحيحة أما إذا حدث عكس ذلك سيقوم المستخدم بإعادة العملية مرة أخري.
المجريات الأساسية	في حالة الإستخدام هذه لابد من إدخال إسم المستخدم وكلمة المرور الخاصة بالمستخدم ليقوم النظام بعد ذلك من التحقق.

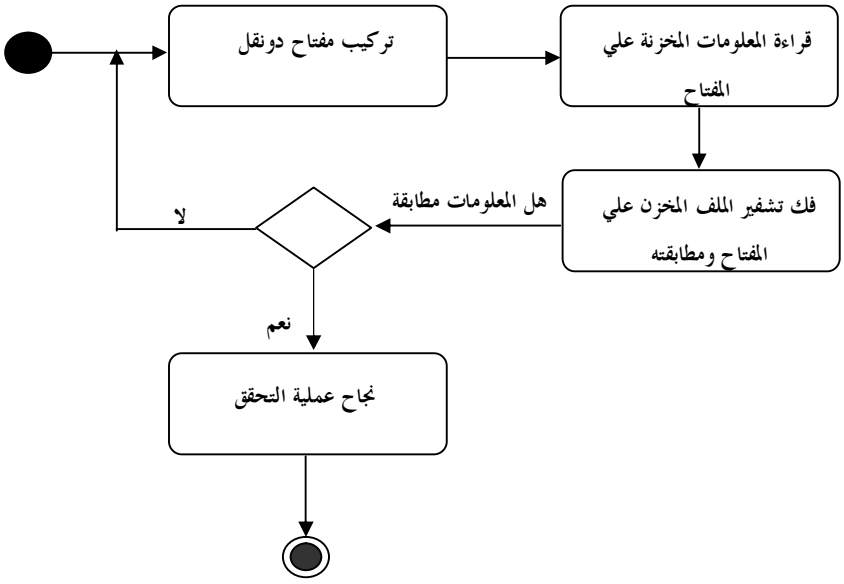
شكل رقم (3.3) نموذج لتوصيف حالة الإستخدام لتسجيل دخول المستخدمين



شكل رقم (4.3) مخطط حالة إستخدام يوضح تسجيل دخول المستخدم في ويندوز



شكل رقم (5.3) مخطط نشاط يوضح التحقق من هوية المستخدم في نظام التشغيل ويندوز



شكل رقم (6.3) مخطط نشاط يوضح ألية التحقق عبر مفتاح Passive Token

4.3 تحليل الحالة التطبيقية للبحث

يري الباحث أن تحليل الحالة التطبيقية التي تتناولها الدراسة يمكن وصفه من خلال عمليتين رئيسيتين هما:

1.4.3 عملية التحقق من الهوية

هذه العملية إعتمد الباحث في تطبيقها علي طريقة المفاتيح Passive

Token مستخدما منفذ USB وأجهزة الفلاش ديسك ولكن بإستخدامها بشكل مختلف عن الطريقة المتبعة بحيث يعتمد نظام التحقق علي قراءة الرقم التسلسلي للفلاش ديسك ومن ثم تشفيره لإستخدامه بدلا عن ملفات مخزنة مسبقا وذلك نظرا لأن تسجيل الملفات يحتاج إلي تصنيع قطع خصيصا لهذا الغرض مما يؤدي الي زيادة في تكلفة نظام التأمين, كما أن كتابة المعلومات مباشرة علي المفتاح تسهل من الوصول اليها ومحاولة تحليلها من قبل المخترقين.

بدراسة الطريقة المستخدمة حاليا في التحقق من الهوية في أنظمة التشغيل والتي يحاول الباحث تطويرها ومعالجة سلبياتها لم تقم الدراسة بالاستغناء عنها ولكن قامت بتطوير طريقة أخري تعمل جنب علي جنب مع الطريقة الموجودة والتكامل معها لتقديم نموذج تأميني ذو كفاءة عالية دون إضافة وحدات عتاد جديدة من شأنها زيادة تكلفة النظام, وتمثلت عملية تكامل الطريقتين في تقديم نموذج تأميني يجمع بين منهجية التحقق بإستخدام الأشياء المعروفة تمثلها تقنية كلمات المرور المستخدمة مسبقا ومنهجية التحقق

بإستخدام الأشياء المملوكة تمثلها تقنية مفاتيح الفلاش ديسك المستخدمة في هذا البحث, ونجد أن الباحث إعتمد علي بيانات المستخدمين المسجلين مسبقا علي نظام التشغيل وإسناد أرقام المفاتيح المشفرة وذلك حتي يتحقق التكامل بين الطريقتين والإستفادة من كافة الإمتيازات التي تقدمها كل طريقة بصورة منفردة.

