|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tablo 1: Proje Bilgi Formu** | | | | | |
| **1-** | Projenin Adı | Güvenli Bulut Yazılımı | | | |
| **2-** | Proje Danışmanı | Doç. Dr. Fatih ÖZKAYNAK | | | |
| **3-** | Proje’nin Yapıldığı Ders | Yazılım Mühendisliği Güncel Konular | | | |
| **4-** | Projeye Genel Bakış | Kullanıcı verilerini kriptoloji bilimiyle beraber verileri olabilecek her türlü istenmeyen durumu (verilerin çalınması vb.) engelleyebilecek yeni nesil depolama sistemi | | | |
| **5-** | Sektör/ Alt Sektör | Bilişim/ Yazılım / Kriptoloji | | | |
| **6-** | Proje Yeri | Fırat Üniversitesi Teknoloji Fakültesi Yazılım Mühendisliği | | | |
| **7-** | Proje Durumu | Devam etmekte | | | |
| **8-** | Proje Başlangıç Tarihi | 08/10/2021 | | | |
| **9-** | Proje Bitiş Tarihi | - | | | |
| **10-** | Proje Sorumluları | **Adı Soyadı**  Furkan Demirel | **İletişim Bilgileri**  Furkan.demirel.056@gmail.com | **Görevi**  Mobil kullanıcı ara yüzü geliştirme ve veri tabı işlemleri |  |
| Muhammet Enes Biçen | 180541012@firat.edu.tr |  |  |
| 11- | Proje Danışmanı Bilgileri | Doç. Dr. Fatih ÖZKAYNAK | ozkaynak@firat.edu.tr | Proje denetleme |  |

1. **Projenin Kapsamı**
   1. **Projenin Amacı ve Gerekçesi:**

Dünya üzerinde geçmiş yıllardan beri bilgi güvenliği konusu hem bir problem yaratmıştır. Verilerini gizlemek isteyen kişiler çeşitli yollara başvurmuşlardır, bazı zamanlar güvenlik tutmuşlar bazı zamanlar kasalarında, evlerindeki gizli odalarda saklamışlardır. Ama artık devir değişti, bu devir eski çözümleri kaldıramayacak kadar modern ve tehlikeli bir devir. Tehlikeli olmasının en önemli sebebi artık saklamak istediğimiz bilgiler eski zamanlara göre çok daha fazla ve önemli. Bu projedeki amacımız kullanıcılarımızın bilgi ve verilerini kriptoloji bilimiyle beraber saklayabilecek yeni nesil bir bulut sistemi geliştirmek.

* 1. **Proje Fikrini Ortaya Çıkaran İhtiyaçlar:**

Günümüzde kullanılan bulut depolama sistemleri aslında göründüğü kadar güvenli olmayabilir. Bu depolama durumu aslında görünmeyen bir savaştır, bir tarafta verilerini korumak isteyenler diğer tarafta verilerinizi çalmak isteyenler. Ne yazık ki kimin tilki postu giydiği belli değil ama belli olan tek şey bizim koyun postu giydiğimiz. Sadece düşman içerde olmaya da bilir bazı zamanlar bizi korumak isteyenler yanlışlıkla hatalar yapabilir. Bizim buradaki çıkma sebebimiz kullanıcıyı rahatlatacak bir çözüm üretmemizdir.

Mutlak durumdaki depolama hizmetleri, sorunları(kısaca)

* **Bulut Depolama Hizmetleri**

1. Dropbox
2. Google Drive
3. OneDrive
4. Amazon Drive
5. Box
6. Apple iCloud
7. SpiderOak
8. Tresorit
9. Mega
10. IDrive

* **Sorunları**

1. **Veri Kaybı:**

Bulut depolama hizmeti sunarken yaşanan en büyük problemlerden biride veri kaybıdır. Korumak istediğiniz verileriniz aslında hiç kaydedilmemiş olabilir. Bazı hatalar sebebiyle verileriniz kaybolabilir.

Hatta kaydedilen veriler şifrelenmemiş olabilir.

1. **Şifre Sızıntısı:**

Bilgilerinizi gizleyen platformlar çeşitli güvenlik açıklarına maruz kalabilir. Sizin bilgileriniz kayıt esnasında güvenlik açıklarına uğrayabilir yani verileriniz daha kayıt aşamasında çalınabilir.

