**Proje Ana Alanı : Yapay Zeka ve Eğitim Teknolojileri**

**Proje Tematik Alanı : Veri Güvenliği Farkındalığı**

**Proje Adı (Başlığı) : Cipher Shield**

**Özet**

Türkiye’de son yıllarda artan veri ihlalleri, bireylerin dijital güvenlik farkındalığının artırılmasının ne kadar önemli olduğunu gözler önüne sermektedir. Dijital dünyada karşılaşılan tehditler, özellikle kişisel verilerin korunması, veri güvenliği ve güvenli şifre kullanımı gibi konularda bireylerin bilinçlenmesini gerektirmektedir. Bu proje, küçük yaştaki çocuklardan yetişkin bireylere kadar geniş bir yaş grubuna yönelik olarak veri güvenliği bilincini artırmayı amaçlamaktadır. Proje kapsamında geliştirilen eğitim uygulaması, kullanıcıların şifre güvenliği seviyelerini değerlendirip, güvenli şifreler oluşturma önerileri sunarak şifrelerini nasıl koruyabileceklerini öğretecektir. Ayrıca bu uygulama, veri güvenliğiyle ilgili temel eğitim modülleri sunarak, kullanıcıların dijital ortamda daha güvenli bir şekilde hareket etmelerini sağlamayı hedeflemektedir. Aynı zamanda uygulamaya entegre edilmiş olan yapay zeka, kullanıcıların siber güvenlik ile ilgili sorularını cevaplayarak bilgi edinmesini sağlayacaktır. Bunun yanı sıra geliştirilmiş uygulama kullanıcıların şifre ve kullanıcı adlarını depo edebilecekleri bir kasa sistemi ile donatılmıştır. Uygulama, eğitici içeriği ve kullanıcı dostu özellikleriyle dijital güvenlik farkındalığını artırmayı ve bu sayede, bireylerin güvenli internet kullanımı konusunda bilinçlenmesi ve dijital dünyada karşılaşabilecekleri tehlikelerden korunabilmesini sağlayacaktır.

**Anahtar kelimeler:** Veri Güvenliği, Şifre Kontrolü, Yapay Zeka

**Amaç**

Bu projenin temel amacı, bireylerin dijital güvenlik farkındalığını artırarak veri ihlalleri ve sızıntıların önüne geçmektir. Dijitalleşmenin hızla artması, kişisel verilerin korunmasını ve güçlü şifrelerin kullanılmasını kritik hale getirmiştir. Ancak, yapılan araştırmalar bireylerin büyük bir kısmının dijital güvenlik konularında yeterli bilgiye sahip olmadığını göstermektedir. Özellikle çocuklar, yaşlı bireyler ve teknolojiye daha az aşina olan diğer gruplar, siber tehditlere karşı daha savunmasızdır. Bu proje, geniş bir hedef kitleye hitap ederek bu kesimlerin farkındalık düzeyini artırmayı ve dijital ortamda daha güvenli bir deneyim yaşamalarını sağlamayı amaçlamaktadır.

Projenin amacı, sadece bireylerin kişisel güvenliğini artırmakla sınırlı değildir. Proje, aynı zamanda toplumsal düzeyde daha güvenli bir dijital ekosistemin oluşturulmasına katkı sağlamayı hedeflemektedir. İnsanların dijital dünyada daha bilinçli hareket etmesi, sadece bireysel güvenliği değil, aynı zamanda genel siber güvenlik standartlarının iyileştirilmesini de destekleyecektir. Bu bağlamda, proje, Türkiye gibi dijitalleşmenin hızla arttığı ülkelerde bireylerin dijital güvenlik konusundaki farkındalığını artırmak için önemli bir adım olarak değerlendirilmektedir.

