



T.C.

FIRAT ÜNİVERSİTESİ

TEKNOLOJİ FAKÜLTESİ

YAZILIM MÜHENDİSLİĞİ BÖLÜMÜ

Proje Dokümantasyonu

CyberEncryption

Proje Ekibi

ERDİ AKKILIÇ / 170542005

SAMET DORA / 180541016

MUSTAFA AKAYDIN / 180541035

MÜCAHİT EREN ÖZCAN / 170541008

1.Giriş

1.1 Projenin Amacı

Teknolojinin hızla ilerlemesi ve gelişmesiyle birlikte kurumlara ve şahsi cihazlarımıza yapılan siber saldırıların da arttığı bir gerçektir. Bu yüzden bazı uygulamaların kullanımı önemli derecede artacaktır. Bunlardan biri CyberEncryption uygulamamızdır. Bu uygulama Dosyalarımızı güvenli bir şekilde şifrelenerek ve gerektiği zaman çözülmesini sağlayarak saklanmasıdır.

1.2 Projenin Kapsamı

Proje herhangi bir depolama yapmadan bir belge ve dosyanın güvenli bir şekilde şifrelenerek saklanmasıdır. Bütün İnsanlar tarafından kullanılması öngörülmektedir.

1.3 Piyasada Bulunan Rakiplerin SWOT Analizi

Piyasada bulunan belli başlı şifreleme sistemleri için yapmış olduğumuz swot analizleri:

S STRENGTHS	W WEAKNESSES	O OPPORTUNITIES	T THREATS
<ul style="list-style-type: none">-Yanlış girilen Parola girişlerini monitörler-256-bit dosya şifreleme yöneti kullanılır-Çevrimiçi yedekleme ile veri kaybı önleme	<ul style="list-style-type: none">- Tasarımın Göze hitap etmemesi	<ul style="list-style-type: none">- Deneme sürümünün bir kaç dosyayı kapsamaması	<ul style="list-style-type: none">- Saldırganlar tarafından ele geçirilmesi halinde dosyaları eline geçirmesi

1.4 CyberEncryption SWOT Analizi

S STRENGTHS	W WEAKNESSES	O OPPORTUNITIES	T THREATS
<ul style="list-style-type: none">- Ekstra depolama alanına ihtiyaç olmaması- Bilgiler çalınamaması	<ul style="list-style-type: none">- Yeterli yoğunlukta test edilememesi	<ul style="list-style-type: none">- Open Source olup geliştirilmeye açık olması- Sınırsız dosya şifrelemesi ve	<ul style="list-style-type: none">- Rakiplerin güçlü olması

1.5 CyberEncryption SMART Analizi

1- Specific (Belirli)

Projede depolama kullanılmadan dosyalarımızı şifreleyerek güvenli bir şekilde saklamayı amaçlar.

2- Measurable (Ölçülebilir)

Projenin güvenliğini reklam ile anlatıp kısa sürede belli popülariteye ulaşmak istenmektedir.

3- Achievable (Başarılabilir)

Kolay çözülecek bir şifreleme algoritması bir işe yaramaz o yüzden projede şifreleme algoritmasını güçlü tutup şifrelemenin kırılması en aza indirgenecek.

4- Relevant (Alakalı)

Projede dosyayı şifreleme güvenliği önemlidir. Şifreleme güvenliği ne kadar az olursa projenin önemi o kadar azalır.

5- Time-Bound (Sınırlı Zaman)

Projenin sunumunu iyi yapıp 6 ay kadar bir süre içinde belli bir indirme sayısına ulaşmak hedeflenmektedir.

2.Proje Planı

2.1 Giriş

Kullanıcı tarafından sisteme yüklenme gereksimi olmadan dosyanın doğru bir şekilde güvenli bir şekilde şifreleyip saklanması, gerektiğinde o dosyaya kolay bir şekilde erişmemizi sağlar. Projemiz Open Source kaynaklı olup gelişime açık olması durumunda daha fazla güvenli hale getirilmesi en büyük amaclarımızdan biri olmasıdır.

2.2 Projenin Plan Kapsamı

Projenin plan kapsamında genel olarak mevcut sistem, sistemin gerekliliği ve bu sistemin güvenilirliğinden yola çıkıldı. Bu projede, hiç bir kayıp olmadan çok gizli dosyalarınızı hiç bir hackleme durumu olsa bile hackerlar tarafından şifreli dosyayı çözmeleri çok zor bir ihtimaldir. Yüklediğimiz Cloud sistemlerin ne kadar güvenli olduğundan şüphe duymakta endişeliyiz. Bu durumu ortadan kaldırmak için hiç bir kütüphane olmadan sadece python 3.8 yüklü olan cihazların hepsinde kolaylıkla olabilir.

