ublic of Yemen
try of Higher Education
d Scientific Research
Future University
culty of Engineering
Information Systems
n Information Systems

Offices Security System

نظام حماية المكاتب

إعداد الطالب

عبدالعزيز أحمد عبدالرحمن الكبسي

أشراف

د / وديع القباطي
د / محمود القباطي

أُنجز هذا المشروع كجزء من متطلبات نيل شهادة البكالوريوس في قسم نظم المعلومات
الافتتاحية
٢٠١٩-٢٠٢٠

{ يأيها الذين ءأمنوا اصبروا وصابروا ورابطوا واتقوا الله لعلكم تفلحون }

آل عمران (٢٠٠)

اهدي ثمرة بحثي الى .....

أمي رمز العطاء و الحنان الدائمين

والى روح والدي العزيز الذي تمنى أن يراني مهندسٍ عظيمً

والى أختي التي ساندتني في كل مراحل دراستي

والى زوجتي التي واستني في ظروفي القاسية

ومسك الختام إلى كل من وقف إلى جانبي

ومد لي العون في إتمام هذا البحث

الباحث

الحمد الله رب العالمين والشكر لفضلة الذي شملنا بواسع رحمتة ووفقنا لأنجاز هذا البحث .

يسرني ان اتقدم بالشكر والتقدير إلى:

الدكتور الفاضل / وديع

الدكتور الفاضل / محمود القباطي

المشرفان على المشروع

والذي كان لهم دور كبير في تشجيعي لإتمام هذا المشروع وابداء الآراء و الملاحظات حول المشروع لإنجاز المشروع بالصورة المطلوبة ، كما اتقدم بالشكر الجزيل لكل من مد لي يد العون في اتمام هذا البحث .

فجزا الله الجميع كل خير ووفقهم لما يحب ويرضى .

قائمة الجداول

الموضوع	رقم الصفحة
الجدوى الاقتصادية جدول رقم ١.١	٣
جدول القطع و الأجهزة جدول رقم ١.٢	١٠
جدول البرمجيات و الأنظمة جدول رقم ٢.٢	١٠-١٢
جدول المقارنة بين النظام الحديث و القديم رقم ١.٣	١٣
جدول بيانات مستخدمي النظام الأمني رقم ١.٤	٢٨
جدول المزامنة رقم ٢.٤	٢٩

قائمة الاشكال

الموضوع	رقم الصفحة
الخطة الزمنية شكل ١.١	٤
Physical Topology شكل رقم ١.٣	14
Logical Topology شكل رقم ٢.٣	15
مخطط الـ BFDشكل رقم ٣.٣	17
مخطط الـ DFD شكل رقم ٤.٣	18
مخطط تدفق البيانات الصفريه شكل رقم ٥.٣	١٩
مخطط تدفق البيانات الصفريه شكل رقم ٦.٣	١٩
مخطط تدفق البيانات الصفريه شكل رقم ٧.٣	٢٠
مخطط تدفق البيانات الصفريه شكل رقم ٨.٣	٢٠
مخطط تدفق البيانات الصفريه شكل رقم ٩.٣	٢١
مخطط الكينونات العلائقيه شكل رقم ١٠.٣	٢٢
مخطط الكينونات العلائقيه شكل رقم ١١.٣	٢٣
خوارزميه واجهة الأتصال شكل رقم ١٢.٣	٢٤
خوارزميه التحقق من الهوية شكل رقم ١٣.٣	٢٥
خوارزميه أدارة النظام الأمني شكل رقم ١٤.٣	٢٦
خوارزميه عرض التقارير شكل رقم ١٥.٣	٢٧
واجهة النظام الرئيسية شكل رقم ١.٣.٤	٣٠
واجهة الإتصال شكل رقم ٢.٣.٤	٣١
واجهة التحقق من الهوية شكل رقم ٣.٣.٤	٣٢
واجهة إعدادات الموظفين شكل رقم ٤.٣.٤	٣٣
واجهة عرض التقارير شكل رقم ٥.٣.٤	٣٤
واجهة طباعة التقارير شكل رقم ٦.٣.٤	٣٤
الدائرة الإلكترونية شكل رقم ٧.٥.٤	٣٥
تصميم الشبكة شكل رقم ٨.٧.٤	٣٦
واجهة الاتصال صورة رقم ١.٢.٥	٣٨
واجهة التحقق من بيانات المستخدم صورة رقم ٢.٢.٥	٣٩
واجهة تسجيل دخول موظف صورة رقم ٣.٢.٥	٣٩
واجهة التسجيل و تعديل بيانات المستخدمين صورة رقم ٤.٢.٥	٤٠
واجهة عرض و إستخراج التقارير صورة رقم ٥.٢.٥	٤١
نتائج المعلومات التي تم البحث عليها صورة رقم ٦.٢.٥	٤٢
أستخراج التقارير على شكل PDF صورة رقم ٧.٢.٥	٤٣
إعداد الحاسوب صورة رقم ٨.٣.٥	٤٦
فحص الأتصال صورة رقم ٩.٣.٥	٤٧
التنفيذ من ناحية القطع و الإجهزة صورة رقم ١٠.٤.٥	٤٨
عملية السماح بالولوج صورة رقم ١١.٤.٥	٤٩
عملية رفض الولوج صورة رقم ١٢.٤.٥	٥٠

الموضوع	رقم الصفحة

الافتتاحية	II
الاهداء	III
شكر وتقدير	IV
قائمة الجداول	VII
قائمة الأشكال	VII
الفهرس	VII VII
الفصل الاول (المقدمة)	
١.١ تمهيد	١
٢.١ المشاكل المراد حلها	١
٣.١ أهداف المشروع	٢
٤.١ الادوات المستخدمة في المشروع	٢
٥.١ دراسة الجدوى	٢
١.٥.١ الجدوى الاقتصادية	٣
٢.٥.١ الجدوى الفنية	٣
٣.٥.١ دراسة تشغيلية	٣
٦.١ هيكلية البحث	4
٧.١ الخطة الزمنية	٤
الفصل الثاني (الخلفية النظرية)	
١.٢ المقدمة	٥
٢.٢ نبذة عن النظام القديم	٥
٣.٢ طرق حماية أمن المعلومات	٦
١.٣.٢ الوسائل التقنية لحماية المعلومات	٦
٢.٣.٢ الوسائل التنظيمية لحماية المعلومات	٦
٣.٣.٢ الحماية البرمجية للمعلومات	٦
٤.٣.٢ الحد من الوصول إلى البيانات	٧
٤.٢ إدارة أمن المعلومات	٧
٥.٢ النظام الجديد	٨
٦.٢ الأدوات (Tools)	٨
١.٦.٢ القسم المادي (Hardware)	٨
٢.٦.٢ القسم البرمجي (software)	٩
الفصل الثالث (التحليل)	
١.٣ المقدمة	١٣
٢.٣ وصف المشكلة	١٣
٣.٣ البدائل	١٣
٤.٣ مخططات اللوحة الالكترونية	١٤
٥.٣ جمع البيانات	١٦
١.٥.٣ قراءة و تحليل المستندات	١٦
٢.٥.٣ المشاهدة	١٦
٦.٣ توصيف النظام المقترح	١٦
٧.٣ رسم مخطط ال (BFD)	17
٨.٣ رسم مخطط تدفق البيانات ال (DFD)	18
٩.٣ مخطط الكينونات العلائقي	22
١٠.٣ خوارزميات	24
الفصل الرابع (مرحلة التصميم)	
١.٤ المقدمة	28

٢.٤ تصميم قاعدة البيانات	28
٣.٤ تصميم شاشات النظام	29
١.٣.٤ تصميم واجهة النظام الرئيسية	30
٢.٣.٤ واجهة الإتصال (Connection Form)	31
٣.٣.٤ واجهة التحقق من الهوية (Check Data User)	32
٤.٣.٤ واجهة إعدادات الموظفين (Registration & Edit User Data)	33
٥.٣.٤ واجهة عرض التقارير (Reports)	34
٦.٣.٤ واجهة طباعة التقارير	34
٤.٤ الهدف من تصميم الدائرة الإلكترونية	35
٥.٤ تصميم الدائرة الإلكترونية	35
٦.٤ الهدف من تصميم الشبكة	36
٧.٤ تصميم الشبكة	36
الفصل الخامس (مرحلة التنفيذ)	
١.٥ المقدمة	37
٢.٥ التنفيذ من ناحية واجهات ونوافذ النظام	37
١.٢.٥ واجهة الاتصال (Connection)	38
٢.٢.٥ واجهة التحقق من بيانات المستخدم (Check Data User)	39
٣.٢.٥ واجهة التسجيل و تعديل بيانات المستخدمين (Registration & Edit User Data)	٤٠
٤.٢.٥ واجهة عرض و إستخراج التقارير (Reports)	٤١
٣.٥ التنفيذ من ناحية الشبكة	50
١.٣.٥ طريقة تصميم الشبكة	٤٤
٢.٣.٥ الأجهزة و البرامج المستخدمة في الشبكة	٤٤
٣.٣.٥ التقنيات و البروتوكولات المستخدمة في الشبكة	٤٤
٤.٣.٥ أعدادات الشبكة	٤٥
٤.٥ التنفيذ من ناحية القطع والاجهزة المرتبطة بالنظام	٤٨
الفصل السادس (الاستنتاجات والمعوقات والتوصيات)	
١.٦ المقدمة	٥١
٢.٦ الاستنتاجات	٥١
٣.٦ المعوقات	٥١
٤.٦ التوصيات	٥٢
المراجع	**٥٣**

الفصل الأول

المقدمة

الفصل الأول

مقدمة

١.١ تمهيد

يعتبر العلم من أحد أهم معالم التطور في القرن العشرين بحيث أنه ساهم في تطوير العديد من المجالات التي يمارسها الانسان في حياتة ومن أهمها الأمن ، بحيث أن الأمن ساهم بشكل كبير في الحفاظ على أمن وسلامة وخصوصية البيانات والمعلومات على مر العصور .

ليس الأمن بشيء جديد ولكنه كان موجود منذ قديم الزمان حيث انه كان يتم أستخدامة من بدايه العصور الحجرية و يستخدم أدوات قديمة مثل الغرف و الابواب و الاقفال الى جانب ذلك وضع حارس او حُراس لحراسه تلك المقتنيات الثمينه و البضائع ، حيث انة كان هنالك مشاكل عديدة مثل ضياع المفاتيح و كسر الاقفال و جهل معرفة من يستخدم المفاتيح ولا يتوفر وجود صلاحيات كما انه يكون دور الحارس غير كاف حيث انه لا يلتزم بموقعة أو في وقت أداء واجبة ، الان سوف نتطرق الى القرن العشرين حيث يتأثر بشكل كبير من ناحية الأمن و في مجالنا سوف نذكر العديد من المشاكل التي تواجهها الشركات و المؤسسات الحكومية و الخاصة من الناحية الأمنية وبهذا نقصد أمن و سلامة المعلومات بحيث لا زال يتم استخدام المفاتيح و الاقفال لحماية مكاتب الموظفين و مخازن البيانات و ايضاً لا زال يتم أستخدام الباسورد في الانظمة المعلوماتية بحيث يتم كسر حمايتها وفي هذا المشروع سوف نقوم بتطوير حماية و أمن و سلامة البيانات و المعلومات و أيضا الاشياء المادية مثل ابواب المكاتب و مخازن البيانات مثل مخزن البيانات (داتا سنتر) و أيضا الاشياء التي تخص الانظمة .

٢.١ المشاكل المراد حلها

١- عدم توفر نظام خاص بأمن المكاتب الادارية .
٢- عدم توفر نظام خاص بحماية مخازن البيانات والمعلومات .
٣- عدم توفر نظام خاص بحماية الانظمة المعلوماتية .
٤- عدم توفر نظام خاص برقابة الموظفين .
٥- عدم توفر الصلاحيات الولوج إلى المكاتب أو الانظمة أو مخازن البيانات .
٦- الدخول الغير المصرح بة .
٧- ضياع المفاتيح و فقدانها و عطب الاقفال .

الفصل الأول

مقدمة

١.٣ أهداف المشروع

١- تصميم نظام خاص بأدارة أمن المعلومات..
٢- تصميم نظام فرعي مرتبط مع النظام السابق يختص بنوع خاص من تقنيات التأمين الحديثة.
٣- تأمين المكاتب والانظمة المعلوماتية ومخازن البينات من خلال ما تم ذكرة في النقاط السابقة.
٤- توفير وتوزيع صلاحيات الولوج الى المكاتب أو الانظمة أو مخازن البيانات .
٥- توفير الرقابة على الموظفين.
٦- منع الدخول الغير مصرح به.
٧- عدم الأحتياج إلى المفاتيح او الأقفال وذلك من خلال استخدام تقنيات التأمين حديثة.

١.٤ الادوات المستخدمة في المشروع

الادوات التي تستخدم في بناء النظام تنقسم الى :

١- الادوات المادية :

- جهاز حاسوب .
- لوحة التحكم التي سيتم برمجتها .
- لوحة الاختبار .
- توصيلات .
- وصلة USB .
- كيبل شبكة .
- خازن كهرباء .
- جهاز الـ RFID .
- البطاقات الممغنطة .

٢- الادوات البرمجية

- برنامج visual studio .
- برنامج تعريف المتحكم .
- برنامج SQL Server .
- برنامج المحاكاة CESCO PACKET TRAZER .

١.٥ دراسة الجدوى

يتطلب هذا الجانب عدد من المراحل لعمل المشروع حيث تم تقسيم الميزانية على حساب الجوانب من مرحلة التحليل الى مرحلة التصميم من ثم الى مرحلة التنفيذ .
فقد اخذت مرحلة التصميم نصيب الاسد من الميزانية بسبب اهميتة في مرحلة عمل النظام وبل لأضافة شراء برامج التصميم و البرامج الداعمة للنظام و البحث عن أجهزة مناسبة يعمل هذا النظام بشكل مرن وسريع الاداء ودقةُ العالية.

الفصل الأول

مقدمة

١.٥.١ الجدوى الاقتصادية :-

المقصود بدراسة الجدوى الاقتصادية هي تلك المتعلقة بنواحي المالية لمعرفة أن كان المشروع المراد أنشائة قابل للتنفيذ أم لا من الناحية الاقتصادية و ذلك من خلال معرفة تكاليف المشروع (النظام الجديد) المقترح.

- يبين الجدول التالي التكلفة التشغيلية للنظام الجديد :-

Part	Type	Count	Unit. Price	Total
-Laptop	CPU Core I5 RAM 4GB HDD 1 TB	1	400$	400$
Arduino	Mega	2	15$	30$
Pins	Male & Female ports	40	2$	2$
LED	Bar Graph Display	10	5$	5$
Check List	Bread Board	1	5$	5$
RFID	RC522	1	8.3$	8.3$
			Total	450.3$

الجدوى الاقتصادية جدول رقم ١.١

٢.٥.١ الجدوى الفنية

النظام الجديد هو عبارة عن نظام حماية تحت مسمى (security cards) وهذا النظام يخدم كافة الشركات و المؤوسسات الحكومية و الخاصة في جميع مجالات الأمن و الحماية وهو عبارة عن نظام أمني يتكون من مكونات مادية و برمجية .

٣.٥.١ دراسة تشغيلية

المشروع قابل للتشغيل و الادارة من قبل موظفي أدارة تقنية المعلومات في اي مؤوسسة حكومية او خاصة في العالم وذلك عندما تنطبق الشروط الواجب توفرها عند تشغيل النظام .

١. التحليل Analysis
٢. التصميم Design
٣. التنفيذ Action
٤. الصيانة maintenance

الفصل الأول

مقدمة

٦.١ هيكلية البحث

تم تقسيم البحث إلى ستة فصول ، الفصل الأول يتضمن اساسيات البحث حيث يتطرق إلى مشكلة البحث و أهداف البحث ، الفصل الثاني ويتضمن الخلفية النظرية للبحث حيث يتطرق الى ماهي أدارة أمن المعلومات للبنوك وطرق الحماية و أنواعها و النظام الجديد ، الفصل الثالث ويتضمن وصف المشكلة و دراسة الجدوى الفنية و الاقتصادية و الادوات المستخدمة في المشروع و إيجاد البدائل و المخططات الرئيسية لنظام الحماية و الخطة الزمنية للمشروع و مخططات تدفق البيانات و الكينونات و الخوارزميات ، الفصل الرابع ويتضمن التصميم التفصيلي للنظام من حيث يتضمن تصميم قاعدة البيانات الخاصة بنظام الحماية والمخططات الخاصة بالدائرة الاكترونية و كذلك الواجهات الخاصة بالنظام ، الفصل الخامس ويتضمن البناء الفعلي للنظام من ناحية التنفيذ و التشغيل و الاختبار ، الفصل السادس ويتضمن الاستنتاجات و المقترحات و التوصيات .

٧.١ الخطة الزمنية

- يبين الجدول التالي الخطة الزمنية (الخطة المقترحة و الفعلية) لتنفيذ المشروع :-

الخطة الزمنية شكل ١.١

الفصل الثاني

الخلفية النظرية

الفصل الثاني

الخلفية النظرية

١.٢ المقدمة

يعتبر التعليم طريقاً وممراً أمنا كل من يرغب الى الوصول الى درجة عالية من العلم ولتحقيق اهدافه المستقبلية و من خلال هذا الطريق استطاع الانسان اكتشاف و اختراع كل ماهو موجوداً في الوقت الحالي وكل شيء يخدم الانسان ويساعده في إدارة شؤنه في جميع المجالات سواء كانت هندسية او اقتصادية او طبية او عسكرية او خدمية او عملية او علمية .....الخ .
بحيث أنه تم التطوير في المجال الأمني على نطاق واسع في مجال التكنولوجيا الحديثة ، حيث ساهم هذا التطوير في زيادة وترقية المستوى الأمني فيما يختص بالاشياء المادية مثل الأبواب ، و الخزائن و بنسبة للأشياء المعلوماتية و البرمجية أو بكل ما يختص في (software) من ناحية تأمين الأنظمة بأستخدام الباسورد أو بما تعرف بكلمة المرور ومع تطور التقنيات الحديثة في مجال الحماية تم الوصول الى ما يعرف الان بلبصمة وتطورت و تفرعت تقنيات البصمة أبتداءٍ ببصمة الإبهام وتليها بصمة الوجة و تطورت تقنايات البصمة الى بصمة العين وأما في الوقت الحاضر تم التوصل الى أحدث وأعلى تقنيات البصمة الى بصمة الحمض النووي DNA ، ولاكن كل هذه التقنيات تتعلق بجسم الانسان لاكن نحن سوف نستخد إيحدى تقنيات البصمة التي لا تتعلق بجسم الانسان وهي التي تسمى بالمفاتيح وهي RFID CARD هي عبارة عن بطاقة تكون ممغنطة بلكامل ويكون المفتاح او الرقم التسلسلي مشفراً ولا يتكرر وفي مشروعنا سوف نقوم بجعل هذه البطاقة تقوم بعمل البصمة او بما يعرف بلبصمة الاكترونية .

٢.٢ نبذة عن النظام القديم

فإذا تكلمنا عن من كان يستطيع الدخول الى أي غرفه في بنك او في أي شركه فهو ممكن أن يدخل اي شخص دون العلم من دخل ولا كيف دخل ولو كانت بالطريقة التقليدية الذي هي المفاتيح و الاقفال و كما تطور العلم و اوجد لنا بصمة الاصبع و بصمة الوجه و ما شابة و إنما اوجد شي يعتبر أمن بشكل افضل الا وهو البطائق الممغنطة ، حيث كانت تضيع المفاتيح ويتم الاعاقة في الاعمال حتى يتم إيجاد المفتاح أو كسر القفل أو مغلقة الباب و بهذا يكون قد أهدرنا وقت كبير في فتح باب مهم و خسرنا عمل أو عدة أعمال وكذلك ارباح قد ربما تزايدت لو كان هناك حل لهذه المشكله كذلك عند ضياع المفتاح ربما يحصله شخص أخر ليس ذو ثقه و قد يتسبب في أي مشاكل قد تضر بالعمل أو بالاموال التي في تلك الغرفه ، إيضاً لو تحدثنا عن التطور التكنولوجي فنجد أنهُ قد دخل الأمن في الحاسوب و أمن البيانات فتم التطوير لتلك البيانات و عملية الأمن في وضع كلمة مرور أو ما يسمى ب password في اللغة الانجليزية كما ان مشاكلها النسيان و صعوبة حفظها .

- **المشاكل الموجودة في النظام القديم**

١. ضياع المفايتح و تعطب الاقفال.
٢. صعوبة في حل المشكله بشكل سريع .
٣. نسيان كلمة المرور .

الفصل الثاني

الخلفية النظرية

٤. تعرض كلمة المرور للإكتشاف من أشخاص آخرين .
٥. قد تكون كلمة السر لعدة حسابات او عدة اشياء فيكون الضرر أكبر .

٣.٢ طرق حماية أمن المعلومات

١.٣.٢ الوسائل التقنية لحماية المعلومات

يُمكن حماية المعلومات والحفاظ عليها من خلال الوسائل التقنية الآتية:

- عمل نسخة احتياطية عادية، وحفظ أهمّ ملفات البيانات من خلال تقنية التخزين عن بعد.
- عمل نسختين احتياطيتين لجميع النظم الفرعية للشبكة المتعلقة بأمن البيانات.
- إمكانية استدعاء مصادر الشبكة عند حدوث خلل بسبب المستخدمين.
- تشغيل أنظمة تزويد الطاقة الكهربائية الاحتياطية عند حدوث خلل ما.
- التأكد من حماية المعلومات من التلف في حال حدوث حريق أو وصول ماء إليها.
- تثبيت البرامج التي تمنع الوصول إلى قواعد البيانات أو أيّ معلومات لمن ليس لديهم الحق في ذلك.

٢.٣.٢ الوسائل التنظيمية لحماية المعلومات

- يتمّ حماية المعلومات بوسائل تنظيمية للشركات وهي كالآتي:
- تخصيص لوائح لقوانين العمل على أجهزة الكمبيوتر والمعلومات السرية.
- تقديم التوجيهات للموظفين، والتفتيش الدائم عليهم، وإبرام عقود مُوقَّعة تُحدّد المسؤولية التي يتحملها الموظف في حال إساءة استخدامه للمعلومات الخاصة بالعمل أو إفشائها.
- تنظيم حدود المسؤولية لتفادي وجود موظف واحد فقط له حق التصرف بملفات البيانات الحساسة.
- توحيد برامج حماية البيانات من النَّسخ أو التدمير لجميع المستخدمين بمن فيهم الإدارة العليا.
- تطوير آليّة استعادة النظام في حالة فشله لسبب ما.

