T.C.

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

EMOJİ İLE GÜÇLENDİRİLMİŞ ŞİFRELER ÜRETEN YENİLİKÇİ ŞİFRE YÖNETİCİ SİSTEMİ

YÜKSEK LİSANS TEZİ

RASHAD MAMMADOV

2300000442

Anabilim Dalı: Bilgisayar Mühendisliği

Programı: Bilgisayar Mühendisliği

Tez Danışmanı: Dr. Öğr. Üyesi Öznur ŞENGEL

HAZİRAN 2025

T.C.

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

EMOJİ İLE GÜÇLENDİRİLMİŞ ŞİFRELER ÜRETEN YENİLİKÇİ ŞİFRE YÖNETİCİ SİSTEMİ

YÜKSEK LİSANS TEZİ

RASHAD MAMMADOV

2300000442

Anabilim Dalı: Bilgisayar Mühendisliği

Programı: Bilgisayar Mühendisliği

Tez Danışmanı: Dr. Öğr. Üyesi Öznur ŞENGEL

Jüri Üyeleri: Prof. Dr. Özgür Koray ŞAHİNGÖZ

Doç. Dr. Fatma PATLAR AKBULUT

HAZİRAN 2025

ÖNSÖZ

Yüksek lisans sürecim boyunca bilgi birikimi, deneyimi ve yol göstericiliğiyle her adımda yanımda olan, eleştirel bakış açısı ve nazik desteğiyle tez çalışmamın şekillenmesine büyük katkıda bulunan tez danışmanım Dr. Öğr. Üyesi Öznur ŞENGEL hocama en içten teşekkürlerimi sunarım.

Bu zorlu süreçte moralimi yüksek tutmamı sağlayan, fikirlerini ve deneyimlerini benimle paylaşmaktan hiç çekinmeyen değerli arkadaşlarım Umud ORUJOV ve Javid ZEYNALOV'a da teşekkür ederim.

Ömrüm boyunca koşulsuz sevgi ve fedakarlıklarıyla bana güç veren ve bu başarıda en büyük paya sahip sevgili babam Vagif MAMMADOV'a, her zaman arkamda durarak motivasyon kaynağım olan annem Elnura MAMMADOVA'ya, varlığıyla beni her daim gururlandıran kıymetli kardeşim Ravan MAMMADOV'a ayrıca eğitim hayatım boyunca bana inanan tüm sevdiklerime sonsuz teşekkür ederim.

06/2025 Rashad MAMMADOV

İÇİNDEKİLER

Sayfa

ŞEKİL LİSTESİ

Şekil Sayfa

TABLO LİSTESİ

Tablo Sayfa

KISALTMALAR

Kısaltma	Tanım
ASCII	American Standart Code for Information Interchange
OTP	One-Time Password (Tek Kullanımlık Şifre)
2FA	Two-Factor Authentication (İki Aşamalı Doğrulama)
SMS	Short Message Service (Kısa Mesaj Servisi)
MFA	Multi-Factor Authentication (Çok Aşamalı Doğrulama)
TOTP	Time-based One-Time Password (Zamana Dayalı Tek Kullanımlık Şifre)
MITM	Man-in-the-middle attack (Ortadaki Adam Saldırısı)
ARP	Address Resolution Protocol (Adres Çözümleme Protokolü)
IP	Internet Protocol Address (İnternet Protokolü Adresi)
DOS	Denial of Service (Hizmet Engelleme)
DDOS	Distributed Denial of Service (Dağıtık Hizmet Engelleme)
XXE	XML External Entity (XML Harici Varlık)
XSS	Cross Site Scripting (Siteler Arası Betikleme)
ECB	Electronic Code Book (Elektronik Kod Kitabı)
CBC	Cipher Block Chaining (Blok Şifre Zincirleme)
GCM	Galois/Counter Mode (Galois/Sayaç Modu)
HKM	Hierarchical Key Management (Hiyerarşik Anahtar Yönetimi)
HSM	Hardware Security Module (Donanım Güvenlik Modülü)
AES	Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
RSA	Rivest, Shamir ve Adleman
SHA	Secure Hash Algorithm (Güvenli Özet Algoritması)
XOR	eXclusive OR