2.3 Proje Zaman-İş Planı

Zaman / İş	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
Proje Planı	+	+	+											
Analiz				+	+	+								
Çözümleme							+	+	+					
Tasarım										+	+			
Gerçekleştirim											+	+	+	
Bakım														+

2.4 Proje Ekip Yapısı

ERDİ AKKILIÇ = Şifreleme Algoritmasının Geliştirilmesi

SAMET DORA = Çözümleme Algoritmasının Geliştirilmesi

MUSTAFA AKAYDIN = Frontend Ve Dokümantasyon

MÜCAHİT EREN ÖZCAN = Frontend Ve Dokümantasyon

2.5 Önerilen Sistemin Teknik Tanımları

- Kriptoloji

2.6 Kullanılan Özel Geliştirme Araçları ve Ortamları

Programlama Araçları:

- Visual Studio Code , Pycharm, CSS

2.8 Eğitim Planı

Projeden kazanılacak en önemli olaylardan biride eğitimidir. Kullanılacak dillerin arayüz editör ve programların kullanımında hâkim olunamaması halinde bu program başarıyla neticelendirilemez.Bu yüzden projede bazı eğitimler alınması gereklidir. Proje kapsamında alınacak olan eğitimler;

- Visual Studio Code

- Pycharm
- CSS

2.9 Test Planı

Proje test ekipleri ve görevleri şu şekildedir;

- Sistem uygunluk testi yapmak,
- Projenin açıklıklarını ve güvenliğini test etmek için güvenlik testi yapmak.
- Projenin çözümlemesinin zor hale getirilmesi

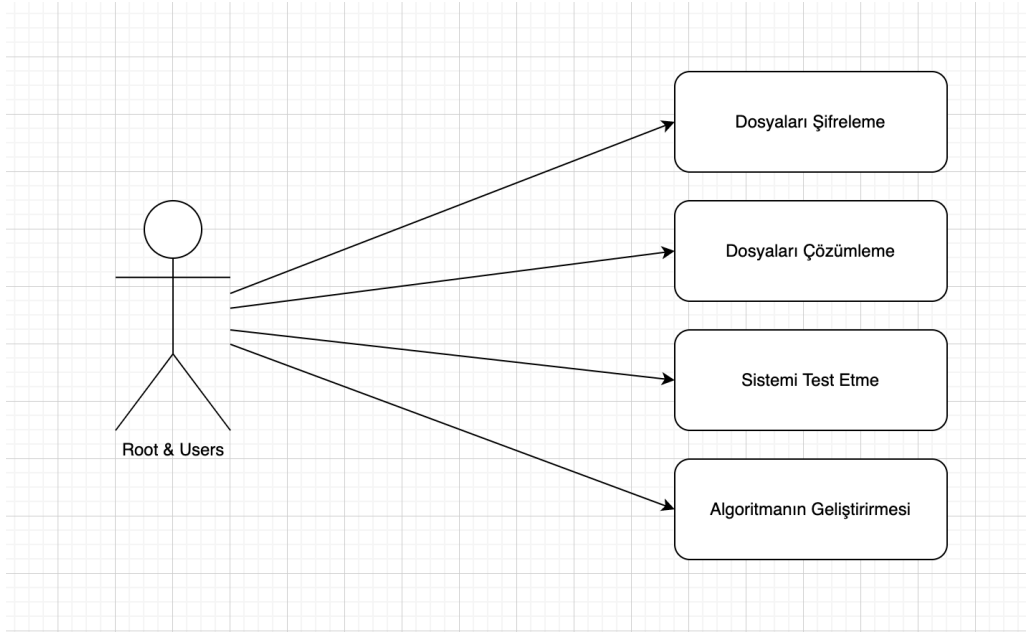
2.10 Bakım Planı

Projenin bakım planında kullanıcıdan geri dönüşleri ve geliştirilmesi doğrultusunda, herhangi bir güvenlik açığında, güncel olarak belirli zaman aralıklarında yapılacak olan değişiklikler bakım planı ile yapılır.