٣.٣.٢ الحماية البرمجية للمعلومات

تستطيع الطرق البرمجية حماية المعلومات بالشكل الآتي :

- طلب الكمبيوتر كلمة مرور عند إعادة التشغيل، وعليه يجب معرفة كيفية اختيار كلمة مرور قوية، والمحافظة عليها بالاستعانة بأدلة الأمان الأساسية الموجودة في أنظمة التشغيل Windows و Linux .
- تشفير عملية تخزين البيانات والمعلومات على أجهزة الكمبيوتر، والأجهزة اللوحية، والأجهزة الذكية.
- تشغيل قفل الشاشة في حال ترك الكمبيوتر، وذلك متاح في أنظمة Windows ، وLinux ، و Mac ، فهي تحتوي على اختصارات تُمكِّن إجراء ذلك بسرعة وسهولة .

الفصل الثاني

الخلفية النظرية

- استخدام خصائص BIOS الخاصة بنظام الحماية والموجودة في إعدادات الكمبيوتر، بحيث تمنع أولاً الدخول إلى نظام التشغيل من جهاز USB أو CD-ROM أوDVD ، ثمّ يتمّ تحديد كلمة مرور قوية على BIOS نفسه بحيث لا يتمكن المتطفل من تغيير طريقة الدخول .

٤.٣.٢ الحد من الوصول إلى البيانات

تسمح المنظمات لعدد محدود من الموظفين الوصول إلى بياناتها الحساسة، وعليه يجب معرفة من لديه الحق في الوصول إلى بيانات العملاء الحساسة، مع شرح الحقوق الخاصة بإمكانية وصول كلّ موظف إلى البيانات، حيث إنّ بعض المديرين في الشركات لا يعرفون تفاصيل إمكانية وصول الموظفين إلى البيانات ولماذا يصلون إليها، ممّا يُشكّل خطراً بفقدان البيانات، أو سرقتها، أو عمليات الاختراق، لذلك يجب على المنظمات الحدّ من الوصول إلى البيانات، وعليه من الضروري أن تحدد المنظمة احتياجات الموظفين المخولين بالوصول إلى البيانات، لضمان وصولهم إلى ما يحتاجونه فقط، هذه المحددات ستساعد المنظمات على حماية بياناتها بشكلٍ أكثر كفاءة وتُجنّبها من السرقة أو الفقدان.

٤.٢ إدارة أمن المعلومات

أمن المعلومات بالإنجليزية (Information Security) :علم مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها فمع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لاخر أصبح أمر أمن تلك البيانات والمعلومات يشكل هاجسًا وموضوعًا حيويًا مهمًا للغاية. يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

- إن حماية المعلومات هو أمر قديم ولكن بدأ استخدامه بشكل فعلي منذ بدايات تطور التكنولوجيا ويرتكز أمن المعلومات إلى :-

- أنظمة حماية نظم التشغيل.
- أنظمة حماية البرامج والتطبيقات.
- أنظمة حماية قواعد البيانات.
- أنظمة حماية الولوج أو الدخول إلى الأنظمة.

الفصل الثاني

الخلفية النظرية

٥.٢ النظام الجديد

هو عبارة عن نظام حماية خاص بتأمين الانظمة المعلوماتية وكذلك الولوج الى المكاتب او الاماكن التي تحتاج الى حماية شديدة بحيث يتحمل الشخص الذي يقوم بالولوج الى الاماكن شديدة الحماية بالمسؤولية التامة وهذا النظام يكون مرفوع على السيرفر ضمن شبكة داخلية ، ومن اساسيات بناء هذا النظام الا وهو الاجهزة او القطع الالكترونية التي تلبي هذا الغرض الا وهو الحماية ، نظام الحماية هنا يستخدم تقنية البطائق الممغنطة والتي تحتوي على تقنيات التشفير الحديثة بحيث أن الجهاز الذي يقوم بقراءة هذة البطائق من خلال ترجمة هذه البطائق وتحويلها الى قيمة رقمية من خلال تقنية التشفير ، أما بالنسبة لألية عمل النظام يقوم المستخدم أو الموظف الحامل لهذه البطاقة الممغنطة بوضعها على الجهاز لفتح الابواب أو الولوج الى الحواسيب او الانظمة بحسب نوع الصلاحية التي يمتلكها ، وإيضاً يقوم هذا النظام بتجهيز وعرض التقارير وإيضاً المعلومات الخاصة بكل موظف للمستخدم الرئيسي (Admin).

٦.٢ الادوات (Tools)

هي الادوات التي يجب استخدامها لتنفيذ المشروع و تعتمد على اساس نوعية القطع و الاجهزة التي سيتم استخدامها في المشروع و إيضا البرامج اللازمة لتنفيذ العمل المطلوب .

- **وتنقسم الادوات (Tools) الى قسمين : القسم المادي و القسم البرمجي**

١.٦.٢ القسم المادي (Hardware)

الآردوينو

الآردوينو بالإنجليزية (Arduino) : هو لوح تطوير إلكتروني يتكون من دارة إلكترونية مفتوحة المصدر مع متحكم دقيق يُبرمج عن طريق الحاسب الآلي ، وهو مصمم لتسهيل استخدام الإلكترونيات التفاعلية في المشاريع متعددة التخصصات . يُستخدم الآردوينو بصورة أساسية في تصميم المشاريع الإلكترونية التفاعلية أو المشاريع التي تستهدف بناء حساسات بيئية مختلفة كدرجات الحرارة ، الرياح ، الضوء و الضغط وغيرها... يّمكن توصيل الآردوينو ببرامج مختلفة على الحاسب الشخصي ، ويعتمد في برمجته على لغة البرمجة مفتوحة المصدر بروسيسنج ، وتتميز الأكواد البرمجية الخاصة بلغة الآردوينو أنها تشبهه لغة السي وتعتبر من أسهل لغات البرمجة المستخدمة في كتابة برامج المتحكمات الدقيقة . أثبتت بعض الدراسات أن شرائح الآردوينو تعتبر مدخل مهم يسهل من خلاله معرفة مبادئ عن علوم الحاسب، هندسة الكهرباء والميكانيكا وكذلك الحرف والفنون، مجتمعة في بيئة واحده .

الفصل الثاني

الخلفية النظرية

RFID

الرقاقات الراديو لاسلكية أو التعرف بترددات الراديو الزيد Radio-frequency Identification واختصاراً تعرف بـ تحديد الهوية بموجات الراديو ..

تقنية (تحديد الهوية بموجات الراديو) وتعني (تحديد الهويه باستخدام موجات الراديو) . والتقنيه عباره عن تحديد الهويه بشكل تلقائي بالاعتماد على جهاز يسمى . (RFID Tags) هذا الجهاز (RFID) (Tagsعباره عن كائن صغير يمكن ادراجه بالمنتجات أو الحيوانات أو الإنسان. يحتوي هذا الكائن على شريحة مصنوعه من السيلكون وهوائي (انتينا) لكي يستطيع استقبال وإرسال البيانات والاستعلامات من خلال موجات الراديو.

٢.٦.٢ القسم البرمجي (software)

C Arduino

لغة أردوينو (Arduino) هي مجرَّد مجموعة من دوال C/C++ أي مشتقة بشكل رئيسي من لغة C++ & C وإطاري العمل Wiring و Processing وهي مفتوحة المصدر . تُستخدَم لغة أردوينو في برمجة لوحات أردوينو بمختلف أنواعها ، إذ توحِّد طريقة برمجة اللوحات مهما اختلفت أنواعها والمتحكمات التي تستند عليها ، وتسِّهل عملية البرمجة على أولئك الذين ليس لديهم خلفية برمجية مسبقة . تتميز لغة أردوينو عن لغة - C المشتقة منها - بأنَّها لغة كائنية التوجه ، إذ تحتوي على أصناف وكائنات عديدة مثل الصنف `String` ، و `Stream` .أضف إلى ذلك أن أردوينو غنية بالكثير من المكتبات التي توفر المزيد من الوظائف مثل العمل مع أي قطعة أو عنصر إلكتروني إضافي وتعديل البيانات ...إلخ . لا يُشترَط استعمال لغة أردوينو مع أردوينو IDE فقط بل يمكن استعمالها مع بيئات تطويرية من طرف ثالث مثل Eclipse .

Microsoft Visual Studio

مايكروسوفت فيجيوال ستوديو بالإنجليزية(Microsoft Visual Studio) : هي بيئة التطوير المتكاملة الرئيسية من مايكروسوفت . تتيح برمجة واجهة المستخدم الرسومية والبرامج النصية إلى جانب ويندوز فورم ومواقع ويب وتطبيقات ويب وخدمات وب مدعومة ب مايكروسوفت ويندوز وويندوز موبايل وإطار عمل دوت نت ومايكروسوفت سيلفرلايت .

الفصل الثاني

الخلفية النظرية

يحتوى فيجيوال استوديو على محرر أكواد يدعم تقنية انتليسنس واعادة كتابة الكود ، ويحتوى أيضا على مترجم يكشف أخطاء وقت التشغيل ومفسر يكشف الأخطاء الاملائية في الأكواد ويحتوى أيضا على مصمم نماذج لبناء واجهة مستخدم رسومية ومصمم ويب ومصمم فئات صنف (علوم الحاسب) ومصمم مخطط قواعد بيانات ومصمم لتقارير الكريستال .

يدعم فيجيوالـ استوديو العديد من لغات البرمجة مثل مايكروسوفت فيجيوال C++ ومايكروسوفت فيجيوال C#ومايكروسوفت فيجيوال بيسك وجافا سكريبت والعديد أيضا من لغات الترميز مثل لغة ترميز النص الفائق ولغة الترميز القابلة للامتداد ولغة ترميز النص الفائق القابلة للتمديد وأكس أس أل .

XAMPP

XAMPP ويلفظ إكزامب ، اكسامب (وهو حزمة تطبيقات حرة ومفتوحة المصدر وتتضمن بشكل رئيسي خادوم إتش تي تي بي أباتشي , ماريا دي بي) (ماي إس كيو إل سابقاً) ، ومفسر للتطبيقات المكتوبة بلغات البرمجة بي إتش بي وبيرل .

- جدول لتلخيص كل قطعة وجهاز مع عرض جميع الوظائف لهذه القطع و الأجهزة :-

القطعة (الجهاز)	الوظيفة
الحاسوب (Computer)	أولاً : الحاسوب سوف يستعمل لبرجمة و تعريف القطع وإيضاً . ثانياً : سوف يستخدم كسرفر في حال تم تطوير المشروع إلى نظام شبكي .
Arduino UNO	سيتم أستخدام هذه القطعة لقرائة و تعريف القطع المرتبطة بها وذلك من خلال برمجة هذه القطعة الحاسوب بأستخدام لغة البرمجة الخاصة بها .
RFID	سيتم أستخدام هذه القطعة من أجل قرائة البطائق الممغنطة من خلال ربط هذه القطعة برمجياً بالوحة الاكترونية (Arduino UNO) .
LED	ستعمل على الاشعار بقبول أو رفض البطاقة .
Pins	سيتم أستخدامها من أجل ربط الاجهزة .
Check List	سيتم أستخدامها من أجل الحفاظ على الاجهزة الاكترونية .

جدول القطع و الأجهزة جدول رقم ١.٢

- جدول لتلخيص البرامج التي سيتم استخدامها وعرض خصائصها :-

الرنامج (Soft Ware)	خصائصة
Microsoft Visual Studio	يتضمن Visual Studio محرر تعليمات برمجية يدعم IntelliSense (مكون إكمال التعليمات البرمجية) بالإضافة إلى إعادة هيكلة التعليمات البرمجية. يعمل المصحح المتكامل

الفصل الثاني

الخلفية النظرية

	كمصحح على مستوى المصدر ومصحح على مستوى الجهاز. تشتمل الأدوات الأخرى المضمنة على محلل تعليمات برمجية ومصمم لإنشاء تطبيقات واجهة المستخدم الرسومية ومصمم الويب ومصمم الفئة ومصمم مخطط قاعدة البيانات. يقبل المكونات الإضافية التي تعزز الوظيفة على كل مستوى تقريبًا - بما في ذلك إضافة دعم لأنظمة التحكم في المصدر (مثل Subversion و Git) وإضافة مجموعات أدوات جديدة مثل المحررين والمصممين المرئيين للغات أو مجموعات الأدوات الخاصة بالمجال للجوانب الأخرى لتطوير البرامج دورة الحياة (مثل عميل Azure DevOps: Team Explorer). يدعم Visual Studio 36 لغة برمجة مختلفة ويسمح لمحرر التعليمات البرمجية ومصحح الأخطاء بدعم (بدرجات متفاوتة) تقريبًا أي لغة برمجة ، شريطة وجود خدمة خاصة باللغة. تتضمن اللغات المدمجة C و [٨] C ++ و CLI / C ++ و Visual Basic .NET و C # و F # و [٩] JavaScript و Typescript و XML و XSLT و HTML و CSS. يتوفر دعم للغات الأخرى مثل Python و [١٠] Ruby و Node.js و M وغيرها من خلال المكونات الإضافية. تم دعم Java (و J #) في الماضي. الإصدار الأساسي من Visual Studio ، إصدار المجتمع ، متاح مجانًا. شعار إصدار مجتمع Visual Studio هو "بيئة تطوير متكاملة مجانية ومميزة بالكامل للطلاب والمطورين المفتوحين والأفراد".
XAMPP	وظيفة البرنامج : يجعل جهازك سيرفر من خلاله تقدر تجرب تعمل موقع تعمل تنصيب لجميع اصدارات المدونات سواء WordPress, Drupal, Joomla او صفحات html او اي صفحات او انشاء دي جي شات او اي دردشة وتقدر فيما بعد تخلي اصدقائك يدخلو عليها من خلال الـ ip الخاص بيك بالاضافة انك تقدر تجرب عليه قواعد

الفصل الثاني

الخلفية النظرية

	البينات التي قمت بأنشائها بنفسك. وعشان كده هنشرح ليكم طريقة تنصيب البرنامج وطريقة تثبيت سكربت الووردبريس.
C Arduino	البرمجة في عصرنا الحالي موجودة في كل مكان. و من الصعب التفكير في عالمنا بدون برمجة. فإذا نظرنا إلى محيطنا سنجد أن كل شيء مبرمج. فالحاسوب الذي تستعمله مبرمج، و المتصفح كذلك مبرمج، الويندوز كذلك هو عبارة عن برمجة. الراديو، التلفاز،الساعة الرقمية، الهاتف، صفحات الويب... كلها برامج في واقع الأمر.لكن كل منها مبرمجة بلغة معينة. ولذلك تعددت لغات البرمجة. و ما يهمنا نحن الآن هو لغة برمجة الأردوينو، و التي ترتكز أساسا على لغة السي بلس بلس و السي كما قلنا في الدرس الأول من دورة الاردوينو.

جدول البرمجيات و الأنظمة جدول رقم ٢.٢

الفصل الثالث

التحليل

الفصل الثالث

التحليل

١.٣ المقدمة

في هذا الفصل سوف نناقش المراحل المهمة في بناء النظام ويشمل وصف المشكلة و دراسة الجدوى والنظام الجديد و الجدوى الفنية و الجدوى الاقتصادية و إنشاء الخطة الزمنية لتنفيذ المشروع .

٢.٣ وصف المشكلة

عند دراسة النظام السابق تم استنتاج عدم وجود كل احتياجات التي تستفيد منها الشركات و المؤوسسات الحكومية و الخاصة منها في مرحلة مايسمى بمرحلة الحماية وصعوبة على كل ما يحتاجة في توفير الحماية و تأمين الانظمة المعلوماتية .

٣.٣ البدائل

١- أستخدام المفاتيح و الاقفال المصنوعة من المعدن .
٢- المسؤولية تجاة حامل المفتاح .
٣- هوية الموظف .
٤- مزامنة الدخول و الخروج .

وجة المقارنة	أستخدام المفاتيح و الاقفال المصنوعة من المعدن	المسؤولية تجاة حامل المفتاح	هوية الموظف	مزأمنة الدخول و الخروج	النظام الجديد
الكفاءة	متوسطة	متوسطة	متوسطة	ضعيفة	عالية
السرعة	متوسطة بعض الاحيان ضعيفة	ضعيفة	ضعيفة	ضعيفة	عالية
التكلفة	متوسطة	عالية	متوسطة	عالية	عالية لمرة واحدة فقط

جدول المقارنة بين النظام الحديث و القديم رقم ١.٣

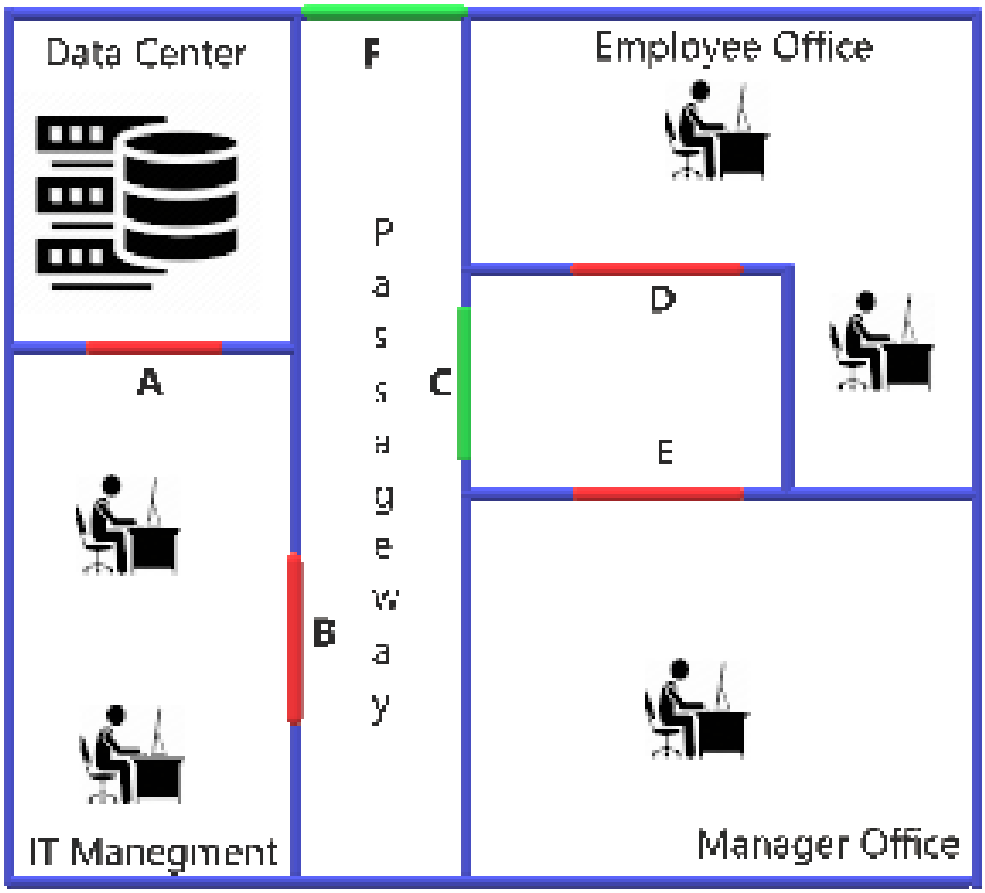
الفصل الثالث

التحليل

٤.٣ مخططات اللوحة الالكترونية :-

١- Physical topology :- ويصف الاجهزة ومساحة المكان التي سوف يكون فيها النظام الأمني من خلال تحديد الاتي :

- مساحة ورشة العمل : الطول ١٠ متر ، العرض ٥ متر .
- عدد الاجهزة في المخطط : عدد الاجهزة المتصلة بالنظام الأمني من خلال اسلاك ايثرنت ٤ أجهزة RFID و إيضاً خمسة أجهزة حاسوب وجهاز ١ سيرفر وكذلك جهاز محول شبكي (switch) .
- الشكل التالي يوضح مخطط Physical topology.



شكل رقم ٣.١ Physical Topology

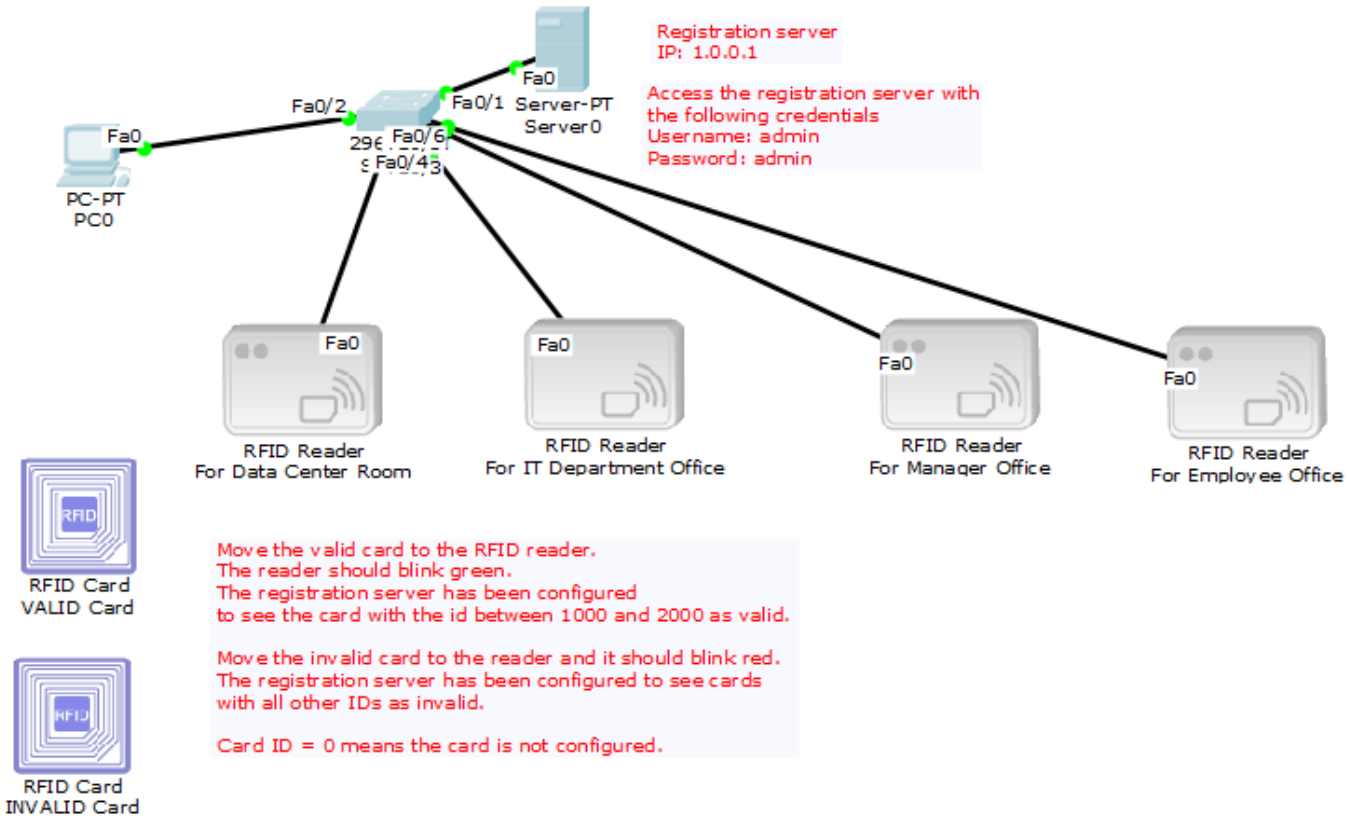
الفصل الثالث

التحليل

- الابواب التي بالون الاخضر (C & F) الباب F هو البوابة الافتراضية الرئيسية ، و الباب C هو البواية الافتراضية للموظفين وقد عُلمت بالون الاخضر لعدم وجود أقفال الكترونية عليها و تعتبر مفتوحة .
- الابواب التي بالون الاحمر (A & B & D & E) هي أبوب مؤمنة ولا يمكن فتحها إلى بلبطائق الممغنطة التي تعمل على RFID للأشخاص المسجلين على قاعدة بيانات هذه الشركة او المنظمة .
- غرفة مركز البيانات (Data Center) : هي غرفة شديدة الحماية و ليس لأي شخص في المنظمة أو المنشأة حق الدخول سوى المخول لهم الدخول فيها كالمدير العام و مدير أدارة الـــــ(IT) وتضم كل البيانات الخاصة والهامة ب المنشأة او المنظمة .

