



الجمهورية العربية السورية

جامعة دمشق

كلية الهندسة المعلوماتية

End to End secure trans

تقرير إنجاز المشروع 1/ في الهندسة المعلوماتية

مُسَوِّدَة

احمد الابراهيم

نتالي سامر صوان

عبدالرحمان حريدين

علاء زيد الخضر

Ninja Team

Supervisor : Ahmad Amadani

28/April 2020

الملخص:

بسبب انتشار التكنولوجيا والملفات المشتركة أصبح من المهم الاهتمام بمواضيع مشاركة الملفات وضمان حماية الملفات وسهولة تنفيذ أعمال الأشخاص حتى نحقق أكبر فائدة من استخدام هذه التقنيات الجديدة ، يتضمن هذا التقرير شرح المشكلة التي تتعرض لها الكثير من الشركات والمؤسسات وسوف نقوم بتقديم الحلول الشائعة والمشاكل التي تواجهها بسبب استخدام هذه الحلول ، وسوف نتطرق الى دراسة الاحتياج لهذا المشروع ولماذا قررنا تطبيق هذا المشروع وما الفائدة المرجوة منه ، ثم يوجد جدول لشرح المصطلحات الخاصة بالمشروع حيث لم يتم شرح مصطلحات المعلوماتية المتفق عليها ، ثم دراسة متطلبات المشروع وفي هذا القسم سوف يتم عرض الخدمات الاساسية التي سوف يتم تحقيقها وهي اساس التطبيق وبعدها سوف نتجه الى المتطلبات غير الوظيفية حيث هذه المتطلبات لا تكون على تماس مباشر مع المستخدم وانا المتطلبات التي يجب توافرها لتطبيق مثل (متطلبات الاداء ، الامان ، التخزين ، العميل) ، وسوف يتم تمثيل مخططات الاستخدام مع شرح عن جميع الحالات التي قد يختارها المستخدم بالاضافة الى اصحاب المنفعة من التطبيق ومن يمكنه استخدام التطبيق والفاعلين واهدافهم ، يوضح مخطط الصفوف ترابط الصفوف مع بعضها وقابلية تطوير المنتج حيث تم بناء التطبيق حتى يتمكن الفريق البرمجي من تطوير التطبيق حسب الحاجة ، وضمن قسم واجهات الاستخدام سوف يتم شرح كيفية استخدام البرنامج ، وكيف يمكننا التنقل بين واجهات الاستخدام والاختفاء التي قد تواجهها ، ثم القسم التقني الذي يشرح الانظمة الجزئية للتطبيق حيث تم استخدام Client/server model بالاضافة الى شرح كيف تقسم النظمة المتوجدة لدينا على العتاد ، ثم سوف يتم شرح اللغة والبرتوكولات المستخدمين مع مقارنات لتوضيح الفرق وافضلية الاستخدام ، بالاضافة الى المعلومات التي سوف يتم تخزينها وتدفق التحكم الاجمالي حيث سوف يتم شرح الاعتماد على الوقت بالاضافة ترتيب تدفق المعطيات والمعلومات ثم التساير حيث سوف يتم شرح النسيب التي قد نحتاجها ونستخدمها ، خطة تقسيم العمل تشرح كيفية تحقيق المتطلبات باسرع شكل بالاعتماد على Agile وفي النهاية الخاتمة والمراجع التي تم جمع التقرير منها وتحقيق المتطلبات .

الكلمات المفتاحية:

Cryptography, RMI, File, Sharing, Store



جدول المحتويات



الفصل الأول:

المقدمة:

بسم الله الرحمن الرحيم

وقل ربي زدني علماً ، بهذه الجملة احببت ان ابدأ مقدمة بحثي نظراً لحبي الشديد لهذه الآية ولأنها تمثل شعار الجامعة التي درست وترعرت بها (جامعة دمشق)، أما بعد .. نقدم هذا البحث إلى جميع من يهتم بالعلم وإلى الاستاذة في جامعتنا والمشرفين علينا بالإضافة الى زملائنا الطلاب في السنوات التالية وإلى كل من يجمعنا بهم رباط العلم من الاصدقاء ، وهذا البحث هو بعنوان (End to End secure Tran) ويتحدث عن (مشاركة البيانات وتخزين الملفات على مخدمات خاصة) ونتمنى أن ينال استحسانكم وأن يكون بحث ملم بكل البيانات والمعلومات المطلوب أن يغطيها حيث تم كتابة (الدراسة المرجعية ، دراسة المتطلبات ، التصميم التقني ، التنجيز والتحقيق). سوف نضع بين أيديكم هذا البحث ونتمنى أن يكون في المستوى المرغوب ونأمل من الله عز وجل أننا لم نهمل أو نقصر في كتابة هذا البحث وتجميعه، ولم نقصر فيما يحتوي عليه من عناصر وأهداف متعددة. وقد حرصنا في هذا البحث على أن نوفق كل العناصر وبعض العوامل التي يصعب ان تتوافق سوياً، حيث تعتبر الساعات والدقائق هي من العوامل التي يجب أن تتخذ في الاعتبار حيث نقسم الوقت بين المهام التي يتكون منها المشروع المطلوب تحقيقه . وقد قمنا بتجميع هذه الموضوعات لتحقيق الهدف الأسمى وهو توصيل العلم والمعرفة ونتمنى من الأساتذة والقراء أن ينظروا إلى كل قسم ومادة علمية بنظرة بها نوع من العمومية كذلك يجب أن يتجنبوا النظر إليها نظره جزئية. ونرجو ألا يبخل علينا الأساتذة والطلاب بملاحظاتهم ومقترحاتهم البناءة والهادفة لتصحيح أي أخطاء حتى نحاول تفاديها لاحقاً ونحاول أن نطور من أنفسنا وكذلك نقوم بتصحيح الأخطاء التي تقع فيها أولاً بأول. ونتمنى من الله عز وجل أن يتم علينا نعمته ويديم علينا علمه ويحفظنا ويحفظكم جميعاً من كل سوء ويحفظ وطننا العظيم من الأعداء .

ونسأل الله أيضاً أن يكتب لنا النجاح والتوفيق إلى كل ما يحبه ويرضيه.



الفصل الثاني: الدراسة المرجعية:

تم كتابة الدراسة المرجعية بعد البحث عن المشكلة بشكل عام حيث قام فريق التطوير بتحديد النقاط الاساسية:

تكون المشكلة حيث اغلب الشركات والمؤسسات الحكومية تقوم بتخزين البيانات ومشاركتها دون الحاجة الى طرف ثالث او وسيط حيث تهتم هذه المؤسسات بسرية البيانات وطرق التشفير الخاصة بالشركة والكلفة المنخفضة للتخزين ، بالاضافة الى تخزين البيانات ورؤية من قام بتحميل الملفات والاشخاص التي تمتلك صلاحية التحميل على الملف ، بلاضافة الى ان بعض الشركات تعتمد مبدا عرض نماذج المسابقات ، او نموذج السيرة الذاتية على لوحة الاعلانات حيث ترغب بعض هذه الشركات الى مشاركة النموذج الى الاشخاص عن طريق تحميل الملفات عن طريق التطبيق الخاصة بالشركة ، وتسعى العديد من الشركات الى مشاركة البيانات وضمان جودة الخدمة وسرعة نقل البيانات وبلاضافة الى التنافس بالاسعار لخلق روح التنافس الى ان بعض البيانات لا يمكن تخزينها على سحابة عالمية وهذا ما نلاحظه على عدد كبير من المؤسسات والشركات ضمن سوريا لذلك كان لابد من دراسة انشاء نظام لمشاركة الملفات ويحتوي ميزات المشاركة بشكل عام حيث ان التطبيق ليس محصور بشركة معينة او انما التطبيق يمكن استخدامه على جميع الشركات او المؤسسات بالاضافة الى التطبيق مفتوح المصدر ويمكن التعديل عليه من مدير التطبيق او فريق التطوير لكي ساعد جميع الشركات والمؤسسات ، وبعد تقييم نتائج الاستبيان الذي طرح على عدد من الاشخاص ضمن الجمهورية العربية السورية تبين ان اغلب هؤلاء الاشخاص يفضلون التخزين على الخدمات الخارجية نظرا للميزات التي توفرها ولاكن لا يتطيعون نظرا الى سرية البيانات والكلفة ، وبعد حساب نسبة المؤسسات والشركات التي تقوم بتخزين البيانات بشكل مركزي تبين لنا انه اغلب الشركات تهتم بتخزين البيانات بشكل مركزي على خدمات خاصة ، وبعد الحصول على النتائج السابقة قرر فريق التطوير انشاء تطبيق يراعي كفة الخدمات العامة من مشاركة الملفات والمجيب الالي الى ضمان تخزين البيانات بشكل محلي ومركزي ومحاولة الفريق تحقيق عدد من ميزات الضمن برامج المشاركة العالمية بالاضافة الى بعض الخدمات الخاصة التي تساعد المستفيدين من تحقيق اعمالهم بشكل اكثر مرونة .

الاصدارات السابقة:

رقم الاصدار	المؤلفون	الشرح	التاريخ
1.0	علاء الخضر ، نتالي صوان احمد الابراهيم، عبد الرحمن حريدين	التصميم الاول حيث تم تعبئة جميع المتطلبات الادارية من التقرير	4/26/2020



الفصل الثالث: دراسة المتطلبات:

1. سيرفر يقوم بتخزين ملفات المستخدمين بشكل مركزي.
2. رفع وتحميل الملفات من السيرفر عن طريق التطبيق بشكل متزامن.
3. تخزين البيانات بشكل مشفر ويفضل استخدام خوارزمية AES & RSA.
4. تنفيذ إنشاء المفاتيح الخاصة والعامة.
5. دعم بروتوكول handshaking الذي يقوم بتبادل مفتاح التشفير بين المرسل والمستقبل.
6. بوت يقوم بالإجابة على العملاء الذين يحتاجون الى تحميل الملفات الأساسية
7. تسجيل جميع نشاطات المستخدم والاحداث التي قام بها.

توصيف مشكلة المستخدم

توصيف المشكلة:

قمنا بوضع التصور الأولي للمشروع بناء على المشكلة التي تتعرض لها اغلب الشركات والمراكز الحكومية من ناحية مشاركة الملفات بين أعضاء الفريق حيث يوجد ملفات لا يمكن مشاركتها عبر برامج المشاركة العالمية نظراً لخصوصية الملفات التي تتم مشاركتها والى التكلفة العالية التي تطلبها شركات مشاركة الملفات بالإضافة الى تخزين المعطيات بشكل مركزي ضمن المبنى وبالإضافة الى تطبيق طريقة تشفير بيانات خاصة بالشركة وعدم استخدام الطرق الشائعة ونظراً للحاجة لتحميل قسم من الملفات للعملاء بشكل يومي دون الحاجة الى إنشاء حساب للعميل أي يتم تحميل الملفات عن طريق مجموعة من الروابط يقوم المجيب الالي بالاجابة على العملاء لكي يتم مشاركة رابط الملف الذي يطلبه المستخدم ومجيب الذي يقوم بإرشاد المستخدم حول انشاء حساب جديد وتسجيل الدخول .



قائمة بالمصطلحات:

في هذا القسم يمكن تعريف وشرح بأية مصطلحات في مجال المشروع قد تكون مبهمة، واستخدامها بشكل متناسق عبر كامل التنسيق. لم يتم التعريف بالمصطلحات المعلوماتية العامة المتفق عليها، والتركيز على المصطلحات الخاصة في سياق المشروع تحديداً.

English term	Arabic term	description
BOOT	المجيب الالى	المجيب الالى سوف يقوم بلاجابة على طلبات المستخدمين
Client	العميل	اي شخص يتصل بالتطبيق
ASR	خوارزميات التشفير	طريق تشفير البيانات
RSA		
handshaking	برتكول المصافحة	يقوم بإنشاء قناة مشاركة والتأكد من التشفير
User-Id	الرقم التسلسلي للمستخدم	الرقم التسلسلي للمستخدم ضمن المخدم
File-Id	الرقم التسلسلي للملف	الرقم التسلسلي للملف ضمن ملفات المخدم
Download-Id	الرقم التسلسلي للتحميل	الرقم التسلسلي للملف التي تم تحميله ضمن ملفات المخدم
Authentication	المصادقة	تستخدم للتأكد من كلمات المرور وتسجيل الدخول
Workshop	مجلد مشترك	المجلد الذي يملك أكثر من مستخدم
receiver	المستلمين	الأشخاص الذين يتم مشاركة الملفات معهم
File Save	الملفات المحفوظة	الملفات التي تم تخزينها على المخدم
File Share	الملفات التي تم مشاركتها	الأشخاص الذين يتم تحديدهم لمشاركة الملفات معهم
User Permission	صلاحيات المستخدم	صلاحيات المستخدم للتعديل على الملف ضمن مجموعات العمل
P2PCast	مشاركة بين طرفين	ارسال الرسالة الى مستخدم محدد



متطلبات النظام:

قائمة المتطلبات الوظيفية:

رقم المتطلب	شرح موجز عن المتطلب
1	سيرفر لتخزين المعطيات .
2	واجهة انشاء حساب جديد للمستخدم واستعادة كلمة المرور
3	جميع المستخدمين الذين يقومون برفع البيانات يملكون حسابات خاصة بالتطبيق.
4	تشفير جميع البيانات وتخزينها على المخدم بشكل دائم.
5	إمكانية رفع وتحميل جميع انواع الملفات الى السيرفر.
6	إرسال الملفات الى المستخدمين الآخرين عن طريق التطبيق
7	قفل الملفات بكلمة سر وتطلب من المستخدم قبل التحميل.
8	يمكن تحميل ملف بدون حساب عن طريق رقم رابط معين(ID)
9	تطبيق مجموعات عمل وتحديد الأشخاص الذين يتعاملون معها.
10	السماح بالردشة عن طريق التطبيق.
11	عرض الملفات وتفاصيل الملفات ومع من تمت مشاركتها ومن قام بتحميل الملفات
12	حظر (حذف)المستخدم من التطبيق وحذف صلاحياته
13	موافقة مدير التطبيق على استعادة كلمة المرور الخاصة بالمستخدم
14	عرض معلومات المستخدم(الشخصية، الملفات التي قام بمشاركتها)
15	مجيب آلي يقوم بالاجابة على طلبات المستخدمين



متطلبات أخرى للنظام

متطلبات المخدم:

- ✚ لا يجب استخدام قواعد البيانات **الاعلاقية** وإنما يجب الاكتفاء باستخدام الأنماط المتاحة من الملفات .
- ✚ جميع الملفات التي توجد في المخدم مشفرة ولا يتم فك تشفير الملفات إلا ضمن أجهزة المستخدمين
- ✚ جميع قيم المقارنة التي تتم ضمن المخدم تتم عن طريق مقارنة القيم المشفرة مع القيم المخزنة ضمن الداتا أي لا يتم فك تشفير البيانات ضمن المخدم.
- ✚ يمكن تغير جميع القيم الافتراضية عن طريق المخدم.