Üniversite : İstanbul Kültür Üniversitesi
Enstitü : Lisansüstü Eğitim Enstitüsü
Anabilim Dalı : Bilgisayar Mühendisliği
Programı : Bilgisayar Mühendisliği
Tez Danışmanı : Dr. Öğr. Üyesi Öznur ŞENGEL
Tez Türü ve Tarihi : Yüksek lisans – Haziran 2025

ÖZET

Günümüzde kullanıcılar, uygulama platformlarında oluşturdukları hesaplarının güvenliğini arttırmak için her uygulama için ayrı ayrı uzun ve karmaşık şifreler üretmek zorunda kalmaktadır. Güçlü şifreler oluşturmak ve bunları akılda tutmak zor olduğundan kullanıcılar ya her platform için aynı şifreyi kullanmayı tercih etmektedir ya da düz metin dosyasına kaydetme, kağıda yazma, tarayıcı aracılığıyla şifre saklama gibi güvenli olmayan saklama yöntemlerini kullanmaktadırlar. Bu teknikler kullanıcı şifrelerini siber saldırılara karşı açık hale getirmektedir.

Zayıf ve tekrarlanan parola kullanımı ile güvensiz saklama alışkanlıklarının getirdiği zayıflığın yanı sıra, mevcut şifre oluşturma yöntemleri çoğunlukla ASCII tabanlı karakterler kullanmakta ve kaba kuvvet ve sözlük saldırılarına karşı daha savunmasız şifreler üretmektedir. Bu tez, dijital platformlarda hesap güvenliğini artırmak amacıyla emoji tabanlı yenilikçi bir şifre yönetim sistemi sunmaktadır. Veri katmanı, iş mantığı katmanı ve sunum katmanından oluşan şifre yönetim sistemi Windows 11 üzerinde Python ve SQLite kullanılarak geliştirilmiştir. Kullanıcı arayüzü Tkinter ile inşa edilerek sanal emoji klavye, mesaj ve onay ekranları ile zenginleştirilmiştir.

Mevcut şifre yönetim sistemlerinin temel özellikleri, avantajları, dezavantajları ile popüler uygulamaların şifre oluşturma kısıtları göz önünde bulundurulmuş ve emoji tabanlı şifre oluşturma algoritması geliştirilmiştir. Geliştirilen şifre oluşturma

algoritması 8, 10, 12 ve 16 birim uzunluğunda, sadece emoji veya emoji ile birlikte kullanıcının belirlediği ASCII karakter kombinasyonlarına göre şifreler oluşturuyor.

Sistemde kaydedilen verilerin güvenliği için 128 bit anahtar uzunluğu ile Gelişmiş Şifreleme Standardı algoritması sayaç modu kullanılmıştır. Algoritmanın ihtiyacı olan 128 bit uzunluğundaki anahtar için bilgisayarın donanım bilgileri ve emoji matrisleri kullanılarak bir anahtar üretim algoritması geliştirilmiştir. Donanım değişimlerinde kurtarma için QR kod entegrasyonu sağlanmıştır.

Uygulama kullanılabilirlik, işlevsellik, güvenlik, birim testleri ve NIST SP 800-22 kriterleriyle değerlendirilmiştir. Sonuçlar, emoji kullanımının şifre çeşitliliğini ve entropisini arttırdığını, böylece kullanıcı deneyimini ve güvenliğini başarıyla korurken kaba kuvvet ve sözlük saldırılarına karşı direnci arttırdığını göstermektedir.