٢- Logical topology:- ويصف الاجهزة التي سوف تكون متصلة عبر physical topology

- قمنا بأستخدام برنامج Cisco packet tracer



شكل رقم ٢.٣ Logical Topology

الفصل الثالث

التحليل

٥.٣ جمع البيانات

كلمة عملية جمع البيانات والتي تساعد في تحديد متطلبات النظام والبيانات المستخدمة في نظام الحماية (RFID) ومن هذه البيانات بيانات حامل البطاقة الموظف ، وبيانات الاجهزة التي سوف يتم حمايتها وبيانات المزامنة ، و إيضاً بيانات البطائق الممغنطة و كذلك الصلاحيات وغيرها من البيانات :

١.٥.٣ قراءة و تحليل المستندات :

تم جمع البيانات عن طريق زيارة إحدى الشركات الخاصة وتم الحصول على كثير من المعلومات :

١- إجرائات تسجيل حاملي البطاقة أو الموظفين بشكل عام .
٢- إجرائات تسجيل المحتوى و أنواعة .
٣- إجرائات ترتيب المحتوى .
٤- كيفية أخراج تقارير عن المحتوى .
٥- كيفية البحث عن المحتوى الموجود .
٦- الفكرة عن عدد الاجهزة و المكونات المادية التي يمكن حمايتها .

٢.٥.٣ المشاهدة :

- تمت عميلة النزول ومشاهدة عملية سير عمل النظام الأمني في بعض الاماكن لفهم :

- حركة سير النظام و الخطوات و الاجرائات التي يقوم بها موظفي الحماية في بعض المكاتب وطريقة عمل تسجيل بيانات منها الحظور و الانصراف وإيضاً بيانات الصلاحيات للولوج للأجهزة .
- معرفة العوائق والصعوبات والمشاكل التي تواجة الشركات و المؤوسسات بما فيها من موظفين و مدراء .

٦.٣ توصيف النظام المقترح

هو عبارة عن نظام أمني يحتوي على نظام يخدم كافة الموظفين من جميع الفئات على تأمين المكاتب الخاصة بها و الانظمة التي يستخدمونها ، و إيضاً التأكد من عدم الولوج إلى الانظمة و المكاتب من قبل اشخاص من غير المخولين لهم ، وكذلك سهولة أستخدام هذا النظام الأمني و المفاتيح الخاصة بة للولوج إلى كل ما يختص بالعمل وتوفر إيضاً الوقت و الجهد لكافة الموظفين ، وكذلك يقوم هذا النظام بحفظ كافة المفاتيح والتي تسمى بلبطاقات الممغنطة من التلف و الضياع وتكون فيها كل الامان لكافة المستخدمين مع ضمان دقة هذا النظام بأنهو يعمل بشكل ممتاز وإيضاً يخدم كافة المؤوسسات والشركات لانهو يحمل المسؤولية الكاملة لحامل البطاقة ويسهل ذلك من خلال :

الفصل الثالث

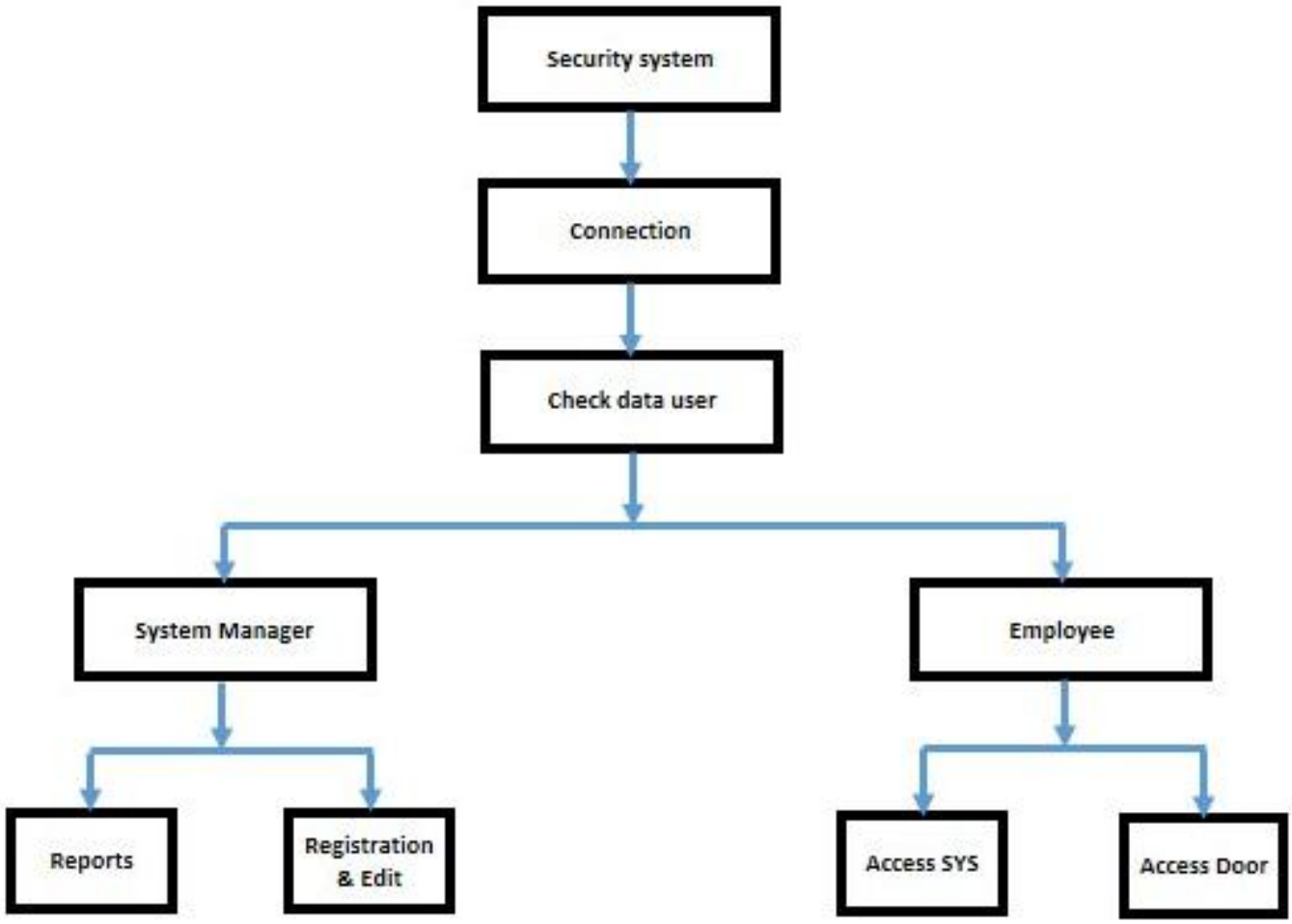
التحليل

٧.٣ رسم مخطط ال (BFD)

أولاً : مدير النظام :

بحث تكون لدية الصلاحية الكاملة في التحكم في النظام من خلال إضافة مستخدمين لهذا النظام الأمني و إعطائهم الصلاحيات المطلوبة لكل مستخدم أو حامل بطاقة(المدير ، الموظف) ويتوفر لكل مستخدم عدة خصائص في النظام :

١- المدير : لهو الصلاحية الكاملة .



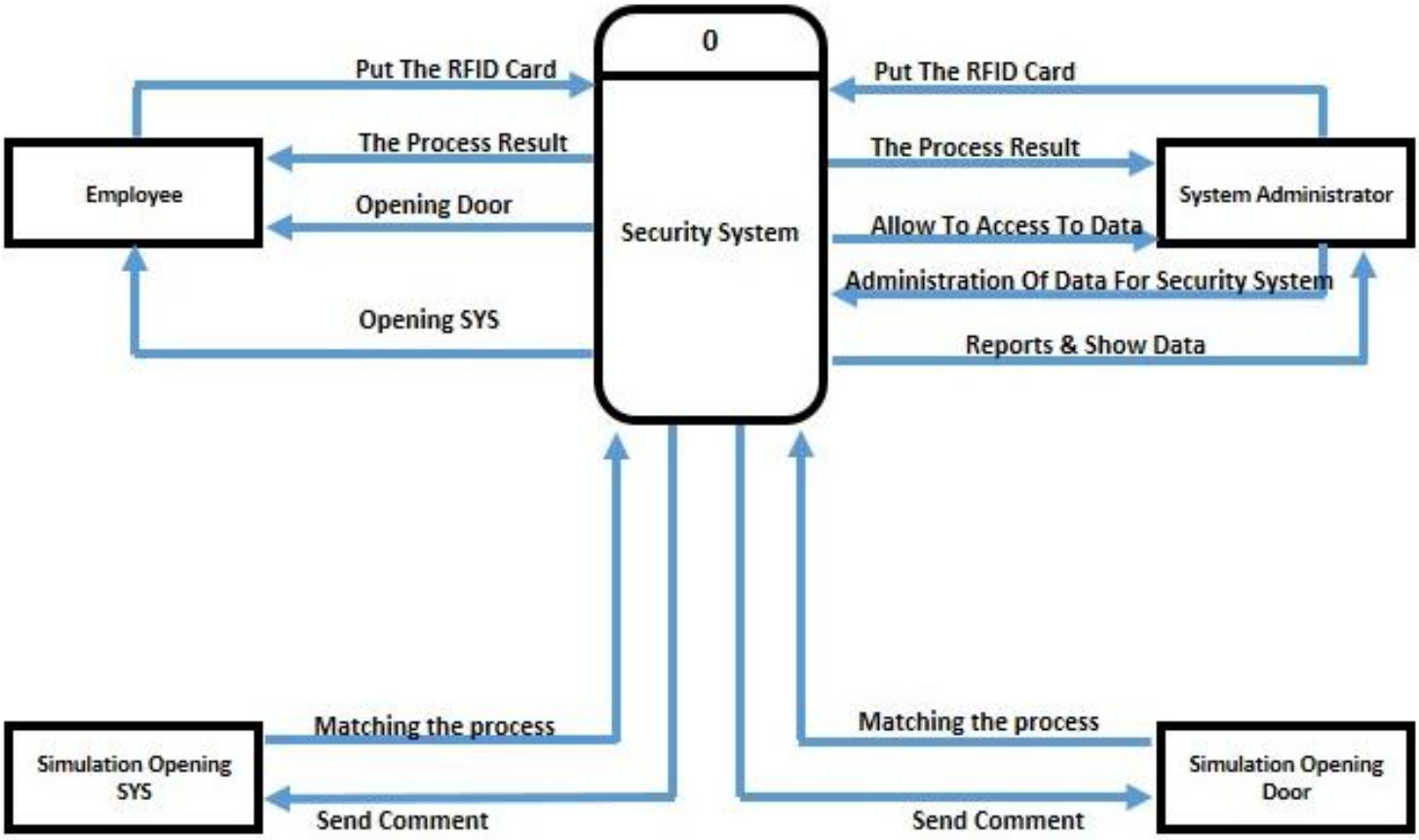
شكل رقم ٣.٣ مخطط الـ BFD

الفصل الثالث

التحليل

٨.٣ رسم مخطط تدفق البيانات ال (DFD)