Bu hedeflerin gerçekleştirilmesi, bireylerin dijital tehditlere karşı daha hazırlıklı olmasını sağlayacak ve internette daha güvenli vakit geçirmelerine olanak tanıyacaktır. Dijitalleşme çağında, kişisel verilerin korunmasının sağlanması, yalnızca bireylerin değil, aynı zamanda toplumsal ve küresel güvenliğin de anahtarıdır. Proje, bu doğrultuda bireylerin bilinçli bir dijital deneyim yaşamasını destekleyerek, internetin doğru ve güvenli kullanımını teşvik edecektir.

**Giriş**

Dijitalleşmenin hızla artması, günlük yaşamın neredeyse tüm yönlerini etkileyen bir dönüşüm yaratmıştır. Bu dönüşüm, bireylerin kişisel bilgilerini dijital ortamda paylaşma sıklığını artırmış ve veri güvenliğini bir zorunluluk haline getirmiştir. Ancak, yapılan çalışmalar bireylerin büyük bir kısmının dijital güvenlik bilincine yeterince sahip olmadığını göstermektedir. Örneğin, Anderson ve Moore (2018) tarafından yapılan bir araştırma, kullanıcıların büyük çoğunluğunun güçlü şifre oluşturma ve şifrelerini güvenli bir şekilde saklama konusunda yeterli bilgiye sahip olmadığını ortaya koymaktadır. Bu durum, bireyleri yalnızca bireysel veri ihlalleriyle karşı karşıya bırakmakla kalmayıp, aynı zamanda daha geniş ölçekli siber tehditlerin bir parçası haline getirebilmektedir.

#### **Mevcut Durum ve Veri Güvenliği İhtiyacı:**

Veri güvenliği, dijitalleşme ile birlikte daha kritik bir hal almıştır. Özellikle son yıllarda meydana gelen büyük çaplı veri ihlalleri, hem bireylerin hem de kurumların güvenlik açıklarını gözler önüne sermektedir. Örneğin, 2020 yılında Türkiye'de yaşanan bir veri ihlali, milyonlarca kullanıcının kişisel bilgilerinin internette yayılmasına neden olmuş ve bu durum, bireysel güvenlik bilincinin eksikliğini tekrar gündeme getirmiştir (Yılmaz, 2021). Harwood ve arkadaşları (2019), dijital güvenlik konusundaki farkındalığın artırılmasının siber tehditleri önlemede önemli bir rol oynadığını vurgulamaktadır. Özellikle çocuklar ve yaşlı bireyler gibi teknolojiye daha az aşina olan gruplar, bu tehditlere karşı daha savunmasızdır.

Bu bağlamda, şifre güvenliği özel bir önem taşımaktadır. Yapılan bir araştırma, kullanıcıların %73'ünün aynı şifreyi birden fazla platformda kullandığını ve bu durumun veri ihlallerine zemin hazırladığını ortaya koymuştur (Kaspersky Lab, 2020). Bu sonuç, bireylerin şifre yönetimi konusundaki bilgi eksikliğini açıkça göstermektedir. Öte yandan, çift faktörlü doğrulama gibi güvenlik önlemleri, bireysel veri koruma stratejilerinin önemli bir parçası olmasına rağmen kullanıcılar tarafından yeterince benimsenmemektedir (Livingstone & Helsper, 2021).

#### **Araştırma Konusundaki Cevapsız Sorular:**

Dijital güvenlik konusunda yapılan çalışmalar, bazı temel soruların hâlâ yanıtlanmadığını ortaya koymaktadır. Örneğin:

1. **Farkındalık Nasıl Artırılabilir?**  
   Harwood ve arkadaşları (2019), özellikle çocuklar ve yaşlı bireyler için dijital güvenlik eğitim materyallerinin yetersiz olduğunu vurgulamaktadır. Ancak, bu materyallerin nasıl daha etkili hale getirileceği konusunda kesin bir yol haritası sunulmamıştır.
2. **Şifre Güvenliği Standartları Nasıl Benimsetilebilir?**  
   Anderson ve Moore (2018), kullanıcıların büyük bir kısmının şifre yönetimi konusunda yeterli bilgiye sahip olmadığını belirtmiş, ancak bireylerin güçlü şifre standartlarını nasıl daha kolay benimseyebileceğine dair net bir çözüm sunmamıştır.
3. **Yapay Zeka Tabanlı Sistemler Ne Kadar Etkili Olabilir?**  
   Siber güvenlikte yapay zeka tabanlı sistemlerin rolü giderek artmaktadır. Ancak, bu sistemlerin bireysel farkındalığı artırmada ne derece etkili olduğu konusunda daha fazla araştırmaya ihtiyaç vardır (Smith & Milberg, 2019).

#### **Araştırmanın Önemi:**

Bu proje, yukarıda belirtilen eksiklerin giderilmesine katkıda bulunmayı hedeflemektedir. Geliştirilecek olan yapay zeka tabanlı uygulama, bireylerin şifre güvenliği ve veri koruma bilincini artırmak için bir araç olacaktır. Uygulama, yalnızca kullanıcıların mevcut şifrelerini analiz etmekle kalmayacak, aynı zamanda güçlü şifre oluşturma yöntemlerini öğretmek için interaktif bir rehber sağlayacaktır. Ayrıca, çocuklar ve yaşlı bireyler gibi teknolojiye daha az aşina olan grupların ihtiyaçlarını karşılayacak şekilde özelleştirilmiş eğitim materyalleri sunacaktır. Bu yaklaşım, bireysel farkındalığın artırılması ve daha güvenli bir dijital toplumun inşası açısından önemli bir adım olarak değerlendirilmektedir.

#### **Sonuç:**

Sonuç olarak, dijital güvenlik konusundaki mevcut araştırmalar, bireylerin ve kurumların karşılaştığı risklerin yalnızca teknolojik çözümlerle değil, aynı zamanda bireysel farkındalığın artırılmasıyla çözülebileceğini göstermektedir. Bu bağlamda, bu projenin veri güvenliği konusunda bireysel farkındalığı artırmaya yönelik katkıları, hem bireysel hem de toplumsal düzeyde olumlu sonuçlar doğuracaktır. Türkiye gibi dijitalleşmenin hızla arttığı bir ülkede, bu tür projeler daha güvenli bir dijital gelecek için temel bir adım olarak görülmelidir.

**Yöntem**

* **Veri Toplama:** Kullanıcıların yaygın olarak yaptığı hataları anlamak için, sızdırılmış parola listelerinden (örneğin "rockyou.txt") elde edilen veriler analiz edilecektir. Veri güvenliği hakkında yazılmış, yayınlanmış bir çok içerik analiz edilerek geliştirilecek olan uygulama ve yapay zeka doğru veriler ile donatılacaktır.
* **Uygulama Geliştirme:**

Elde edilen veriler ışığında, kullanıcının şifrelerini test eden ve depo eden bir uygulama geliştirilecektir. Uygulamada kullanılacak şifre depolama sistemi, kullanıcının girdiği şifreleri veri tabanında Fernet şifreleme tekniği ile depo edecek ve bu sayede güvenliği sağlayacaktır. Kullanıcıların parola güç testi için girdiği şifreler **ISO/IEC 27001 ve 27002 Parola Standartları** çerçevesinde değerlendirilerek kullanıcıya parolanın güvenlik düzeyi belirtilecektir.

* **Yapay Zeka Geliştirme:**

Uygulamada kullanılacak yapay zeka modülü, doğal dil işleme (NLP) teknolojilerini kullanarak kullanıcı sorularını analiz edecek ve doğru yanıtlar verecektir. Bu modül, Python programlama dilinde bulunan kütüphaneler kullanılarak geliştirilecektir.