3. Sistem Çözümleme

3.1 Gereksenen Sistemin Mantıksal Modeli

3.1.1 İşlevsel Model



3.1.2

Genel Bakış

Uygulamamız herhangi bir giriş sayfası olmadan bir veritabanı olmadan herkes tarafından rahatlıkla kullanılabilecek bir sistem oluşturmak. Bu yüzden tek sayfa olacak. Bir index sayfamız ve sayfamızın üzerinde dosya yükleme alanı, şifre çözme ve şifreleme olacak şekilde olacak.

3.1.2 Başarım Gereklileri

Mevcut sistemler incelendi ve sistemin başarımı için:

- Güvenlik
 - Güvenilirlik
 - Kullanım kolaylığı
- vb. kıstaslar temel gereklilikler olarak tespit edilmiştir.

Teknoloji Hazırlık Seviyeleri (YAZILIM) TRL Hesaplama Metodolojisi: Her TRL seviyesinde Ortalama Tamamlanma Yüzdesi Hesaplanır. Ortalama Tamamlanma Yüzdesi ≥ 80 olan son TRL seviyesi, Projenin Teknolojik Hazırlık Seviyesi olarak kabul edilir.*				Tamamlanma Derecesi (Her satırda yalnızca bir kutucuğa X - Büyük Harf ile- koyunuz)						Otomatik Olarak Hesaplanır
		Cevap olarak yalnızca ilgili kutuya Evet yazınız		0	1	2	3	4	5	
TRL Seviyesi	Açıklama**	Yürütülen / Yürütülmüş Proje Dahilinde Tamamlanmıştır	Yürütülen / Yürütülmüş Proje Dışında Tamamlanmıştır	Başlanmadı	Yeni Başlandı	Başlandı, az ilerleme kaydedildi	Çalışmaların yaklaşık yarısı tamamlandı	Çalışmaların büyük bölümü tamamlandı	Tamamlandı	Tamamlanma Oranı (%)
TRL 1 Tanımı	Temel Bilimsel Araştırmalar: Yazılım ürününün matematiksel formülasyonları ve temel özelliklerine ilişkin bilimsel bilginin geliştirildiği aşamadır.									88
1	Yazılım gereksinimleri genel hatlarıyla tanımlandı mı?	Evet							X	100
	Hedeflenen yazılım ürününün temel özellikleri, matematiksel formülasyonu ve genel algoritmasını destekleyen halihazırdaki bilimsel bilgiler elde edildi mi?	Evet							X	100
	Yazılım gereksinimlerini ve bu gereksinimleri karşılayabilecek yazılım ürününü destekleyen/sınayan temel prensipler, bilimsel kurallar ve varsayımlar tanımlandı mı?	Evet							X	100
	Destekleyici/sınayıcı temel prensipler, bilimsel kurallar ve varsayımlar gözlemlendi ve doğrulandı mı?	Evet						X		80
	Gözlem ve doğrulama/sınama araştırmaları sonucunda yazılım mimarisine ilişkin bilimsel bilgi geliştirildi mi?	Evet					X			60
TRL 2 Tanımı	Temel Bilimsel Araştırmalardan Yazılım Konsepti Tasarımı: Yazılım konseptinin, temel özelliklerinin ve modellemeye sinanan potansiyel uygulamalarının formüle edildiği aşamadır.									90
2	Hedeflenen yazılımın potansiyel uygulamaları belirlendi mi?	Evet							X	100
	Potansiyel uygulamaların yapılabilişliği (fizibilitesi) doğrulandı mı?	Evet							X	100
	Algoritmaların ve yazılım konseptinin temel özellikleri tanımlandı mı?	Evet					X			60
	Yazılımın üzerinde çalışacağı donanım halihazırda mevcut mu?	Evet							X	100
TRL 3 Tanımı	Yazılımın kritik performans özelliklerinin doğrulanması amacıyla, entegre edilmemiş yazılım bileşenleri kullanılarak, sınırlı işlevsellğin (limited functionality) geliştirildiği aşamadır.									10
3	Yazılımın performans özellikleri ve geliştirilen algoritmalar, modellenen temsili veri setleriyle veya analitik çalışmaları gerçekleştirildi mi? (Verification)	Evet			X					20
	Yazılıma ilişkin algoritmaların ana hatları dokümanite edildi mi?	Evet			X					20
	İlk yazılım kodlamaları, yazılımın operasyonel gereksinimi karşıladığını gösteriyor mu? (Verification)			X						0
	Algoritmaların, temsili (surrogate) bir işlemcide başarılı bir şekilde çalıştığının fiziki gösterimi yapıldı mı? (Demonstration)			X						0
TRL 4 Tanımı	Yazılımın kritik bileşenlerinin entegre edildiği, fonksiyonellik bakımından doğrulandığı, birarada çalışabilirliğin (interoperability) ve sistem mimarisinin geliştirilmeye başlandığı aşamadır.									0
4	Veri formatlarının analizi tamamlandı mı?			X						0
	Her bir modülün yazılım mimari modeliyle uyumluluğu sağlandı mı?			X						0
	Yazılım, yapay tam-ölçek problemleri çözümlüyor veya temsili veri setlerini tam olarak işleyebiliyor mu (data processing) ?			X						0
	Tüm işlevlerin veya modüllerin laboratuvar ortamında fiziki gösterimi yapıldı mı? (Demonstration)			X						0
	İşlevlerin veya modüllerin geçici entegrasyonunun fiziki gösterimi yapıldı mı? (Demonstration)			X						0
	Entegre edilen işlevlerin veya modüllerin fonksiyonel olarak doğrulanması yapıldı mı? (Validation)			X						0
