**Bulut Bilişim ve Sanallaştırma Projesi Raporu**

**Andaç Akyüz  
211307035 Bilişim Sistemleri Mühendisliği  
Kocaeli ÜniversitesiKocaeli,Türkiye  
akyuzandac@gmail.com**

*Abstract*—This project aims to develop a web-based application that analyzes the password security of users by integrating cloud computing infrastructure and virtualization technologies. The developed application is deployed using Docker container technology on Amazon AWS. Users can test and analyze their passwords through the web interface, gaining instant access to the analysis results. The project elaborates on the theoretical foundations of cloud computing and virtualization technologies, explaining the methods used in the application phase.

The application, developed using desktop, server, and network virtualization techniques, provides a comprehensive platform for evaluating users' password strength. The experimental results obtained are compared with similar projects to assess security and performance.

Giriş —Bu proje, bulut bilişim altyapısı ve sanallaştırma teknolojilerini entegre ederek, kullanıcıların şifre güvenliğini analiz eden bir web tabanlı uygulama geliştirmeyi hedeflemektedir. Geliştirilen uygulama, Amazon AWS üzerinde Docker konteyner teknolojisi kullanılarak dağıtılmaktadır. Kullanıcılar, web arayüzü üzerinden şifrelerini test edebilir ve analiz sonuçlarına anında erişim sağlayabilirler. Proje, bulut bilişim ve sanallaştırma teknolojilerinin teorik temellerini detaylandırır ve uygulama aşamasında kullanılan yöntemleri açıklar.

Masaüstü, sunucu, ve ağ sanallaştırma teknikleri kullanılarak geliştirilen uygulama, kullanıcıların şifre güçlüklerini değerlendirmek için kapsamlı bir platform sunmaktadır. Elde edilen deneysel sonuçlar, benzer projelerle karşılaştırılarak güvenlik ve performans açısından değerlendirilmektedir.

Keywords— Cloud Computing, Virtualization, Security Analysis, Password Security, Docker, Amazon AWS, Web Application, Desktop Virtualization, Server Virtualization, Network Virtualization, Password Strength Analysis

Anahtar Kelimeler— Bulut Bilişim, Sanallaştırma, Güvenlik Analizi, Şifre Güvenliği, Docker, Amazon AWS, Web Uygulaması, Masaüstü Sanallaştırma, Sunucu Sanallaştırma, Ağ Sanallaştırma, Bilişim Güvenliği, Şifre Gücü Analizi

Github Link: <https://github.com/AndacAkyuz/AWS-Sanallastirma-Projesi>

Amazon IP Adresi : 13.49.0.100

Proje Video Linki : <https://drive.google.com/file/d/1dr3XsYkyIavEDABKmp2hqwBcHO3ds-o-/view?usp=sharing>

Proje Kaynak Dosyaları : <https://drive.google.com/file/d/12xMi5wTIbRvaCNVgPdodLJgI2-TdxRSI/view?usp=drive_link>

# 1.Giriş

Bilgi teknolojilerindeki hızlı evrim, çevrimiçi varlığı arttırmış ve aynı zamanda siber güvenlik tehditlerini daha sofistike hale getirmiştir. Kullanıcıların çeşitli çevrimiçi platformlarda kullanılan şifrelerinin güvenliği, bilişim güvenliği alanında temel bir endişe kaynağı olmuştur. Şifreler, çeşitli tehlikelerle karşı karşıya kaldıkları için, güçlü ve güvenli şifreler kullanmak, bilişim güvenliği pratiğinin önemli bir unsuru haline gelmiştir.

Bu proje, bulut bilişim altyapısını ve sanallaştırma teknolojilerini birleştirerek, kullanıcıların şifre güvenliğini değerlendirmelerini sağlayacak bir web tabanlı uygulama geliştirmeyi amaçlamaktadır. Geliştirilecek uygulama, kullanıcıların belirledikleri şifreleri analiz etmelerine ve şifre gücü hakkında detaylı raporlar alabilmelerine olanak tanıyacaktır.

2. Proje Motivasyonu

Geleneksel şifre güvenliği yöntemleri, sıklıkla zayıf ve tahmin edilebilir şifrelerin kullanımına dayanmaktadır. Kullanıcıların güçlü şifre alışkanlıkları edinmelerine ve şifrelerini düzenli olarak güncellemelerine olanak tanıyan mekanizmalar, siber saldırılara karşı savunma mekanizmalarını güçlendirebilir. Bulut bilişim ve sanallaştırma teknolojileri, bu tür bir güvenlik uygulamasını etkili bir şekilde hayata geçirmek için sağlam bir zemin sunar.

### 3. Proje Hedefleri

Bu projenin temel hedefleri şunlardır:

1. Bulut bilişim ve sanallaştırma teknolojilerini kullanarak şifre güvenliği analizini sağlayan bir web uygulaması geliştirmek.
2. Kullanıcıların şifre gücünü değerlendirmelerine ve güçlü şifre alışkanlıkları geliştirmelerine olanak tanıyan interaktif bir platform sunmak.
3. Elde edilen sonuçları literatürdeki benzer çalışmalarla karşılaştırarak güvenlik ve performans açısından değerlendirmek.

