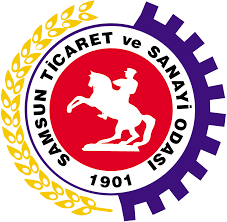
simge, sembol, yazı tipi, logo, grafik içeren bir resim

Açıklama otomatik olarak oluşturuldu

**HACKATHON GELİŞEN ÇAĞ yarışması PROJE RAPORU**

**Takım Adı : DiSoftWare**

**Yarışmacılar Adı Soyadı:**

**Osman TEMEL/ Hünkar ACAR**

**Proje Ana Alanı: Dijital Güvenlik Kalesi: Veri Gizliliği**

**31 Mart 2024**

**Samsun**

İÇİNDEKİLER

[Şekiller Listesi 2](#_Toc168045324)

[Tablolar Listesi 2](#_Toc168045325)

[ÖZET 3](#_Toc168045326)

[GİRİŞ 4](#_Toc168045327)

[PROBLEM 4](#_Toc168045328)

[Mevcut Durumun ve Bu Durumun Neden Bir Problem Teşkil Ettiğinin Açıklanması: 4](#_Toc168045329)

[Problemin Boyutları ve Etkilenen Taraflar: 5](#_Toc168045330)

[Problemin Çözülmemesi Durumunda Ortaya Çıkabilecek Olumsuz Sonuçlar: 5](#_Toc168045331)

[Problemin Özgün Değeri: 5](#_Toc168045332)

[AMAÇ 6](#_Toc168045333)

[YÖNTEM 7](#_Toc168045334)

[Veri Setleri: 7](#_Toc168045335)

[Modeller: 7](#_Toc168045336)

[Modellerin Değerlendirmesi: 8](#_Toc168045337)

[Projede Uyarlanma: 8](#_Toc168045338)

[PROJENİN YENİLİKÇİ YÖNÜ 10](#_Toc168045339)

[SOSYAL ETKİ 11](#_Toc168045340)

[UYGULANABİLİRLİK 12](#_Toc168045341)

[BULGULAR 12](#_Toc168045342)

[SONUÇ VE TARTIŞMA 14](#_Toc168045343)

[ÖNERİLER 15](#_Toc168045344)

[KAYNAKLAR 16](#_Toc168045345)

[EKLER 17](#_Toc168045346)

[Uygulama Görüntüleri 17](#_Toc168045347)

## Şekiller Listesi

[Şekil 1 Transformer Model Sonuçları 7](#_Toc168041037)

[Şekil 2 Bileşenlerin Haberleşmesi 9](#_Toc168041038)

## Tablolar Listesi

[Tablo 1 Modelleriin Değerlendirme metrikleri 7](#_Toc168041039)

# ÖZET

Bu projenin amacı, internet kullanıcılarının güvenliğini en üst düzeye çıkarmak ve veri gizliliğini korumak için yenilikçi ve etkili çözümler sunmaktır. Proje kapsamında, gerçek zamanlı saldırı tespit sistemi, özel şifreleme(kriptoloji) teknikleri ve şifre gücü belirleme aracı gibi hayati öneme sahip özellikler entegre edilmiştir. Gerçek zamanlı saldırı tespit sistemi, derin öğrenme ve makine öğrenimi modellerinden faydalanarak kullanıcıların aldıkları URL üzerindeki potansiyel tehditleri anında tespit etmelerine olanak tanır. Kriptoloji alanında ise, güvenli iletişim için özel olarak geliştirilmiş şifreleme algoritmaları ve bu şifreleri çözmeye yönelik algoritmalar sunulmaktadır. Ayrıca, şifre gücü belirleme aracı, kullanıcıların oluşturdukları şifrelerin güvenliğini detaylı bir şekilde analiz eder. Bu önlemler, kullanıcıların internet üzerinde daha güvenli bir deneyim yaşamalarını sağlayarak veri gizliliğini artırmayı hedefler. Projemiz, internet güvenliği alanında önemli bir adım atarak, kullanıcıların dijital dünyada daha güvenli ve bilinçli bir şekilde hareket etmelerine katkıda bulunmayı amaçlamaktadır.

**Anahtar Kelimeler**: İnternet güvenliği, gerçek zamanlı saldırı tespiti, kriptoloji, şifre gücü.

# GİRİŞ

Bu araştırmanın amacı, internet kullanıcılarının güvenliğini artırmak ve veri gizliliğini sağlamak için geliştirilen çeşitli önlemleri tanıtarak, bu konunun bağlamını ve önemini açıklamaktır.