	Yazılım mimari modelinin birlikte çalışabilirlik (interoperability), güvenilirlik (reliability), sürdürülebilirlik (maintainability), genişletilebilirlik (extensibility), ölçeklendirilebilirlik (scalability) ve güvenlik (security) konularını içerecek şekilde geliştirilmesine başlandı mı?			X						0
TRL 5 Tanımı	Simüle edilmiş (benzetimli) ortamda, uçtan uca yazılım unsurlarının (işlevler/modüller) entegre edildiği, arayüzlerin geliştirildiği ve fiziki gösteriminin (demonstration) yapıldığı aşamadır.									0
5	Her bir işlevin/modülün kodlaması tamamlandı mı?			X						0
	Her bir işlevin/modülün hata ayıklaması (debugging) yapıldı mı?			X						0
	Uçtan uca yazılım unsurlarının (işlevler/modüller) simüle edilmiş (benzetimli) ortamlı uyumu mevcut sistemler/simülasyonlar ile arayüzleri geliştirildi mi?			X						0
	İşlevlerin/modüllerin simüle edilmiş (benzetimli) ortamda entegrasyonunun fiziki gösterimi yapıldı mı? (Demonstration)			X						0
	Uçtan uca yazılım sisteminin öngörülen performansı gösterdiği doğrulandı mı?			X						0
	Algoritmalar, operasyonel ortama yerleştirilebilecek özellikteki bir işlemcide çalıştırıldı mı?			X						0
	Yazılım mimarisi tamamlandı mı?			X						0
	Veritabanı yapısı ve arayüzlerin yapısı tamamlandı mı?			X						0
TRL 6 Tanımı	Yazılım prototipinin tasarlandığı, tam ölçekteki gerçekçi problemler ile test edildiği ve fiziki gösteriminin (demonstration) yapıldığı aşamadır. (Yazılımın ön versiyonu - Alpha version)									0
6	Yazılımın prototip uygulamalarının, tam ölçekteki gerçekçi problemler üzerinde fiziki gösterimi yapıldı mı? (Demonstration)			X						0
	Yazılım algoritmaları, mevcut donanım/yazılım sistemleri ile entegre edildi mi?			X						0
	Yazılım prototipinin "mühendislik fizibilite analizi" tamamlanarak, fizibilitesinin fiziki gösterimi yapıldı mı? (Demonstration)			X						0
	Yazılım geliştirme belgeleri (kullanıcı belgeleri, bakım belgeleri, eğitim belgeleri) hazırlanmaya başlandı mı?			X						0
	Zamanlama kısıtlarının (timing constraints) analizi, tatmin edici sonuçlarla tamamlandı mı?			X						0
TRL 7 Tanımı	Gerçek (Operasyonel) Ortamda Yazılım Prototipinin Fiziki Gösterimi: Yazılım prototipinin gerçek (operasyonel) ortamda tüm fonksiyonlarının fiziki gösteriminin (demonstration) yapıldığı aşamadır. (Yazılımın çalışır versiyonu - Beta version)									0
7	Yazılım prototipi fiziki gösterim (demonstration) ve test için gereken tüm kilit işlevlere sahip olacak şekilde geliştirildi mi?			X						0
	Operasyonel fizibiliteyi gösteren donanım/yazılım sistemlerinin entegrasyonu başarılı bir şekilde yapıldı mı?			X						0
	Yazılım hataları (software bugs) büyük oranda düzeltildi mi?			X						0
	Yazılım geliştirme belgeleri (kullanıcı belgeleri, bakım belgeleri, eğitim belgeleri) kısmen hazırlandı mı?			X						0
	Entegre edilmiş yazılım prototipinin, gerçek (operasyonel) ortamda fiziki gösterimi yapıldı mı? (Demonstration)			X						0
TRL 8 Tanımı	Gerçek Ortamda Yazılım Performans Değerlendirmesi ve Belgelendirmesi: Yazılımın geliştirme sürecinin tamamlandığı, belgelendirildiği ve son halinin beklenen koşullar altında çalışır durumda olduğu aşamadır. (Yazılımın ilk versiyonu - v.1.0)									0
8	Yazılım teknolojsi operasyonel donanım ve yazılım sistemleriyle tam olarak entegre edildi mi?			X						0
	Yazılım hatalarının (software bugs) tamamı ayıklandı mı?			X						0
	Yazılım geliştirme belgeleri (kullanıcı belgeleri, bakım belgeleri, eğitim belgeleri) tamamlandı mı?			X						0
	Yazılımın tüm işlevlerinin, simüle edilmiş (benzetimli) operasyonel senaryolarda başarılı bir şekilde fiziki gösterimi yapıldı mı? (Demonstration)			X						0
	Metodoloji ve yazılım "Gerçekleme ve Doğrulama" (Verification and Validation - V&V) tamamlandı mı?			X						0
TRL 9 Tanımı	Gerçek Ortamda Başarı ile Performans Gösteren Yazılım: Geliştirilen teknoloji/sistemin gerçek ortamında çalışır durumda olduğunun kanıtlandığı aşamadır.									0
9	Entegre yazılım teknolojsi operasyonel donanım ve yazılım sistemleriyle birlikte çalışır durumda mı?			X						0
	Yazılım teknolojsi gerçek ortamda ve gerçek senaryolarda başarılı şekilde çalışır durumda mı?			X						0
	Yazılım teknolojsi gerçek operasyonel ortamda halihazırda, tekrar edilebilir ve yeniden kullanılabilir şekilde (repeatable and reusable) mı?			X						0
	Yazılım mühendisliği desteği mevcut ve sürdürülebilir mi?			X						0