Anahtar Kelimeler: Anahtar üretimi, Emoji tabanlı şifre, Gelişmiş Şifreleme Standardı, Parola yöneticisi

University : T.C. İstanbul Kültür University
Institute : Institute of Graduate Studies
Department : Computer Engineering
Program : Computer Engineering
Supervisor : Assis. Prof. Dr. Öznur ŞENGEL
Degree Awarded and Date : MSc – June 2025

ABSTRACT

Today, users are compelled to come up with complex and long passwords for each program to secure their digital platform account better. Since it is hard to generate tough passwords and recall them, users reuse the same password for multiple platforms or resort to unsafe storage methods such as saving in plain text files, written on paper, or password storage through the browser. The techniques leave user passwords exposed to cyber-attacks.

Aside from the weakness brought by weak and habituated password usage and insecure storage habits, current methods of password creation mostly employ ASCII-based characters and generate more defenseless passwords to brute-force and dictionary attacks. This thesis presents a new system based on emoji for password management to improve account security on online platforms. The system, composed of a data layer, business logic layer, and presentation layer, is executed with Python and SQLite on Windows 11. Tkinter is employed to develop the user interface and enhance with a virtual emoji keyboard, message screens, and confirmation screens.

The basic traits, advantages, and disadvantages of existing password management systems, and password generation restrictions of popular applications were explored to design a new emoji-based password generation algorithm. This algorithm generates

8, 10, 12, and 16 units long passwords based on only emojis or combinations of emojis with user-defined custom ASCII characters.

To protect stored data, the Advanced Encryption Standard counter mode algorithm with a 128-bit key was employed. A specially designed key generation algorithm utilizing the computer's hardware specifications and emoji matrices for generating the encryption key was implemented. QR code integration during recovery in case of hardware alteration was incorporated.

The application was also tested for usability, functionality, security, unit tests, and on the foundation of NIST SP 800-22. The results indicate that emoji usage increases password diversity and entropy, thereby enhancing resistance to brute-force and dictionary attacks while successfully maintaining user experience and security.

Keywords: Key generation, Emoji-based password, Advanced Encryption Standard, Password manager

1. GİRİŞ

Günümüzde dijital platformlarda hesap güvenliği, kullanıcıların karşılaştığı en büyük sorunlardan biri haline gelmektedir. Kullanıcıların zayıf ya da tekrar eden şifreler kullanması siber saldırılara maruz kalmalarına zemin oluşturuyor. Aynı zamanda, güçlü şifreleri oluşturmaksa bu şifrelerin akılda kalmasını zorlaştırmaktadır. Bu yüzden kullanıcılar tarafından dijital platformlarda hesap oluştururken kolay şifreler tercih edilmektedir. Bunun yanı sıra, şifreleri kaydetmek için güvenli olmayan yöntemler kullanılmaktadır. Kullanıcılar genel olarak şifrelerini cihazlarının not defterinde, düz metin dosyalarında, tarayıcılar üzerinde ve ekran görüntüleri olarak saklamaktadır. Bazı kullanıcılar her hesapları için farklı şifreler belirlemek yerine bir şifre seçimi yaparak tüm hesaplarında bu şifreleri kullanmayı tercih ediyor. LastPass tarafından 2023 senesinde yapılmış araştırma sonucunda kullanıcıların yüzde 62'sinin aynı şifreyi farklı platformlarda da kullandıkları tespit edilmiştir [1]. Bu gibi yanlış kullanıcı alışkanlıkları son kullanıcıların saldırılara maruz kalma oranlarını arttırmaktadır. 2023 senesinde yapılan ihlallerin yüzde 82'sini bu şifreler oluşturmaktadır [1].

Kullanıcılar hesaplarını tehdit eden güvenli şifrenin üretilmesi ve şifrenin güvenli bir şekilde saklanması şeklindeki iki temel soruna çözüm olarak şifre yönetim sistemleri kullanmaktadır. Şifre yönetim sistemleri, kullanıcılar için farklı dijital platformlarda kullanabileceği güçlü ve benzersiz şifreler üreten ve bu şifreleri saklayan bir yazılım ya da hizmettir. Kullanıcıların tüm gereken verileri (e-posta, kullanıcı adı, şifre, site ismi) bulut ya da yerel veri tabanlarında şifreli ya da özet fonksiyonu kullanılmış bir şekilde saklanmaktadır. Bu sebepten şifre yönetim sistemleri kullanıcıları tehdit eden bu iki önemli sorunu ortadan kaldırmaktadır.