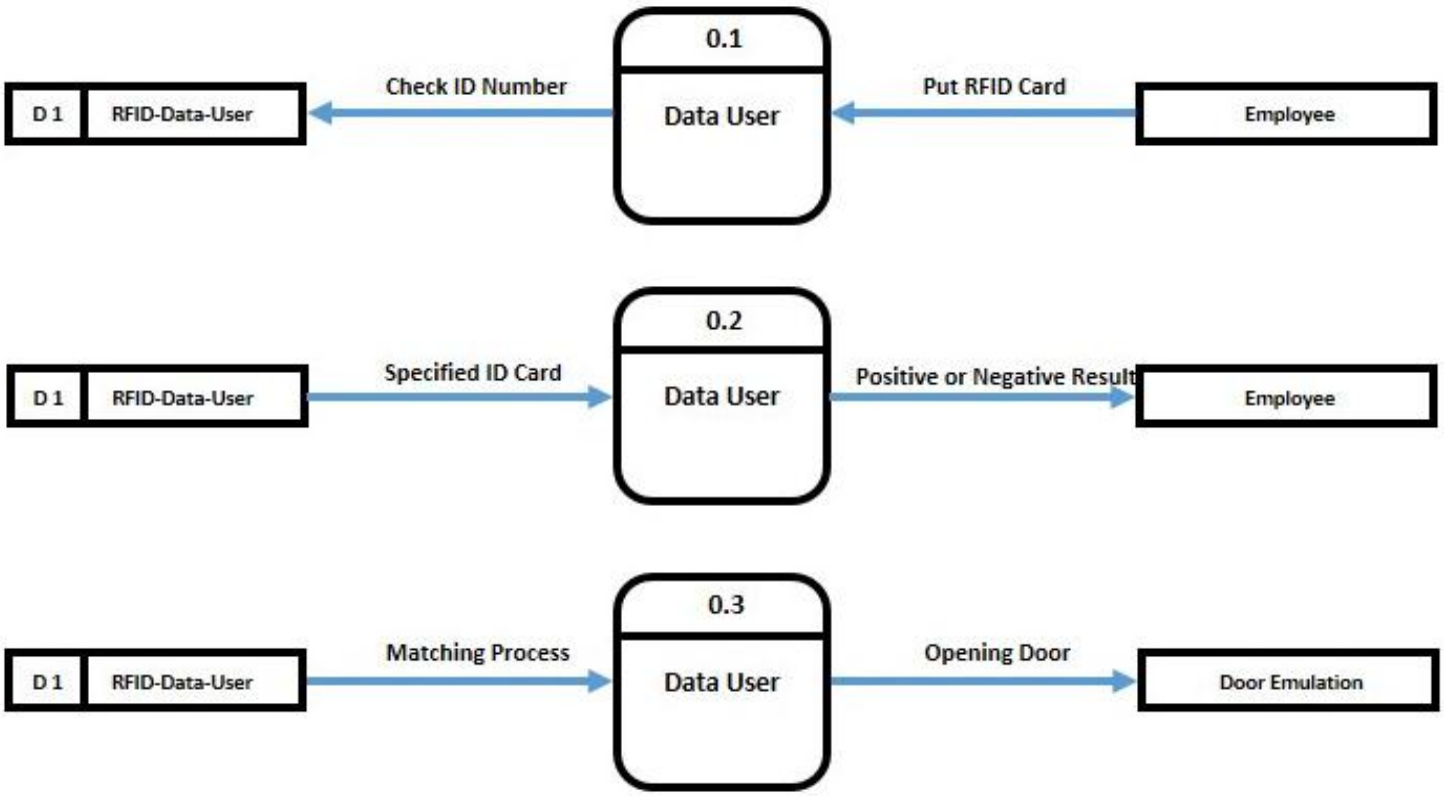
أولاً : مخطط تدفق البيانات DFD



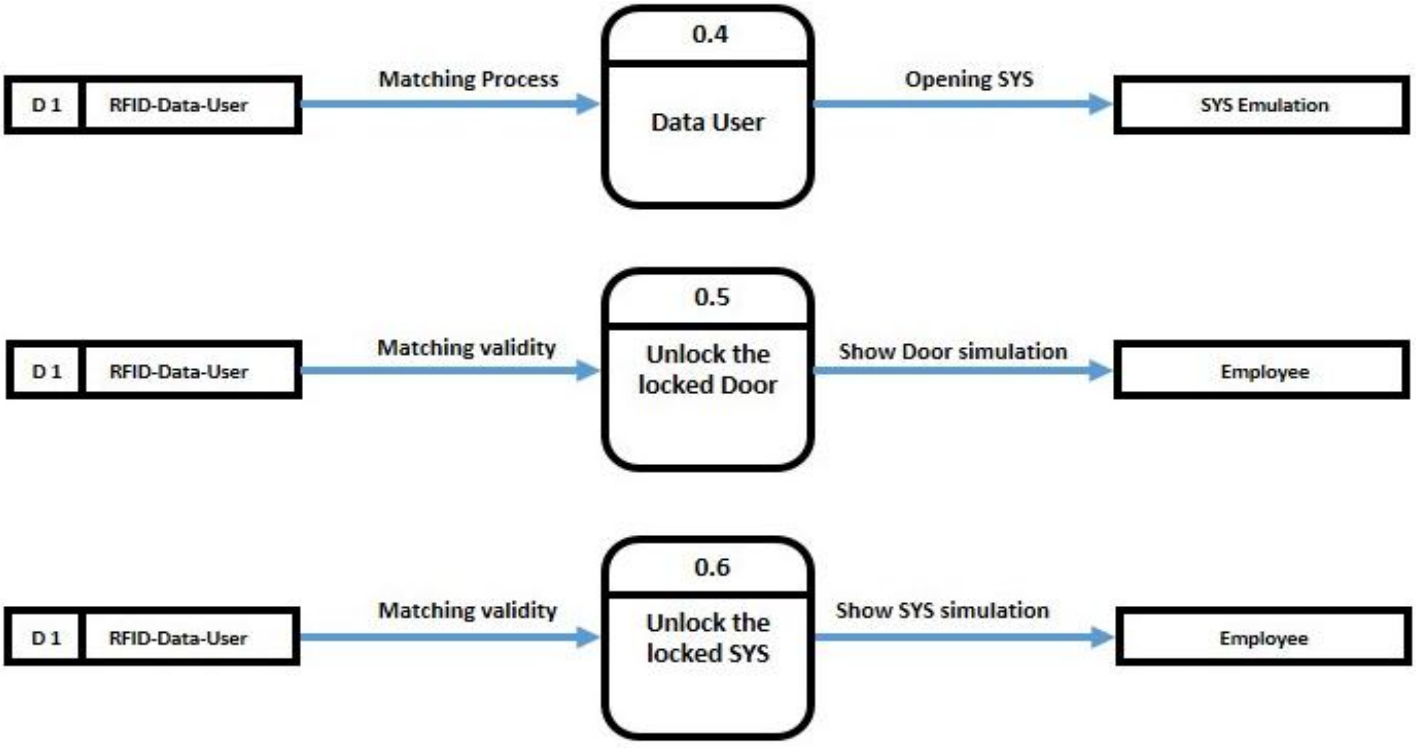
شكل رقم ٤.٣ مخطط الـ DFD

الفصل الثالث

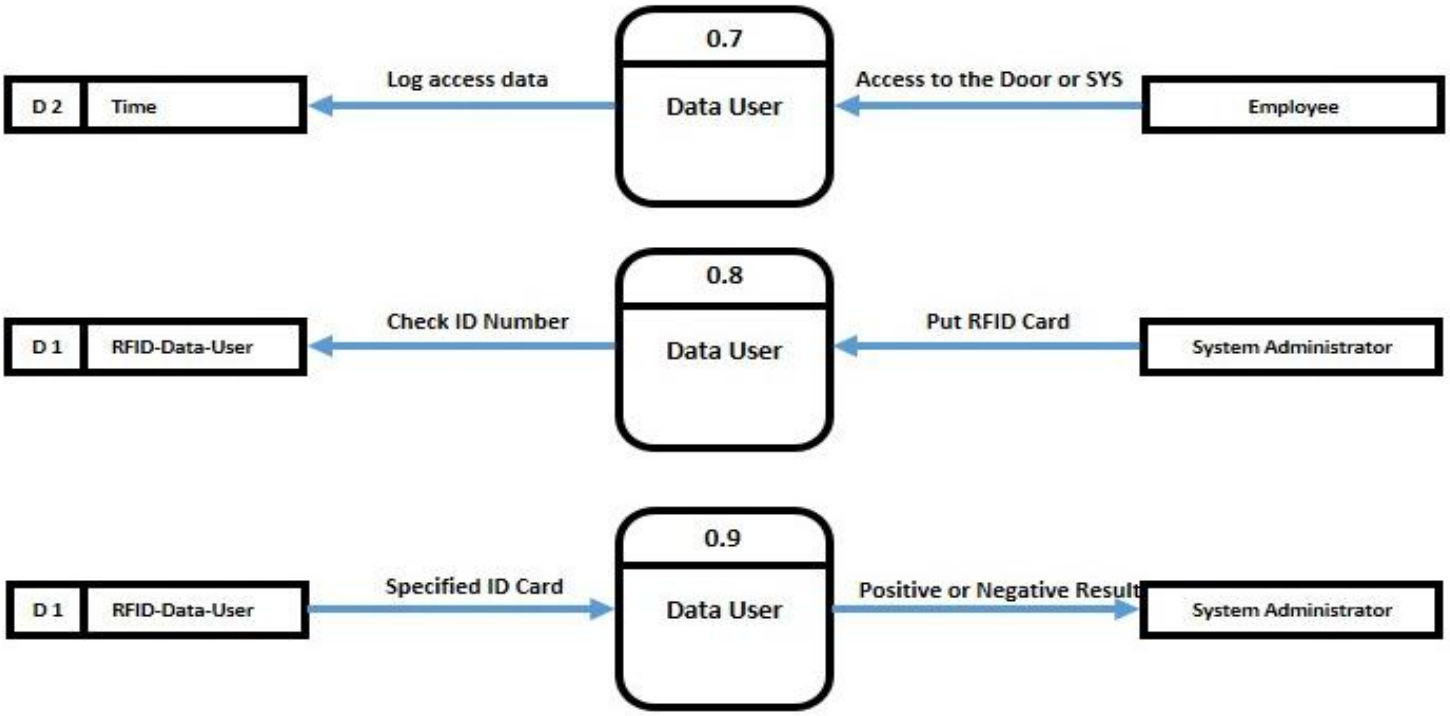
التحليل



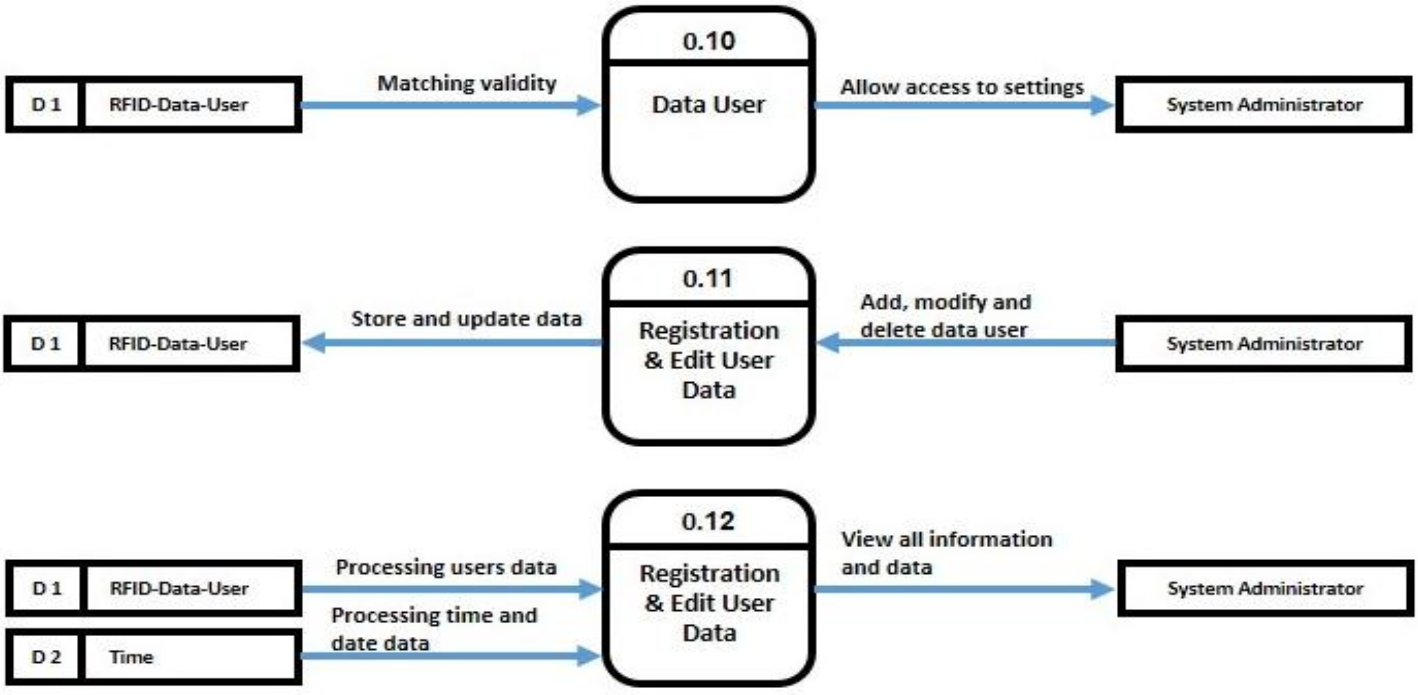
مخطط تدفق البيانات الصفريه شكل رقم ٣.٥



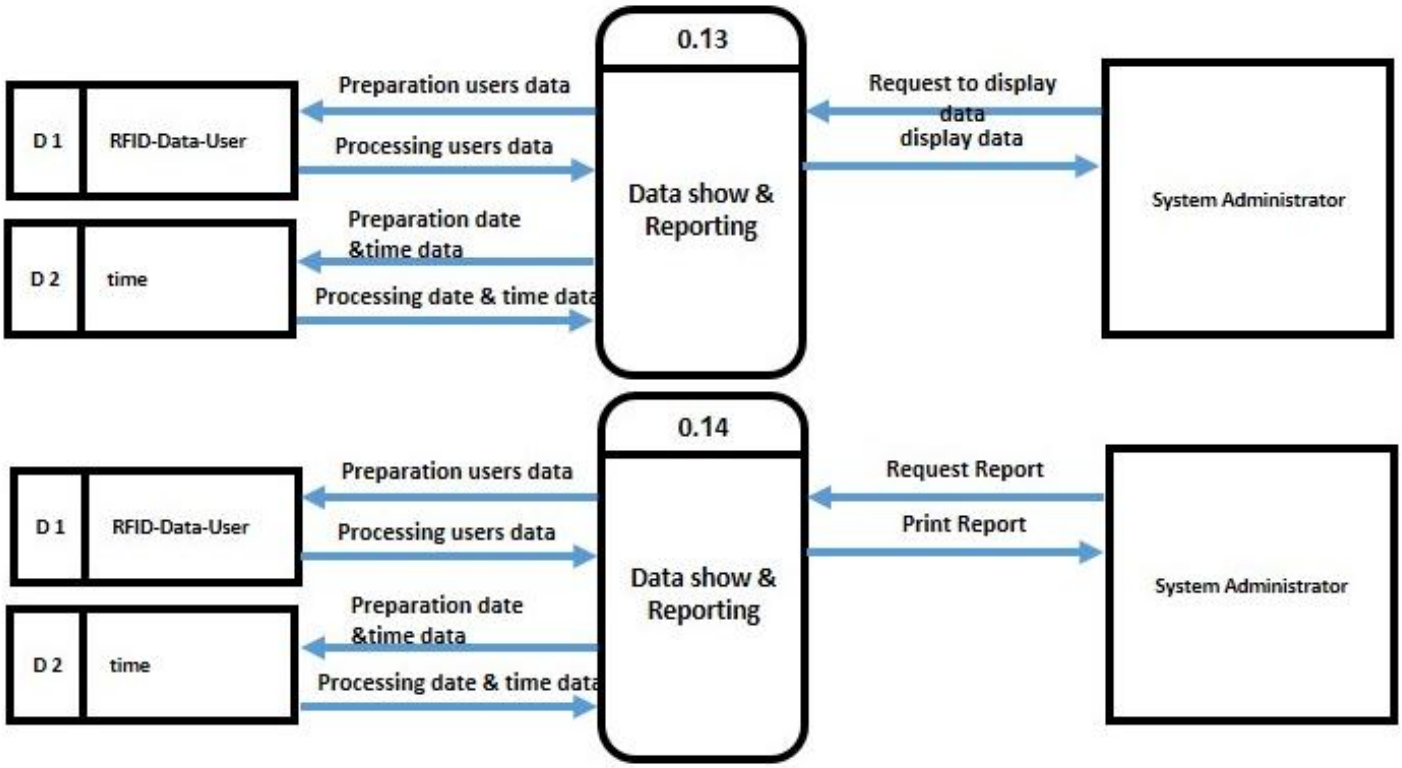
مخطط تدفق البيانات الصفريه شكل رقم ٣.٦



مخطط تدفق البيانات الصفريه شكل رقم ٣.٧



مخطط تدفق البيانات الصفريه شكل رقم ٣.٨



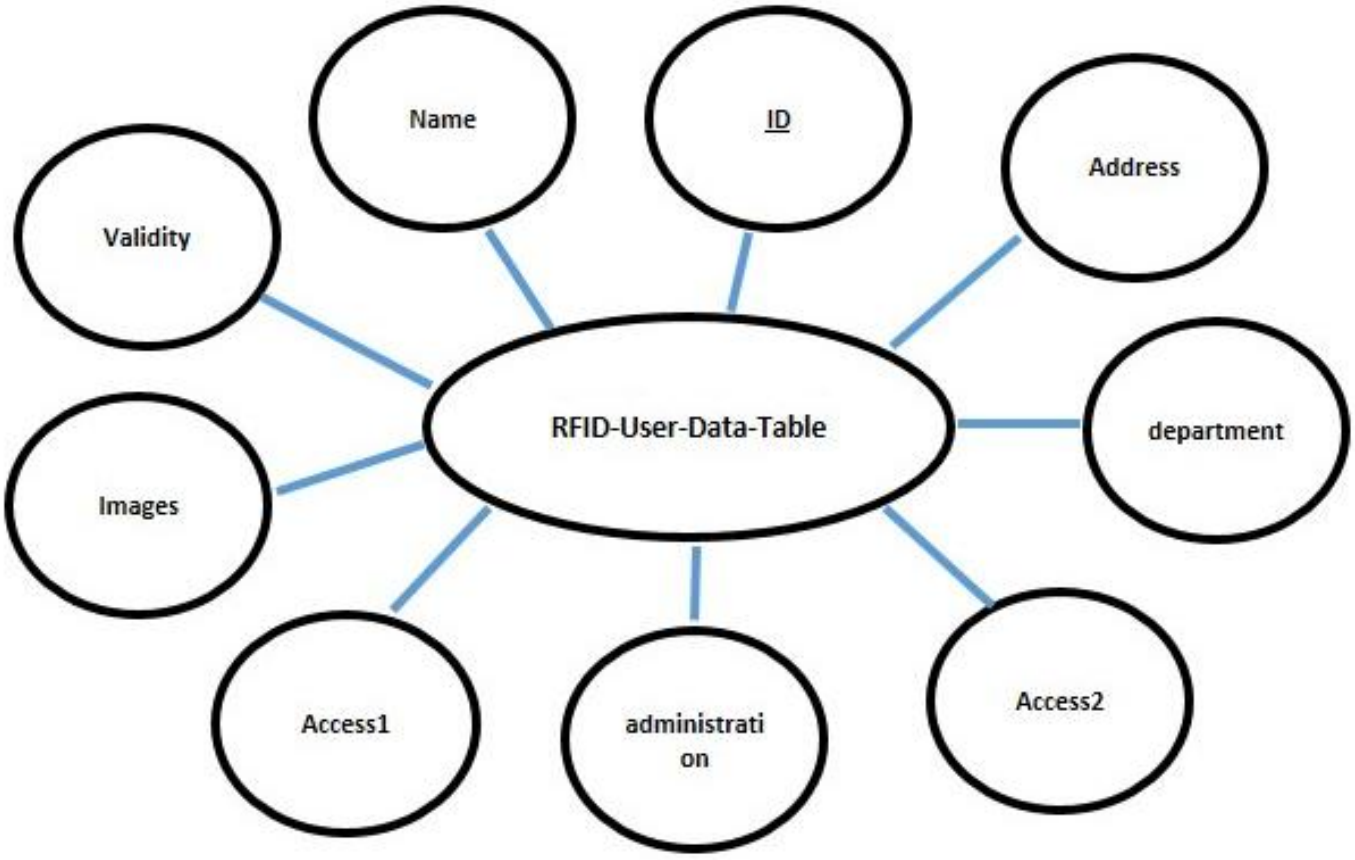
مخطط تدفق البيانات الصفريه شكل رقم ٣ .٩

الفصل الثالث

التحليل

٩.٣ مخطط الكينونات العلائقي

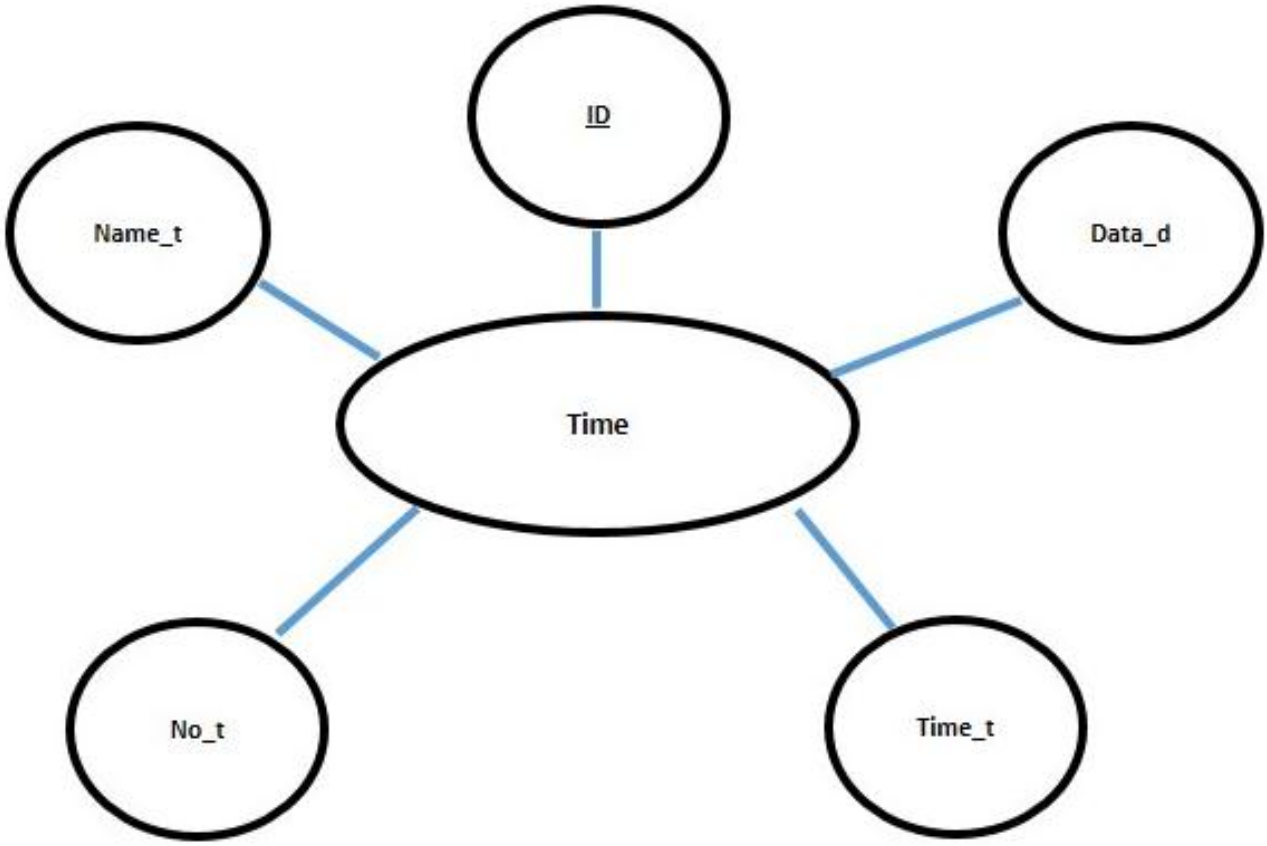
هو عبارة عن عرض لأشكال الجداول وسيتم شرحها في فصل التصميم بشكل مفصل ...



مخطط الكينونات العلائقيه شكل رقم ٣ .١٠

الفصل الثالث

التحليل



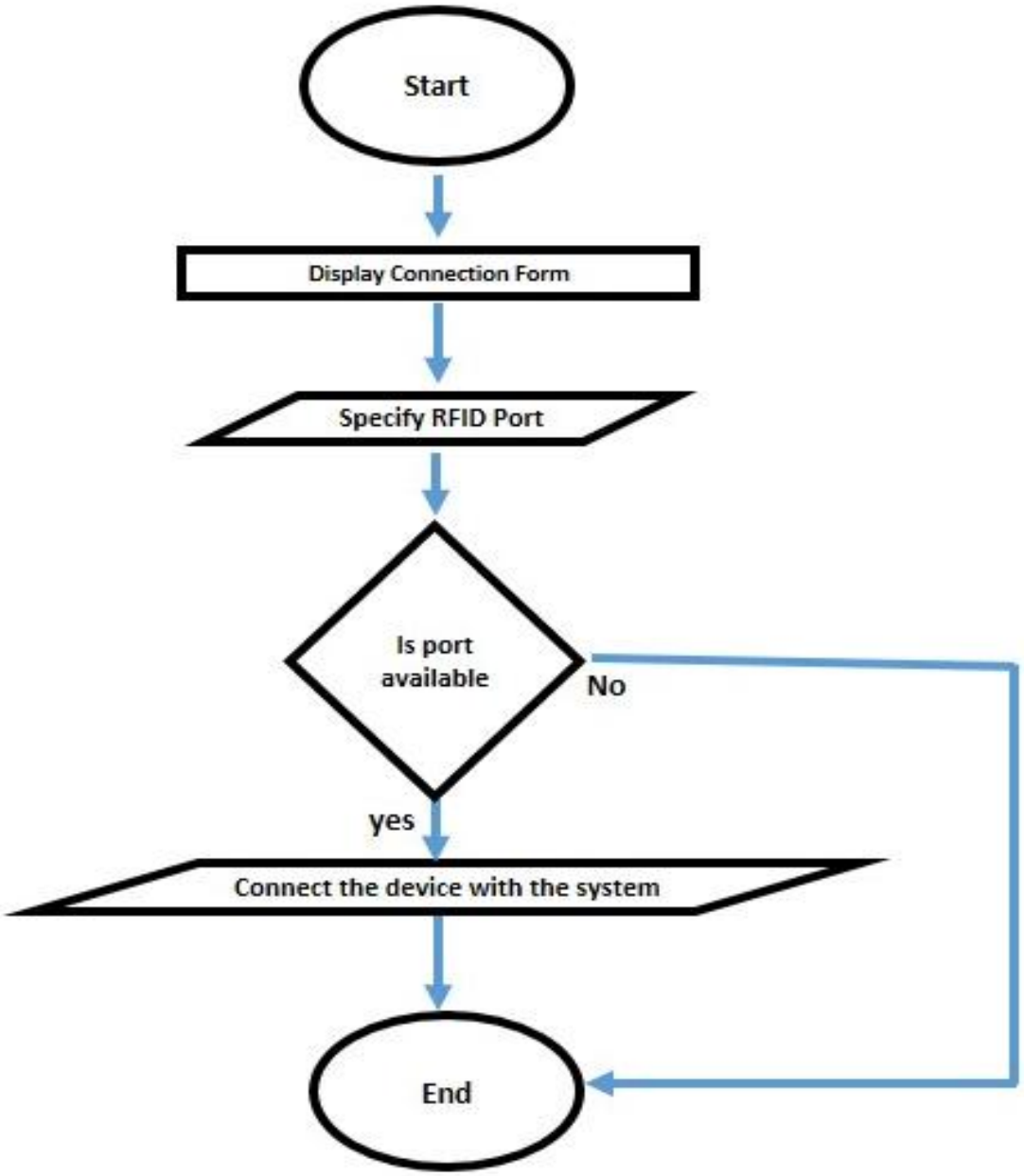
مخطط الكينونات العلائقيه شكل رقم ٣.١١

الفصل الثالث

التحليل

١٠.٣ خوارزميات

١- خوارزمية واجهة الاتصال (connection)

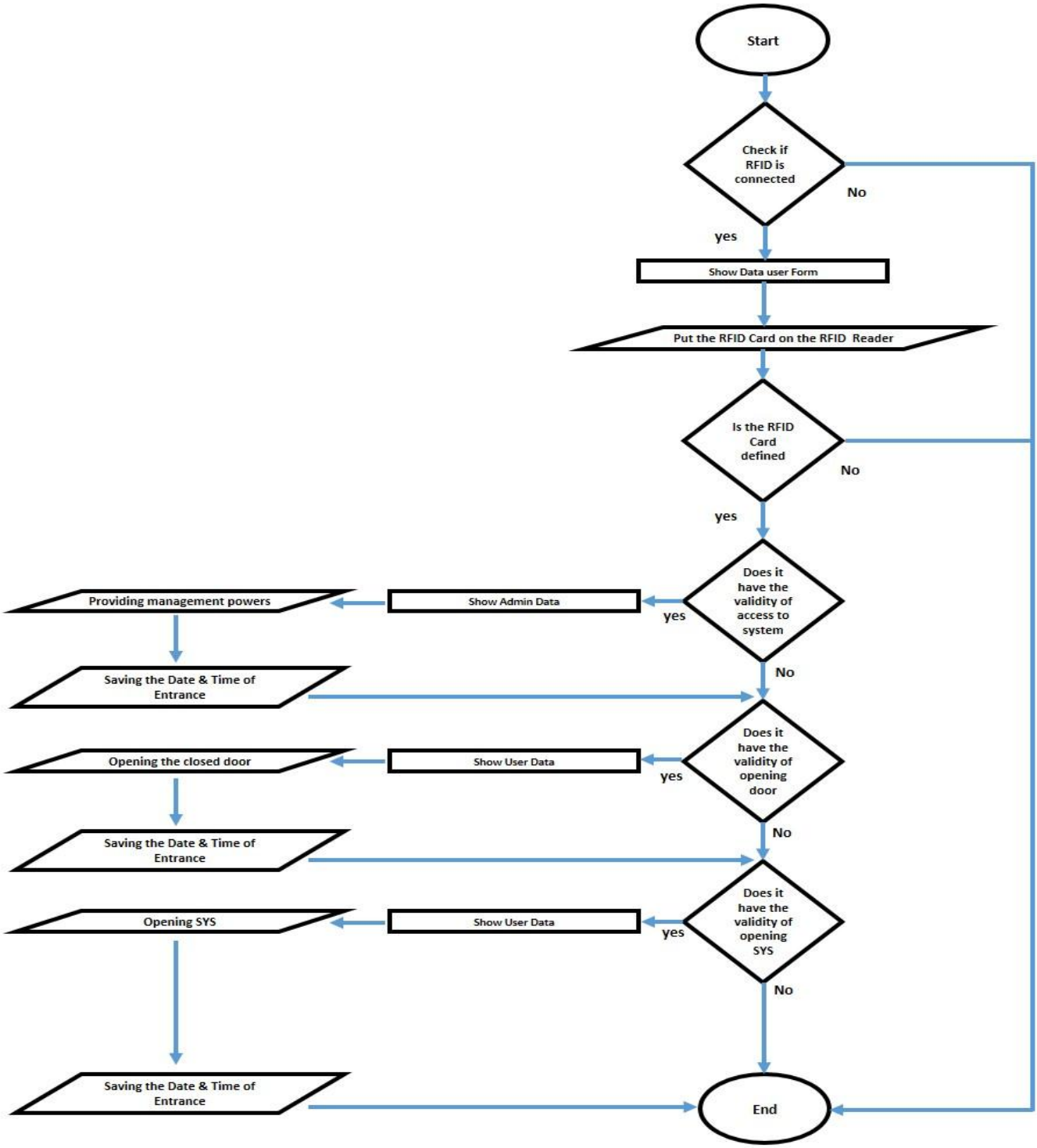


خوارزميه واجهة الأتصال شكل رقم ١٢.٣

الفصل الثالث

التحليل

٢- مخطط واجهة التحقق من الهوية (Identity verification)