1. **Sunucu Çökmesi:**

Eski sunucular bazı zamanlar kısa bir süreliğine de olsa sunucular çökebilir. Ve ne yazık ki sadece bilgilerinizi başka kişilerin elinde gördüğünüzde veya firmanızın ya da kişiler bilgilerinizi kullanmak istediğiniz bu durumu anlayabilirsiniz.

* 1. **Projenin Hedef Kitlesi:**
* Bilgilerini güvenli bir şekilde saklamak isteyen, başını yastığa koyduğunda verilerinin güvenle saklandığını hissetmek isteyen bütün kişi ve kuruluşlar.
  1. **Projenin Uygulanması:**
* Web ve mobil tarafı ile kullanıcılara hizmet sağlayacak.
* Mobil uygulamayı indirerek kayıt yapacak.
* 3 Adımlı doğrulama servisi ile sisteme giriş yapabilecek

1. Adım: Kendi belirlediği şifre
2. E- posta ile doğrulama kodu
3. Biyometrik bilgileri ile

* Uygulama içerinde saklamak istediği verilerini (Ses, resim, video, fotoğraf ve metinler) servisimize kayıt edecek.
* Kaydedilen veriler kaydedilmeden önce şifrelenecek ve güvence altına alınacak.
* Verileri kaydedildikten sonra bilgilendirme mesajı ile bilgilendirilecek
* Bütün bu adımlar esnasında herhangi bir reklam ile karşılaşmayacak
* Kullanıcı istediği zaman sistem ile alakalı problemlerini bize geri dönüş sayfamızda yapabilecek. Ve müşteri sistem arasında bir etkileşim yakalanacak.
* Servisimiz içerinde her haftada 1 olacak şekilde sistem bakımı ve testi uygulanacak.
* Kişisel Verileri Koruma Kanunu (KVKK) ile birlikte paralel bir işlem sürdürülecek.

1. **Proje Faaliyet Zaman Çizelgesi**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Faaliyet | 1.Hafta | 2.Hafta | 3.Hafta | 4.Hafta | 5.Hafta | 6.Hafta | 7.Hafta | 8.Hafta | 9.Hafta | 10.Hafta |
| Proje Ekibinin  Belirlenmesi |  |  |  |  |  |  |  |  |  |  |
| Mutlak problemin araştırılması |  |  |  |  |  |  |  |  |  |  |
| Proje amaç ve gerekçesinin belirlenmesi |  |  |  |  |  |  |  |  |  |  |
| Proje Bilgi Formunun oluşturulması |  |  |  |  |  |  |  |  |  |  |
| Proje kullanılacak teknoloji ve sistemlerin belirlenmesi |  |  |  |  |  |  |  |  |  |  |
| Proje hedef kitle ve nasıl uygulanacağının tespiti |  |  |  |  |  |  |  |  |  |  |
| Ekip görev dağılımının yapılması |  |  |  |  |  |  |  |  |  |  |
| Donanım ve yazılım tespitlerinin yapılması |  |  |  |  |  |  |  |  |  |  |
| Prototip bir tasarımın yapılması |  |  |  |  |  |  |  |  |  |  |
| Fonksiyonel Gereksinimlerin belirlenmesi |  |  |  |  |  |  |  |  |  |  |
| Fonksiyonel Olmayan Gereksinimlerin belirlenmesi |  |  |  |  |  |  |  |  |  |  |
| **IPO(Input-Process-OutPut) Diyagramının oluşturulması** |  |  |  |  |  |  |  |  |  |  |
| **Mevcut sistemlerin analizi** |  |  |  |  |  |  |  |  |  |  |
| **Veri Akış diyagramının oluşturulması** |  |  |  |  |  |  |  |  |  |  |
| **Use case diyagramının oluşturulması** |  |  |  |  |  |  |  |  |  |  |
| **Sınıf Diyagramının oluşturulması** |  |  |  |  |  |  |  |  |  |  |
| Hangi testlerin uygulanacağı ve performans kriterlerinin belirlenmesi ve oluşturulması |  |  |  |  |  |  |  |  |  |  |
| kullanıcı profilleri, entegrasyon ve test işlemlerinin **akış diyagramının yapılması** |  |  |  |  |  |  |  |  |  |  |
| Ortak alt sistemlerin arasındaki bağlantının belirtilmesi ve şemalize edilmesi |  |  |  |  |  |  |  |  |  |  |
| Sistemin gerçekleştirilmesi |  |  |  |  |  |  |  |  |  |  |
| Kullanılan standartların açıklanması |  |  |  |  |  |  |  |  |  |  |
| Gerçekleştirim aşamasında oluşabilen olağan dışı durumların nasıl yönetileceğinin açıklanması |  |  |  |  |  |  |  |  |  |  |
| Test Aşamasının başlaması |  |  |  |  |  |  |  |  |  |  |
| Test planı için**hangi yöntemlerin neden ve nasıl kullanıldığının açıklanması** |  |  |  |  |  |  |  |  |  |  |
| **Kullanılacak test araçları varsa işleyişinin açıklanması** |  |  |  |  |  |  |  |  |  |  |
| **Önerilen sistem gerçekleştirilirken hangi test türü ve araçlarının neden seçildiğinin açıklanması** |  |  |  |  |  |  |  |  |  |  |
| **Bakım aşamasına başlanması** |  |  |  |  |  |  |  |  |  |  |
| **Kurulum** aktivitelerinin belirlenmesi |  |  |  |  |  |  |  |  |  |  |
| Kurulum ve entegrasyon aşamalarında yapılacaklar hakkında bilgiler verilmesi |  |  |  |  |  |  |  |  |  |  |
| Sonuç |  |  |  |  |  |  |  |  |  |  |
| Kaynaklar |  |  |  |  |  |  |  |  |  |  |