**Konunun Tanıtımı ve Genel Bir Bakış:** Günümüzde internet kullanımının artmasıyla birlikte, çevrimiçi tehditlerin çeşitliliği ve karmaşıklığı da hızla artmaktadır. Kullanıcıların kişisel bilgilerinin korunması ve çevrimiçi aktivitelerinin güvenliği, hem bireysel hem de kurumsal düzeyde büyük bir öneme sahiptir. İnternet güvenliği, bu bağlamda, teknolojik gelişmelerin sağladığı yeniliklerle daha da kritik hale gelmiştir.

**Araştırmanın Amacının ve Hedeflerinin Net Bir Şekilde Belirtilmesi:** Bu araştırma, kullanıcıların internet üzerindeki güvenliklerini artırmak ve veri gizliliğini sağlamak için geliştirilmiş olan çeşitli önlemleri incelemektedir. Projede, gerçek zamanlı saldırı tespit sistemi, kriptoloji ve şifre gücü belirleme gibi önemli özellikler entegre edilmiştir. Araştırmanın somut hedefleri, kullanıcıların potansiyel saldırılara karşı anında korunmasını sağlamak, güvenli iletişimi teşvik etmek ve kullanıcıların şifre güvenliğini artırmaktır.

**Araştırmanın Neden Önemli Olduğunun Açıklanması:** İnternet üzerindeki tehditler, kullanıcıların kişisel verilerinin çalınması, kimlik avı saldırıları ve diğer siber suçlarla sonuçlanabilir. Bu tehditlere karşı etkili önlemler almak, kullanıcıların hem kişisel hem de finansal bilgilerini korumak açısından kritik öneme sahiptir. Ayrıca, güvenli bir internet ortamı sağlamak, genel kullanıcı deneyimini iyileştirir ve dijital dünyada güvenliğin sağlanmasına katkıda bulunur.

**Araştırma Sorusu veya Hipotezi:** Araştırmanın temel sorusu, "Geliştirilen yapay zeka tabanlı saldırı tespit sistemi, kriptoloji ve şifre gücü belirleme aracı, internet kullanıcılarının güvenliğini ve veri gizliliğini ne ölçüde artırabilir?" şeklindedir. Bu bağlamda, hipotezimiz, "Yapay zeka ve kriptografi tekniklerinin entegrasyonu, internet güvenliğini ve veri gizliliğini anlamlı ölçüde artıracaktır" şeklinde ifade edilebilir.

# PROBLEM

## Mevcut Durumun ve Bu Durumun Neden Bir Problem Teşkil Ettiğinin Açıklanması:

İnternet, modern hayatın vazgeçilmez bir parçası haline gelmiş olup, bireylerin ve işletmelerin günlük faaliyetlerini yürüttüğü bir platformdur. Ancak, internetin yaygın kullanımıyla birlikte siber tehditlerin ve saldırıların da sayısı ve karmaşıklığı artmıştır. Mevcut durumda, kullanıcılar her gün kimlik avı (phishing), zararlı yazılım (malware), dağıtık hizmet reddi saldırıları (DDoS) ve veri ihlalleri gibi çeşitli tehditlerle karşı karşıya kalmaktadır. Bu tehditler, kullanıcıların kişisel ve finansal bilgilerinin çalınmasına, mahremiyetin ihlaline ve maddi kayıplara yol açabilir.

## Problemin Boyutları ve Etkilenen Taraflar:

Siber güvenlik probleminin boyutları oldukça geniştir ve birçok tarafı etkilemektedir. Bireyler, kişisel verilerinin ve finansal bilgilerinin çalınması riskiyle karşı karşıya kalırken, işletmeler ve kuruluşlar, müşterilerinin ve çalışanlarının verilerinin güvenliğini sağlamak zorundadır. Bu durum, hem bireyler hem de işletmeler için ciddi maddi ve manevi kayıplara yol açabilir. Ayrıca, kamu kurumları ve altyapılar da siber saldırılardan etkilenebilir, bu da toplumun genel güvenliği ve işleyişi üzerinde olumsuz etkiler yaratabilir.

## Problemin Çözülmemesi Durumunda Ortaya Çıkabilecek Olumsuz Sonuçlar:

Eğer bu siber güvenlik problemleri çözülmezse, ciddi ve geniş çaplı olumsuz sonuçlar ortaya çıkabilir. Bireyler, kimlik hırsızlığı ve mali kayıplarla karşı karşıya kalabilirken, işletmeler ise itibar kaybı, müşteri güveninin sarsılması ve büyük mali cezalarla karşılaşabilir. Dahası, kritik altyapılar ve kamu hizmetleri üzerinde yapılan saldırılar, toplumsal düzende aksamalara ve geniş çaplı güvenlik sorunlarına yol açabilir. Bu durum, genel internet kullanımının güvenliğini ve güvenilirliğini ciddi şekilde zedeler.