Şifre yönetim sistemlerinin temel özellikleri:

1. Parola saklama ve yönetimi: Şifre yönetim sistemleri kullanıcılarının dijital platformlardaki kimlik bilgilerini (kullanıcı adı, parola vb.) şifreli bir şekilde saklamalıdır. Bu sistem kullanıcılarının şifrelerini unutma oranlarını azaltır, aynı zamanda güvenlik sağlamaktadır.
2. Güçlü şifre üretimi: Kullanıcılar için tahmin edilemez ve saldırılara dirençli şifreler üretmelidir.
3. Ana parola mekanizması: Şifre yönetim sistemleri kullanıcılar için kayıt esnasında ana parola seçimi sunar. Bu şifre üretilecek olan şifrelere erişim için kullanılmaktadır.
4. İki faktörlü kimlik doğrulama (2FA): Kullanıcıların ana parolalarının çalınması halinde kullanıcının özel verilerine erişilmemesi için kullanılmaktadır.
5. Parola güvenliği takibi: Kullanıcılar için üretilen şifrelerin zayıf ya da güçlü olduğunu, üretilen şifrelerin daha önce sızdırılmasıyla ilgili bilgilendirme yapmalıdır.

Genellikle dijital platformlarda şifre seçimi zamanı klasik ASCII tabanlı metinsel şifreler kullanılmaktadır. Lakin metinsel şifrelerinde kendine özgün dezavantajları var.

Metinsel tabanlı şifrelerin dezavantajları:

1. Metinsel tabanlı basit şifrelerin daha kolay tahmin edilir olması.
2. Metinsel tabanlı karmaşık şifrelerin kullanıcılar tarafından daha zor hatırlanabilir olması.
3. Sözlük, kaba kuvvet ve sosyal mühendislik saldırılarına sık sık maruz kalması.
4. Kullanıcılara kısıtlı karakter kullanımı sunması.

NordPass tarafından her sene paylaşılan raporun 2024 senesindeki verilere baktığımız zaman kullanıcıların en fazla kullandığı şifreler “123456”, “123456789”, “12345678”, “secret”, “password”, “qwerty123”, “qwerty1” olarak belirlenmiştir [2]. Günümüzde hala bu kadar kolay ve kaba kuvvet saldırılarına karşı savunmasız şifreler kullanılması hesap güvenliğini tehdit etmektedir. Şifre seçimi yaparken sadece uzunluğu değil şifre yapısı da dikkate alınmalıdır. Küçük harf ve rakamlardan oluşan 15 birim uzunlukta “123456789abcde” gibi bir şifrenin kaba kuvvet saldırısı kullanılarak kırılması küçük

ve büyük harf, rakam ve özel karakterlerden oluşan 8 birim uzunlukta “8Md2.Fa0” gibi karmaşık bir şifrenin kırılmasından daha hızlı olacaktır.

Teknolojiye olan bağlılıkları her geçen gün artan bireyler için mobil iletişim yoluyla farklı iletişim yolları geliştirilmiştir [3], [4]. Bu iletişim yollarından biri de emojilerdir. Günümüzde en fazla kullanılan iletişim araçlarından olan WhatsApp uygulamasına baktığımızda kullanıcılarının %92 si konuşma esnasında emojiler kullanıyor [5], [6]. Konuşma esnasında emojilerin bu kadar fazla kullanılması, bireylerin yazılı iletişimde duygularını ve ifadelerini daha etkili bir şekilde aktarma ihtiyacından kaynaklanmaktadır. Ancak, emojilerin yalnızca iletişimde değil, aynı zamanda dijital güvenlik alanında da yenilikçi çözümler sunma potansiyeli bulunmaktadır.