1. **Ekip Görev Dağılımının Yapılması**

1) Furkan Demirel:

- Mobil kullanıcı ara yüzünü yapması

- 3 adımlı güvenlik doğrulamasını gerçekleştirmesi

- E posta doğrulama

- Kullanıcı şifresi

- Biyometrik doğrulama

- Yeniden kayıt ve hesap silme seçeneklerini eklemesi

- Kayıt, giriş ve depolama sayfalarını yapması

- Kaydedilmek istenen verileri şifrelemesi

- Veri tabanı crud işlemlerini yapması

- Hızlı giriş seçeneğini sunması

- Veri tabanı denetimini gerçekleştirmesi

- Form sayfa tasarımını yapması

- Form veri tabanı crud işlemlerini gerçekleştirmesi

- Depolama hizmetinin güvenliğinin test edilmesi

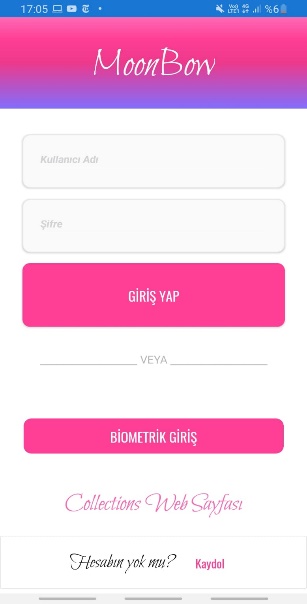
1. **Donanım ve Yazılım Geliştirme Araç ve Ortamları**
   1. **Önerilen Sistemin Teknik Tanımları: Donanım**