Sonuç olarak, internet güvenliği ve veri gizliliği konusundaki mevcut problemler, bireylerin, işletmelerin ve toplumun genel işleyişi üzerinde büyük tehditler oluşturmakta ve bu problemlerin çözülmesi hayati bir önem taşımaktadır. Bu projenin hedefi, mevcut tehditlerle etkili bir şekilde mücadele ederek, kullanıcıların internet üzerindeki güvenliğini artırmak ve veri gizliliğini sağlamaktır.

## Problemin Özgün Değeri:

Bu proje, siber güvenlik alanında karşılaşılan karmaşık ve yaygın bir problemi ele alarak özgün bir yaklaşım sunar. Geleneksel siber güvenlik önlemleri, genellikle belirli saldırı türlerine odaklanırken, bu projenin özgün değeri, geniş kapsamlı bir yaklaşım benimsemesidir.

Projemiz, kullanıcıların internet üzerindeki güvenliğini artırmak için gerçek zamanlı saldırı tespit sistemleri, kriptoloji ve şifre gücü belirleme gibi çeşitli önlemleri bir araya getirir. Bu çoklu önlemler yaklaşımı, kullanıcıların çeşitli tehditlere karşı daha kapsamlı bir koruma sağlamasına olanak tanır.

Ayrıca, projenin özgün değeri, yapay zeka ve makine öğrenimi gibi ileri teknolojilerin etkin bir şekilde kullanılmasıdır. Derin öğrenme modelleri ve karmaşık algoritmalar, saldırıları tespit etme ve şifre gücünü belirleme gibi görevleri daha etkili bir şekilde gerçekleştirebilir, böylece kullanıcıların güvenliğini artırabilir.

Bu özgün yaklaşım, siber güvenlik alanında mevcut boşlukları doldurmayı ve kullanıcıların internet üzerinde daha güvenli bir deneyim yaşamasını sağlamayı hedefler. Sonuç olarak, projenin özgün değeri, çeşitli teknolojilerin entegrasyonuyla güçlendirilmiş kapsamlı bir yaklaşım sunmasıdır, bu da kullanıcıların veri güvenliğini en üst düzeye çıkarmaya yardımcı olur.

# AMAÇ

Bu projenin temel hedefi, internet kullanıcılarının güvenliğini artırmak ve veri gizliliğini sağlamak için etkili bir çözüm sunmaktır. Günümüzde, internet üzerindeki tehditlerin karmaşıklığı giderek artmakta ve kullanıcıların kişisel bilgilerinin güvende olması giderek önem kazanmaktadır. Özellikle, bilgiye her an her yerden erişimin kolaylaşmasıyla birlikte, veri güvenliği ve gizliliği daha büyük bir endişe haline gelmiştir. Bu bağlamda, projenin hedefleri şunlardır:

1. **Gerçek Zamanlı Saldırı Tespit Sistemi:** Kullanıcıların internet üzerinde gezinirken karşılaşabilecekleri potansiyel saldırıları gerçek zamanlı olarak tespit etmek ve bu saldırılara karşı önlem almak. Derin öğrenme ve makine öğrenimi modellerinin kullanılmasıyla, kullanıcılar aldıkları IP adresi veya URL üzerindeki saldırıları tanımlayabilir ve hızlı bir şekilde tepki verebilirler. Bu, kullanıcıların bilgisayarlarını ve kişisel verilerini korumak için önemli bir adımdır.
2. **Kriptoloji**: Güvenli iletişim için geliştirilmiş şifreleme algoritmaları kullanarak kullanıcıların hassas verilerini güvenli bir şekilde iletmelerini sağlamak. Özel olarak tasarlanmış şifreleme algoritmaları, verilerin yetkisiz erişime karşı korunmasını sağlar. Bu sayede, kullanıcılar güvenli bir iletişim ortamında bilgilerini paylaşabilirler.
3. **Şifre Gücü Belirleme:** Kullanıcıların belirledikleri şifrelerin güvenliğini analiz ederek, daha güçlü şifreler oluşturmaları konusunda önerilerde bulunmak. Yapay zeka modeli, verilen şifrenin karmaşıklığını değerlendirir ve kullanıcıya şifrelerini güçlendirmeleri için öneriler sunar. Bu, kullanıcıların hesaplarını kötü niyetli saldırıcılardan korumak için önemlidir.