ASCII her karakteri 7 bit olan 128 karaktere sahip bir standart olduğu için kullanıcılar şifre seçimi esnasında kısıtlamalar yaşamaktadır. Unicode standardında kullanabileceğimiz emojilere baktığımız zaman güncel olarak 3600’den fazla emoji kullanılmaktadır ve yeni güncellemelerle bu sayılar artmaktadır. Emojilerin şifre seçiminde kullanılması, kullanıcılara şifre seçimi esnasında çok fazla şifre kombinasyonu sunmaktadır [6].

Özellikle, geleneksel şifre sistemlerindeki güvenlik açıklarını düşündüğümüzde, emoji tabanlı kimlik doğrulama sistemleri yeni ve daha güvenli bir alternatif olarak öne çıkmaktadır. Kullanıcıların şifrelerini hatırlamasını kolaylaştıracağı ve saldırganların şifreleri tahmin etmesini imkânsız hale getireceği düşünülmektedir. Saldırganların tahmin etmesini bu kadar zorlaştıran sistemler siber güvenlik alanında yeni bir çığır açabilir. Bu çalışmada emoji ile güçlendirilmiş yenilikçi bir şifre yönetim sistemi tasarlanması ve güvenlik açısından sağlanan avantajların incelenmesi ve üretilen şifrelerin güvenlik testlerinin yapılması amaçlanmaktadır.

Geliştirilen uygulama kullanıcılar için emojileri kullanarak karmaşık algoritmalarla 8, 10, 12 ve 16 karakter uzunluğunda şifreler oluşturarak yerel veri tabanında şifreli bir şekilde kaydetmeyi amaçlamaktadır. Artık tüm site ve uygulamaların özel şifre gereksinimleri olduğu için uygulama şifre üretim esnasında bu gereksinimleri de kontrol ederek şifreyi üretmektedir. Bunun yanı sıra yalnız ASCII tabanlı karakterler

kabul eden site ve uygulamalar için ise alternatif yöntemler sunmaktadır.

Bu konuyla ilgili daha önce yapılmış araştırmalarda emoji kullanarak Android sistemler için kilit ekranı [7], [8], emoji ile doğrulama sistemi [9] ve emoji ile şifre oluşturmak için klavye çalışması da var [10]. Lakin araştırma esnasında emoji ile şifre üretilen şifre yönetim sistemi hakkında Kaspersky'nin raporlarda yazılar olsa da bunu uygulamalarına entegre etmemiştir. Bu çalışmadaysa emojiler kullanılarak şifre yönetim sistemi hazırlanmış ve üretilen şifrelerin güvenliği için kabul testi, işlevsellik testi, güvenlik testi, birim testi ve Ulusal Standartlar ve Teknoloji Enstitüsü Özel Yayını 800-22 (National Institute of Standards and Technology Special Publication 800-22- NIST – SP 800-22) ile testler yapılmıştır.

2. ARKA PLAN

2.1. Kimlik Doğrulama

Kimlik doğrulaması bir kullanıcının platformlara ya da sitelere giriş yaparken iddia ettiği verilerin doğru olup olmadığını kanıtlaması olarak tanımlanmıştır [11], [12]. Yani bir bilgi sisteminde giriş yapmak isteyen kişinin kim olduğunu kanıtlaması işlemine kimlik doğrulaması denir. Bu işlemde ilk önce kullanıcı giriş yaparken kullanıcı adının sistemde olup olmadığının kontrolü yapılıyor ardından kullanıcının girdiği şifrenin doğrulaması yapılmaktadır. Artık günümüzde kullanıcıların kullanıcı adı ve şifresinin yanı sıra biyometrik verileri, tek seferlik şifreler ve iki adımlı doğrulama yöntemleri gibi farklı kimlik doğrulama teknikleri de kullanmaktadır.

2.1.1 Kimlik Doğrulamanın Temel Türleri

Kimlik doğrulamasının temel türleri üç başlık altında toplanmaktadır.