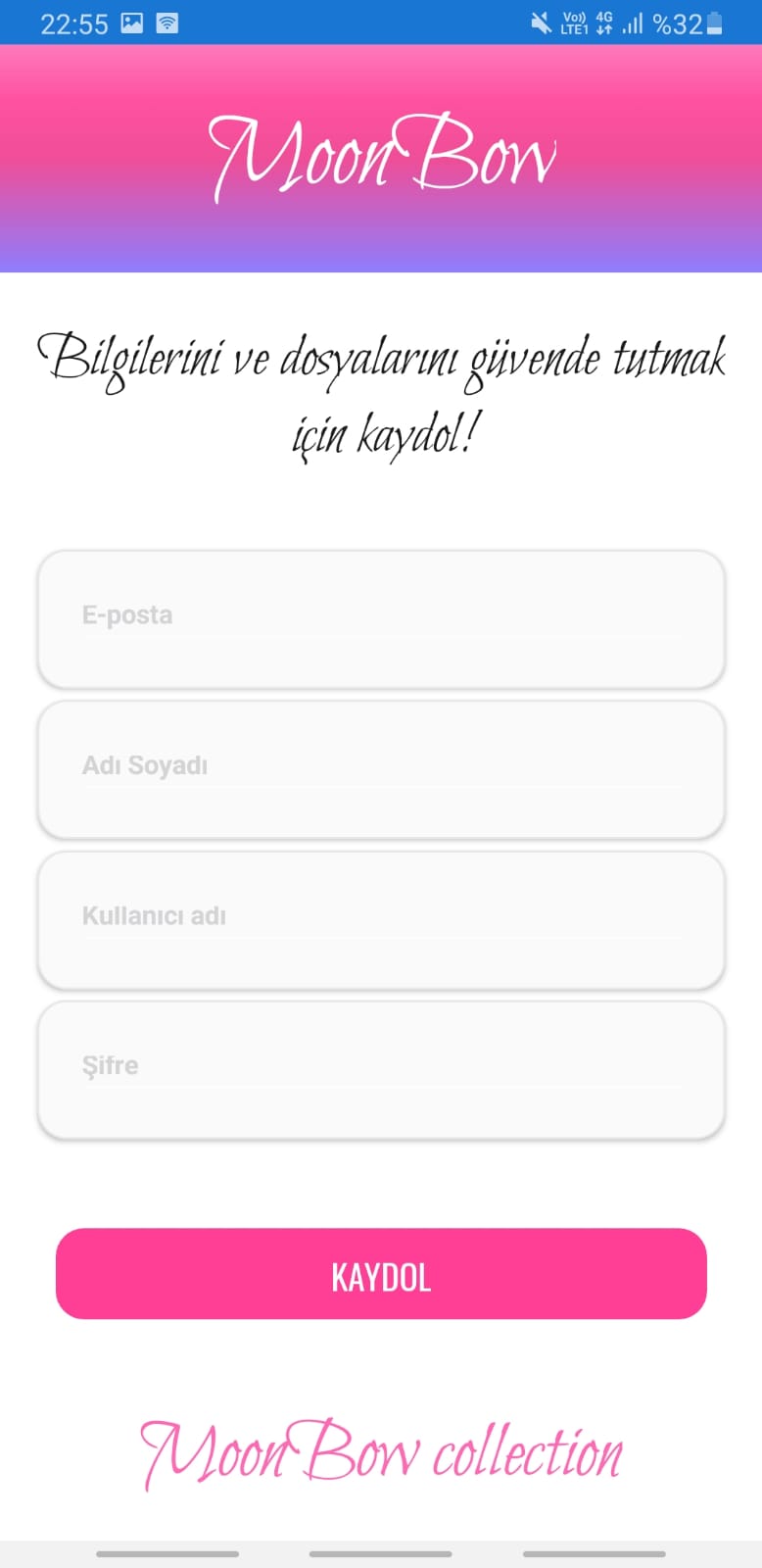
|  |  |  |
| --- | --- | --- |
| **Donanım** | **Teknik Özellikler** | **Kullanım Amacı** |
| Sunucu |  | Veri paylaşımını ve geliştirilmesini sağlamak. |
| Masaüstü Bilgisayar |  | Verilere erişim, kontrol ve test. |
| Dizüstü Bilgisayar |  | Verilere erişim, kontrol ve test. |
| Akıllı telefon | Android 5.0(API düzeyi 21- lollipop)-  Android 11.0(API düzeyi 30 – R) | Veri ekleme, silme, güncelleme ve gösterme.  Kullanıcı kaydetme ve sisteme ekleme. Kullanıcı için bir ara yüz desteği sağlama. |

* 1. **Önerilen Sistemin Teknik Tanımları: Yazılım**

|  |  |  |
| --- | --- | --- |
| **Yazılım** | **Kullanılan Alt Sistem** | **Kullanım Amacı** |
| Firebase | Veri tabanı | Her türlü crud işlemini gerçekleştirmesi. |
| Visual Studio 2019 | Xamarin Forms Cross Platform | Mobil aplikasyon çıkartma  Veri ekleme, silme, güncelleme ve gösterme.  Kullanıcı kaydetme ve sisteme ekleme. Kullanıcı için bir ara yüz desteği sağlama. |
| Visual Studio 2019 | C# Form | Testlerin yapılması ve loğların tutulması |
| enes | enes | enes |