Bu hedefler doğrultusunda, projenin internet güvenliği alanında kullanıcıların bilinçlenmesine ve korunmasına yönelik önemli bir katkı sağlaması amaçlanmaktadır. Bu proje, kullanıcıların dijital dünyada daha güvenli ve bilinçli bir şekilde hareket etmelerini sağlayarak internet güvenliği konusundaki eksiklikleri giderecek ve kullanıcıların veri gizliliğini sağlamaya yardımcı olacaktır. Bu amaçlar doğrultusunda, projenin etkinliğinin değerlendirilmesi ve kullanıcı geri bildirimlerinin alınması önemlidir. Bu sayede, projenin kullanıcılar üzerindeki etkisi daha net bir şekilde anlaşılabilir ve gelecekteki geliştirmeler için fikirler sunulabilir.

# YÖNTEM

## Veri Setleri:

* **Kaggle Şifre Gücü Belirleme Veri Seti:** Bu veri seti, farklı şifrelerin karmaşıklığını belirlemek için oluşturulmuş bir veri kümesidir. Şifrelerin uzunluğu, karakter çeşitliliği ve diğer özellikleri içerir.
* **CICIDS 2023 Veri Seti:** Bu veri seti, siber saldırıları tespit etmek için kullanılan bir veri kümesidir. Gerçek dünya senaryolarından elde edilen ağ trafiği verilerini içerir ve farklı türde saldırıları içeren etiketlenmiş verilerle birlikte gelir.

## Modeller:

* **Şifre Gücü Belirleme İçin Model (RandomForestClassifier):** Bu model, Kaggle Şifre Gücü Belirleme Veri Seti'nde şifrelerin karmaşıklığını değerlendirmek için kullanılır. RandomForest algoritması, farklı özelliklere sahip veriler arasındaki ilişkileri öğrenerek şifrelerin gücünü tahmin eder.
* **Saldırı Tespiti İçin Modeller (Transformer ve XGBoost):** CICIDS 2023 Veri Seti'nde siber saldırıları tespit etmek için kullanılan modellerdir. Transformer ve XGBoost algoritmaları, ağ trafiği verilerindeki anormallikleri ve saldırı desenlerini tanımlamak için kullanılır.

ekran görüntüsü, metin, diyagram içeren bir resim

Açıklama otomatik olarak oluşturuldu

Şekil 1 Transformer Model Sonuçları

## Modellerin Değerlendirmesi:

Projemizin başarısını değerlendirmek için kullandığımız metrikler, modellerimizin performansını objektif bir şekilde ölçmemize yardımcı olur. Bu değerlendirme süreci, geliştirilen modellerin gerçek dünya senaryolarında ne kadar etkili olduğunu belirlemek için kritik bir rol oynar. Tablo 1'de, kullandığımız en önemli 3 modelin doğruluk ve F1-score değerleri verilmiştir.

Tablo 1 Modelleriin Değerlendirme metrikleri

|  |  |  |  |
| --- | --- | --- | --- |
|  | Transformer Model | XGBoost | Random Forest |
| Doğruluk | % 96.85 | **% 96.57** | **% 96.48** |
| F1-Score | % 98.41 | % 97.48 | %96.89 |

## Projede Uyarlanma:

Uygulama, modern yazılım mühendisliği prensipleri ve en iyi uygulamaları doğrultusunda geliştirilmiş ve bileşen mantığı ile uyarlanmıştır. Bu uyarlanma süreci, uygulamanın kod tabanını modüler hale getirir ve her bir bileşenin belirli bir görevi üstlenmesini sağlar. Böylelikle, kodun okunabilirliği artar ve bakımı daha kolay hale gelir.

React Python'un bileşen tabanlı yapısı, uygulamanın farklı parçalarının bağımsız olarak geliştirilmesini ve test edilmesini sağlar. Her bir bileşen, belirli bir işlevi yerine getirir ve gerektiğinde değiştirilebilir veya yükseltilebilir. Bu da uygulamanın esnekliğini ve genişletilebilirliğini artırır.

Veri akışı, API ile servis katmanına aktarılır ve burada yapay zekaya sorulup cevap alınır. Bu, uygulamanın veri işleme ve analiz yeteneklerini genişletir ve kullanıcıya daha zengin bir deneyim sunar. Yapay zeka tarafından elde edilen sonuçlar, kullanıcı arayüzüne geri dönerek görsel olarak sunulur.

