TC
FIRAT ÜNİVERSİTESİ
TEKNOLOJİ FAKÜLTESİ
YAZILIM MÜHENDİSLİĞİ BÖLÜMÜ

YMH459 YAZILIM MÜHENDİSLİĞİ GÜNCEL KONULAR DERSİ PROJESİ GEREKSİNİM ANALİZİ DOKÜMANI

Proje Adı

CRYPIT(Fotoğraf Şifreleme için Mobil Uygulama)

Proje Logosu

Proje Ekip Lideri

SÜMEYYE GÜLNUR DADAK (16542503)

Proje Çalışma Grubu

ABDULKADİR DOĞANER (16541563)
ARZU KÜBRA YILAR (175541031)
BERNA UZUNOĞLU (16542513)
ENİS CAN YILMAZ (15541531)
HÜSEYİN BİTİKÇİ (16541509)
İHSAN CENKIZ (175541022)
İSMAİL ÇAĞAN (16541542)
KÜBRA ATICI (14545522)
MEHMET CAN AKKAŞ (14542518)
MEHMET FURKAN KEMALLI (185541087)
MERT BEKTAŞ (16541522)
MUSTAFA ENES ÖZÇELİK (175541068)
TUGAY AYAR (15542514)

Proje Yürütücüleri

Doç. Dr. Fatih ÖZKAYNAK

ELAZIĞ
2020-2021

İÇİNDEKİLER

ŞEKİLLER

TABLOLAR

1 GİRİŞ

1.1 Projenin Amacı

Son zamanlarda artan teknolojik imkânlar beraberinde birde dijital güvenlik ve gizlilik ihtiyacı doğurmaktadır. İnsanlar iki binli yılların başında oldukça güvenli hissederek bütün sistemlere giriş yapmaktaydı. Ancak son birkaç yılda artan bilgi çalma ve hassas verilerin toplanması gibi olaylardan kaynaklı insanlar artık verilerine daha fazla sahip çıkmakta ve gizliliğine önem vermektedir. Bu gizlilik gereksinim hissedilen bir alan ise kişisel fotoğrafların WhatsApp ve Telegram gibi iletişim kanalları vasıtası ile paylaşımı sırasında gerek servis sağlayıcılara gerekse üçüncü taraf saldırganlara gösterilmemesidir. Bu probleme bir mobil uygulama ile çözüm sağlamak projenin ana amacıdır.

1.2 Projenin Kapsamı

Mobil uygulama mağazalarında bulunacak proje, fotoğraf göstermek isteyen ve güvenliği önemseyen kullanıcıların tümüne yöneliktir. Daha uzun vadede ise dosyaların şifrelenmesi gibi işlevsel özelliklerde kazandırılarak kullanım alanı genişletilebilir. Bazı örnek kullanım alanları şunlar olabilir;

- Özel ofis dosyalarının paylaşılması.
- Özel yazışmaları taşıyan dosyaların başlaması.

1.3 Kısaltmalar

- PUF = Physical Unclonable Function = Fiziksel Klonlanamaz Fonksiyon
- RAM = Random Access Memory = Rastgele Erişimli Hafıza

1.4 Hedefler ve Başarı Kriterleri

Gerçekleştirilecek sistemin hedefleri;

- Projemizin öncelikli hedeflerinden birisi kişisel bilgilerin gizliliğinin korunmasıdır.
- Gerçekleştirilen sistem ile gönderici ve alıcı arasında güvenli bir iletişim ortamı oluşturulmalıdır.
- Sistemde kullanıcı ve alıcıdan hariç üçüncü şahıslara bilgi ve müdahale hakkı doğmamalıdır.

Başarı kriterleri nelerdir?

- RAM verisinden değer elde edilip SHA3 / SALSA 20 / RSA / AES algoritmasından geçirilmiş olmalıdır.
- Hash fonksiyonun başlangıç kabul edilerek rasgele bit dizisi üretilmelidir.
- Mobil aplikasyon ile cihazdan herhangi bir resim seçilebilmelidir.
- Resimde fraktal bir görüntü oluşturulmalıdır. Mobil uygulama kesintisiz çalışmalı ve performans sorunu vermemelidir.
- Kullanıcılar için kolay kullanıma hitap eden uygulama ara yüzü sunulmalıdır.
- Kullanıcı fotoğraf seçebilmeli, fotoğrafı şifreleyebilmeli ve paylaşabilmelidir.
- Alıcı gelen ID ile deşifre işlemi gerçekleştirildikten sonra orijinal fotoğrafı görüntüleyebilmelidir.