2.4.3 عملية كشف محاولة الإختراق

قدم الباحث في هذه العملية ألية لكشف المحاولات بالدخول الغير مصرح به علي نظام التشغيل وتعتمد هذه الألية علي تقنية خدمة الرسائل القصيرة وذلك بإستخدامها لإرسال رسالة نصية الي رقم الهاتف الجوال الخاص بشخص يتم تعريفه كمدير للنظام. بالنظر لهذه العملية نجد أن هذه العملية ترتبط إرتباط مباشر بالعملية الأولي أي عملية التحقق حيث تبدأ هذه العملية بعد رصد العملية الأولي لثلاث محاولات غير ناجحة سواء كان ذلك من خلال محاولة الدخول دون تركيب مفتاح أو تركيب مفتاح غير مصرح له بالدخول.

5.3 تحليل الإجراءات

هنالك عدة إجراءات لابد من إتباعها لإكمال العمليات المراد تطبيقها في النظام المقترح من قبل الباحث ويتم تنفيذ هذه الإجراءات من خلال عدة مستويات هنالك إجراءات تتم عبر مستوي المشرف علي النظام وأخري عبر مستوي المستخدمين العاديين إضافة لبعض ألإجراءات التي يقوم بها النظام من تلقاء نفسه بإستدعاء بعض الوظائف البرمجية المتعلقة بنظام التشغيل ويندوز ويمكن تقسيم هذه الإجراءات الي:

- إضافة / تعديل البيانات الخاصة بجهاز الحاسوب.
- إضافة / بحث/ تعديل / حذف بيانات المستخدمين المسجلين علي نظام التشغيل.
- إضافة / بحث/ تعديل / حذف بيانات المفاتيح.
- تفعيل / إيقاف المفاتيح المسجلة.
- إضافة / تعديل بيانات جهاز إرسال الرسائل القصيرة.
- تفعيل / إيقاف خدمة التنبيه بإستخدام الرسائل القصيرة.

- إضافة / تعديل بيانات المشرف المستلم للرسائل التنبيهيه عند محاولات الإختراق.

6.3 تحليل المكونات

في هذه الدراسة نجد أن الباحث قام بإعادة إستخدام لبعض المكونات البرمجية والعمل علي تكاملها في إطار عمل يمثل النظام المقترح حيث يمثل كل مكون من المكونات وظيفة يحتاجها النظام لتحقيق هدفه ويمكن تقسيم هذه المكونات:

- Windows API للتعامل مع بعض وظائف نظام التشغيل بطريقة برمجية.
- RSA Encryption لتشفير بيانات المفاتيح.
- SMS Active X لإرسال الرسائل التنيهية.

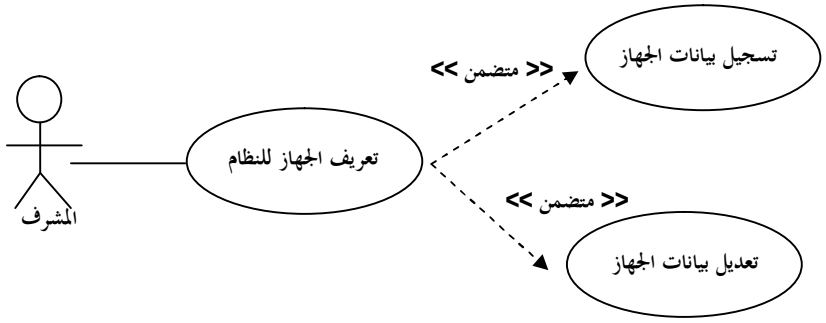
7.3 مخططات ونماذج وصف لإجراءات النظام المقترح