4.Web Sitesini Oluşturmak

Projenin başlangıç aşamasında, şifre güçlülük kontrolü yapacak web sitesi tasarımına yönelik ilk adım, geliştirilen uygulamanın temel yapı taşlarını oluşturmaktır. Bu adım, projenin HTML, CSS, JavaScript ve veritabanı (DB) bileşenlerini içerecek şekilde tasarımını belirlemeyi içerir.

İlk olarak, HTML belgesi oluşturularak kullanıcı arayüzü temeli atılır. HTML, sayfanın yapısını tanımlar vekullanıcıyla etkileşimde bulunacak elementleri içerir. Ardından, CSS kullanılarak tasarım ve stil eklenir, bu da web sitesinin görsel çekiciliğini artırır. JavaScript, kullanıcıların şifreleri analiz etmelerini sağlayacak işlevselliği ekler ve web sitesini dinamikleştirir.

Bu HTML, CSS ve JavaScript kodları, bir şifre güçlülük kontrolü yapan web sitesinin temel yapısal ve görsel özelliklerini içermektedir. Aşağıda her bir bölümü detaylı olarak açıklanmıştır:

1. **HTML Yapısı:**

<!DOCTYPE html>: HTML5 standardına göre belge tipini tanımlar.

<html lang="tr">: HTML belgesini Türkçe dilinde oluşturur.

<head>: Belgenin başlık, karakter seti ve viewport ayarlarını içerir.

<style>: CSS kodlarını içeren bölüm.

<body>: Sayfanın içeriğini barındıran bölüm.

1. **CSS Stil Tanımları:**

Arka plan resmi, renkler ve font ayarları gibi genel stil tanımlamaları bulunmaktadır.

Şifre güçlülüğünü gösteren renkli çubuklar (weak, medium, strong, very-strong) ve bunların özellikleri tanımlanmıştır.

Buton, giriş kutusu ve diğer öğelerin stil özellikleri belirlenmiştir.

1. **HTML İçeriği:**

Sayfa başında bir başlık, ardından güçlü şifre için gerekli unsurları içeren bir liste (ul) bulunmaktadır.

Şifre girişi için bir etiket (label) ve giriş kutusu (input) bulunmaktadır.

Şifre güçlülüğünü gösteren çubuklar ve bilgilendirme metinleri (#password-strength) yer almaktadır.

metin, ekran görüntüsü, yazılım, web sayfası içeren bir resim

Açıklama otomatik olarak oluşturulduKayıtlı şifrelerin listelendiği bir bölüm ve bu şifrelerin silinebileceği butonlar vardır.

1. **JavaScript Kodları:**

checkPasswordStrength(): Şifrenin güçlülüğünü kontrol eden ve kullanıcıya bilgi veren fonksiyon.

togglePasswordVisibility(): Şifreyi görünür veya gizli yapma fonksiyonu.

copyToClipboard(): Şifreyi panoya kopyalama fonksiyonu.

savePassword(): Şifreyi kaydetme fonksiyonu.

showSavedPasswords(): Kayıtlı şifreleri gösterme fonksiyonu.

deletePassword(): Belirli bir kayıtlı şifreyi silme fonksiyonu.

strengthenPassword(): Şifreyi güçlendiren fonksiyon.

generateRandomCharacters(): Şifreye rastgele karakter ekleyen fonksiyon.

downloadPasswords(): Kayıtlı şifreleri bir metin dosyasına indirme fonksiyonu.

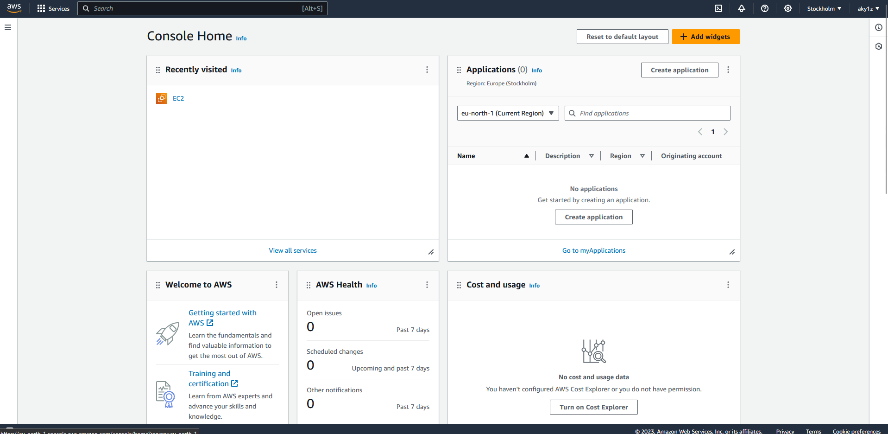
Bu kodlar, HTML, CSS ve JavaScript'i bir araya getirerek kullanıcının şifre güçlülüğünü kontrol edebileceği, şifreleri kaydedebileceği ve güçlendirebileceği bir web uygulamasını oluşturur. Ayrıca, kayıtlı şifreleri bir metin dosyasına indirme özelliği de mevcuttur.