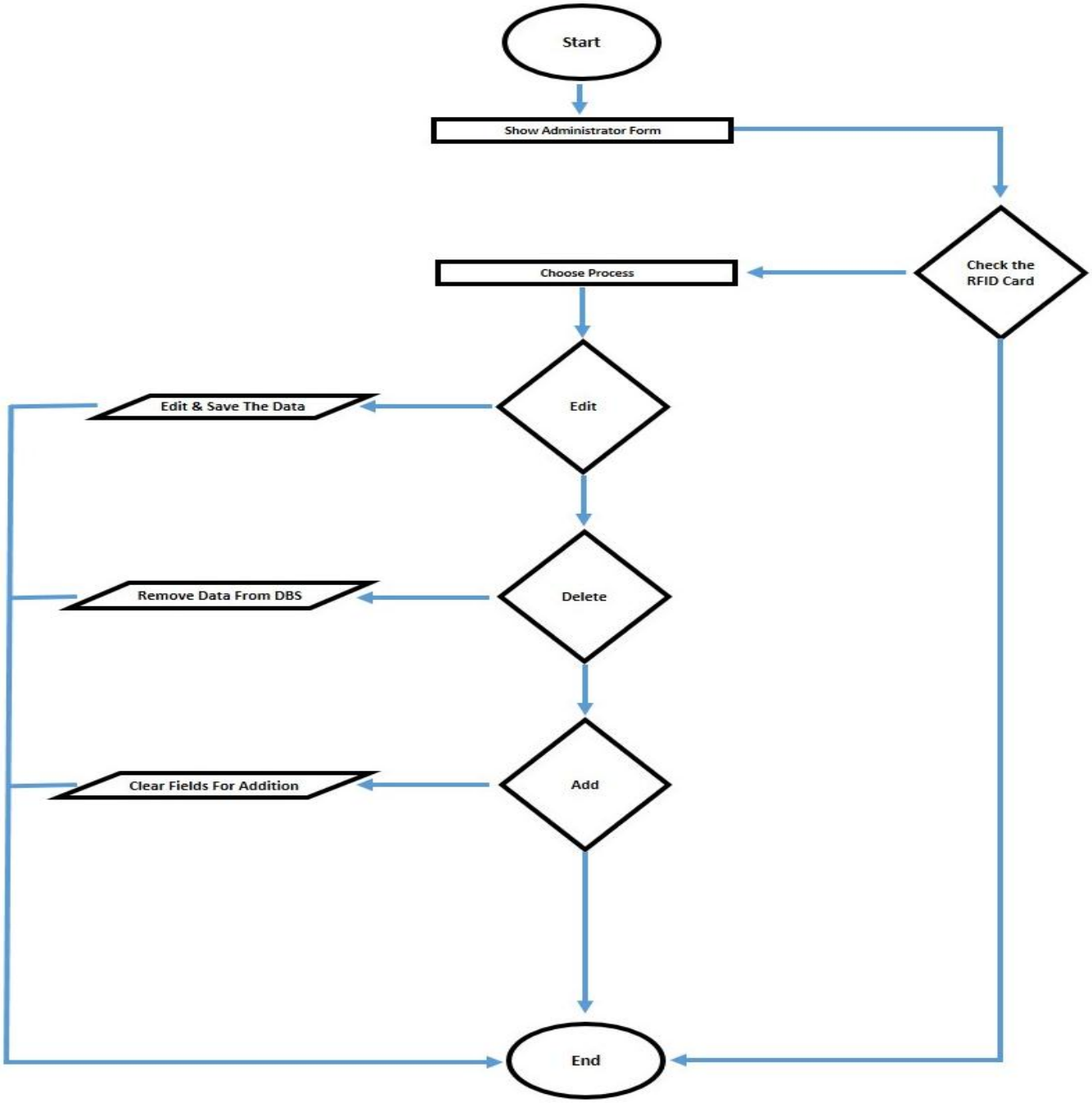


خوارزميه التحقق من الهوية شكل رقم ٣.١٣

الفصل الثالث

التحليل

٣ - خوارزمية أدارة مستخدمي النظام الأمني (Security System Users)

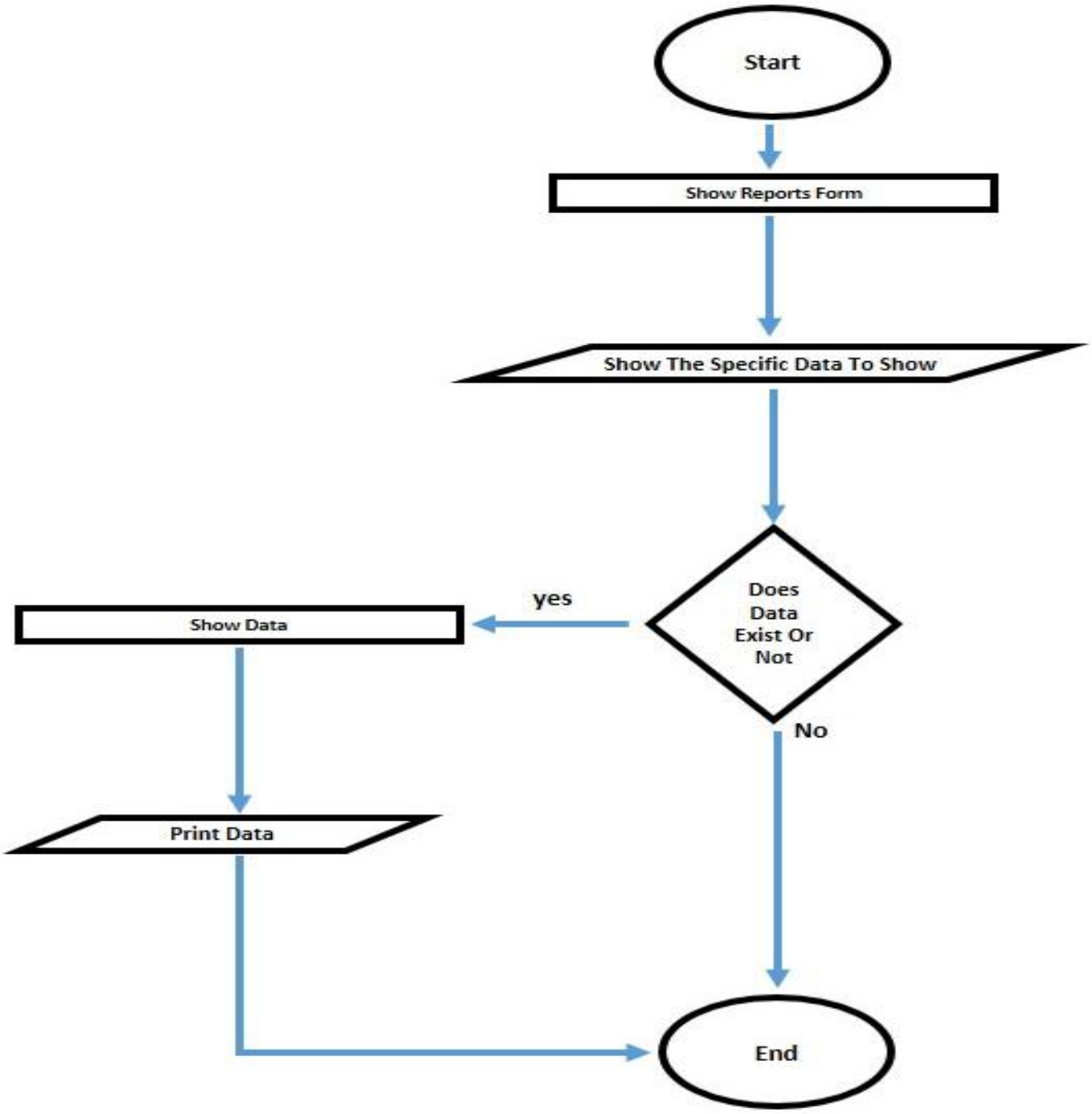


خوارزميه أدارة النظام الأمني شكل رقم ٣ .١٤

الفصل الثالث

التحليل

٤- مخطط عرض تقارير البيانات (Reports)



خوارزميه عرض التقارير شكل رقم ٣.١٥

الفصل الرابع

مرحلة التصميم

الفصل الرابع

مرحلة التصميم

١.٤ المقدمة

في هذا الفصل سيتم التطرق الى تصميم النظام أبتداً من تكوين قاعدة البيانات و الشاشات و أنتهاءٍ بالتقارير بدايةٍ سوف يتم شرح قاعدة البيانات و مكوناتها من الجداول و الحقول ثم بعد سوف يتم الأنتقال الى تصميم واجهات المستخدم مثل الشاشة المفتاحية و الشاشة الرئيسية وواجهات الادخال وشاشات مدخلات الاستعلام و شاشات مخرجات الاستعلام و التقارير .

٢.٤ تصميم قاعدة البيانات

تتكون قاعدة البيانات من جداول تحتوي هذه الجداول على بيانات يتم حفظها بواسطة مدير النظام وهي البيانات التي يتم حفظها لكي تعرض على بعض الشاشات على شكل معلومات .

١- جدول بيانات مستخدمي النظام الأمني RFID :

ويقوم هذا الجدول RFID ويتم فية حفظ بيانات كافة المستخدمين الذين يستخدمون النظام الأمني بحفظ وتسجيل بيانات البطاقة وتخزين الرقم السري فيها و إيضاً يقوم بحفظ كافة بيانات المستخدمين مثل:الاسم ، العنوان ، الفرع ، رقم البطاقة ، الولوج ١ ، الولوج ٢ ، الصلاحية ، الصورة ، الإدارة.

- جدول بيانات مستخدمي النظام الأمني RFID (rfid_user_data_table)

NO	Name	Type	NULL or NOT NULL	Key
١	Name	Varchar(100)	NOT NULL	
٢	ID	Varchar(10)	NOT NULL	Primary
٣	Address	Varchar(100)	NOT NULL	
٤	Department	Varchar(50)	NOT NULL	
٥	Administration	Varchar(50)	NOT NULL	
٦	Image	Long blob	NOT NULL	
٧	Validity	Varchar(50)	NULL	
٨	Access1	Varchar(50)	NULL	
٩	Access2	Varchar(50)	NULL	

جدول بيانات مستخدمي النظام الأمني رقم ٤. ١

الفصل الرابع

مرحلة التصميم

الفصل الرابع

مرحلة التصميم

٢- جدول المزامنة Timing

ويقوم هذا الجدول بحفظ وقت وتاريخ لكل عملية ولوج الى إي مكان سوى كان فتح باب أو ولوج للنظام ، وبيانات الوقت فيها : الاسم ، التاريخ ، الوقت ، رقم البطاقة ، رقم الدخلات .

- جدول المزأمنة (Time)

NO	Name	Type	NULL or NOT NULL	Key
1	ID	Varchar(10)	NOT NULL	
2	Name_t	Varchar(100)	NOT NULL	
3	Data_d	Varchar(100)	NOT NULL	
4	Time_t	Varchar(100)	NOT NULL	
5	No_t	INT(25)	NOT NULL	PRIMARY

جدول المزامنة رقم ٢.٤

٣.٤ تصميم شاشات النظام

في هذه المرحلة تتم عملية رسم و تخيل الشاشات المتوقعة للنظام والتي تم رسمها بأستخدام برنامج الباوربوينت وكذلك معرفة التسلسل في الوصول و التنقل بين الشاشات المختلفة للنظام كماهو موضح في تصميم الواجهات .

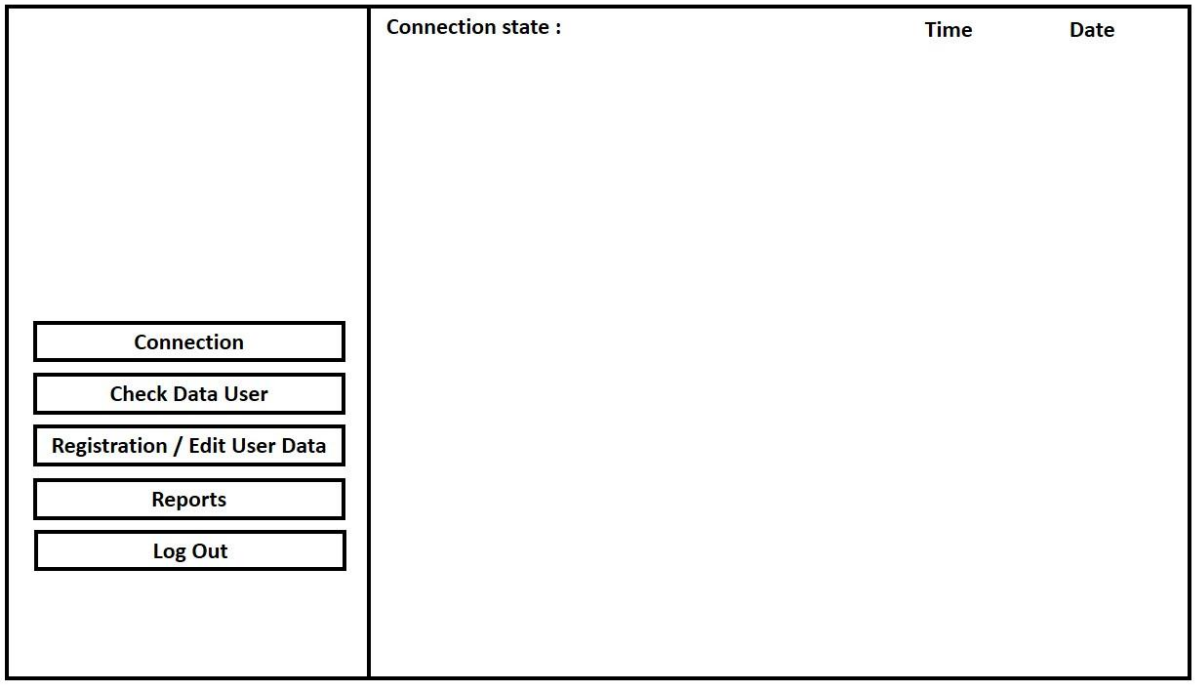
- أن تصميم الواجهات من شأنة توضيح الرؤية الاولى للنظام التي سوف يستخدمها مستخدم النظام حتى تتضح الفكرة بشكل واضح قمنا بتصميم قوالب عن شاشات النظام المتوقعة وسوف يتم عرضها في ما يلي مع شرح موجز لكل واجهة :

الفصل الرابع

مرحلة التصميم

١.٣.٤ تصميم واجهة النظام الرئيسية :

يحتوي الشكل التالي على الواجهة الاولى للنظام وهي الرئيسية و تتكون هذه الواجهة على مجموعة من الإعدادات الخاصة بالعرض وهذه الإعدادات هي عبارة عن وسائل لعرض المعلومات المبدئية لأستخدام النظام ، ومن هذه الإعدادات إعدادات الوصول الى الواجهات الاخرى مثل الازرار وكما يبين الشكل التالي لدينا أربعة أزرار وهي عبارة عن أزرار للوصول الى الواجهات الاخرى مثل واجهة الاتصال (Connection) والتي تقوم بنقل المستخدم الى واجهة الاتصال الخاصة بربط النظام بجهاز الـــ RFID أو ما يسمى بجهاز كشف الهوية بأستخدام البطائق الممغنطة وهي أول واجهة يتم الدخول عليها إجبارياً و أما بالنسبة للزر الذي يلية وهو زر يقوم بنقل المستخدم بنقل الواجهة الى التحقق من الهوية (Check Data User) و أما الزر الاخر هو عبارة عن زر يعمل على النقل الى واجهة أدارة المستخدمين كما يعمل الزر الذي يلية على عرض و أستخراج لكل البيانات على شكل تقارير ، أما عن أدوات عرض المعلومات فلدينا التحقق من حالة الاتصال (Connection State) في القطعة و إيضاً أدوات عرض التاريخ و الوقت وهذه الادوات موجودة في كافة الادوات.



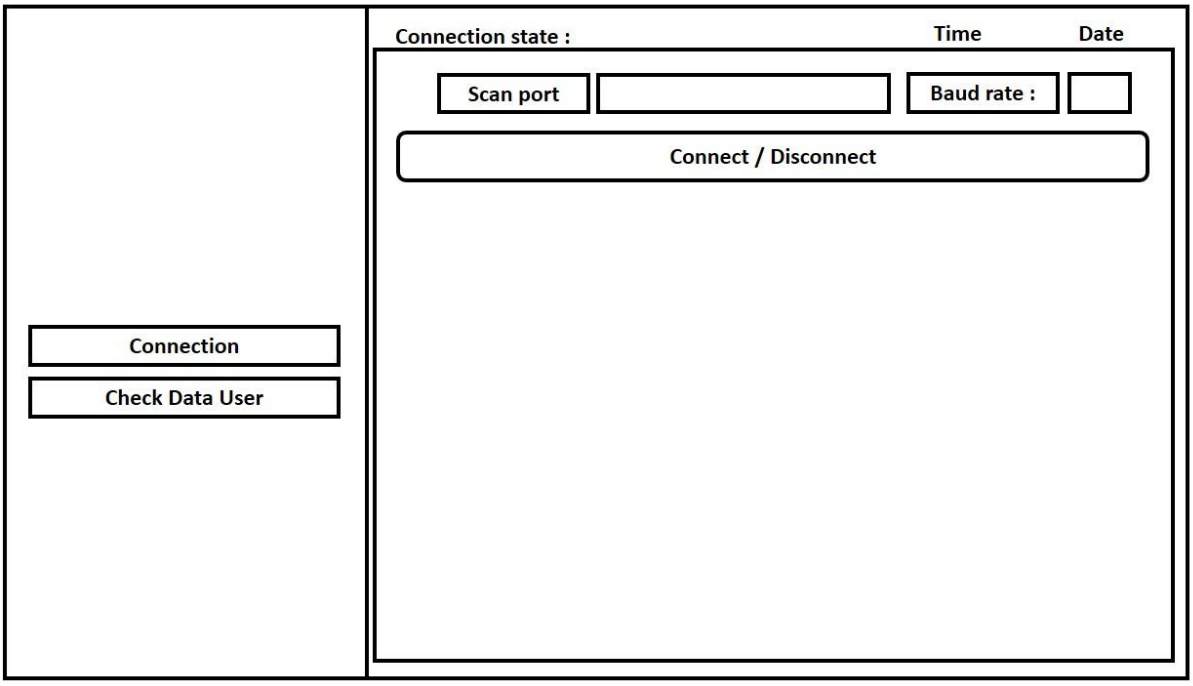
واجهة النظام الرئيسية شكل رقم ١.٣.٤

الفصل الرابع

مرحلة التصميم

٢.٣.٤ واجهة الإتصال (Connection Form) :

ويتم فتح هذه الواجهة تلقائياً أثناء تشغيل النظام لكي يتم ربط جهاز الـــ (RFID) بالنظام و تحتوي هذه الواجهة على إعدادات خاصة بربط النظام بجهاز الـــ RFID ،
عند الضغط على زر Scan Port يقوم البرنامج بالبحث على البورت الخاص بالـــ RFID و يقوم زر البوردريت بتحديد رقم البورت بعد تحديد كلاً من أسم البورت ورقمة يتم الضغط على زر الاتصال وقطع الاتصال Connect / Disconnect .



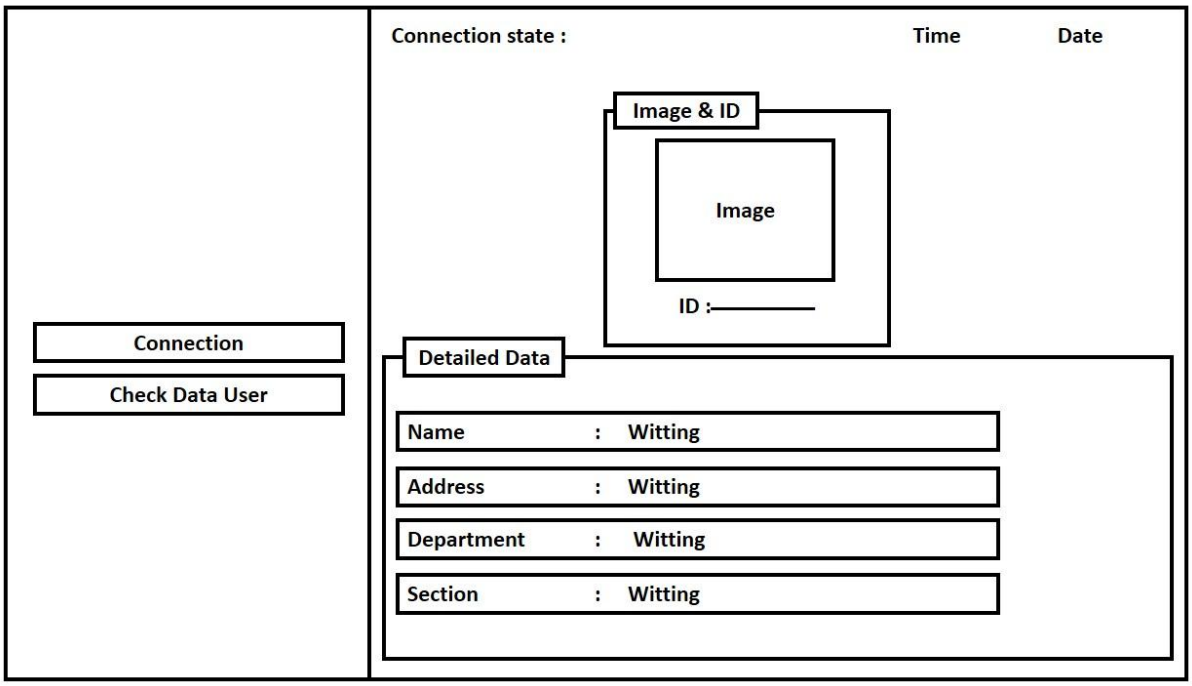
واجهة الإتصال شكل رقم ٢.٣.٤

الفصل الرابع

مرحلة التصميم

٣.٣.٤ واجهة التحقق من الهوية (Check Data User) :

في هذه الواجهة يقوم النظام باعطأ رسائل التحقق من هوية المستخدم سواء كانت إيجابية أم سلبية ويعمل على وضع الصورة في مربع Image & ID كما تعرض باقي البيانات على مربع Detailed Data التي تم جلبها من قاعدة البيانات كما موضح في الشكل أن الاسم يتم وضعة في الـــ Name و كذلك الموقع يتم وضعة على الـــ Address و إيضاً يتم عرض الفرع الذي ينتمي إلية المستخدم في الـــ Section و كذلك تعرض الإدارة التي يعمل عليها ذلك المستخدم وتسمى بـــ Department .