2 TEKLİF EDİLEN SİSTEM

2.1 Fonksiyonel Gereksinimler

- İp-1 Paketi: RAM verisi okunmalı.
  RAM verisinden elde edilen çıktıya SHA3 algoritması uygulanmalı.
  Çıktı olarak 256-bit çıktı oluşturulmalı.
- İp-2 Paketi: İp-3 paketi içerisinde anahtar üretimi için başlangıç koşullarını sağlamalı.
- İp-3 Paketi: Hash fonksiyonu ile başlangıç değeri seçilmeli.
  Başlangıç koşulu kullanılarak rasgele bit dizisi ile anahtar üretilmeli.
- İp-4 Paketi: İş Paketi-1 ve İş Paketi-3 fonksiyonelliği için sunucu işlemlerini gerçekleştirecektir.
- İp-5 Paketi: Mobil uygulamada cihazdan herhangi bir fotoğraf seçilmeli.
  Fotoğraf (hem gri hem renkli) şifreleme fonksiyonlarından geçip firebase' e gitmeli ve 16 Haneli ID kullanıcıya sunulmalı
  Sunulan ID Decryption sekmesinde textfield a işlenip şifreli bit dizisine erişilmeli ve telefonun içerisinde şifre çözülüp kullanıcıya sunulmalı
  Mobil uygulama kullanıcıya hitap etmeli.

2.2 Fonksiyonel Olmayan Gereksinimler

Kullanılabilirlik: Kullanabilirlik olarak her seviyedeki insana hitap edeceği için rahat ve hızlı şekilde kullanımı desteklemek amacı ile karmaşık renklerden, menü yapısından kaçınılacaktır. En kullanışlı menü tasarımı yapılacaktır.

Güvenilirlik: Şifrelenecek olan medya görüntüsünün encryption işleminden sonra decryption işlemi gerçekleşince aynı medyaya ulaşılacak.

Performans: Gerçekleştirilen sistemde şifreleme, şifre çözümleme, paylaşma vs. işlemlere en kısa sürede ve hızlı bir şekilde cevap vermesi sağlanacaktır.

Desteklenebilirlik: Gerçekleştirilen sistem mobil cihazlar için geliştirilecek olup Android ve IOS işletim sistemini tarafından desteklenecektir.

Arayüz: Veri girişi için şifrelenecek resim dokunmatik olarak tasarlanan buton ile cihaz içerisinden alınacaktır. Daha sonra şifrelenmiş resme ait ID ekrana çıktı olarak verilecektir. ID decryption bölmesinde girilip şifre çözümleme için gerçekleştirilecektir.