1. **Prototip Tasarım**
   1. **Kayıt ve Giriş Sayfası**

****



* 1. **Biyometrik ve E- Posta Doğrulama Sayfası**

****



**6 Fonksiyonel Gereksinimlerin Belirlenmesi:**

**1. Hoş geldin Sayfası:**

Kullanıcı uygulamaya ilk girdiğinde karşısına 1 saniyeliğine bir “hoş geldin” karşılayacak. Ve kendi kendine kapanacak ve doğrudan giriş sayfasına yönlendirecek. Kullanıcının “hoş geldin”(splash page) sayfasında herhangi bir şey yapmasına gerek yoktur.

**2. Giriş Sayfası:**

Kullanıcı uygulamayı ilk kez girdiği zaman “GİRİŞ YAP” ve “BİYOMETRİK GİRİŞ” butonları aktif olmayacak çünkü herhangi bir kaydı bulunmuyor. Bu sebepten ötürü kullanıcı sayfanın en aşağısında bulunan “Kaydol” yazısına tıklayacak ve karşısına kayıt sayfası açılacak. Eğer kullanıcının kaydı varsa butonlar aktif olacak. Eğer isterse biyometrik giriş isterse belirlediği şifre ile giriş yapabilecek. Ve doğrudan “Ana Sayfa” içerisine yönlendirilecek. Kullanıcı sadece bir kez kayıt ve giriş işlemi yapacak, sonraki seferlerde “Hoş geldin” sayfası doğrudan “Ana Sayfa” içesine gönderek.

**3. Biyomerik Giriş Sayfası:**

Kullanıcı bu sayfada “GİRİŞ YAP” butonuna bastıktan sonra karşısına bilgilendirme mesajı aracılığıyla cihazında gerekli alana parmağını okutması gerektiği yazacak. Bu durum her telefonda olmayacağından tekrardan kullanıcı “GİRİŞ SAYFASINA” dönebilir. Kullanıcı parmağını okutup doğrudan “Ana Sayfaya” yönlendirilecek.

**4. Kayıt Sayfası:**

Kullanıcı kayıt sayfasında gerekli 4 alanı doldurmak zorundadır. Bunlar;

* E-posta
* Adı Soyadı
* Kullanıcı adı
* Şifre

Bu bilgilerini girdikten sonra kullanıcıya e-postasına doğrulama kodu gönderilecek. Kullanıcı gelen doğrulama kodunu uygulama içerinde butona bastıktan sonra açılan popUp page sayfasında gerekli alana yazıp “DOĞRULA” butonu ile kaydı tamamlamış olacak.

**5. Ana Sayfa:**

Ana sayfa içerinde hemen sol üst köşedeki 3 çizgiye basarak ayarlar bölümünü görebilecek. Ana sayfada kullanıcı eski eklemiş olduğu belgeleri görebilecek ve inceleyebilecek.

**6. Ayar Sayfası:**

Ayar Sayfasında 4 buton bulunacak “Anket”, “Hesap Bilgileri”, ”Hesabı Kaldır” ve “Depola” bu dört buton ile uygulama içerinde istediği gibi hareket edebilecek. Bunu yaparken sayfa yığını oluşması engellenecek.

**7. Hesap Bilgileri:**

Kullanıcı hesap bilgilerine ulaşmak için “Şifre” alanını ve “Doğrulama Kodu” alanını doğru girmek zorunda eğer yanlış giriş yaparsa uyarı gösterilerek kullanıcı bilgilendirilecek. Eğer doğru giriş yaparsa hesap bilgileri kullanıcıya gösterilecek.

**8. Hesabı Kaldır:**

Kullanıcı hesabı kaldırmak isterse “HESABI KALDIR” butonu ile bunu başarabilecek. Ama önceden “Şifre” alanını ve “Doğrulama Kodu” alanını doğru girmek zorunda eğer kullanıcı hesabı kaldırmak istemezse “GERİ DÖN” butonu ile “Ana Sayfa” içerisine gidebilecek. Kullanıcı bu işlemleri yaparken 2 buton arasında bulunan KVKK bildirimini okuyabilecek.