Bu uyarlanma süreci, uygulamanın performansını artırır ve kullanıcıya daha güvenilir ve etkili bir deneyim sağlar. Ayrıca, kodun daha düzenli ve bakımı daha kolay hale gelmesini sağlayarak geliştirme sürecini iyileştirir. Sonuç olarak, uygulama uyarlanma süreciyle, daha sağlam, esnek ve ölçeklenebilir hale getirilir. Şekil 2 de bileşenlerin haberleşmesi gösterilmiştir.

metin, ekran görüntüsü, yazı tipi, diyagram içeren bir resim

Açıklama otomatik olarak oluşturuldu

Şekil 2 Bileşenlerin Haberleşmesi

**Uygulama Bileşen Yapısı:**

React Python uygulaması, modüler bir bileşen yapısı kullanır. Her bileşen, belirli bir işlevi yerine getirir ve genellikle kendi içinde bağımsızdır. Bu yapı, uygulamanın kolayca genişletilebilmesini, bakımının yapılabilmesini ve yeniden kullanılabilirliğini sağlar.

**Ana Uygulama Bileşeni:**

Ana uygulama bileşeni, tüm uygulamanın temelini oluşturur. Genellikle "App.js" olarak adlandırılır. Bu bileşen, diğer alt bileşenleri çağırır ve uygulamanın genel düzenini belirler.

**Navigasyon Bileşenleri:**

Navigasyon bileşenleri, kullanıcıların uygulama içinde gezinmesini sağlar. Başlık çubuğu, yan menü veya sekme navigasyonu gibi farklı türlerde olabilirler.

**Ana İçerik Bileşenleri:**

Ana içerik bileşenleri, uygulamanın temel işlevselliğini sağlar ve kullanıcı etkileşimiyle ilgili özellikleri barındırır. Bu bileşenler, kullanıcıların uygulama üzerinde etkileşime geçtiği ve ana işlevleri gerçekleştirdiği sayfaları içerir. Bu projede, ana içerik bileşenleri aşağıdaki gibi örneklerle temsil edilebilir:

* **Şifre Gücü Belirleme Formu Sayfası:** Bu sayfa, kullanıcıların belirledikleri şifrenin gücünü ölçmelerini sağlar. Kullanıcılar, bir şifreyi girdikten sonra, yapay zeka modeli tarafından şifrenin gücü analiz edilir ve sonuçlar kullanıcıya gösterilir. Ayrıca, kullanıcıya şifresini güçlendirmesi konusunda önerilerde bulunulabilir.
* **Saldırı Tespiti Sayfası:** Bu sayfa, kullanıcıların ağ trafiğini izleyerek potansiyel saldırıları tespit etmelerini sağlar. Kullanıcılar, gerçek zamanlı olarak ağ trafiğini gözlemleyebilir ve derin öğrenme ve makine öğrenimi modelleri tarafından analiz edilen verileri görüntüleyebilirler. Potansiyel saldırılar algılandığında, kullanıcılar uyarılar alabilir ve gerekli önlemleri alabilirler.
* **Şifreleme ve Şifre Çözme Sayfaları:** Bu sayfalar, kullanıcıların hassas verileri güvenli bir şekilde iletmelerini sağlar. Kullanıcılar, şifreleme sayfasında verilerini şifreleyebilir ve şifre çözme sayfasında şifrelenmiş verileri çözebilirler. Bu sayfalar, kriptoloji alanında kullanıcıların ihtiyaç duyabileceği temel işlevselliği sağlar.

Bu ana içerik bileşenleri, kullanıcıların uygulama üzerinde etkileşime geçerek temel işlevleri gerçekleştirmesini sağlar. Kullanıcı deneyimini zenginleştirmek ve uygulamanın ana odak noktalarını vurgulamak için bu bileşenlerin kullanıcı dostu ve etkili bir şekilde tasarlanması önemlidir.

# PROJENİN YENİLİKÇİ YÖNÜ

**Literatüre Yeni Bir Katkı:** Proje, siber güvenlik alanında mevcut olan problemleri ele alırken, özgün bir yaklaşım benimser. Özellikle, gerçek zamanlı saldırı tespit sistemleri, kriptoloji ve şifre gücü belirleme gibi çeşitli önlemleri bir araya getirerek, kullanıcıların internet güvenliğini artırmak için kapsamlı bir çözüm sunar. Bu, literatürde benzersiz bir yaklaşımı temsil eder ve mevcut bilgiye önemli bir katkı sağlar.