1. Kullanıcının bilgilerine dayalı kimlik doğrulama: Kullanıcının giriş yapabilmesi için kullanıcı adı ve şifresini bilmesi yeterlidir. Doğru bilgiler girildiği anda sisteme giriş sağlanıyor.
2. Kullanıcının kullandığı herhangi bir fiziksel nesne kullanılarak kimlik doğrulama: Kullanıcı giriş esnasında donanım ya da yazılım jetonlarını, Kısa Mesaj Servisi (Short Message Service) ile gönderilmiş doğrulama kodlarını ve kimlik doğrulaması için kullanılan uygulamaları (Google Authenticator, Authy, Microsoft Authenticator vb.) kullanarak kimlik doğrulama işlemi yapmasıdır. Bu işlem çok faktörlü kimlik doğrulamasının bir adımı olarak kabul edilmektedir.
3. Biyometrik verilere dayalı kimlik doğrulama: Kullanıcının iris, ses, parmak izi, yüz gibi verileri kullanılarak kullanıcının kimlik doğrulama işlemi yapılmaktadır.

Temel türlerin kombinasyonun kullanılması ile kullanıcıların güvenliklerinin artırılmasının hedeflediği çoklu faktörlü kimlik doğrulaması (MFA) işlemi kullanılmaktadır. Kullanıcı giriş sırasında hem biyometrik veri hem de telefon numarasına alacağı kısa mesajda yer alan kodu aynı anda kullanmaktadır.

Kullanıcının bir platforma giriş yapma süreci incelendiğinde, sistem tarafından genellikle kayıt esnasında alınan kullanıcı adı ve şifre bilgileri talep edilmektedir. Kullanıcı bu bilgileri doğru şekilde girdiğinde, sistem tarafından tanınarak platforma giriş yapmasına izin verilmektedir. Ancak bu süreçte bazı güvenlik açıkları söz konusu olabilmektedir. Özellikle, giriş bilgilerini kullanan kişinin gerçekten hesap sahibi olup olmadığı konusunda çeşitli şüpheler ortaya çıkabilmektedir. Kullanıcıya ait özel bilgilerin kötü niyetli kişilerce ele geçirilmesi durumunda, bu kimlik bilgileri yetkisiz kişiler tarafından kullanılabilir hale gelmektedir. Bu noktada, ek bir kimlik doğrulama yöntemi kullanılmadığı takdirde, sistemin giriş yapan kişinin kimliğini kesin olarak doğrulaması mümkün olmamaktadır. Bu durum, kullanıcı hesaplarının ele geçirilmesi riskini önemli ölçüde arttırmaktadır. Google tarafından 2019 yılında yayımlanan bir rapora göre, kullanıcıların telefon numaralarına gelen SMS ile gerçekleştirilen iki aşamalı kimlik doğrulama yöntemini tercih etmeleri durumunda, toplu kimlik avı saldırılarının %99'unun ve hedefli saldırıların %66'sının engellenebildiği tespit edilmiştir [13]. Bu bulgu, ek güvenlik önlemlerinin kullanıcı hesaplarının korunmasında ne denli etkili olduğunu ortaya koymaktadır.

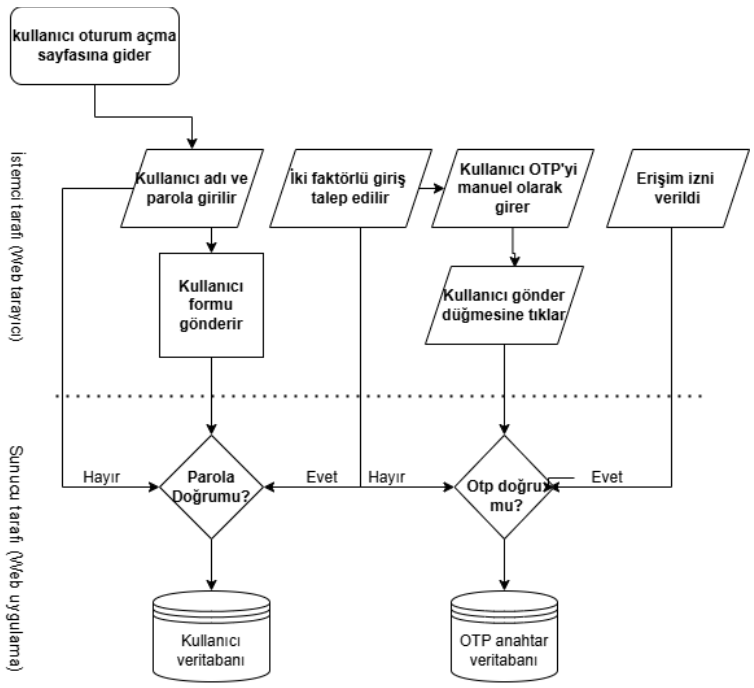
2.1.2. Kimlik Doğrulama Yöntemlerinin Güvenlik Önlemleri