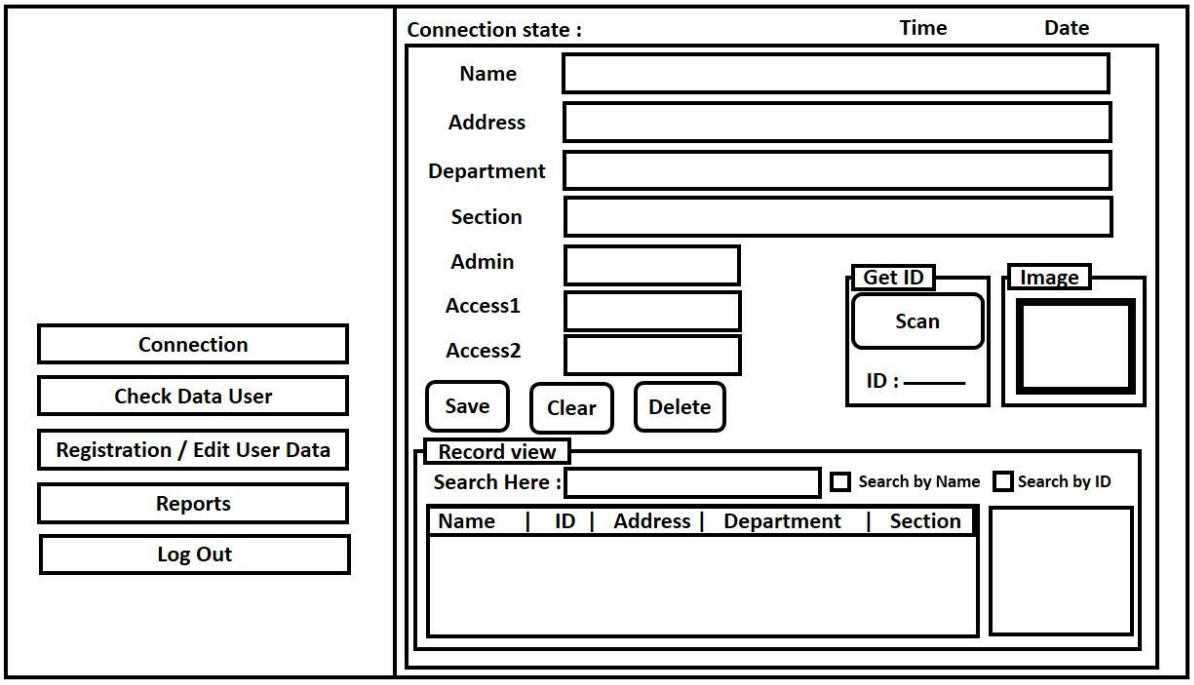
واجهة التحقق من الهوية شكل رقم ٣.٣.٤

الفصل الرابع

مرحلة التصميم

٤.٣.٤ واجهة إعدادات الموظفين (Registration & Edit User Data) :

تقوم هذه الواجهة على ادارة مستخدمي النظام الأمني بحيث يتم اضافة او حذف او تعديل اي بيانات متعلقة بالمستخدمين ، وذلك من خلال فحص البطاقة المدخله وتشفيرها بمعنى تحويل البطاقة الى رقم من خلال الضغظ على الزر Scan بعد عملية الفحص يتم ادخال البينات او حفظها او تعديلها وإيضا يستخدم الزرار Scan بفحص البطاقة الممغنطة من اجل تعديل اي مستخدم او حذفة ، وكما هو موجود في الشكل التالي يتم تحديد الصلاحيات على كل مستخدم والشخص الوحيد القادر على الدخول الى هذه الواجهة هو مدير النظام فقط .



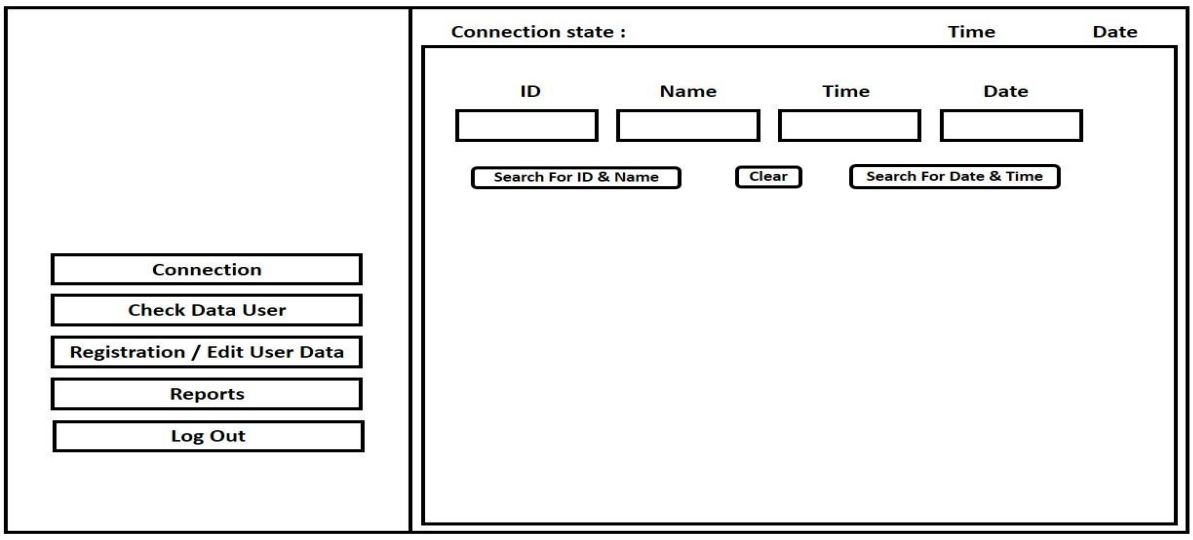
واجهة إعدادات الموظفين شكل رقم ٤.٣.٤

الفصل الرابع

مرحلة التصميم

٥.٣.٤ واجهة عرض التقارير (Reports) :

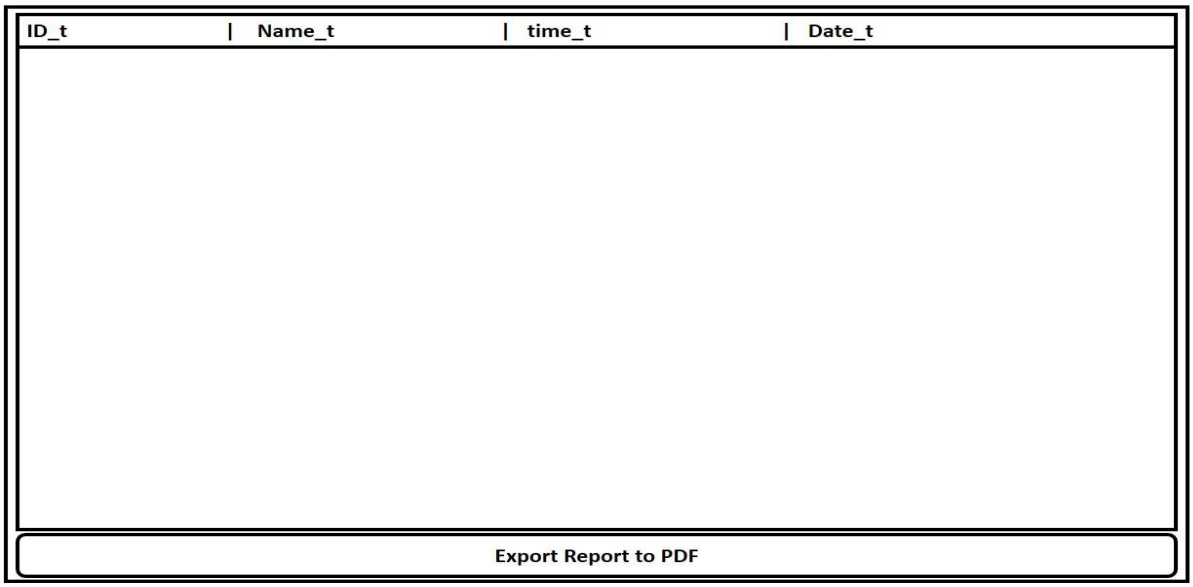
ويتم في هذه الواجهة أدخال او البحث عن البيانات المراد عرضها على شكل تقارير(Reports) من العديد من البيانات التي يصعب إيجادها من قاعدة البيانات في وقت ضئيل ومن هذه البيانات رقم البطاقة الممغنطة للموظف كذلك أسم الموظف وتسجل وقت تسجيل تلك البطاقة المراد عرضها وكذلك التاريخ من ما يسهل البحث على شخص أو موظف أو تقارير عن وقت أو تاريخ معين .



واجهة عرض التقارير شكل رقم ٥.٣.٤

٦.٣.٤ واجهة طباعة التقارير :

في هذه الواجهة يتم عرض البيانات التي تم البحث عنها في واجهة عرض التقارير و منها يمكن أستخراج التقارير على شكل ملفات PDF وذلك من خلال الضغط على زر طباعة التقرير كما يوضح



واجهة طباعة التقارير شكل رقم ٦.٣.٤

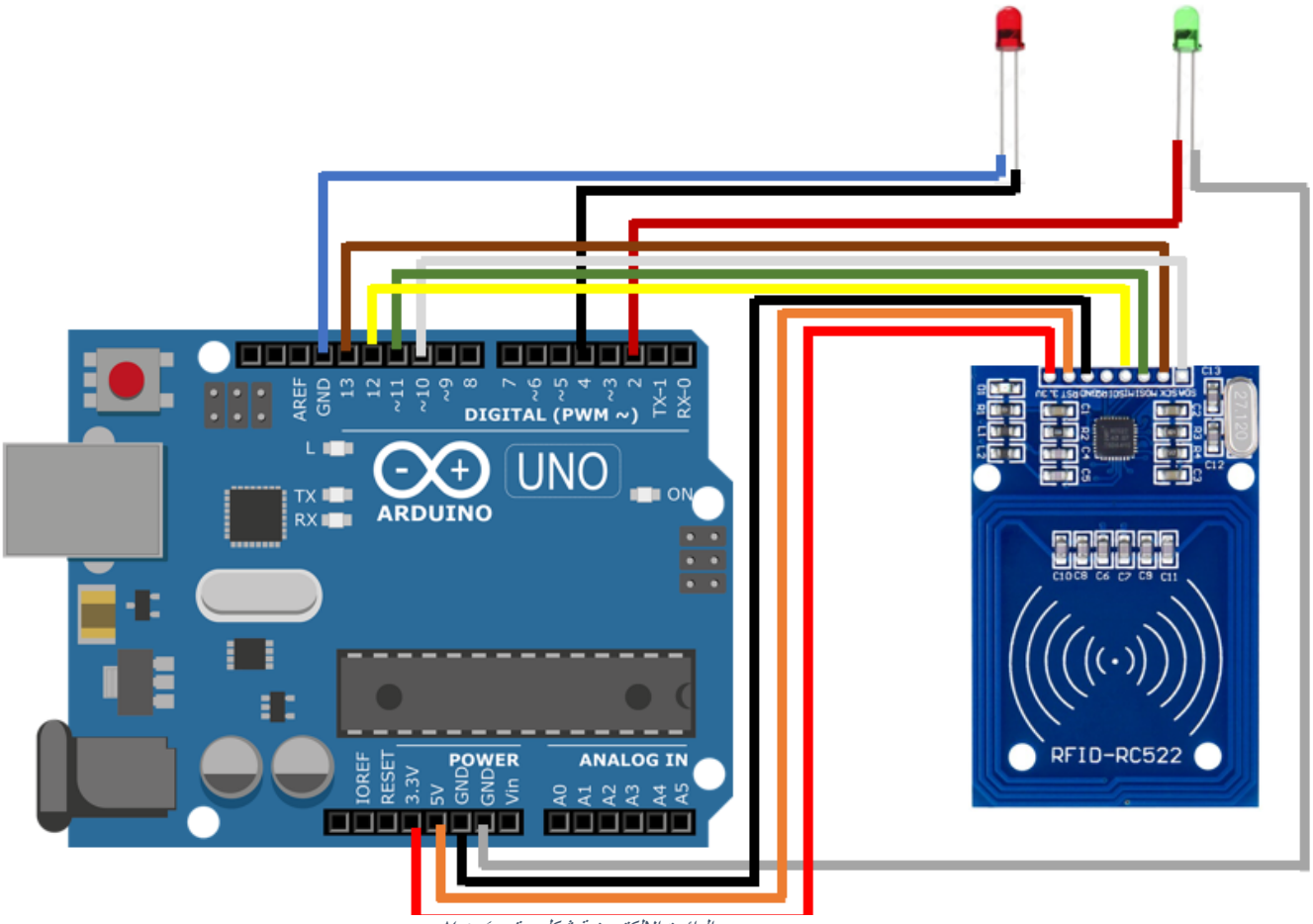
الفصل الرابع

مرحلة التصميم

٤.٤ الهدف من تصميم الدائرة الإلكترونية

الهدف من تصميم الدائرة الإلكترونية هو من أجل تلبية متطلبات النظام وصنع جهاز خاص بالحماية المعلوماتية بحيث كل قطعة موجودة في التصميم تلبي غرض معين ، و القطعة الرئيسية الا وهي اللوحة الأم لتكوين هذا الجهاز الأمني و أسم هذه القطعة الـ (Arduino) وتقوم هذه القطعة بمعالجة البيانات وترجمتها من لغة الإلة الى بيانات رقمية (١-٠) وتأتي هذه البيانات قبل ترجمتها من القطعة الاخرى التي بجانب قطعة الـــ (Arduino) وتسمى هذه القطعة بالـــ (RFID) وتقوم هذه القطعة المرتبطة بالقطعة السابقة بقراءة البطائق الممغنطة على شكل بيانات مشفرة لكي يتم أرسالها الى قطعة سابقة من أجل ترجمتها الى بيانات رقمية ، وإيضاً يوجد لدينا في المخطط لمبات (LED) وتقوم هذه اللمبات بلتمويض في ما إذا كانت البطاقة الممغنطة معرفة أو غير معرفة في النظام و السبب يرجع الى ارتباط هذه الدائرة الالكترونية بجهاز السرفر (Server) بحيث تسمى هذه الدائرة الالكترونية بجهاز (RFID Security) وذلك من خلال ما يقوم بة هذا الجهاز كدورة في الحماية بحيث تقوم هذه القطعة بتأمين أبواب المكاتب و إيضاً أنظمة العمل الموجودة في الاجهزة الحاسوبية .

٤.٥ تصميم الدائرة الإلكترونية



الدائرة الإلكترونية شكل رقم ٤.٥.٧

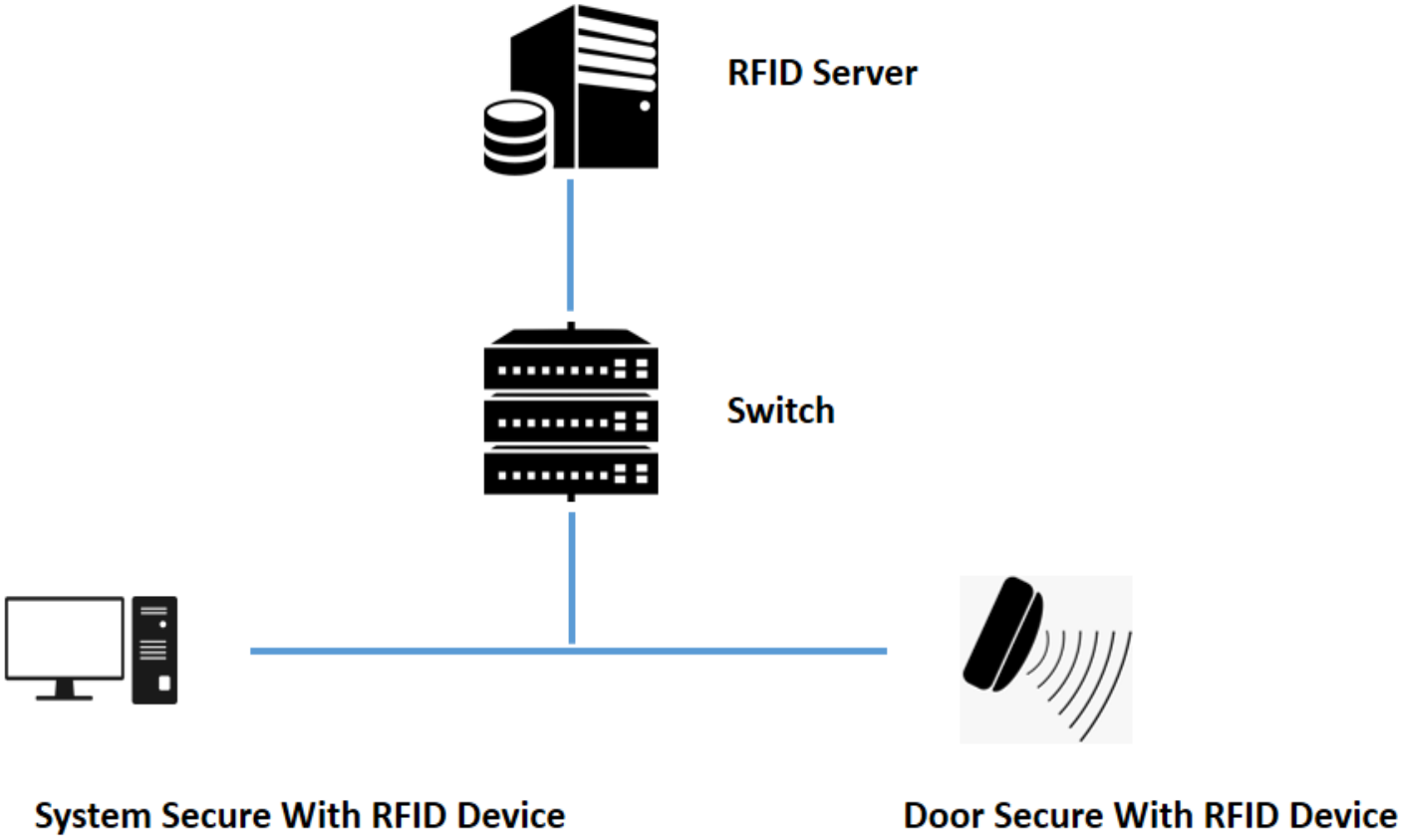
الفصل الرابع

مرحلة التصميم

٦.٤ الهدف من تصميم الشبكة

الهدف من تصميم وبناء هذه الشبكة هو تلبية المتطلبات الاساسية لنقل البيانات وإيضاً الاستخدام المرن وكونها شبكة داخلية خاصة بالنظام الأمني فأنها تلبي كافة أحتياجات كافة الموظفين في المؤسسة من عدة نواحي ، من الناحية الأمنية فيتم أستخدام هذه الشبكة من أجل ربط الاجهزة بنظام ، أما بالنسبة للناحية الاخرى الا وهي تسهيل وصول البيانات الى السرفر بشكل مرن ومتزأمن ، ويمكن أستخدام هذا النظام الشبكي في إي مكان يتعلق بالناحية الأمنية مثل المستشفيات كغرف العنايات المركزة وإيضاً الغرف الخاصة بمخازن البيانات المتواجدة في الشركات و المؤسسات الحكومية و الخاصة ويساعد هذا النظام الشبكي من الناحية الأمنية في سرعة أرسال البيانات الخاصة بالموظفين إلى مخزن البيانات الخاصة بلنظام الأمني .

٧.٤ تصميم الشبكة



تصميم الشبكة شكل رقم ٤.٧.٨

الفصل الخامس

مرحلة التنفيذ

الفصل الخامس

مرحلة التنفيذ

١.٥ المقدمة

سوف نقوم في هذا الفصل بعرض صور خاصة بالنظام الأمني و آلية عملة وفي كل ما يختص بواجهات هذا النظام وإيضاً عرض طريقة عمل الإجهزة و القطع المرتبطة بالنظام وقت التنفيذ وسيتم شرح كل عملية يتم القيام بها وقت التنفيذ من قبل كافة الموظفين وكذلك مدير النظام .

٢.٥ التنفيذ من ناحية واجهات ونوافذ النظام

هنا سوف يتم شرح كافة الواجهات و النوافذ التي تختص بألية عمل النظام الأمني كنظام حاسوبي ، سيتم هنا عرض معلومات عن النظام بشكل مفصل وقت التنفيذ ومنها الواجهه او النافذه الرئيسية والتي تحتوي على اولى الواجهات الا وهي واجهة الاتصال بالجهاز او القطعة التي تم اعدادها و برمجتها وتسمى بواجهة (Connection) ، وايضا الواجهة التي تليها الا وهي واجهة التعريف بالمستخدم وتسمى بواجهة (Check Data User) ، وايضا عرض محاكاة لكل صلاحية يتم منحها لكل موظف ،هذا فيما يختص بكافة الموظفين بخلاف المستخدم الرئيسي او الموظف الذي يدير هذا النظام ، فيما يختص بمدير النظام سيتم عرض واجهة ادارة بيانات النظام الأمني وتسمى بواجهة (Registration& Edit User Data) ، وايضا سيتم عرض الواجهة الخاصة بمراقبة سير العمليات التي تحدث في النظام مع عرض كل عملية ولوج تم في هذا النظام الأمني وإيضا أستخراج هذه المعلومات كتقارير وتسمى هذه الواجهة (Reports).

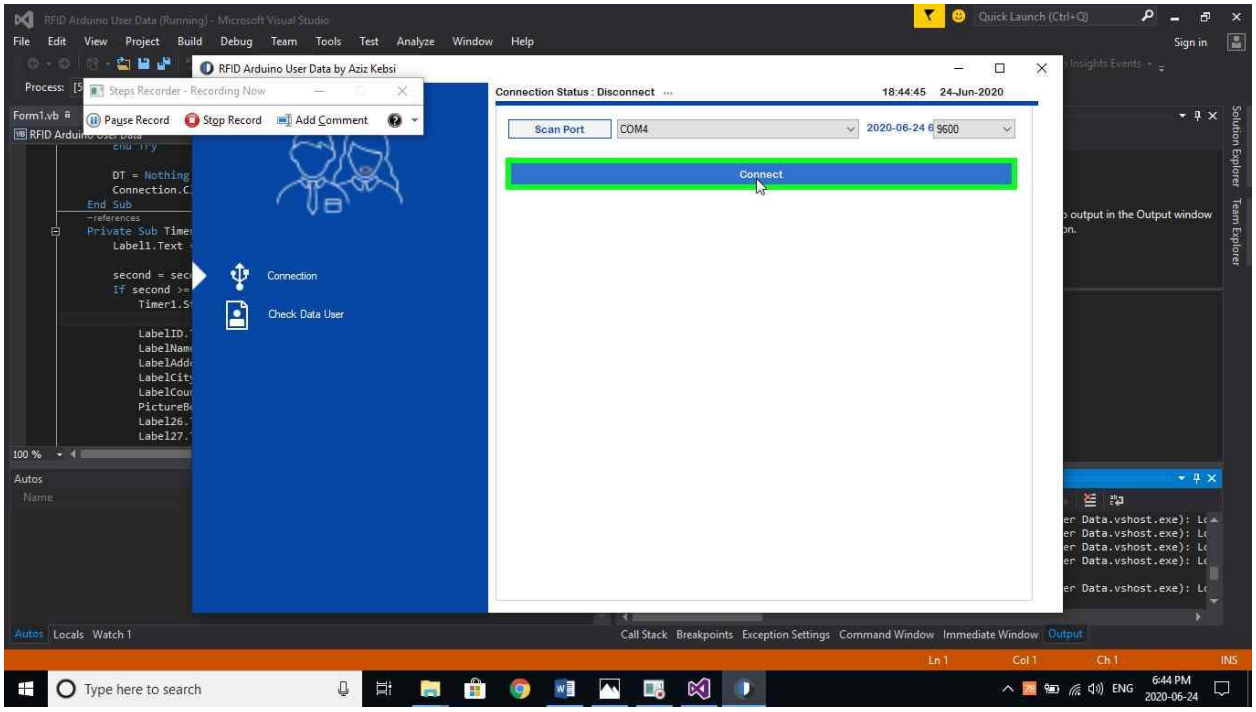
الفصل الخامس

مرحلة التنفيذ

١.٢.٥ واجهة الاتصال (Connection)

تقوم هذه الواجهة بربط الجهاز الذي يقوم بتحليل بيانات الموظفين والتحقق منها مع النظام الذي تم تصميمة لتلبية ذلك ، ويتم ذلك بمجموعة من الخطوات بشرح آلية عمل ربط النظام بالجهاز الذي يقوم بتحليل بيانات الموظفين كما في الاتي :

- أولاً : يتم الضغط على زر (Scan Port) والذي يقوم بفحص كل منافذ الجهاز الحاسب لأظهار المنفذ (Port) الخاص بجهاز التحقق من بيانات الموظفين (ARDUINO).
- ثانياً : تحديد المنفذ (Port) من خلال الاداة (Check Box).
- ثالثاً : يتم الضغط على زر (Connect) لبداء عملية الإتصال بلقطعة.