متطلبات العميل:

- ✚ لا يتم ارسال الملفات الا بعد التأكد من التشفير الكامل للملفات
- ✚ واجهات استخدام سهلة وتفاعلية ذات الألوان متناسقة
- ✚ العميل يمكنه تحميل الملفات من الحاسب او من الهاتف المحمول نظام اندرويد 5.0.1 وما فوق.

متطلبات الأداء:

- ✚ لا ينهار هذا البرنامج فجأة في أي كارثة مثل انقطاع الطاقة.
- ✚ يجب أن يكون جدول هذا البرنامج في أذهاننا.
- ✚ يجب أداء كل وظيفة بشكل جيد.
- ✚ في كل خطوة يكون ناتج المرحلة الأولى هو مدخل المرحلة الأخرى وستكون موثوقة ودقيقة.
- ✚ يجب أن يؤخذ عامل الخطر كخطوة أولية لتحسين التطبيق .
- ✚ بالنسبة للمستخدم الفردية ، سيكون الأداء جيدًا.
- ✚ لتسجيل الدخول بكلمة مرور ، سيتم مطابقة اسم المستخدم مع كلمة المرور مع القيم المخزنة ضمن الداتا.
- ✚ حفظ في قاعدة البيانات وبالتالي يمكن فقط للمستخدمين المصرح لهم تسجيل الدخول.
- ✚ ستكون هناك طرق مختلفة لاستعادة البيانات ووقت أقل.
- ✚ لا يتم مشاركة الملفات التي يزيد حجمها عن 3 ميجا.

متطلبات الأمن:

- ✚ سيكون هناك تأمين مناسب فيما يتعلق بالوصول إلى البيانات.
- ✚ يمكن توفير الأمن الخارجي عن طريق إعطاء مصادقة تسجيل الدخول.
- ✚ أن تكون البيانات المخزنة في قاعدة البيانات خاصة.
- ✚ هناك أيضا مصادقة المستخدم المطلوبة.
- ✚ هناك أيضا مرفق حيث يمكن للمدير قفل بياناته الخاصة التي لن يتم الوصول إليها من قبل أي شخص.
- ✚ البرنامج بأكمله آمن من الوصول الخارجي لأنه يعمل على شبكة داخلية .



متطلبات خوارزميات التشفير:

- ✚ يجب ان لا يؤدي سقوط نظام التشفير بأيدي اي طرف ثالث(متسلل) الى اختراق النظام.
- ✚ صلابة وممانعة الخوارزميات للتفكيك والاعتمادية على مفاتيح التشفير وفك التشفير.
- ✚ يجب ان تكون مفاتيح التشفير قابلة للتغيير.
- ✚ ينبغي ان يكون النص المشفر قابل للانتقال عبر قنوات الاتصال الامنة.
- ✚ دعم تشفير جميع انواع الملفات .
- ✚ القدرة على معالجة مفاتيح التشفير بمختلف الاحجام (128 او 192 او 256).
- ✚ يجب ان تكون جميع البيانات المرسلة بين العميل والمخدم مشفرة.

متطلبات الملفات والتخزين:

- ✚ يتم تخزين ملفات المستخدمين من النمط txt/bin.
- ✚ يتم تخزين حسابات المستخدمين من النمط xlsx.
- ✚ يتم تنظيم ملفات المستخدم ضمن مجلد خاص لكل مستخدم يكون اسمه مشابه لل ID الخاص بالمستخدم.
- ✚ يتم تنظيم الملفات العامة من مجلد Public.
- ✚ جميع المستخدمين يمتلكون مساحة 200 ميغا لتخزين الملفات .

توصيف المتطلبات الوظيفية:

أصحاب المنفعة:

يتم استخدام هذا التطبيق من قبل الشركات أو المراكز المؤسسات التي تحتاج الى نقل الملفات ضمن المراكز أو بين فروع الشركة دون الحاجة إلى استخدام برامج نقل الملفات العامة نظرا الى سرية البيانات التي يتم نقلها ضمن المراكز او النشاطات التي تريد أن تخزن البيانات ضمن المخدم المركزي لديها من أجل نظرا لتكاليف التخزين السحابي المرتفع.

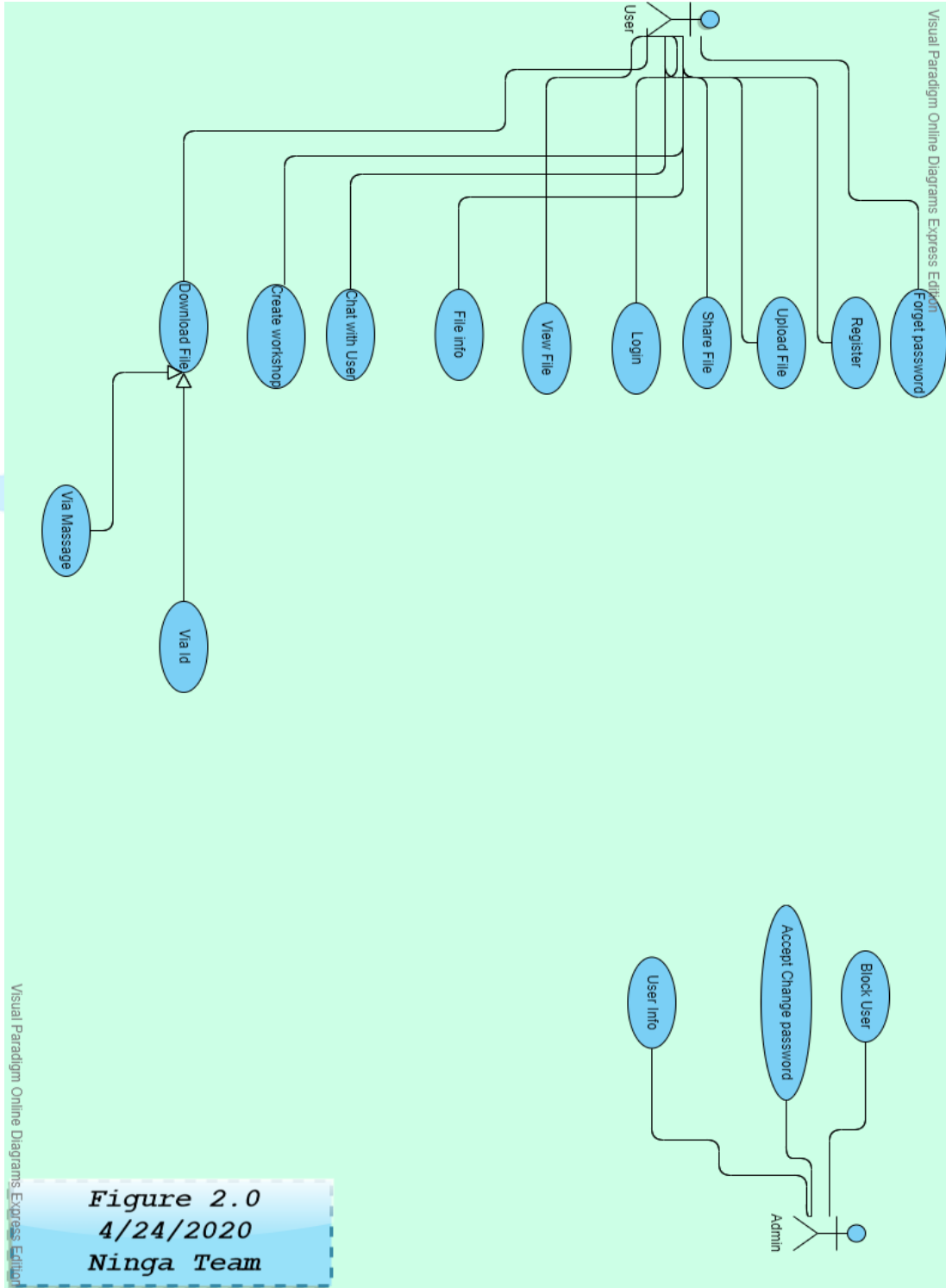
الفاعلون وأهدافهم:

- 1- الأشخاص الذين يمتلكون حساب داخل التطبيق.
- 2- الأشخاص الذين لا يمتلكون حساب داخل التطبيق.
- 3- مدير النظام الذي يقوم بتعديل الحسابات .
- 4- مدير المعلوماتية ضمن الشركة في حال كان التطبيق خاص ضمن الشركات.



حالات الاستخدام:

يوضح المخطط 2.0 Figure حالات الاستخدام التي سوف يقوم فريق التطوير بتطبيقها.



حالات الاستخدام ذات التوصيف العام:

رقم المتطلب	توصيف عام لحالة الاستخدام	حالة الاستخدام
3	تستخدم هذه الحالة يقوم المستخدم بتسجيل الدخول الى النظام	Login
3	تستخدم هذه الحالة لتسجيل حساب جديد على النظام	Register
3	تستخدم هذه الحالة لاستعادة كلمة المرور	Forget password
3	تستخدم هذه الحالة لتسجيل الخروج من الموقع	Logout
5	تستخدم هذه الحالة لرفع الملفات وتخزينها على السيرفر	Upload File
8&6	تستخدم هذه الحالة لمشاركة الملف التي تمت رفعه الى السيرفر الى مستخدم على التطبيق او انشاء رقم فريد لتحميله (سيتم شرح التحميل الفريد عن طريق ID في الحالة (Download file via ID)	Sharing File
11	تستخدم هذه الحالة لعرض الملفات التي تم رفعها وتخزينها على المخدم	View File
11	تستخدم هذه الحالة لعرض معلومات الملفات التي تم تخزينها وعدد مرات التحميل ومن قام بتحميل الملفات ويمكن أيضا تعديل صلاحيات الوصول وتعديل اسم الملف او الملف او حذف الملف	File info
8	تستخدم هذه الحالة لتحميل الملفات التي تمت مشاركته معي	Download File
8	تستخدم هذه الحالة لتحميل ملف عن طريق ID دون الحاجة الى انشاء حساب على الموقع وهذا يفيد الأشخاص الذين لا يريدون انشاء حساب على الموقع وإنما فقط تحميل الملف	Download file via id
10	تستخدم هذه الحالة لكي يستطيع الافراد مشاركة الرسائل النصية ضمن التطبيق.	Chat with user
9	تستخدم هذه الحالة لإنشاء Directory يستطيع أفراد المجموعة التعديل عليه حسب الصلاحيات التي تم منحهم إياها (تعديل، تعليق، عرض)	Create workshop
12	تستخدم هذه الحالة إلغاء صلاحيات الوصول للمستخدم للتطبيق	Block User
13	تستخدم هذه الحالة لقبول طلب استعادة كلمة المرور	Accept reset pass
14	تستخدم هذه الحالة لعرض معلومات الشخص وملفاته والملفات التي قام بمشاركتها	User Info



حالات الاستخدام ذات التوصيف المفصل:

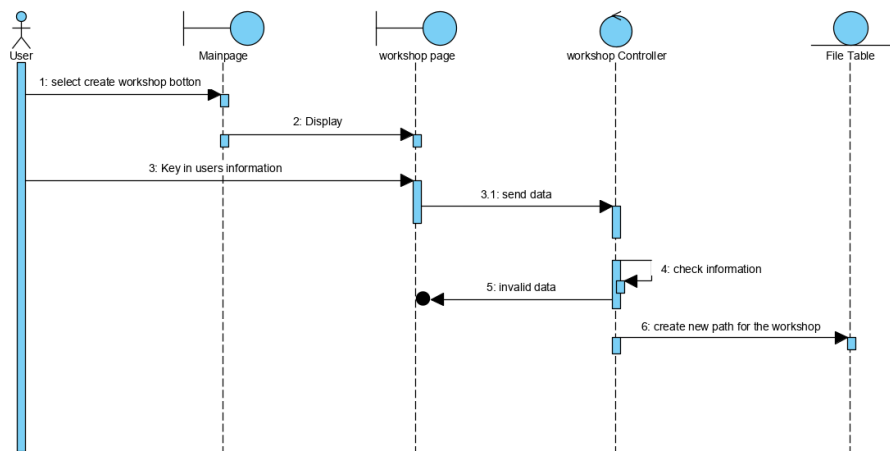
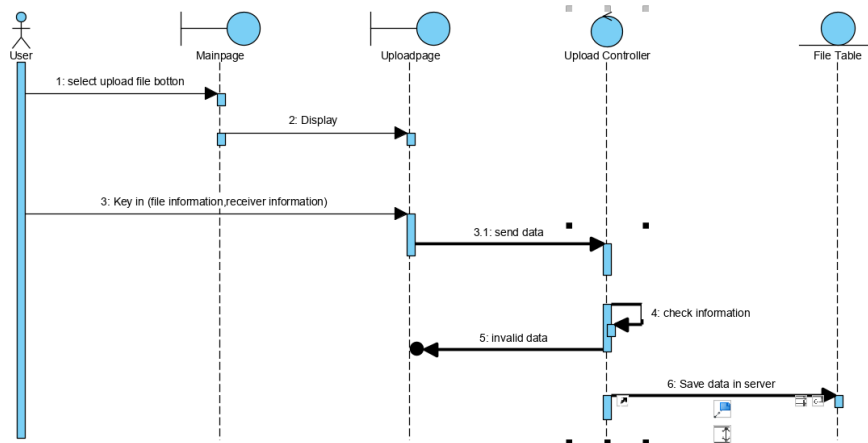
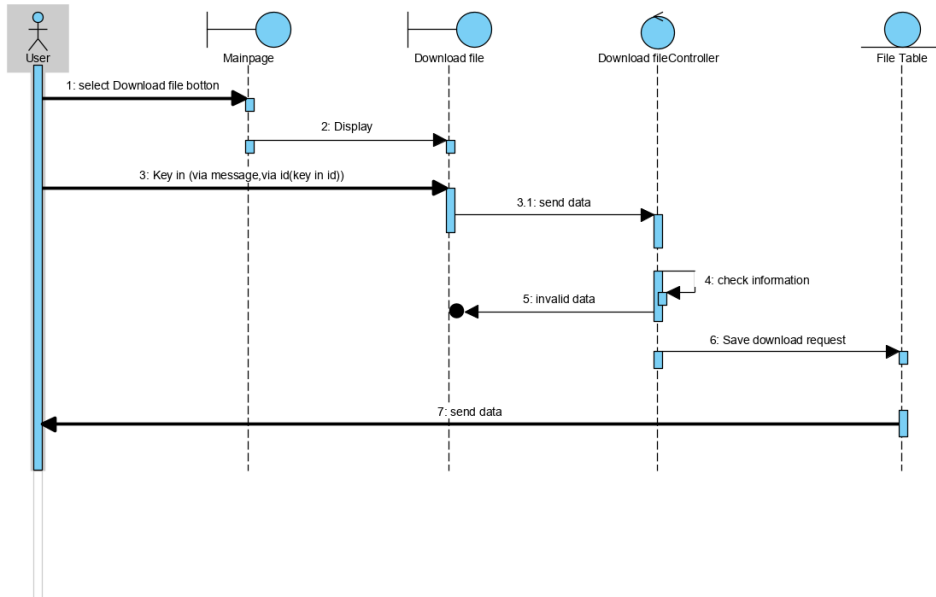
تم تحديد عدد من حالات الاستخدام الجوهرية وتوصيفها على شكل خطوات مفصلة من بداية حالة الاستخدام إلى نهايتها.