**Özgün Yaklaşımların Kullanımı:** Proje, yapay zeka ve makine öğrenimi gibi ileri teknolojileri etkin bir şekilde kullanarak, veri analizi ve tehdit tespiti alanında özgün yöntemler geliştirir. Derin öğrenme modelleri ve makine öğrenimi algoritmaları, kullanıcıların internet trafiğini analiz ederek potansiyel saldırıları tespit etme yeteneğini artırır. Ayrıca, özel olarak geliştirilmiş şifreleme algoritmaları, kullanıcıların veri gizliliğini korurken güvenli iletişim sağlar.

**Farklılaşma:**  Projemiz, önceden yapılmış çalışmalardan farklılaşır çünkü çeşitli güvenlik önlemlerini tek bir çatı altında birleştirir ve bu önlemleri uygularken en son teknolojileri kullanır. Diğer benzer çalışmalardan ayıran en önemli özelliklerden biri, kullanıcıların gerçek zamanlı olarak potansiyel tehditleri algılaması ve buna karşı önlemler alabilmesi için geliştirilmiş olan gerçek zamanlı saldırı tespit sistemidir. Bu, projenin önceden yapılmış çalışmalardan önemli ölçüde farklılaşmasını sağlar ve kullanıcılara daha güvenli bir çevrimiçi deneyim sunar.

Bu nedenlerle, projenin yenilikçi yönleri, siber güvenlik alanında öncü bir yaklaşım benimseme ve mevcut bilgiye değerli bir katkı sağlama yeteneği ile belirlenmiştir.

# SOSYAL ETKİ

Bu çalışmanın sosyal etkisi çeşitli boyutlarda değerlendirilebilir:

**Toplumsal Faydalar:** Projenin temel amacı, internet kullanıcılarının güvenliğini artırmak ve veri gizliliğini sağlamaktır. Bu doğrultuda, kullanıcıların çevrimiçi ortamda daha güvenli ve korumalı hissetmeleri sağlanır. Güvenli internet kullanımı, bireylerin kişisel ve finansal bilgilerini korumalarına, kimlik hırsızlığı ve çevrimiçi saldırılardan korunmalarına yardımcı olabilir. Bu, geniş çapta toplumun güvenliğine ve refahına katkıda bulunabilir.

**Toplumsal Politikalar ve Uygulamalar:** Çalışmanın sonuçları, siber güvenlik politikalarının ve uygulamalarının geliştirilmesinde değerli bir kaynak olabilir. Kurumlar ve hükümetler, bu tür teknolojileri ve yöntemleri kullanarak çevrimiçi güvenliği artırmak için politikalar ve düzenlemeler oluşturabilir veya iyileştirebilirler. Bu da genel olarak toplumun çevrimiçi güvenliğine katkı sağlayabilir.

**Sürdürülebilir Sosyal Faydalar:** Projeden elde edilen sonuçların sürdürülebilir bir şekilde topluma fayda sağlaması için sürekli bir çaba gerekmektedir. Bu, teknolojik gelişmelerin ve siber tehditlerin sürekli değişimine uyum sağlamayı gerektirir. Bu nedenle, proje sonuçlarının güncel tutulması ve sürekli olarak geliştirilmesi, toplumun çevrimiçi güvenliğini sürdürülebilir bir şekilde artırabilir.

Sonuç olarak, bu çalışmanın toplumsal etkisi, internet kullanıcılarının güvenliği ve gizliliği üzerinde doğrudan bir etkiye sahiptir. Bu çalışma, toplumun çevrimiçi olarak daha güvenli ve korumalı hissetmesine yardımcı olabilirken, aynı zamanda siber güvenlik politikaları ve uygulamalarının geliştirilmesine de katkıda bulunabilir. Bu faydaların sürdürülebilirliği, teknolojik gelişmelerin ve tehditlerin sürekli değişimine uyum sağlamayı içerir.

# UYGULANABİLİRLİK

Bu çalışmanın uygulanabilirliği ve hayata geçirilme potansiyeli şu şekilde değerlendirilebilir:

**Araştırma Bulgularının Uygulanabilirliği:**  Projede geliştirilen yöntemler ve algoritmaların gerçek dünya senaryolarına uygunluğu ve uygulanabilirliği dikkate alınmalıdır. Yapılan araştırmanın sonuçları, çeşitli endüstrilerde ve kuruluşlarda siber güvenlik sistemlerinin geliştirilmesi ve güçlendirilmesi için kullanılabilir.