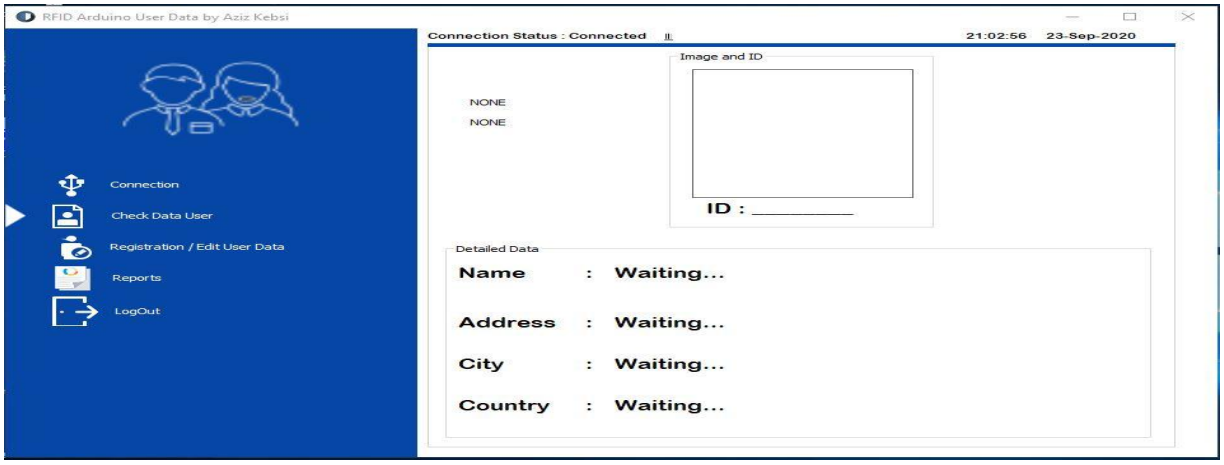
الفصل الخامس

مرحلة التنفيذ

٢.٢.٥ واجهة التحقق من بيانات المستخدم (Check Data User)

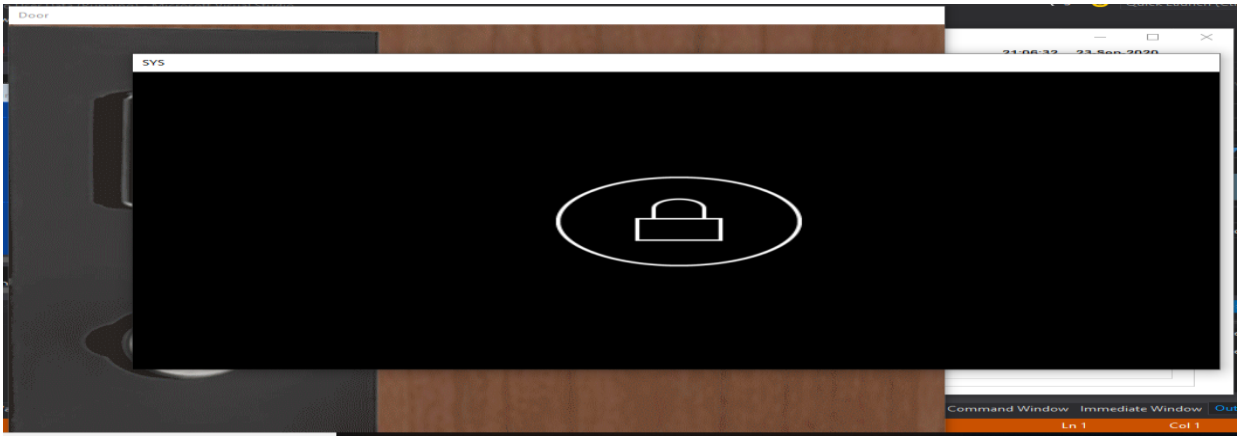
تقوم هذه الواجهة بعملية فحص لكلاً من البطاقة و قاعدة البيانات و التحقق من وجود رقم البطاقة على قاعدة البيانات بحيث يتم تمييز صلاحية هذا الرقم ما أذا كان مديراً أو مسؤول الـ (IT) أو موظف عادي و تحديد ما أذا كانت عملية الولوج كانت للنظام أو لفتح قفل الباب أو الرفظ في حالة عدم تطابق رقم البطاقة الممغنطة مع أرقام البطائق الممغنطة الموجودة على قاعدة البيانات لهذا النظام ، وسوف يتم توضيح ذلك من خلال عرض الخطوات التي يقوم بها الموظفين التي تختلف بأختلاف الصلاحيات بين كل موظف الى آخر :

- أولاً : تسجيل دخول مسؤول النظام سيتم ذلك من خلال وضع البطاقة على جهاز الـ (RFID) للولوج الى أعدادات النظام بعرض كافة الصلاحيات التي منحت لمسؤول النظام.



واجهة التحقق من بيانات المستخدم صورة رقم ٢.٥.٢

- ثانياً : تسجيل دخول موظف بحيث تكون هذه الواجهة في حالة الانتظار حتى يأتي الموظف ويضع بطاقتة الممغنطة في جهاز (RFID) من أجل الولوج الى مكتب الموظف ومن بعد التحقق من هوية الموظف من خلال التحقق من بيانات الموظف من على قاعدة البيانات يعود النظام لدينا بنتيجة القبول ثم أعطاء أمر لفتح الباب .



واجهة تسجيل دخول موظف صورة رقم ٢.٥.٣

الفصل الخامس

مرحلة التنفيذ

١- واجهة التسجيل و تعديل بيانات المستخدمين (Registration & Edit User Data)

في هذه الواجهة يتم إضافة و تعديل و حذف البيانات الخاصة بالموظفين او المستخدمين ويتم ذلك من خلال خطوات معينة يقوم بها مسؤول النظام والذي يمتلك الصلاحية للوصول الى هذه الواجهة وهذه الخطوات الا وهيا :

- الخطوة الاولى : وهي إضافة موظف والذي يمتلك صلاحية للولوج الى المكتب أو فتح أي باب من الابواب التي ضمن هذه الصلاحية ، يتم أضافة بيانات المستخدم الجديد من خلال أدخال بياناتة أما عن كيفية أضافة صورة المستخدم وهي تعتبر من ضمن البيانات المهمة لتعريف المستخدم وكما يتم قراءة وأضافة الرقم الممغنط للبطاقة الى جدول البيانات مع آلية حفظ البيانات للموظف الحالي :
- الخطوة الثانية : تعديل بيانات المستخدمين

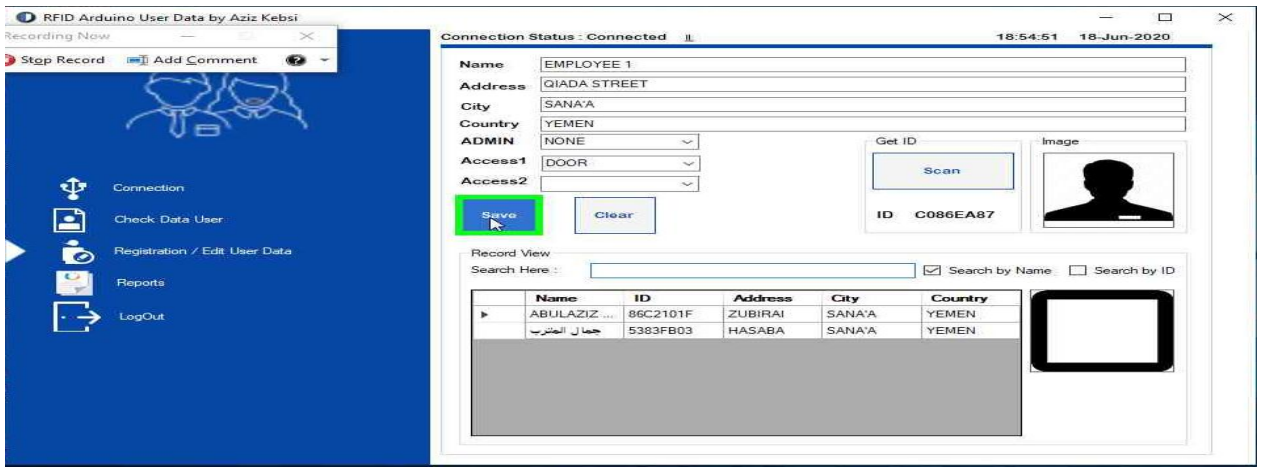
يتم تعديل بيانات المستخدمين أو الموظفين من خلال مجموعة من الخطوات التي لابد من أستخدامها لأنجاح عملية التعديل :

١- يتم تحديد المستخدم من خلال الضغط على زر (Scan) المراد تعديل بياناته عن طريق وضع البطاقة الممغنطة على الـــ (RFID) لكي يتم مسح رقمها ومن ثم يمكن تعديل أي بيانات يراد تعديلها أو تصحيحها:

٢- هنا يتم تعديل أو تغيير صورة الموظف بعد تعريف البطاقة الممغنطة على سبيل المثال تغيير الصورة فقط

٣- هذه الصورة توضح عملية أختيار صورة من الصور المراد التعديل بها ويجب أن تكون ذات حجم قليل كي تتقبلها قاعدة البيانات لأن من طبيعة قاعدة البيانات لا تتقبل الملفات الكبيرة ومن ثم الضغط على زر (Open) لتكملة عملية أستبدال الصور.

٤- هنا يتم الضغط على زر الحفظ (Save) لتعديل البيانات و تظهر رسالة تأكيد لتعديل البيانات المراد تعديلها كما في الصورة التالية :



1- واجهة التسجيل و تعديل بيانات المستخدمين صورة رقم ٥.٢.٤

الفصل الخامس

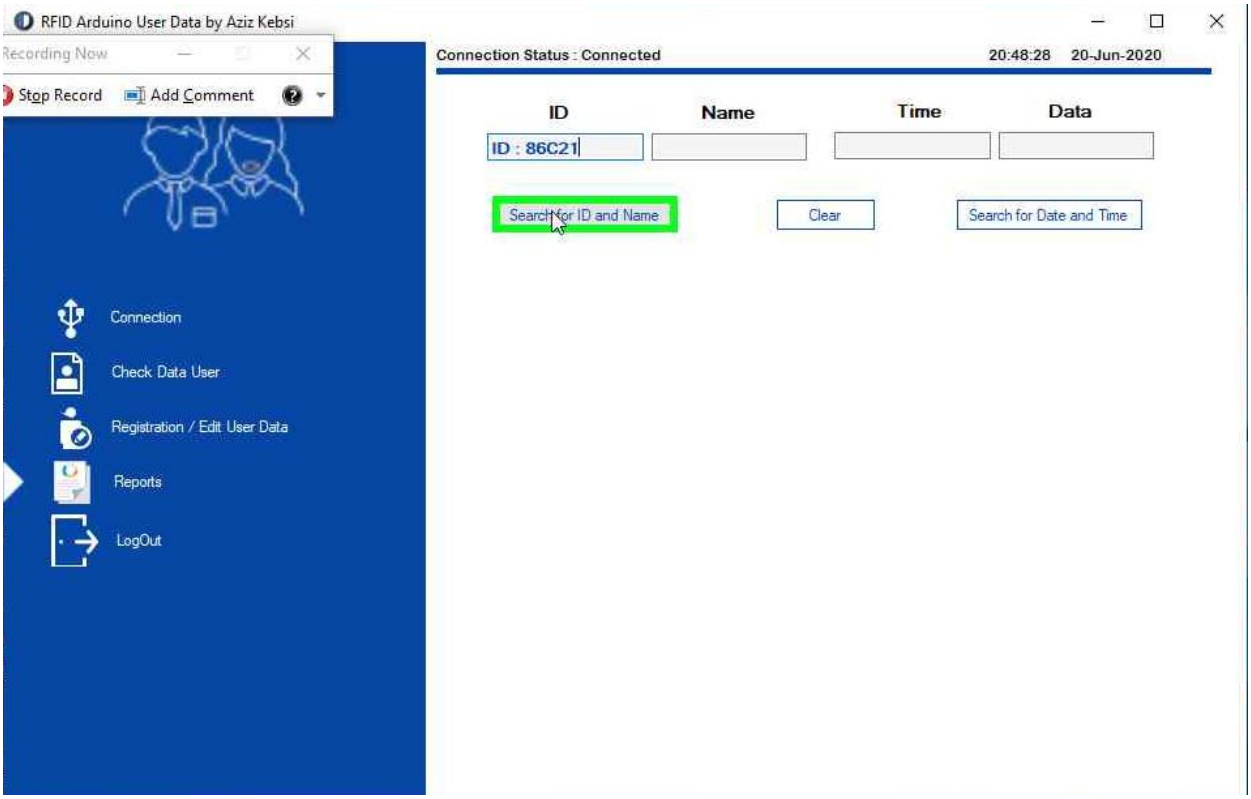
مرحلة التنفيذ

٢- واجهة عرض و إستخراج التقارير (Reports)

في هذه الواجهة يتم عرض كافة المعلومات التي تختص بالنظام الأمني و مستخدميها بكل التفاصيل من رقم البطاقة الممغنطة و أسم الموظف و تاريخ تسجل تلك العملية و وقتها ويتم عرض المعلومات و أستخراجها كتقارير بمجموعة من الخطوات وهي كالأتي :

- الخطوة الاولى : أستعراض البيانات بكافة انواعها

في مجموعة من الخطوات يتم البحث عن معلومات الموظف عن طريق رقم البطاقة و اسم الموظف و تاريخ ووقت تسجيل الدخول الى النظام الأمني وكما توضح الصورة التالية الية ادخال البيانات المراد عرض معلومات عنها :

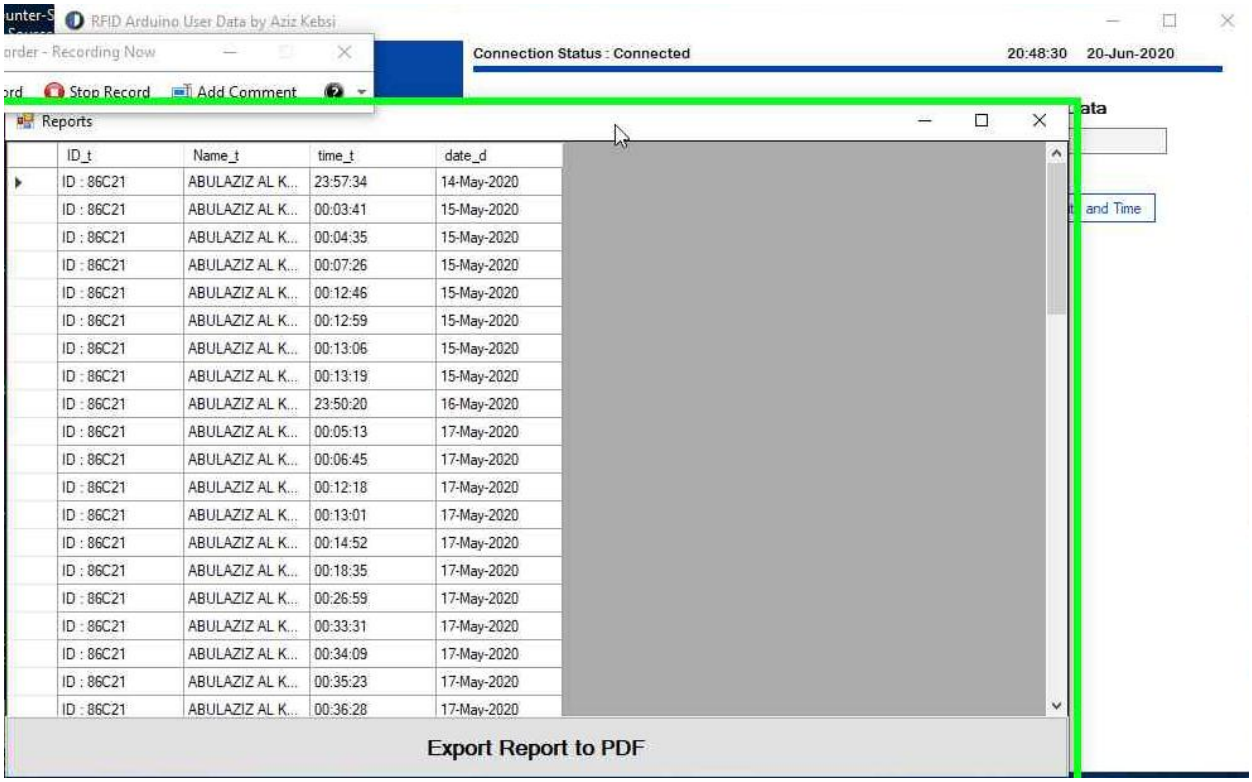


واجهة عرض و إستخراج التقارير صورة رقم ٥.٢.٥

الفصل الخامس

مرحلة التنفيذ

و هذه الصورة توضح نتائج المعلومات التي تم البحث عليها.



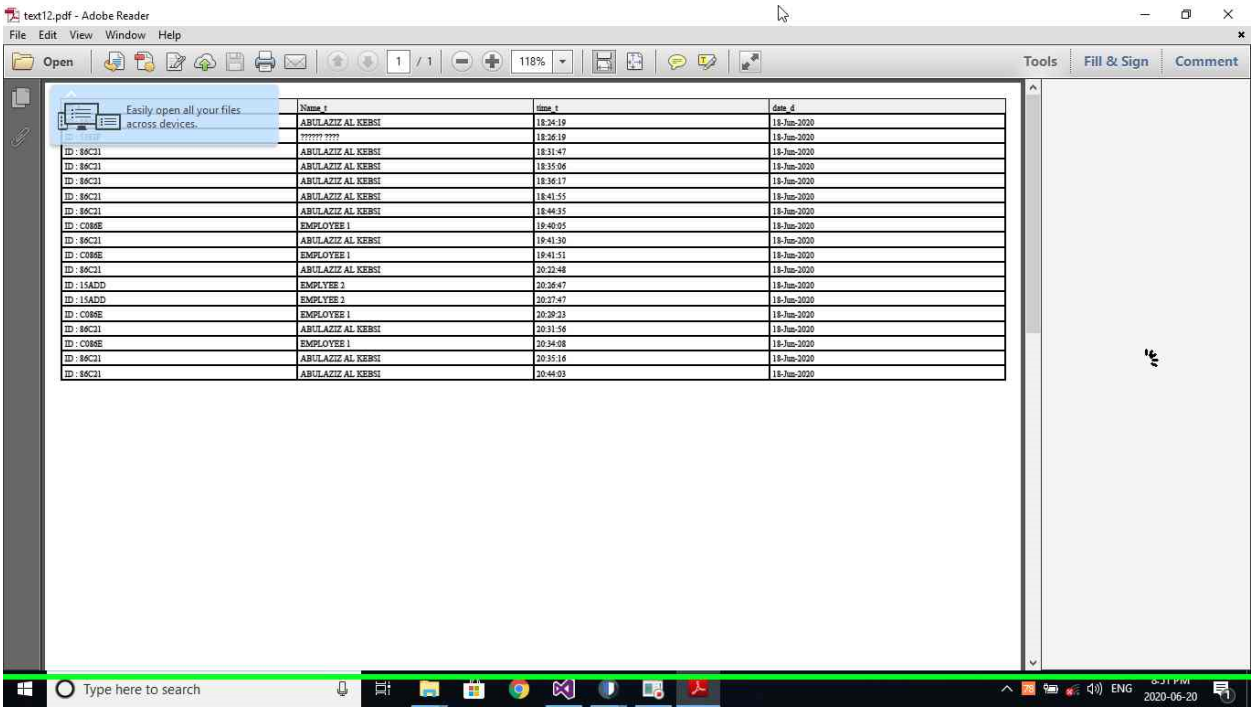
ID_t	Name_t	time_t	date_d
ID : 86C21	ABULAZIZ AL K...	23:57:34	14-May-2020
ID : 86C21	ABULAZIZ AL K...	00:03:41	15-May-2020
ID : 86C21	ABULAZIZ AL K...	00:04:35	15-May-2020
ID : 86C21	ABULAZIZ AL K...	00:07:26	15-May-2020
ID : 86C21	ABULAZIZ AL K...	00:12:46	15-May-2020
ID : 86C21	ABULAZIZ AL K...	00:12:59	15-May-2020
ID : 86C21	ABULAZIZ AL K...	00:13:06	15-May-2020
ID : 86C21	ABULAZIZ AL K...	00:13:19	15-May-2020
ID : 86C21	ABULAZIZ AL K...	23:50:20	16-May-2020
ID : 86C21	ABULAZIZ AL K...	00:05:13	17-May-2020
ID : 86C21	ABULAZIZ AL K...	00:06:45	17-May-2020
ID : 86C21	ABULAZIZ AL K...	00:12:18	17-May-2020
ID : 86C21	ABULAZIZ AL K...	00:13:01	17-May-2020
ID : 86C21	ABULAZIZ AL K...	00:14:52	17-May-2020
ID : 86C21	ABULAZIZ AL K...	00:18:35	17-May-2020
ID : 86C21	ABULAZIZ AL K...	00:26:59	17-May-2020
ID : 86C21	ABULAZIZ AL K...	00:33:31	17-May-2020
ID : 86C21	ABULAZIZ AL K...	00:34:09	17-May-2020
ID : 86C21	ABULAZIZ AL K...	00:35:23	17-May-2020
ID : 86C21	ABULAZIZ AL K...	00:36:28	17-May-2020

نتائج المعلومات التي تم البحث عليها صورة رقم ٥ .٢ .٦

الفصل الخامس

مرحلة التنفيذ

- الخطوة الثانية : أستخراج التقارير الى الملف الخاص بها وسيتم ذلك عن طريق مجموعة من الخطوات :
  - اولا : عرض لمعلومات المراد استخراجها كتقارير كما توضح الصور التالية :
- ومن ثم النقر على الزر الخاص بأستخراج التقارير(Export Report to PDF) لكي يتم أستخراجة على شكل ملف (PDF) .
  - ثانيا : تحديد مسار ملف التقرير المراد انشاة كما توضح الصور التالية :
  - ثالثا : فتح الملف الخاص بالتقرير المنشأه مسبقا كما توضح الصور التالية :
  - رابعا : استعراض التقرير بعد فتح الملف كما توضح الصور التالية :



أستخراج التقارير على شكل PDF صورة رقم ٥ .٢ .٧

الفصل الخامس

مرحلة التنفيذ

٣.٥ التنفيذ من ناحية الشبكة

١.٣.٥ طريقة تصميم الشبكة .