بعد عرض المخططات والنماذج التي تتناول تحليل الوضع الحالي سيتم توصيف النظام المراد بنائه وإختباره علي الحالة التطبيقية للبحث لتوضيح التفاعلات بين المستخدمين والنظام والإجراءات التي يجب القيام بها وذلك من خلال تكوين النماذج والمخططات الأتية:

حالة الإستخدام	تعريف جهاز الحاسوب المراد تأمينه للنظام
وصف مختصر	تمثل حالة الإستخدام هذه العملية الرئيسية التي يتم من خلالها تسجيل وتعديل معلومات جهاز الحاسوب علي النظام المقترح.
شروط سابقة	لابد من إمتلاك المستخدم لصلاحية القيام بهذه العملية.
شروط لاحقة	لاتوجد شروط لاحقة إذا ما تمت عملية تعريف الجهاز للنظام بطريقة صحيحة.
المجريات الأساسية	في حالة الإستخدام هذه يقوم النظام بإستدعاء بعض المعلومات الخاصة بالجهاز مثل إسم

	الكمبيوتر والرقم المتسلسل للقرص الصلب ليقوم المستخدم بتحديد حرف سواقة القرص المراد المراد إستخدامه لتعريف مفاتيح الدخول ليتم بعد ذلك حفظ هذه البيانات.

شكل رقم (7.3) نموذج لتوصيف حالة إستخدام تعريف جهاز الحاسوب للنظام

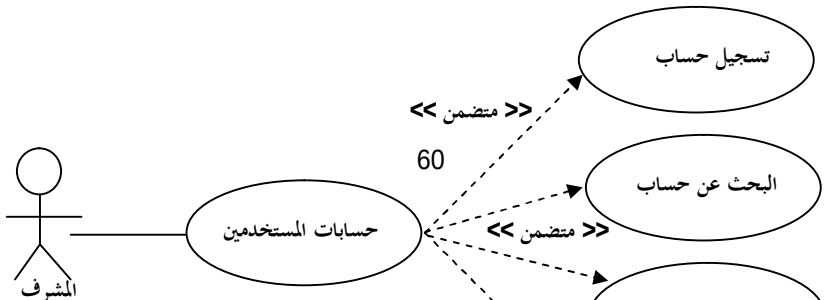


شكل رقم (8.3) مخطط حالة الإستخدام لتعريف جهاز الحاسوب للنظام

حالة الإستخدام	حسابات الدخول لمستخدمي النظام
وصف مختصر	تمثل حالة الإستخدام هذه العملية الرئيسية التي يتم من خلالها إضافة وحذف وتعديل حسابات المستخدمين.

شروط سابقة	- لابد من إمتلاك المستخدم لصلاحية القيام بهذه العملية. - تعريف جهاز الحاسوب للنظام كما هو موضح في نموذج حالة الإستخدام السابقة شكل رقم (7.3)
شروط لاحقة	لاتوجد شروط.
المجريات الأساسية	في حالة الإستخدام هذه يتم إختيار إسم الكمبيوتر الذي تم تعريفه مسبقا وإدخال إسم المستخدم وتحديد نوع الحساب ومن ثم حفظه في قاعدة البيانات , أما فيما يتعلق بإجراء البحث أو الحذف يتم إدخال إسم المستخدم وإستعراض السجل.