رقم المتطلب	توصيف مفصل لحالة الاستخدام	حالة الاستخدام
8 & 6	<ol style="list-style-type: none"> 1- يقوم المستخدم بالنقر على مشاركة ملف 2- يقوم التطبيق بتحميل الملفات التي يملكها المستخدم من المخدم 3- يقوم المستخدم بتحديد الملف المطلوب رفعه (اما رفع الملف او اختيار ملف تم رفعه مسبقا) 4- تحديد اسماء حسابات المستلمين 5- التأكد من حسابات المستخدمين ضمن المخدم 6- رسالة نجاح عملية المشاركة 	Sharing File
11	<ol style="list-style-type: none"> 1- تحديد الخيار FILE لعرض الملفات التي تم رفعها على المخدم . 2- الانتظار لتحميل اسماء الملفات التي يمتلكها المستخدم 3- البحث عن الملف المطلوب ضمن القائمة 4- الضغط على ايقونة Info لأؤية تفاصيل الملف 5- يتم تحميل تفاصيل الملف وعرضها للمستخدم 	View File
9	<ol style="list-style-type: none"> 1- يقوم المستخدم بالنقر على انشاء مجموعة عمل 2- يقوم المستخدم بتحديد اسم المجموعة والشرح 3- تتم اضافة اسماء الاشخاص الذين يملكون صلاحيات على المجموعة مع تحديد الصلاحيات التي يملكونها 4- تحديد الملفات التي سوف تتم اضافتها الى مجموعة العمل 5- رسالة تأكيد نجاح العملية واطافة المستخدمين والملفات الى الى المجلد المشترك. 	Create workshop
12	<ol style="list-style-type: none"> 1- يقوم مدير التطبيق بتسجيل الدخول 2- النقر على حظر مستخدم 3- يقوم المخدم بارسال اسماء جميع المستخدمين 4- يختار المدير اسم مستخدم وينقر على حظر 5- ينتظر رسالة نجاح عملية الحظر 	Block User
5	<ol style="list-style-type: none"> 1. يقوم المستخدم بتسجيل الدخول 2. ثم يقوم المستخدم بالضغط على (رفع ملف) 3. يختار المستخدم الملفات التي يرغب بتخزينها على السيرفر ثم يقوم بتأكيد رفع الملفات 4. ينتظر المستخدم حتى تظهر رسالة نجاح العملية 	Upload File

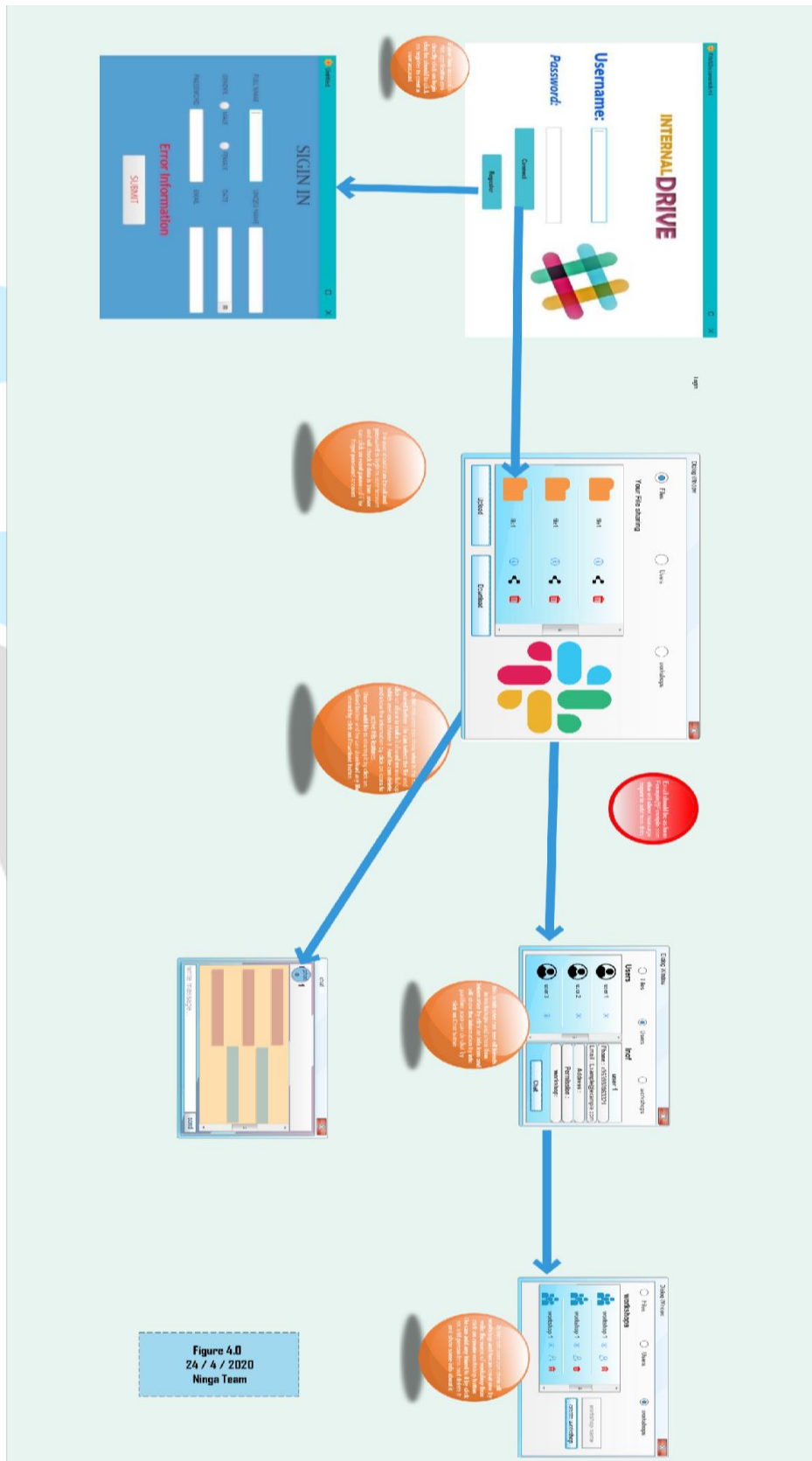
تم تمثيل جزء من الحالات على شكل مخططات تسلسل لسهولة الفهم للقارئ



توضیح مخططات التسلسل المنطقی لحالات الاستخدام ذات التوصیف المفضل:



توصيف واجهة الاستخدام:



الفصل الرابع: التصميم التقني:

مخطط الصفوف:

يوضح المخطط Figure 3.2 مجموعة الصفوف والعلاقات التي تترابط بينهم.