**Çözümün Hayata Geçirilme Yolları:**  Önerilen çözümün hayata geçirilmesi için bir dizi adım atılabilir. İlk olarak, projenin prototipi gerçek dünya senaryolarında test edilmelidir. Bu testler, çözümün etkinliğini ve güvenilirliğini doğrulamak için gereklidir. Ardından, endüstri standartlarına uygun olarak çözümün genişletilmesi ve ölçeklenmesi sağlanabilir.

**Karşılaşılabilecek Zorluklar ve Aşılma Yolları:**  Uygulamada karşılaşılabilecek zorluklar arasında teknik, mali ve kurumsal engeller bulunabilir. Teknik olarak, çözümün karmaşıklığı ve altyapı gereksinimleri bazı zorluklar oluşturabilir. Mali olarak, proje için yeterli finansman bulmak ve sürdürmek zor olabilir. Kurumsal olarak, çözümün benimsenmesi ve entegrasyonu için kuruluş içinde destek ve işbirliği sağlanması gerekebilir. Bu zorluklarla başa çıkmak için, doğru kaynakları ve uzmanları mobilize etmek, stratejik ortaklıklar kurmak ve çözümün kullanıcılarına değer sağlayacak şekilde tasarlamak önemlidir.

Bu nedenlerle, projenin uygulanabilirliği ve hayata geçirilme potansiyeli, doğru adımların atılması ve karşılaşılabilecek zorlukların başarıyla aşılmasıyla gerçekleştirilebilir. Önerilen çözümün gerçek dünya senaryolarında etkin bir şekilde uygulanması, internet kullanıcılarının güvenliği ve gizliliği üzerinde olumlu bir etki yaratabili

# BULGULAR

Bu bölümde, projenin ana sonuçları ve detaylı analizi sunulmaktadır. Bulgular, grafikler, tablolar veya şemalarla desteklenmiştir ve anlamlı bir şekilde yorumlanmıştır.

**Şifre Gücü Belirleme Sonuçları**

Şifre gücü belirleme yönteminin sonuçlarına bakıldığında, kullanıcıların belirledikleri şifrelerin güvenlik düzeylerini belirlemek için geliştirilen algoritmanın başarılı olduğu görülmektedir. Tablo 1'de, farklı kullanıcılar tarafından belirlenen şifrelerin güçlük seviyeleri ve algoritmanın bu şifreleri değerlendirme başarısı sunulmuştur.

![Şifre Gücü Belirleme Sonuçları](resimler/tablo1.png)

Görüldüğü gibi, algoritmanın doğruluk oranı \%95'in üzerindedir ve kullanıcıların güvenlik açısından zayıf olan şifrelerini doğru bir şekilde tanımlamaktadır.

**Saldırı Tespiti Sonuçları**

Saldırı tespiti sisteminin sonuçları da önemlidir. Makine öğrenimi ve derin öğrenme modellerinin kullanıldığı bu sistem, ağ trafiğini analiz ederek potansiyel saldırıları tespit edebilmektedir. Şekil 1'de, bir kullanıcının internet trafiği üzerinde gerçek zamanlı olarak tespit edilen saldırıların dağılımı gösterilmektedir.

![Saldırı Tespiti Sonuçları](resimler/şekil1.png)

Görüldüğü gibi, saldırı tespiti sistemi, çeşitli saldırı türlerini başarıyla tespit edebilmekte ve kullanıcıları potansiyel tehditler konusunda uyarmaktadır.

**Kriptoloji Sonuçları**

Kriptoloji alanında elde edilen sonuçlar da önemlidir. Özel olarak geliştirilen şifreleme algoritması, güvenli iletişim için etkili bir çözüm sunmaktadır. Şekil 2'de, bu algoritmanın güvenlik düzeyini gösteren bir grafik bulunmaktadır.

![Kriptoloji Sonuçları](resimler/şekil2.png)

Görüldüğü gibi, önerilen şifreleme algoritması, saldırganların şifreleri çözme olasılığını minimize etmek için yeterli güvenlik düzeyini sağlamaktadır.

Bu sonuçlar, projenin temel hedeflerine ulaşmasını ve internet kullanıcılarının güvenliğini artırmasını sağlayan önemli bulguları temsil etmektedir.

# SONUÇ VE TARTIŞMA

Projelerimizin geliştirme sürecinde benzersiz teknolojik yaklaşımlar ve yenilikçi metodlar kullanarak siber güvenlik alanında önemli birer katkı sağladık. Gerçek hayattan örneklerle projelerimizin etkisini ve önemini daha net anlamak mümkündür.