**7.Fonksiyonel Olmayan Gereksinimler:**

- Kullanıcı kayıt sayfasında ilgili her alanını doldurmak zorunadır

- E- postası uygun formaya göre girilip girilmediği kontrol ediliyor. Eğer girilmemişse kullanıcı bilgilendiriliyor.

- Şifre en az 5 haneli olup rakam ve harf içermek zorundadır.

- Doğrulama kodu gelmeden kayıt yapılmıyor ve buton 15 saniyeliğine pasif hale getiriliyor.

- Doğrulama kodunu girdikten sonra sayfa kapanıyor ve giriş sayfasına yönlendiriliyor. Kullanıcı bir daha kayıt sayfasına dönemiyor.

- Giriş sayfasında kullanıcıya kolaylık sağlamak için sadece şifre yazması bekleniyor, e-postası kullanıcıya gösteriliyor. Kullanıcı şifresini doğru yazmak zorundadır ve şifre alanını boş bırakamaz.

- Eğer kullanıcının kaydı yoksa ya da kaydını silmişse giriş butonları pasif hale geçiyor.

- Biyometrik giriş sayfasında kullanıcı tekrar giriş sayfasına gitmek isterse bu işlevi telefonundaki geri butonu ile yapamıyor sayfa içerindeki Giriş yazısına basarak yönlendiriliyor.

- Hesabı kaldır sayfasında e-postasına gönderilmiş olan doğrulama kodu ve belirlediği şifreyi doğru girmek zorunda veri tabanı sorgusu ile bunu gerçekleştiriyoruz.

- Hesabı bilgilerini gör sayfasında e-postasına gönderilmiş olan doğrulama kodu ve belirlediği şifreyi doğru girmek zorunda veri tabanı sorgusu ile bunu gerçekleştiriyoruz.

**8. Şifreleme Algoritmasının Belirlenmesi ve Prototip Yapılması:**

Piyasadaki kullanılan şifreleme algoritmalarını incelediğimiz zaman karşımıza çıkan 2 tane şifreleme algoritması oldu. Bunlar;

* 3 DES algoritması ve
* AES algoritmasıdır.

Biz kendi gereksinimlerimizi göz önüne aldığımız zaman AES şifreleme algoritmasını kullanmaya karar verdir. Piyasayı incelerken feyz aldığımız ve Türkçeye çevirdiğimiz Doç. Dr. Fatih ÖZKAYNAK hocamızın yapmış olduğu makalelerden yararlandık. Makale linkleri;

* <https://www.mdpi.com/2073-8994/13/5/824>
* <https://ieeexplore.ieee.org/abstract/document/9044816>

Kısaca AES ve 3 DES algoritmalarını kıyaslarsak AES’i seçme sebebimiz ortaya çıkacaktır.

* AES’in anahtar uzunluğu 128, 192, 256 bittir ama DES sadece 56 bittir.
* AES substitution - permutaion mantığıyla çalışırken DES feistel mantığıyla çalışır.
* AES’in tasarım gerekçesi açıkken Des’in tasarım mantığı kapanmıştır.
* AES, DES şifresinden daha güvenilirdir ve dünya standardıdır.

**8.1. Deneme AES Algoritması Sayfası**

Kullanıcı sayfa içerisine “Bir Metin Yazınız” alanına metni yazdıktan sonra “Metni Şifrele” butonu ile şifrelenen metin “Şifreli Metin” label’ına yazdırılıyor. Butona bastıkça metin şifreleniyor. Eğer kullanıcı metni çözmek isterse “Metini Çöz” butonu ile bunu başarıyor ve “Çözülmüş Metin” label’ına yazdırılıyor. Biz bu yapıyı kullanıcıya göstermeden veri tabanına verilerini kaydedeceğimiz zaman işlemleri doğrudan gerçekleştirip veri tabanına (firebase real time) şifreli bir şekilde ekleyeceğiz. Bu yaptığımız çalışma sadece tecrübe kazanmak ve çıkabilecek sıkıntılara çözüm bulmak için yapıldı. Kaynak kodları ve tasarımı için;

****