شكل رقم (9.3) نموذج لتوصيف حالة إستخدام حسابات دخول المستخدمين

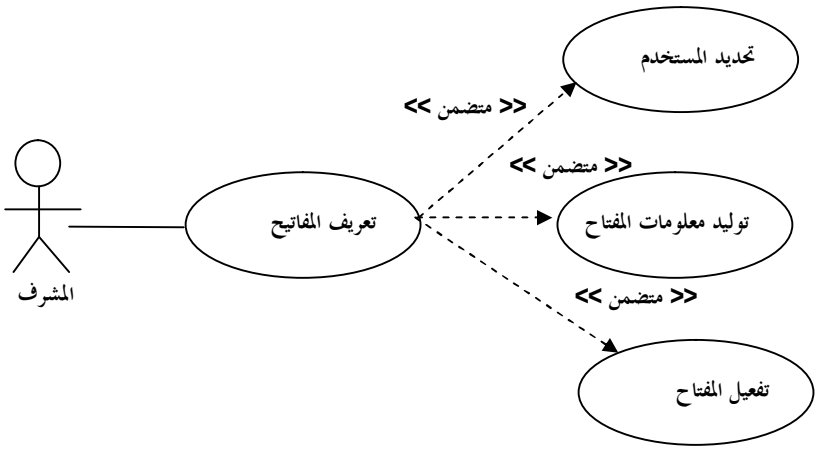


شكل رقم (10.3) مخطط حالة إستخدام
حسابات دخول المستخدمين

حالة الإستخدام	تعريف مفاتيح الدخول
وصف مختصر	تمثل حالة الإستخدام هذه العملية الرئيسية التي يتم من خلالها إضافة معلومات مفاتيح Token.
شروط سابقة	- لابد من إمتلاك المستخدم لصلاحية القيام بهذه العملية. - تعريف جهاز الحاسوب للنظام كما هو موضح في نموذج حالة الإستخدام السابقة شكل رقم (7.3). - تسجيل حسابات المستخدمين كما هو

	موضح في نموذج حالة الإستخدام السابقة شكل رقم (9.3)
شروط لاحقة	لابد من تفعيل المفتاح بعد إضافته.
المجريات الأساسية	في حالة الإستخدام هذه يتم تحديد إسم المستخدم والرقم المتسلسل للمفتاح بعد تشفيره ومن ثم حفظ هذه البيانات في قاعدة البيانات .