2.3 Sistemde Yer Alacak Aktörlerin Senaryoları

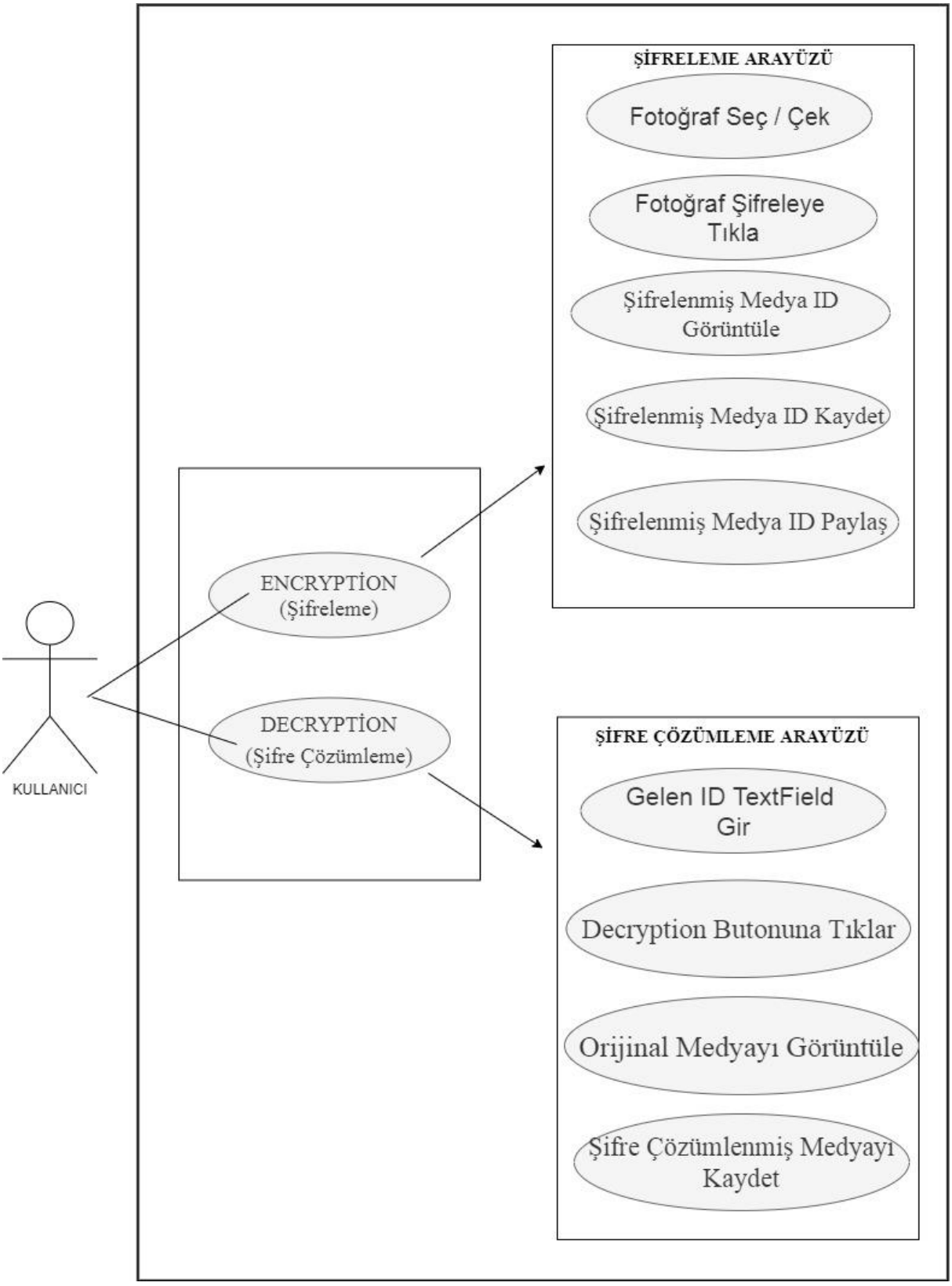
Senaryo Adı	Fotoğraf Şifreleme
Senaryoya katılan varlık	Kullanıcı
Olay akışı	1. Kullanıcı uygulamayı açar. 2. Kullanıcı şifreleme ara yüzünün açar. 3. Kullanıcı fotoğraf şifrele(Encryption) butonuna tıklar. 4. Kullanıcı cihazdan fotoğrafı seçer yada fotoğraf çeker. 5. Kullanıcı şifrelenmiş medyaya ait ID görüntüler. 6. Kullanıcı şifrelenmiş medyaya ait ID yi kaydeder. 7. Kullanıcı şifrelenmiş medyaya ait ID yi paylaşır.

Tablo 1 - Sistem Modeli Fotoğraf Şifreleme Senaryosu

Senaryo Adı	Fotoğraf Şifre Çözümleme
Senaryoya katılan varlık	Kullanıcı
Olay akışı	1. Kullanıcı uygulamayı açar. 2. Kullanıcı şifre çözümleme ara yüzünün açar. 3. Kullanıcı fotoğraf şifre çözümleme(Decryption) sekmesine tıklar. 4. Kullanıcı gelen ID yi textfield a yapıştırır. 5. Decrypt it butonuna tıklar. 6. Kullanıcı şifre çözümleme ile orijinal medyayı görüntüler. 7. Kullanıcı şifre çözümlenmiş medyayı kaydeder.