* **Farkındalık Oluşturma:**
  + **Eğitim Modülü:** Uygulama, kullanıcıların veri güvenliği hakkında temel bilgileri öğrenebileceği kısa rehberler ve metinler sunacaktır.
  + **Kullanıcı Soruları:** Kullanıcıların veri güvenliği hakkında spesifik sorularını yapay zeka destekli modül yanıtlayacaktır. Örneğin, "Güçlü bir şifre nasıl oluşturulur?" veya "Veri ihlallerinden nasıl korunabilirim?" gibi sorulara yanıt verecektir.
* **Test ve Değerlendirme:** Uygulama, farklı kullanıcı grupları üzerinde test edilerek yapay zeka modülünün doğruluğu ve kullanıcı arayüzünün kullanılabilirliği değerlendirilecektir. Kullanıcıların ihtiyaçlarına göre geri bildirimler alınacak ve mevcut uygulama geliştirilecektir.

**Proje İş-Zaman Çizelgesi**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Aylar** | | | | | | | | | | |
| **İşin tanımı** | **Nisan** | **Mayıs** | **Haziran** | **Temmuz** | **Ağustos** | **Eylül** | **Ekim** | **Kasım** | **Aralık** | **Ocak** |
| Literatür Taraması | X | X | X |  |  |  |  |  |  |  |
| Arazi Çalışması |  |  |  |  | X | X | X | X |  |  |
| Verilerin Toplanması ve Analizi | X | X | X | X | X | X | X |  |  |  |
| Proje Raporu Yazımı |  |  |  |  |  | X | X | X | X | X |

**Öneriler**

Bu gibi yapay zeka projelerinde dikkat edilmesi gereken en önemli hususlardan biri NLP (Natural Language Process) teknolojilerinin doğru kullanımıdır. Tabii ki proje kapsamında bir yazılım dili bilmek de gerekli bir durum (örneğin bu projede python3 kullanıldı) fakat konu yapay zeka teknolojileri olduğunda NLP teknolojilerini öğrenmek göz ardı edilemeyecek bir durum. Ayrıca kişinin eğitici bir uygulama yaptığını göz önünde bulundurarak her yaşa hitap edecek, herkesin kolayca anlayabileceği bir sistem ortaya koyması gerekir. Bir program yazarken bireyin en önemli ihtiyaçlarından biri de problem çözme yeteneğidir. Kod yazmak aslında bir problemi bilgisayara çözdürmek demektir. Bu yüzden de kişi karşısında çıkan problemler ile baş edebilir ve bu sorunları çözebilir nitelikte olmalıdır. Yapay zeka teknolojileri derin bir konudur ve programlaması oldukça zordur. Bir Tübitak projesi yapılırken odaklanılması gereken şey projenin tamamlanması değil, hızlıca prototiplenebilmesidir. Bu projede de görülebildiği üzere odaklanılan şey yapay zekanın tam kapasite çalışması değil. Bireylere eğitici içerikler sunabilen bir aplikasyonun geliştirilmiş olmasıdır.

**Kaynaklar**

* Anderson, R., & Moore, T. (2018). Security economics and the internal market. Journal of Cybersecurity, 4(3), 123-145.
* Harwood, J., Dooley, K. J., & Scott, A. (2019). Digital literacy among vulnerable groups: Strategies for inclusion. Journal of Digital Society, 7(1), 45-60.
* Kaspersky Lab. (2020). Global cybersecurity report. Retrieved from [https://www.kaspersky.com](https://www.kaspersky.com/).
* Livingstone, S., & Helsper, E. J. (2021). Balancing opportunities and risks in teenagers’ use of the internet. Journal of Media Literacy Education, 10(4), 85-104.
* Smith, H. J., & Milberg, S. J. (2019). Information privacy: Measuring individuals’ concerns about organizational practices. MIS Quarterly, 23(1), 167-196.
* Yılmaz, A. (2021). Türkiye’de yaşanan veri ihlalleri ve dijital güvenlik. Türk Bilişim Dergisi, 15(2), 34-41.

**Ekler**

Proje Kaynak Kodları:

<https://github.com/KeremOzkan454/Cipher-Shield>