شكل رقم (11.3) نموذج لتوصيف حالة إستخدام تعريف دخول المستخدمين

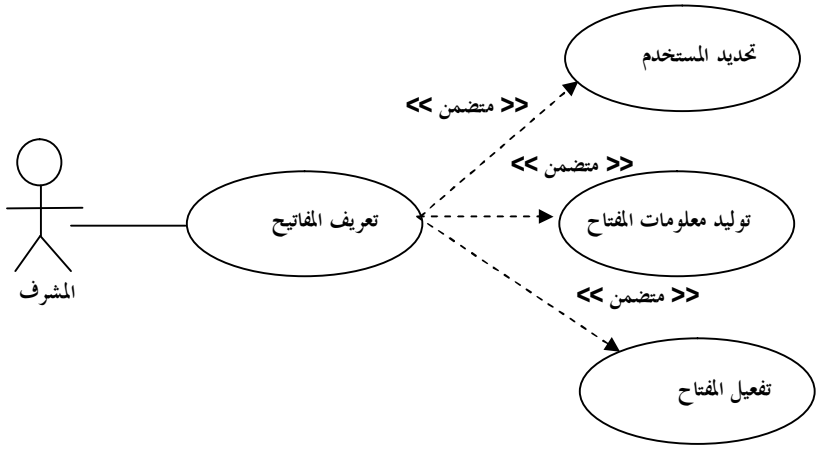


شكل رقم (12.3) مخطط حالة إستخدام تعريف مفاتيح دخول المستخدمين

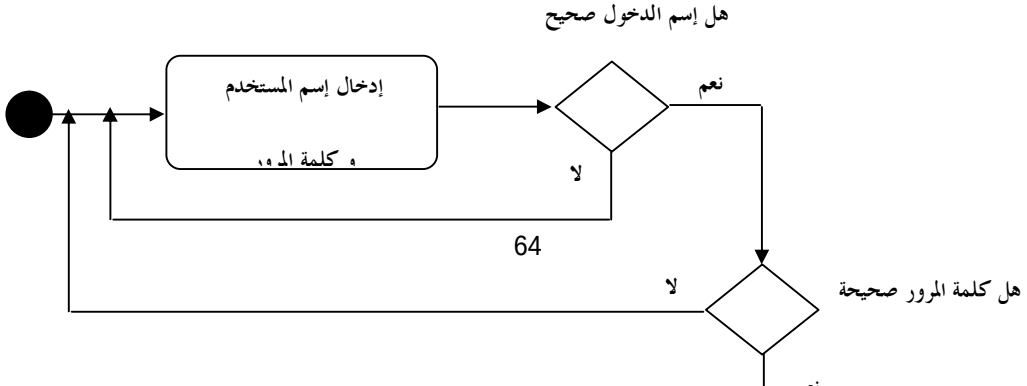
حالة الإستخدام	تفعيل التنبيه عبر خدمة SMS
وصف مختصر	تمثل حالة الإستخدام هذه العملية الرئيسية التي تفعيل خدمة الرسائل النصية القصيرة لإستخدامها كوسيلة تنبيه عند محاولات الدخول الغير مصرح بها.
شروط سابقة	- لابد من إمتلاك المستخدم لصلاحية القيام بهذه العملية. - توصيل جهاز GSM Modem وتعريفه علي نظام التشغيل. - تسجيل حسابات المستخدمين كما هو موضح في نموذج حالة الإستخدام السابقة شكل رقم(3-9)
شروط لاحقة	بعد تفعيل الخدمة يتم إستخدام هذه الخدمة عندما تكون هنالك محاولات دخول غير صحيحة بشرط أن يبلغ عدد هذه المحاولات

	ثلاث محاولات.
المجريات الأساسية	في حالة الإستخدام هذه يتم تحديد رقم المنفذ الذي سيتم إستغلاله من قبل جهاز GSM و تحديد رقم الهاتف الجوال للشخص المستلم للرسائل ومن ثم حفظ هذه البيانات في قاعدة البيانات .

شكل رقم (13.3) نموذج لتوصيف حالة إستخدام تعريف دخول المستخدمين



شكل رقم (14.3) مخطط حالة إستخدام تعريف تفعيل خدمة الرسائل القصيرة SMS



شكل رقم (15.3) مخطط نشاط يوضح ألية التحقق من المستخدمين النظام المقترح

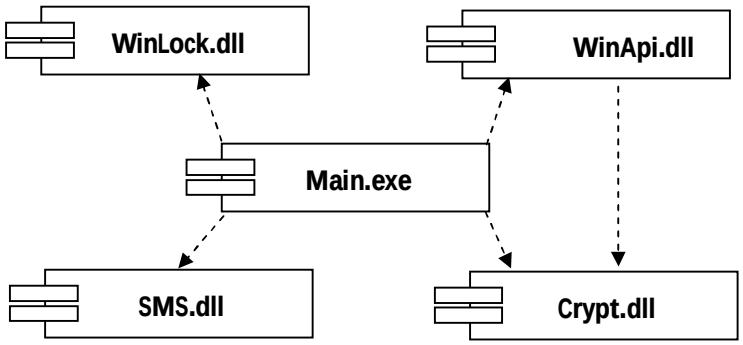
8.3 مخططات ونماذج وصف لمكونات بناء النظام المقترح

إسم المكون	وصف مختصر للمكون

WinLock.dll	يعتبر هذا المكون من أهم المكونات التي يستدعيها النظام ويتم عن طريقه التحكم في بعض وظائف الويندوز بصورة برمجية مثل تعطيل وظائف إختصارات لوحة المفاتيح وظهور سطح المكتب ووظائف الفأره والدخول علي مدير المهام.
SMS.dll	يتم عن طريقه إستخدام خاصية إرسال الرسائل القصيره داخل النظام.
Windows Api.dpl	يتيح التعامل مع مكتبات التعريف المستخدمة من قبل النظام التشغيل للتعامل مع الأجهزة المتصله به مثل القرص الصلب Usb Devices كما يتيح إستدعاء المعلومات من نظام التشغيل مثل إسم الكمبيوتر وإسم المستخدم وغيره.
Crypt.dll	يتم عن طريقه خوارزمية التشفير RSA لتشفير

	البيانات وفك تشفيرها من داخل النظام والتحكم في ذلك برمجيا من داخل لغات البرمجة التي تستخدمها.