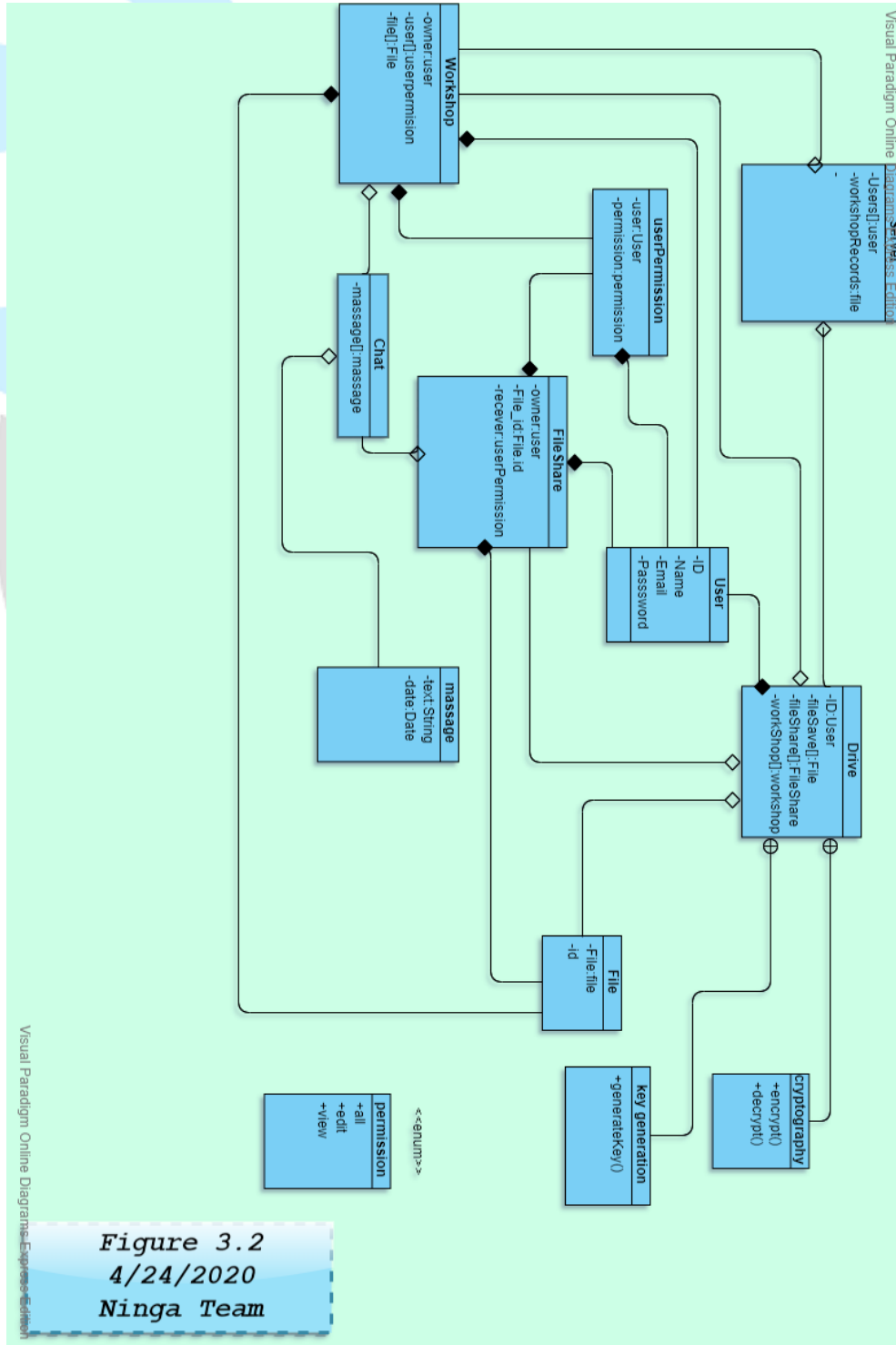


Figure 3.2
4/24/2020
Ninga Team



أنواع المعطيات وتوابع العمليات:

في هذا القسم تقوم بتوصيف أنواع المعطيات Data Types وتوابع العمليات Operation Signatures وذلك من أجل كل صف من الصفوف الوارد في القسم السابق.

1. ضمن صف User:

يحتوي هذا الصف على المعلومات الأساسية للمستخدم :
Name وهو من نمط المعطيات String
Email الفريد وهو من نمط المعطيات String
password وهو من نمط المعطيات String
ID وهو من نمط المعطيات String
معلومات أخرى عن المستخدم
يحتوي هاد الصف على توابع: Constructor ,setter ,getter

2. ضمن صف Message:

يحتوي هذا الصف على المعلومات الأساسية message :
text وهو من نمط المعطيات String
date الفريد وهو من نمط المعطيات Date
يحتوي هاد الصف على توابع: Constructor ,setter ,getter

3. ضمن صف chat:

يحتوي هذا الصف على المعلومات الأساسية chat :
message وهو من الصف message
يحتوي هاد الصف على توابع: Constructor ,setter ,getter

4. ضمن صف File:

يحتوي هذا الصف على المعلومات الأساسية File :
File وهو من نمط المعطيات File
ID وهو من نمط المعطيات String
يحتوي هاد الصف على توابع: Constructor ,setter ,getter

5. ضمن صف User Permission:

يحتوي هذا الصف على المعلومات الأساسية User Permission :
User وهو من الصف User
permission وهو من الصف permission
يحتوي هاد الصف على توابع: Constructor ,setter ,getter

6. ضمن صف work shop:

يحتوي هذا الصف على المعلومات الأساسية work shop :
Owner وهو من الصف User
User list وهو من الصف permission
file وهو من الصف file
يحتوي هاد الصف على توابع: Constructor ,setter ,getter



7. ضمن صف Driver:

يحتوي هذا الصف على المعلومات الاساسية Driver :
File save وهو من نمط المعطيات 🚩
File share الفريد وهو من نمط المعطيات 🚩
Work shop وهو من نمط المعطيات 🚩
ID وهو من الصف User 🚩
يحتوي هاد الصف على توابع: getter, setter, Constrictor

8. ضمن صف key generation:

يحتوي هذا الصف على المعلومات الاساسية key generation:
يحتوي هاد الصف على توابع: getter, setter, Constrictor
generate Key وهو تابع يقوم بتوليد المفاتيح 🚩

9. ضمن صف cryptography:

يحتوي هذا الصف على المعلومات الاساسية للمستخدم :
يحتوي هاد الصف على توابع: getter, setter, Constrictor
Encrypt تابع يقوم بتشفير البيانات 🚩
Decrypt تابع يقوم بفك تشفير البيانات 🚩

10. ضمن صف Server:

يحتوي هذا الصف على المعلومات الاساسية server :
User list وهو من نمط المعطيات 🚩
Work shop الفريد وهو من نمط المعطيات 🚩
password وهو من نمط المعطيات String 🚩
ID وهو من نمط المعطيات String 🚩
معلومات اخرى عن server
يحتوي هاد الصف على توابع: getter, setter, Constrictor

11. ضمن صف File share:

يحتوي هذا الصف على المعلومات الاساسية file share :
owner وهو من نمط المعطيات user 🚩
File_id الفريد وهو من نمط المعطيات file 🚩
recever وهو من نمط المعطيات permission 🚩
معلومات اخرى عن File share
يحتوي هاد الصف على توابع: getter, setter, Constrictor

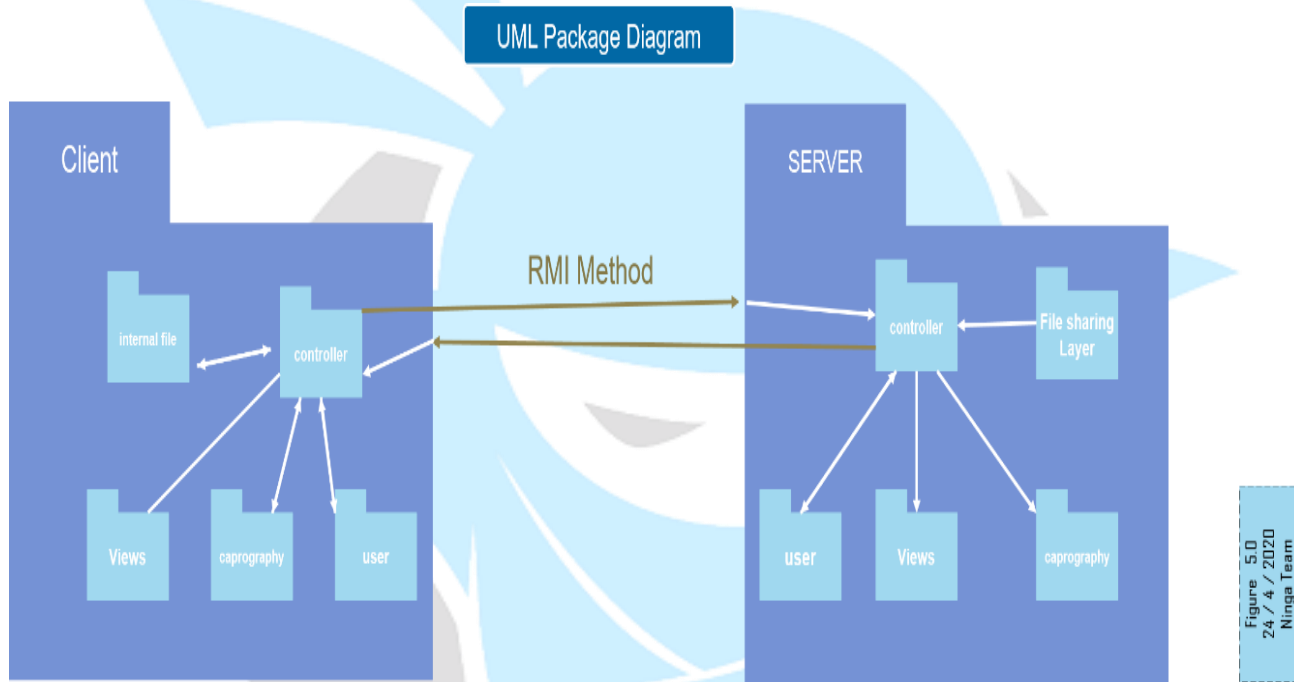


المعمارية وتصميم النظام:

الأنساق المعمارية وأنساق التصميم المستخدمة:

الأنظمة الجزئية المكونة:

يوضح المخطط Figure 5.0 مجموعة الصفوف والعلاقات التي تترابط بينهم.



توزيع الأنظمة الجزئية على العتاد:

يعمل التطبيق على أكثر من جهاز حيث تم تطبيق معمارية Client/server model والتي تقوم بتقسيم العمل الى أكثر من جهاز حيث ونحتاج لجهاز يعمل بشكل مستمر وهو السيرفر حيث يقوم بتأكيد مصادقة الاتصال وإعطاء عنوان فريد لكل جهاز يتصل بالتطبيق عن طريق الرابط الذي يعبر عن موقع السيرفر ويقوم بضمان عملية تسجيل الدخول والاجابة على الطلبات ويحتاج للعمل بشكل دائم لأنه لا يمكن القيام بأي عمل في حال خروج المخدم عن العمل ، وباقي الاجهزة التي تمثل العملاء ، حيث يستطيع العميل الاتصال بالمخدم باستخدام الهاتف الذكي أو الحاسب حيث يمتلك التطبيق المخصص للعميل طريقة الوصول إلى الشبكة .



تخزين المعطيات الدائم:

- ✚ يتم تخزين المعطيات بشكل دائم لأنه يجب حفظ حسابات المستخدمين ومعلوماتهم وحساب مدير التطبيق وملفات المستخدمين التي تم رفعها والمستخدمين الذين قاموا بتحميل الملف.
- ✚ سوف يتم تخزين معلومات المستخدمين على نسيب خاص حتى يتم التخزين بشكل سريع وله أولوية عالية
- ✚ يتم تخزين الملفات بشكل مؤقت ضمن رتل بشكل مؤقت ، يقوم نسيب بتخزين الملفات بشكل دائم بحسب دور الملف داخل الرتل.

صيغة الملف file format المستخدمة:

- ✚ سوف يتم استخدام الملفات النصية TXT لتخزين الملفات
- ✚ ملفات الثنائية bin لتخزين ملفات الوسائط المتعددة
- ✚ ملفات الاكسل xlsx لتخزين معلومات المستخدمين

البروتوكولات الشبكية:

- ✚ سوف يتم استخدام تقنية Java RMI حيث تمكنا هذه التقنية من انشاء السيرفر الذي يقوم المستخدمين بالاتصال به ونقل البيانات ضمن الواجهة وتنفيذ الكود على JVM ثاني .
- ✚ كنا قد اقترحنا استخدام Socket ولكن تكون المشكلة في استخدام السوكيت حيث أفضل الطرق لنقل بين العميل والخادم هي ملفات JSON حيث في كل عملية نقل نحتاج الى نقل أكثر من قيمة لذلك تم الاستغناء عن السوكيت واستخدام التقنية السابقة .
- ✚ قمنا باستخدام البروتوكول Handshake Protocol الذي يسمح هذا للعميل والخادم بالاتفاق على طريقة تشفير وإثبات من يستخدمان مفاتيح التشفير قبل إرسال أي بيانات بينهما.

أنواع الرسائل المتبادلة ومضمون وصيغة هذه الرسائل:

- ✚ رسائل اتصال المستخدم (تسجيل دخول ، تسجيل حساب جديد ، فقدان كلمة المرور، تسجيل الخروج)
- ✚ رسائل مشاركة الملفات (رفع ملف، تحميل ملف)
- ✚ رسائل تعديل صلاحيات الملف
- ✚ رسائل الدردشة



تدفق التحكم الإجمالي

✓ ترتيب التحقيق:

النظام الذي نقوم ببنائه ليس مقاد باجرائية ثابتة حيث يتم الاستجابة للأحداث بناء على طلبات المستخدم أو الشروط التي يفرضها الخادم حيث يمكن أن تؤثر طلبات المستخدم على سير عمل الملفات الخادم وبالإضافة لعمليات المزامنة ضمن المجلدات المشتركة

✓ الاعتماد على الوقت:

لا يوجد اعتماد على الوقت ضمن المشروع، حيث يتم الجواب على كافة الطلبات التي قد تأتي من العميل من عرض ملفات او تحميل ملف أو..... وتكون التي يجب أن تنفذ بكل مباشر منها تعديل صلاحية ملف او تغيير اسم الملف او حذف او رفع ملف الى المجلد المشترك.