في هذه المرحلة تم تصميم الشبكة من خلال ربط جهازين لابتب من خلال توصيلة (Fast Ethernet) بحث أن الجهاز الاول يحتوي على السرفر الخاص بنظام الحماية بينما الجهاز الاخر يحتوي على النظام فقط أما بنسبة لفكرة الشبكة فقد تم أنشاها لعدة أغراض و أهم غرض هو الولوج الى السرفر للوصول الى قاعدة البيانات الخاصة بالنظام الأمني أما الغرض الاخر الى وهو عمل محاكاة خاصة بالشبكة كمثال بسيط للولوج الى السرفر وتم ذلك من خلال توزيع العناوين بين الجهازين و أستخدام العديد من البروتوكولات التي يتم من خلالها منح الصلاحيات للوصول الى قاعدة البيانات أو السرفر .

٢.٣.٥ الأجهزة و البرامج المستخدمة في الشبكة .

- الاجهزة المستخدمة :

١-أجهزة حاسوب نوع (laptop) العدد (٢) .

٢- توصيلة شبكية من نوع (Ethernet).

- البرامج المستخدمة :

١- البرنامج الخاص بالسرفر (Xampp).

٢- البرنامج المرتبط بالسرفر (Php MyAdmin) وهو نظام خاص بقاعدة البيانات المتواجدة في السرفر (Xampp).

٣.٣.٥ التقنيات و البروتوكولات المستخدمة في الشبكة.

- التقنيات و الخدمات :

١- تم أستخدام تقنية العنونة الجيل الرابع (IPV4).

٢- الخدمات (Service) التي يقدمها نظام التشغيل الخاص بالحاسوب للولوج الى أي سرفر أو أي خدمة.

- البروتوكولات المستخدمة في الشبكة .

١- بروتوكول ال(DNS).

٢- بروتوكول ال(TCP) المرتبط بالخدمات التي يقدمها نظام التشغيل .

٣- بروتوكول ال(DHTCP) ولن يتم أستخدامة الى في حالة توسيع النظام و الشبكة.

الفصل الخامس

مرحلة التنفيذ

٤.٣.٥ أعدادات الشبكة.

يوجد هنا جهاز سرفر وهو الجهاز رقم (١) ويحتوي على نظام Windows 10 اصدار ٦٤ bit ويحتوي هذا الجهاز على نظام الـ XAMPP ، والذي بدورة يقوم بجعل هذا الجهاز يعمل كسرفر لأن هذا النظام أو البرنامج يحتوي على المكونات أو مزايا تجعل هذا الجهاز يعمل كسرفر ومن هذه الميزات أو الخصائص الا وهي حزمة PHPMYADMIN وتعتبر هذه الحزمة كنوع من أنواع قواعد البيانات الا وهي SQL Server أما بالنسبة للخاصية التي تليها الا وهي حزمة Apache Server تتميز هذه الحزمة بكونها نوع من أنواع كغيرها مثل تقنية الـــ IIS والتي تعمل على جعل الجهاز يعمل كخادم أو سرفر و تمتاز هذه الخاصية على توسعة مدى تقنية البروتوكول أو التقنية التي تسمى بـــ Domain وهذه الخاصية تسمح بربط النظام المتصل بقاعدة البيانات مع كافة الاجهزة المتواجدة في الشبكة على مستوى الصلاحيات المطلوبة و كذلك كتعيين لعدد من الاجهزة الوصول الى الخاد أو السرفر بينما الخاصية الثالثة لهذا البرنامج الا وهي خاصية السرفس وتقوم هذه الخاصية بسماح المباشر و الغير مباشر بمشاركة كافة الخاصائص الذي يمتاز بها برنامج الـــ XAMPP.

يتوفر ايضاً هنا جهاز حاسوب آخر رقم (٢) يحتوي على نظام Windows 10 أصدار 64bit وإيضاً يحتوي هذا الجهاز على النظام الخاص بالحماية وذلك دون أحتوائة على قاعدة البيانات ولن يعمل النظام بدون الوصول الى قاعدة البيانات الا من خلال الشبكة المرتبطة بالسرفر وأيضاً يوجد هنا ضمن هذه الشبكة و كمكون أساسي الا وهو كابل الشبكة المسمى Ethernet والذي يقوم يقوم الجهاز رقم (١) الذي يعمل كسرفر مع الجهاز رقم (٢) لجعلهما يعملان ضمن شبكة واحدة.

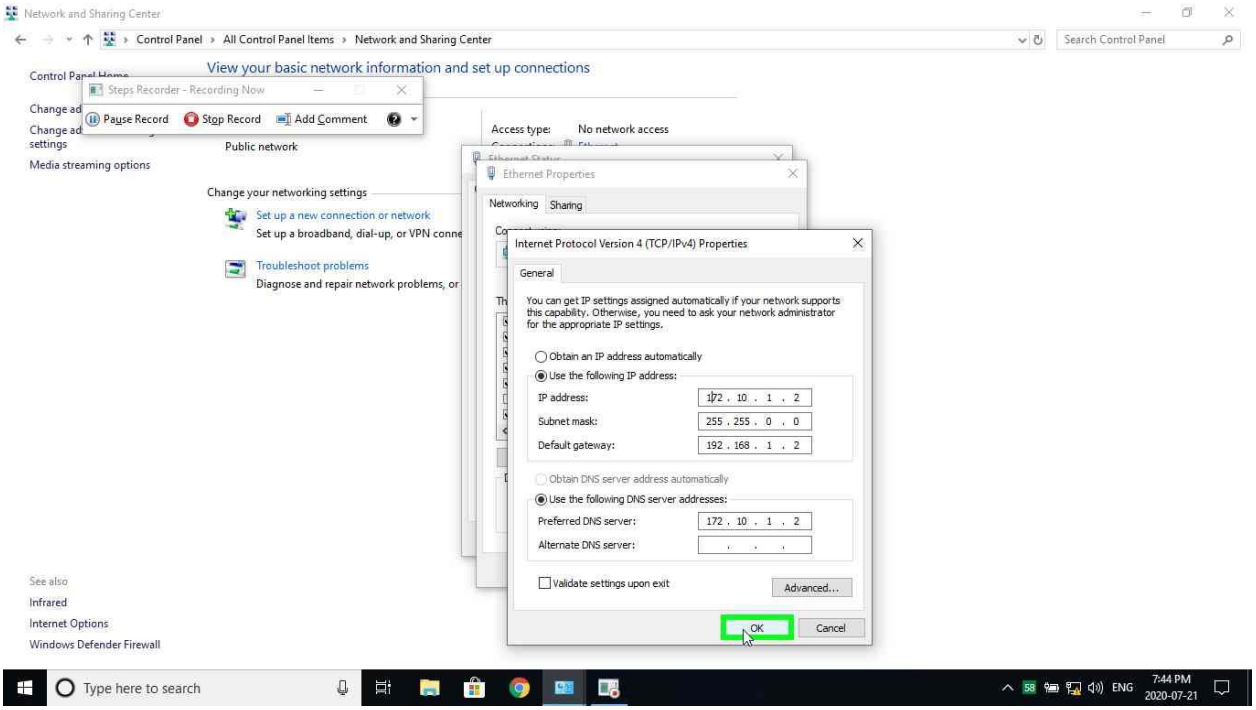
الفصل الخامس

مرحلة التنفيذ

- إعداد الحاسوب رقم ١ (السيرفر):-

هنا يتم الدخول الى قائمة (Control Panel) ثم يتم أختيار (Network & Sharing Center) بعد ذلك يتم الضغط على زر (Ethernet) الموضح بجانبة شكل الكيبل , من بعد الضغط على زر (Ethernet) سوف تظهر لنا نافذتة هنا يتم الضغط على زر (Properties) ،ويتم أختيار نوع الشبكة الا وهو (Internet Protocol Version 4 (TCP/IPV4) ،و يتم تغيير الخيار الى Use The Following IP Address : ومن ثم ضبط رقم الــ IP Address و الــ Subnet Mask بعد ذلك و أخيراً يتم ضبط الــ Default Gateway

في الصورة التالية يتم الضغط على زر (OK) لكي يتم حفظ أرقام الــ IP :



إعداد الحاسوب صورة رقم ٥ .٣ .٨

الفصل الخامس

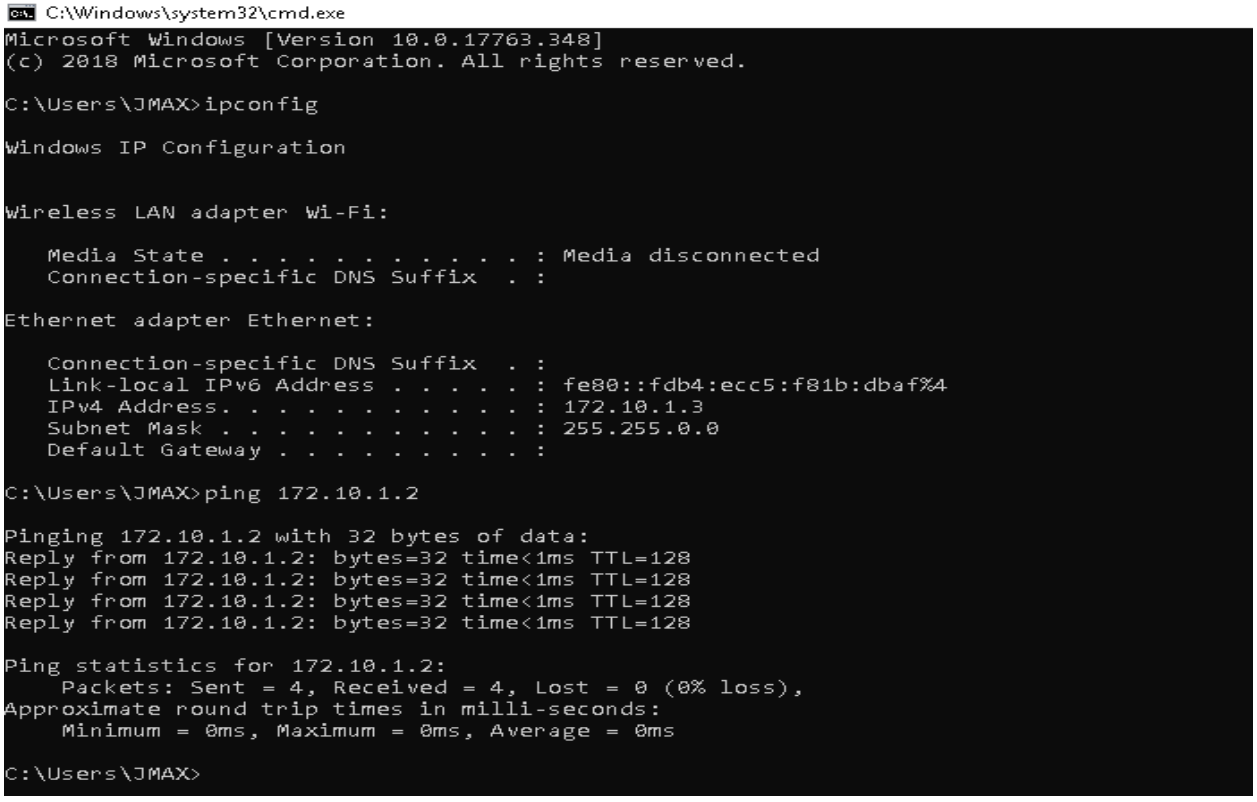
مرحلة التنفيذ

- اعداد الحاسوب رقم ٢ (الذي يحتوي على النظام الأمني):-

وسيتم ذلك بنفس الخطوات السابقة في اعداد الحاسوب رقم ١ الأ ان الأختلاف سيكون في العنوان الخاص بالجهاز ،في هذا الجهاز سوف يكون العنوان ١٧٢.١٠.١.٣ هذا للعنوان فقط ،اما بالنسبة لنطاق الشبكة (Default gateway) والخادم المسمى بال (DNS) سيكون ١٧٢.١٠.١.٢ لكلا الحقلين .

- اجراء فحص الاتصال من الحاسوب رقم ٢ الى الحاسوب رقم ١ (السيرفر):-

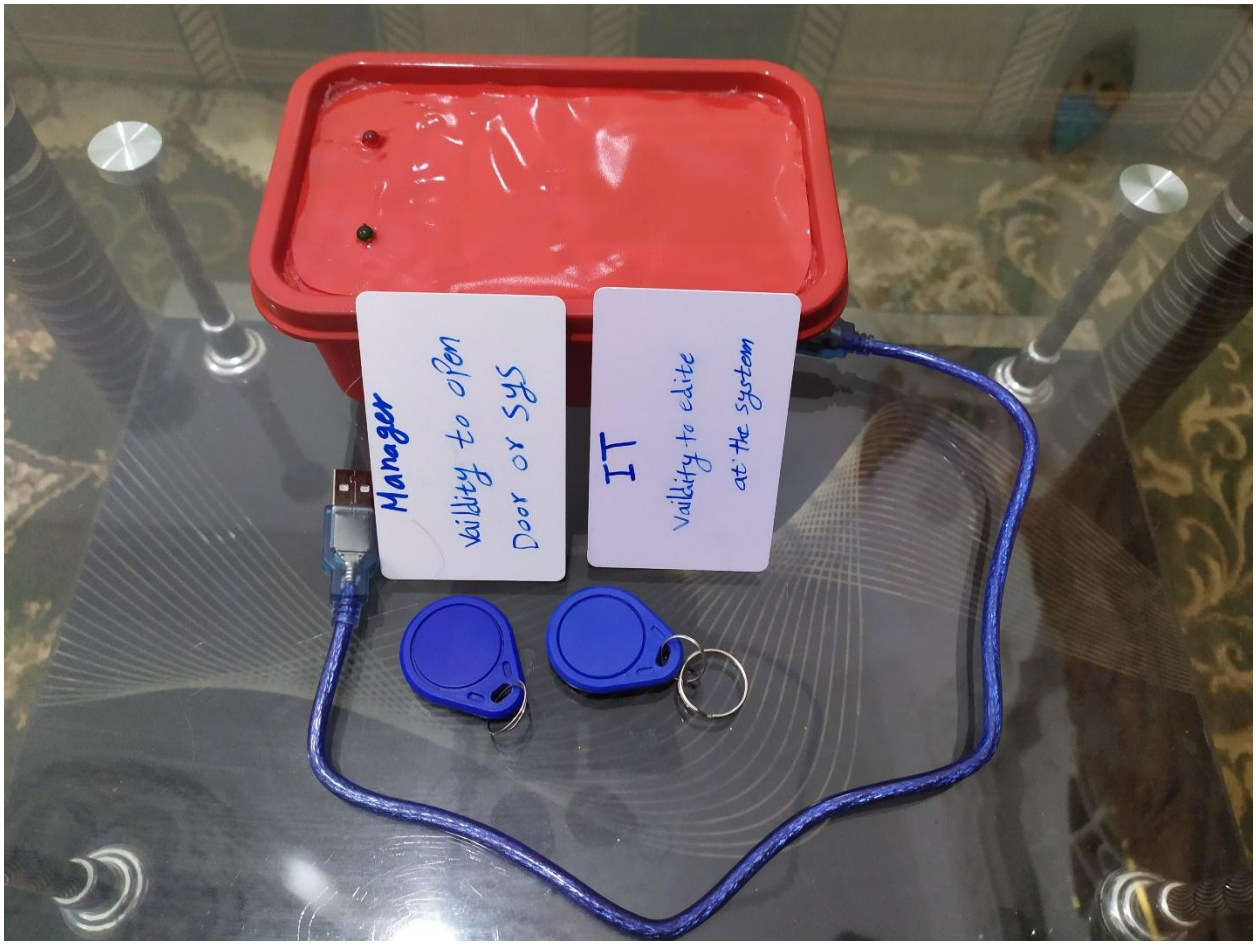
سيتم فحص الأتصال من خلال فتح نافذة ال (Run) من خلال الضغط على ويندوز مع الحرف R ، ومن ثم كتابة امر فتح شاشة موجه الأوامر ال (CMD) من خلال كتابة cmd على نافذة ال (Run) ،بعد ظهور شاشة موجه الاوامر سيتم كتابة الأمر الخاص بفحص الاتصال بين الجهازين الحاصوب والسيرفر وهذا الأمر هو (Ping 172.10.1.2) الخاص بالسيرفر وسيتم الفحص من الجهاز رقم ٢ ، وكما توضح الصور التالية .



الفصل الخامس

مرحلة التنفيذ

٤.٥ التنفيذ من ناحية القطع و الإجهزة المرتبطة بالنظام



يتم التنفيذ من ناحية القطع و الاجهزة المرتبطة بالنظام من خلال تصوير الاجهزة في الوقت الفعلي لكل عملية ومن تلك العمليات السماح للولوج و رفض الولوج بحيث أن هناك أشارات دلالية توضح نتائج هذه العمليات التي سوف نقوم بأجرائها للتأكد من أن الاجهزة المتواجدة داخل الصندوق متوافقة مع النظام .

التنفيذ من ناحية القطع و الإجهزة صورة رقم ٤.٥.١٠

الفصل الخامس

مرحلة التنفيذ

- العمليات التي سيتم اجرائها :-

١- عملية تسجيل الدخول للولوج الى النظام أو العمل (السماح بالولوج).

يتم وضع البطاقة اللمغنطة على الجهاز الفاحص الذي يقوم بفحص البطاقة للحصول على رقم البطاقة بعد عملية فك تشفيرها ومقارنتها مع أرقام البطائق الممغنطة المتواجدة على قاعدة البيانات ،يقوم الجهاز الفاحص بأرجاع القيمة من خلال تمويض احد الاضواء الخاصة بالأشعار بالسماح بالولوج كما توضح الصورة التاليه :

عملية السماح بالولوج صورة رقم ٥.٤.١١

الفصل الخامس

مرحلة التنفيذ

٢- عملية تسجيل الدخول للولوج الى النظام أو العمل (رفض الولوج).

يتم وضع البطاقة اللمغنطة على الجهاز الفاحص الذي يقوم بفحص البطاقة من نوع ميدالية للحصول على رقم البطاقة بعد عملية فك تشفيرها ومقارنتها مع أرقام البطائق الممغنطة المتواجدة على قاعدة البيانات ،يقوم الجهاز الفاحص بأرجاع القيمة من خلال تمويض احد الاضواء الخاصة بالأشعار برفض الولوج كما توضح الصورة التاليه :

عملية رفض الولوج صورة رقم ٥.٤.١٢

الفصل السادس

الأستنتاجات والمعوقات والتوصيات

الفصل السادس

الأستنتاجات والمعوقات والتوصيات

١.٦ المقدمة

هذا الفصل هو الفصل الأخير في هذا المشروع او البحث ،ولذي من خلاله سيتم ذكر ما تم استنتاجه من خلال عمل هذا النوع من الأنظمة الأمنية ،وايضا ذكر المعوقات التي واجهناها في انجات هذا النظام ،واخيرا ذكر التوصيات لمن اراد ان يعمل نظام مشابه او تطويره او التعديل لهذا النظام .

٢.٦ الاستنتاجات

- ان النظام قادر على انجاز المهام والعمليات التي تم بناء النظام من أجله.
- ان النظام يساعد في توفير الحماية للمكاتب والأجهزة الحاسوبية ويوفر الجهد لكل من الأمن والأدارة من عدة نواحي ، وايضا الدقة العالية في تحليل بيانات الموظفين الخاصة بالحضور والأنصراف .
- ان النظام يعكس كل المشاكل في النظام السابق او البدائي الى حلول ذكية وتقنية تساعد في مجال الحماية المعلوماتية وايضا الحماية المادية .

٣.٦ المعوقات

واجهنا هنا في هذا النظام الكثير من المعوقات ومن ابرزها المعوقات المادية وذلك لتنفيذ افكار جديدة واقتراحات جديدة تساهم في تطوير المشروع وجعلة ناجحا بنسبة ٩٩% وذلك من خلال توسيع نطاق الشبكة وايضا شراء العديد من الاجهزة والمتحكمات الذكية وايضا الأقفال الألكترونية وذلك لجعل النظام ذو خصائص عالية ومتميزة من حيث السيطرة بشكل كامل على الحماية المعلوماتية والأمنية ،اما المعوق الثاني الا وهو الوقت لم نملك الوقت الكافي لتطوير المشروع وايضا الخبرة التي تحتاج الى الوقت لأنجاز المهام والوظائف والأضافات الى النظام الموجودة تحت عنوان التوصيات في هذا الفصل .

الفصل السادس

الأستنتاجات والمعوقات والتوصيات

٦.٤ التوصيات

- استكمال بناء وتطوير الشبكة من ناحية المعدات والأجهزة لتوسيع نطاق الشبكة وايضا نطاق الحماية .
- توسعة الشبكة وربطها ظمن شبكة خارجية وداخلية بأستخدام الأجهزة الحديثة .
- تحديث وتطوير الاجهزة الذكية وايضا اجهزة الفحص والتعرف على الهوية .
- الأخذ بعين الاعتبار بأن المحاكاه اساس بناء اي نظام حماية او نظام خدمي .
- تعيين مسؤل خاص بأنظمة الحماية وان يكون مختص في تقنية المعلومات لأدارة النظام الأمني .

المراجع

١- Mohanna, Mohammed (٢٠١٨-٠٥-٣٠). "نظرية التصنيع والبناء" Mohammed Mohanna (باللغة الإنجليزية) مؤرشف من الأصل في ٠٧ ديسمبر ٢٠١٩ . اطلع عليه بتاريخ ٢٠ أغسطس ٢٠١٩

٢- Klaus Finkenzeller, RFID Handbook, Radio-Frequency Identification Fundamentals and Applications, Wiley, 1999

٣- موسوعة Wiki (https://wiki.hsoub.com/Arduino)

٤- The Programming Languages Beacon v16 - March 2016

٥- MySQL Developer Zone

٦- the science of secrecy from ancient Egypt to quantum cryptography

٧- Sina Misr

٨- "Methods to Protect Information" www.searchinform.com, Retrieved 20-9-2018. Edited.

٩- "PROTECT YOUR INFORMATION FROM PHYSICAL THREATS", www.securityinabox.org,28-6-2018، Retrieved 20-9-2018. Edited.

١٠- Ways to Enhance Data Security www.globalsign.com، 2017، Retrieved 20-9-2018. Edited.