Açıklamalar ve Referanslar

* Hesaplama metodolojisi için yararlanılan kaynak: Setiawan ve Sulaswatty, "Production technology readiness assessment of surfactant in the research center for Chemistry-Indonesian Institute of Sciences", AIP Conference Proceedings, 2017

** Tanımlar ve sorular hazırlanırken aşağıdaki referanslardan faydalanılmıştır:

- Lavoie and Daim, "Technology Readiness Levels Improving R&D Management: A Grounded Theory Analysis", PICMET '17: Technology Management for Interconnected World, Portland State University, ABD, 2017
- "Savunma Sanayii için Teknoloji Hazırlık Seviyesi Kılavuzu", Savunma Sanayii Müsteşarlığı, Türkiye, 2015
- "The TRL Scale as a Research & Innovation Policy Tool", EARTO Recommendations, 2014
- "TRL Questionnaire", <https://docs.gatesfoundation.org/documents/trl-questions-tool.xlsx>, Bill & Melinda Gates Foundation, ABD (Erişim: Ağustos 2018)
- Homeland Security Studies and Analysis Institute, "Security Science and Technology Readiness Level Calculator (Ver 1.1)", ABD, 2009
- US Department of Defense; Defense Research and Engineering (DDR&E), "Technology Readiness Assessment (TRA) Deskbook", 2009
- Blanchette et al, "Beyond Technology Readiness Levels for Software: U.S. Army Workshop Report", Software Engineering Institute, Carnegie Mellon University, ABD, 2010
- William L. Nolte, "Did I Ever Tell You about the Whale: or Measuring Technology Maturity", Information Age Publishing, ABD, 2008
- "Technology Readiness Levels - TRL, NASA's contribution to Horizon 2020", https://www.wmahsn.org/storage/resources/documents/EIT_Health_KIC_A_guide_to_TRL-EIT_health.pdf, (Erişim: Ekim 2018)