Tablo 2 - Sistem Modeli Fotoğraf Şifre Çözümleme Senaryosu

2.4 Use-Case Diyagramı



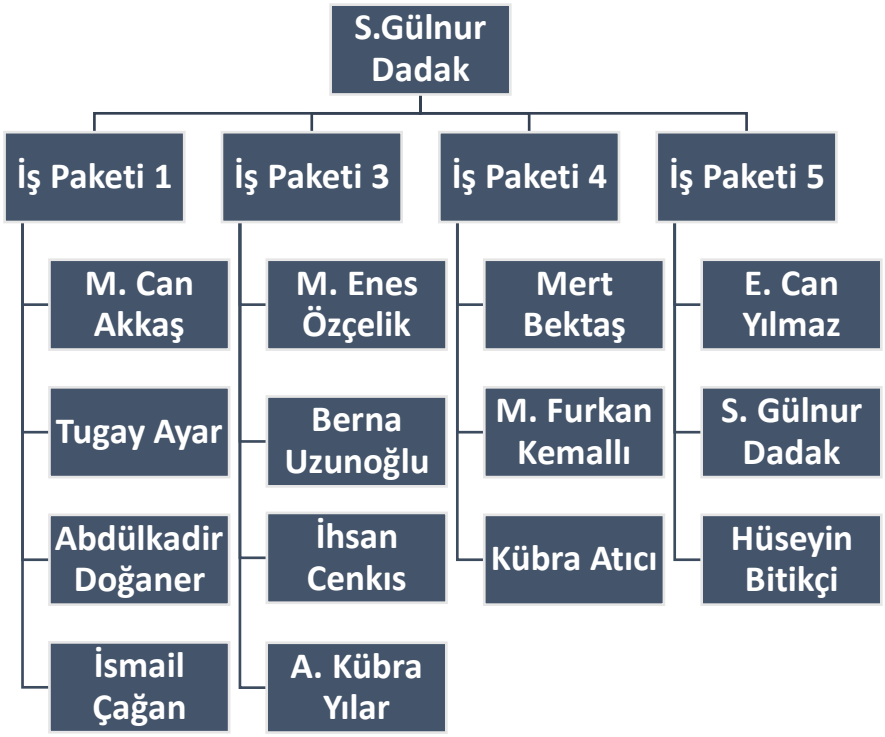
Şekil 1- Sistemin Genel Use-Case Diyagramı

2.5 Proje İş-Zaman Çizelgesi

	Görev İsmi	1.Hafta	2.Hafta	3.Hafta	4.Hafta	5.Hafta	6.Hafta	7.Hafta	8.Hafta	9.Hafta	10.Hafta	11.Hafta	12.Hafta	13.Hafta	14.Hafta
1	Complete project execution														
2	Proje Genel Yapısı														
3	Proje Genel Yapısı ve Anlatımı														
4	Proje Ekibinin Belirlenmesi														
5	Proje Ekibinin Gruplara Ayrılması														
6	Projenin Planlanması ve Teknik Konuların Anlatımı														
7	Geliştirme Platformunun Belirlenmesi														
8	Genel Yapının Oluşturulması														
10	Uygulamanın Arayüz Tasarımlarının Taslak. Hazırlanması														
11	Projenin Alt Sistemlerinin Kodlanması														
12	Projedeki İşlevlerin Güncellenmesi ve Kodlanması														
13	Uygulama Testleri ve Raporlarının Hazırlanması														
14	Proje Dokümanının Hazırlanması														

Tablo 3 - Projenin İş Zaman Çizelgesi

2.6 Proje Ekip Yapısı



Şekil 2 - Proje Ekip Yapısı Çizelgesi

2.7 Önerilen Sistemin Teknik Altyapısı

- Kullanılan Teknolojiler
  - Flutter (Geliştirme Platformu)
  - Dart (Kullanılan Programlama Dili)
  - Firebase (Veri Tabanı)
  - Microsoft Azure (Sunucu Geliştirme Platformu)
  - Python (Sunucuda Kullanılan Programlama Dili