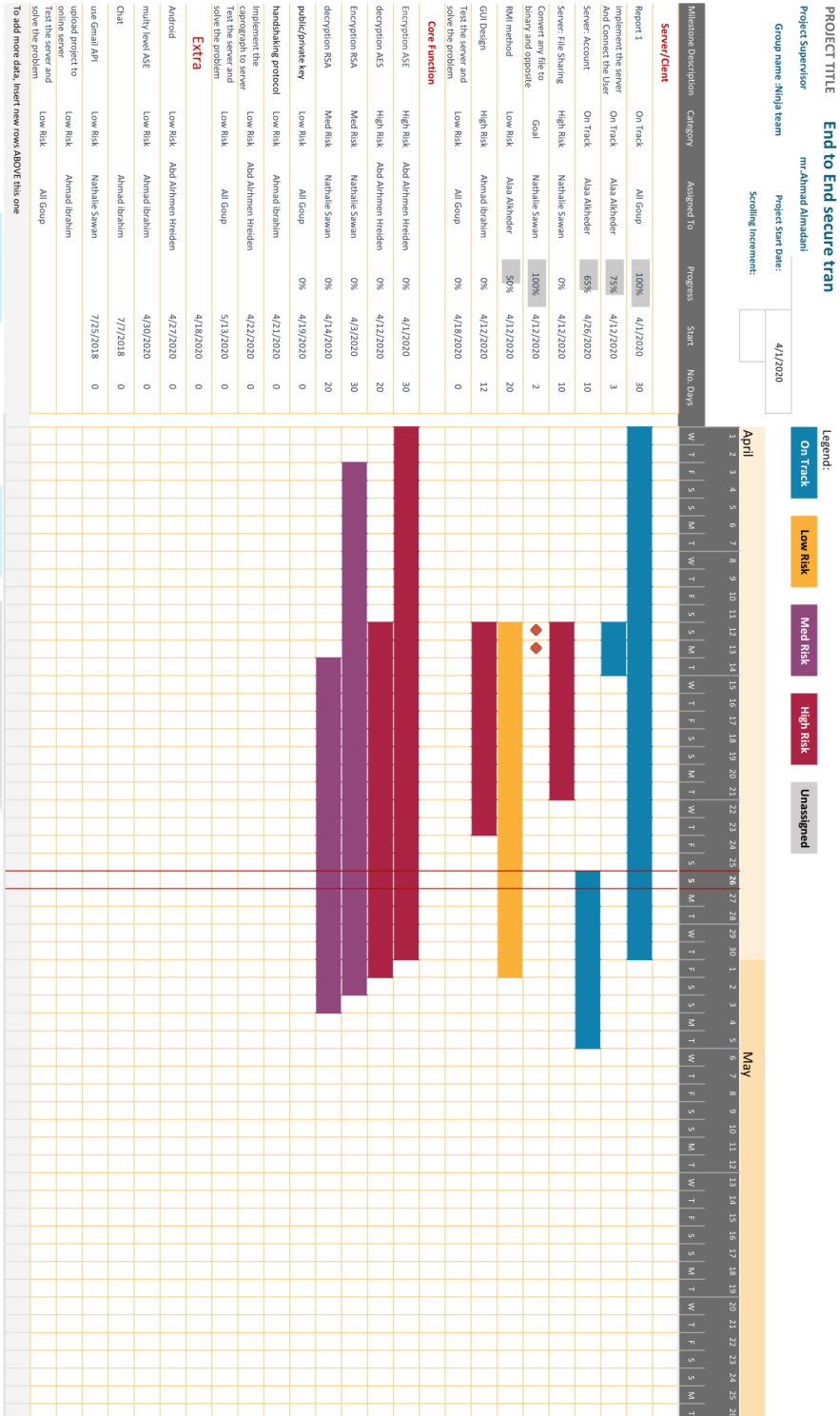
✓ التساير:

يستخدم الخادم اكثر من نسيب حيث لكل عميل يتصل بالخادم يوجد نسيب خاص به يبقى في وضع السكون إلى أن يأتيه طلب من العميل.
يستخدم العميل اكثر من نسيب من اجل تحميل ورفع الملفات حيث عند طلب تحميل او رفع ملف لايسبب سكون الواجهات.



خطة تقسيم العمل

رابط المخطط الزمني الذي يقوم فريق التطوير بالتعديل عليه بشكل مستمر حتى يتمكن المشرف من متابعة سير العمل



الفصل الخامس: التنجيز والتحقق

يترك هذا الفصل فارغاً عند إرسال التقرير الأول. تشا



الفصل السادس: الخاتمة:

وفي ختام الموضوع ومما سبق يتضح لنا أهمية هذا الموضوع، لهذا كان لازماً أن تتوجه إليه كل الجهود والرعاية والاهتمام نظراً للجهود التي يسعى لها النائب العلمي ورئاسة القسم ومسؤول المادة بالاضافة الى المشرفين على المادة لانها تعتبر المشروع الهندسي الاول ضمن الكلية الذي يعتمد على قدرات الطالب بشكل عام ، ومن الدروس المستفادة التي نخرج بها من هذا الأمر (كتابة التقرير بكل تفاصيله ، القدرة على دراسة المشروع وتحديد الاحتياجات ، تحديد تصميم الواجهات والتصميم التقني ، تقسيم العمل على الوقت المخصص ، اقتراح التحسينات على المشروع). ولان الموضوع هام نرجو أن يستفيد كل المهتمين بمادة المشروع 1 بهذا الموضوع الذي تم دراسته، في مشاريعهم العلمية، وهذه المادة مفيدة للباحثين، وقد توصلت لبعض النتائج الهامة في التطور، وقد قمت بتلخيص نبذة عن التقرير وهي (تقوم الكثير من برامج مشاركة الملفات عبر الانترنت باستخدام خوارزميات التشفير advanced encryption standard حيث هذه الخوارزمية متينة ،ويمكن استخدام لغة البرمجة JAVA لانها تمكنا من انشاء المخدم والعملاء باستخدام 'RMI method Or Socket' وايضاً تمكنا من ربط المخدم مع تطبيق Android لان لغة الاندرويد مبنية على لغة الجافا وهذا ما يمكننا الاستفادة من جميع ميزات لغة الجافا)، وبهذا أكون قد انتهيت من كتابة هذا التقرير

وادعوا الله بالتوفيق لي ولكم بإذن الله تعالى

فريق التطوير



المراجع:

- [1] Secretary, "AES", FIPS PUBS, 2001, 197, 51.
- [2] Bruce Eckel, "*Thinking in Java*", Prentice Hall , 2006, 10TH, 1079.
- [3] Ian Sommerville, "Software Engineering", Sommerville's, 1982, 4TH, 608.
- [4] Jean-Philippe Aumasson, "serious Cryptography", no starch press, 2008, 1, 434.

المراجع الالكترونية:

- + <https://www.geeksforgeeks.org/unified-modeling-language-uml-introduction/>
- + <https://www.geeksforgeeks.org/unified-modeling-language-uml-class-diagrams/>
- + https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
- + <https://docs.oracle.com/javase/7/docs/technotes/guides/rmi/hello/hello-world.html>
- + <https://docs.oracle.com/javase/tutorial/networking/sockets/index.html>
- + https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

المواقع الالكترونية:

- + <https://online.visual-paradigm.com/>
- + <https://docs.google.com/>
- + <https://www.office.com/launch/excel>