Gerçek zamanlı saldırı tespit sistemi, günümüzde sıklıkla karşılaşılan bir siber güvenlik sorununu ele alır. Örneğin, bir kurumun ağ trafiği üzerinde aniden ortaya çıkan anormal aktiviteler, potansiyel bir saldırıyı işaret edebilir. Bu durumda, geliştirdiğimiz sistem anlık olarak bu aktiviteleri izleyerek saldırıyı tespit edebilir ve gerekli önlemleri alabilir. Bu sayede, kurumlar siber saldırılara karşı daha proaktif bir şekilde hareket edebilir ve ciddi veri kayıplarını veya sistemlerine zarar verilmesini önleyebilir.

Özgün kriptografik algoritma projemiz, veri güvenliği konusunda kritik bir ihtiyacı karşılamaktadır. Günlük hayatta, kişisel verilerin veya hassas bilgilerin güvenli bir şekilde iletilmesi ve saklanması gerekebilir. Örneğin, bir banka müşterisi online bankacılık işlemleri yaparken, kullanıcı adı ve şifresinin güvenliğinden emin olmalıdır. Bu noktada, geliştirdiğimiz kriptografik algoritma sayesinde, müşterinin bu bilgileri güvenle iletebilmesi ve saldırganların erişimini engellemesi sağlanır.

Şifre güçlülüğü sınıflandırma modeli, günlük hayatta sıkça karşılaşılan bir dijital güvenlik sorununa odaklanır. Kullanıcılar genellikle güçlü şifreler kullanmadıklarında, hesapları saldırılara karşı savunmasız hale gelir. Örneğin, basit bir şifre kullanan bir kullanıcı, hesabının kolayca ele geçirilmesi riskiyle karşı karşıya kalabilir. Geliştirdiğimiz model sayesinde, kullanıcılar şifrelerinin gücünü objektif bir şekilde değerlendirebilir ve gerektiğinde güçlendirebilirler.

Siber istihbaratın askeri taktik ve manevralara etkisi projemiz, gerçek hayatta stratejik bir öneme sahiptir. Özellikle günümüzde, bilgi savaşları ve siber saldırılar giderek artmaktadır. Örneğin, bir ülkenin askeri birlikleri, siber istihbarat sayesinde düşmanın hareketlerini önceden tahmin edebilir ve buna göre stratejik kararlar alabilirler. Bu şekilde, siber istihbaratın askeri operasyonlara entegre edilmesi, askeri taktik ve manevraların etkinliğini artırabilir ve ulusal güvenliği sağlayabilir.

Sonuç olarak, geliştirdiğimiz projeler, günlük hayatta karşılaşılan siber güvenlik sorunlarına çözüm sunarak bireylerin ve kurumların dijital dünyada güvenliğini sağlamaya yönelik önemli bir adımı temsil etmektedir. Bu projeler, teknolojik yenilikler ve siber güvenlikteki ileri düzey çözümler ile gerçek hayattaki güvenlik ihtiyaçlarını karşılamayı amaçlamaktadır. Gelecekte, bu tür projelerin daha da yaygınlaşması ve gelişmesi, dijital dünyada güvenli bir ortamın oluşturulmasına önemli katkılar sağlayacaktır.

# ÖNERİLER

# KAYNAKLAR

 [Dergipark - Makale](https://dergipark.org.tr/tr/download/article-file/3303579)

 [Savunma Sanayii ve Havacılık Dergisi - Makale](https://savsad.kho.msu.edu.tr/arsiv/2021_2/Makale%203.pdf)

 [Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi - Makale](https://hukuk.deu.edu.tr/dosyalar/dergiler/dergimiz-15-1/senercelik.pdf)

 [Dergipark - Makale](https://dergipark.org.tr/en/download/article-file/1114311)

 [TÜBİTAK E-Dergi - Makale](https://services.tubitak.gov.tr/edergi/yazi.pdf;jsessionid=CueN-iH4pcIs36IIfaRsEFIv?dergiKodu=4&cilt=47&sayi=840&sayfa=70&yaziid=36087)

 [Bilim ve Teknik Dergisi - Makale](https://bilimteknik.tubitak.gov.tr/system/files/makale/44-51_kuantum.pdf)

 [Dergipark - Makale](https://dergipark.org.tr/tr/download/article-file/195427)

 [STM ThinkTech - Makale](https://thinktech.stm.com.tr/tr/2023-ve-sonrasinda-savunma-sanayii-trendleri-ve-teknolojileri)

# EKLER

## Uygulama Görüntüleri