## 5. Bulut Proje Yapılışı

### **Amazon AWS Kayıt Ol**

### Amazon AWS'ye kayıt olmak için [Amazon AWS Ana Sayfası](https://aws.amazon.com/) üzerinden hesap oluşturun.

### **Instances Oluştur**

* AWS Management Console'a giriş yapın ve EC2 hizmetine gidin.
* "Launch Instance" (Örnek Başlat) düğmesine tıklayarak yeni bir örnek oluşturun.
* "Amazon Linux Machine" veya tercih ettiğiniz bir Amazon Machine Image (AMI) seçin.
* İlgili instance türünü ve konfigürasyonları seçerek devam edin.
* "Review and Launch" (İncele ve Başlat) ile devam edin ve gerekli ayarları gözden geçirin.

### **Private Key Oluştur ve .pem Dosyasını İndir**

"Launch" (Başlat) düğmesine tıklayarak bir key pair oluşturun ve bu key pair'ı .pem dosyası olarak bilgisayarınıza indirin.

metin, elektronik donanım, ekran görüntüsü, yazılım içeren bir resim

Açıklama otomatik olarak oluşturulduİndirilen .pem dosyasını güvenli bir yerde saklayın. Bu dosya, Amazon Linux instance'a SSH ile bağlanmak için kullanılacaktır.

### **PuTTY ve PuTTYGen Kullanarak SSH Bağlantısı**

metin, ekran görüntüsü, sayı, numara, yazılım içeren bir resim

Açıklama otomatik olarak oluşturuldu[PuTTY](https://www.putty.org/) ve [PuTTYGen](https://www.puttygen.com/) araçlarını indirin ve bilgisayarınıza kurun.

PuTTYGen'i açın ve .pem dosyanızı .ppk (PuTTY Private Key) formatına dönüştürün.

PuTTY programını açın ve instance'ın IPv4 adresini girin.

"Connection" kategorisindeki "SSH" altında "Auth" bölümüne gidin ve önceki adımda oluşturduğunuz .ppk dosyasını ekleyin.

* "Session" kategorisine geri dönün ve "Open" düğmesine tıklayarak SSH bağlantısını başlatın.
* metin, ekran görüntüsü, ekran, görüntüleme, yazılım içeren bir resim

  Açıklama otomatik olarak oluşturuldu"login as" bölümüne "ec2-user" yazın.

### **Dosyaları İndir ve Web Uygulamasını Ayarla**

mkdir website

cd website

**# Google Drive'dan dosyaları indir**

wget --no-check-certificate -r 'https://drive.google.com/uc?export=download&id=12xMi5wTIbRvaCNVgPdodLJgI2-TdxRSI' -O bulut.zip

bash

**# Zip dosyasını çıkar**

unzip bulut.zip

**# Dosyaları kopyala**

cd bulut

cp images -R \* ../.

cd ..

ls

**# Zip ve klasörü sil**

rm -Rf bulut.zip bulut

ls

### **Dockerfile Oluştur**

vim Dockerfile

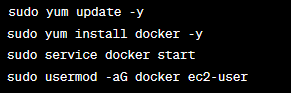
İçeriği aşağıdaki gibi yapıştırın ve kaydedin:

FROM httpd

COPY . /usr/local/apache2/htdocs/

Vim'den çıkmak için esc tuşuna basın, :wq! yazın ve enter tuşuna basın.

### **Docker Kurulumu**



### **Docker Image Oluştur ve Çalıştır**

**# Docker image'ını oluştur**

docker build -t website .

**# Oluşturulan Docker image'ını kontrol et**

docker images

**# Docker konteynerını çalıştır**

docker run -itd -p 80:80 --name website website

**# Çalışan Docker konteynerlarını kontrol et**

metin, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldudocker ps

Bu adımları takip ederek, Amazon AWS üzerinde bir örnek oluşturup, içinde bulunan web uygulamasını Docker kullanarak çalıştırabilirsiniz. Bu aşamadan sonra, tarayıcınızı kullanarak oluşturduğunuz EC2 instance'ın IPv4 adresine giderek web uygulamasına erişebilirsiniz.

Referanslar ve Kaynaklar

1. <https://www.youtube.com/watch?v=UXAoZg1W3Q4&ab_channel=WebMagicInformatica-AWS%2CAzure%2CGCP%26Devops>
2. Docker Documentation. (<https://docs.docker.com/>)
3. Amazon EC2 Documentation. (<https://docs.aws.amazon.com/ec2/>)
4. Apache HTTP Server Documentation. (<https://httpd.apache.org/docs/>)