شكل رقم (16.3) نموذج وصف للمكونات المستخدمة في بناء النظام المقترح



شكل رقم (17.3) مخطط مكونات البرامج يوضح إعتمادية المكونات في بناء النظام المقترح

9.3 منهجية بناء النظام المقترح

1.9.3 الأدوات

- جهاز حاسوب يعمل علي منصة نظام التشغيل ويندوز 32.
- جهاز GSM Modem به شريحة SIM.
- USB Flash Disk.

2.9.3 البرمجيات

سوف يتم إستخدام لغة البرمجة Borland Delphi7 في تطوير وبرمجة

النظام وذلك نظرا لما تتمتع به هذه اللغة من مرونة في إضافة العديد من المكونات الجاهزة وامكانية تعاملها مع العديد من محركات قواعد البيانات بصورة مباشرة. ويمكننا تعريفها بأنها لغة برمجة من إنتاج شركة بورلاند مبنية علي لغة باسكال الكائنية حيث تعتبر تطويراً للغة باسكال القديمة. تستخدم دلفي لتطوير البرامج والتطبيقات بشكل سريع ولذلك يشار إليها بأنها ذات صفة بيئة تطوير متكاملة R.A.D وهذه الصفة تعني تطوير البرامج بسرعة أي Rapid Application Development وذلك يتحقق باستخدام مكونات وأدوات جاهزة تنسق بالشكل المطلوب ويتم برمجتها بكتابة عدة برامج مرتبطة بأحداث معينة خاصة بهذه المكونات أو العناصر ويشار إلي هذا النوع من البرمجة بالبرمجة بالأحداث.

هذا فيما يتعلق بلغة البرمجة التي سيتم إستخدامها لبناء النظام ولكن هنالك أيضا بعض البرامج والأدوات المساعده التي يمكن الإستعانه بها مثل برنامج التصميم الشهير Adobe Photo Shop الذي يمكن إستخدامه في تصميم ومعالجة الصور التي يمكن وضعها علي

واجهات النظام حتي تكون مقبولة الشكل ومريحة في التعامل معها من قبل المستخدمين.

3.9.3 تحليل المدخلات

يعتمد النظام المقترح تطبيقه علي بعض البيانات التي لابد من تسجيلها حتي يتم إستدعائها من قبل النظام عند تشغيله, وسيتم إنشاء قاعدة بيانات بواسطة برنامج محرك قاعدة البيانات Microsoft SQL Server 2000 ونجد أن الإختيار قد وقع علي هذا النوع من قواعد البيانات من قبل الباحث حتي تكون هنالك المزيد من التوافقية خاصة أن هذا النوع من محركات البحث هو أحد منتجات شركة مايكروسوفت وهي نفس الشركة المنتجة لنظام التشغيل ويندوز الذي يمثل إطار العمل للحالة التطبيقية في هذا البحث.

بعد تحليل البيانات بصورة تسمح من سهولة تكاملها والوصول لها من قبل النظام المقترح تطبيقه بصورة سليمة, تم تصنيف البيانات التي سيتم إدخالها علي قاعدة البيانات لاحقا علي النحو التالي:

- **معلومات الجهاز**

يتم إدخال إسم الكمبيوتر, الرقم المتسلسل للقرص الصلب, حرف سواقة القرص كما في الجدول (1.3).

- **معلومات المستخدمين**

يتم إدخال إسم المستخدم, الرقم المتسلسل للقرص الصلب, نوع المستخدم كما موضح في الجدول (2.3).

- **معلومات المفاتيح**

يتم إدخال الرقم المتسلسل للقرص الصلب, شفرة المفتاح, حالة المفتاح كما موضح في الجدول

(3.3).

- **معلومات خدمة SMS**

يتم إدخال إسم المستخدم, رقم الجوال, رقم المنفذ, حالة الجهاز كم موضح في الجدول (4.3).

10.3 الجداول المستخدمة وقاموس البيانات

جدول رقم (1.3) جدول معلومات الجهاز

إسم الحقل
إسم الكمبيوتر
الرقم المتسلسل للقرص الصلب
سواقة القرص
رقم متسلسل للسجل

جدول رقم (2.3) جدول معلومات المستخدمين

إسم الحقل
إسم المستخدم
الرقم المتسلسل للقرص الصلب
نوع المستخدم

جدول رقم (3.3) جدول معلومات المفاتيح

إسم الحقل
الرقم المتسلسل للقرص الصلب

شفرة المفتاح
حالة المفتاح

جدول رقم (4.3) جدول خدمة SMS

إسم الحقل
إسم المستخدم
رقم الجوال
رقم المنفذ
حالة الجهاز

جدول رقم (5.3) قاموس البيانات لجدول معلومات الجهاز

إسم الحقل	نوع البيانات	الطول	الترميز	الوصف
رقم متسلسل للسجل	رقمي	10	drive_id	رقم تلقائي
إسم الكمبيد	حرفي	100	computer_name	

وتر				
رقم متسلسل للقرص الصلب	حرفي	100	hard_volum	مفتاح أساسي
حرف سواقة القرص	حرفي	2	drive_letter	

جدول رقم (6.3) قاموس البيانات لجدول معلومات المستخدمين

إسم الحقل	نوع البيانات	الطول	الترميز	الوصف
رقم متسلسل للقرص الصلب	حرفي	100	hard_volum	مفتاح أجنبي
إسم مستخدم ويندوز	حرفي	70	windows_user	مفتاح أساسي

نوع المستخدم	حرفي	10	usr_level	

جدول رقم (7.3) قاموس البيانات لجدول معلومات المفاتيح

إسم الحقل	نوع البيانات	الطول	الترميز	الوصف
إسم مستخدم ويندوز	حرفي	70	windows_user	مفتاح أجنبي
شفرة المفتاح	حرفي	255	key_code	مفتاح أساسي
حالة الإستخدام	حرفي	10	usr_status	

جدول رقم (8.3) قاموس البيانات لجدول معلومات جهازGSM

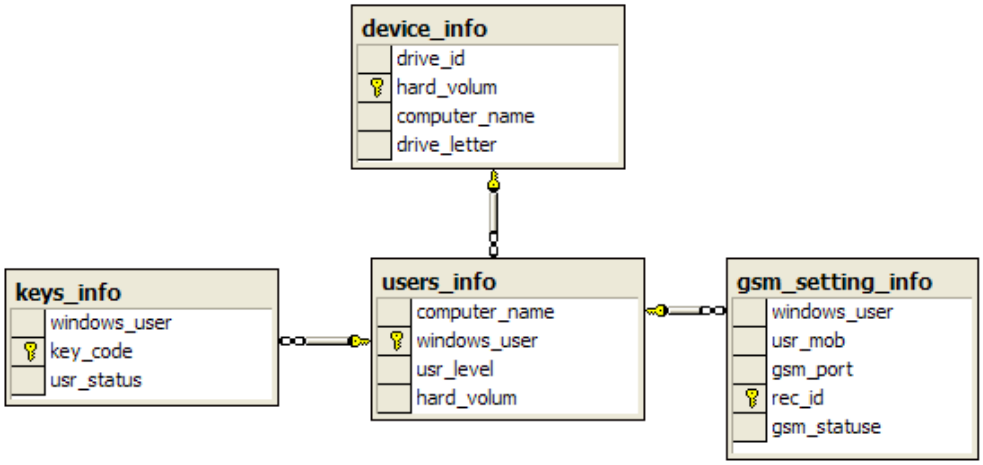
إسم الحقل	نوع البيانات	الطول	الترميز	الوصف

متسلسل للسجل	رقمي	3	rec_id	مفتاح أساسي
إسم مستخدم ويندوز	حرفي	70	windows_user	مفتاح أجنبي
رقم جوال المستخدم	حرفي	20	usr_mob	
منفذ البورت	رقمي	3	gsm_port	
حالة الجهاز	حرفي	10	gsm_statuse	

11.3 علاقات الكيانات

هنالك علاقات تربط الكائنات مع بعضها البعض ويمكن وصفها علي النحو التالي:

- علاقة واحد الي متعدد بين جدول Device_info وجدول User_Info.
- علاقة واحد الي متعدد بين جدول User_Info وجدول Key_info.
- علاقة واحد الي واحد بين جدول User_Infoوجدول Gsm_Info



شكل رقم (18.3) يوضح العلاقات بين الجداول المكونة لقاعدة بيانات النظام