Kimlik doğrulama sistemleri, kullanıcıların dijital platformlara erişimi sırasında kritik bir erişim kontrol mekanizması işlevi görmektedir. Ancak bu sistemler zaman zaman çeşitli tehditlere karşı savunmasız kalabilmekte ve dolayısıyla güvenlik açıkları oluşabilmektedir. Bu nedenle, sistem güvenliğinin sağlanması adına birtakım önlemlerin alınması zorunlu hale gelmiştir. Bu güvenlik önlemlerinin başında, kullanıcıların güçlü ve güvenli şifreler belirlemesi gelmektedir. Kimlik doğrulama süreçlerinde şifreler temel bir bileşen olduğundan, kullanıcıların kolay tahmin edilebilecek parolalardan kaçınmaları büyük önem taşımaktadır. Günümüzde çoğu dijital platform, güvenliği artırmak amacıyla belirli şifre politikaları uygulamaktadır.

Bununla birlikte, kullanıcıların bu politikalara tam anlamıyla uymadığı durumlar da söz konusu olabilmektedir [14].

Genel olarak şifre politikaları, en az sekiz karakter uzunluğunda olan ve büyük harf, küçük harf, rakam ile özel karakter içeren parolaların kullanımını zorunlu kılmaktadır. Ancak, bazı kullanıcıların bu kurallara yüzeysel olarak uyduğu; örneğin, "Password123!" gibi karakter tekrarları içeren ya da kolay tahmin edilebilir kombinasyonlar tercih ettiği gözlemlenmektedir [2]. Bu tür seçimler, şifre güvenliğini önemli ölçüde zayıflatmakta ve çeşitli güvenlik tehditlerine açık bir zemin hazırlamaktadır [14].

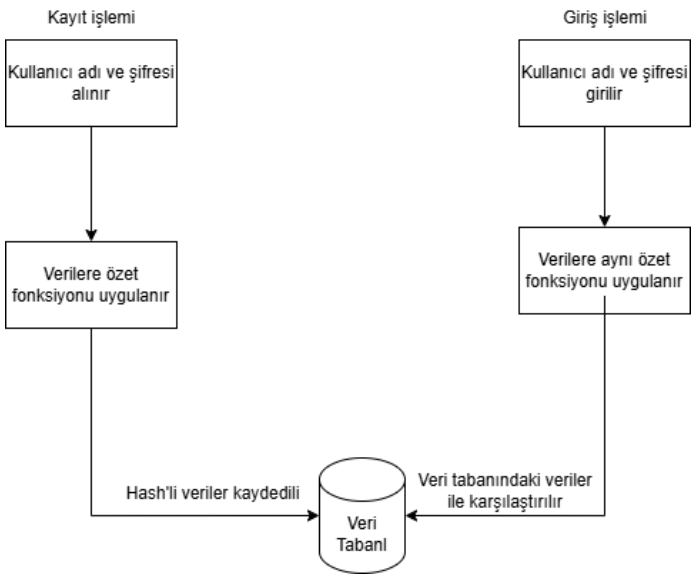
Dijital güvenliğin artırılmasına yönelik önlemler arasında yer alan iki faktörlü kimlik doğrulama (2FA), kullanıcı hesaplarına yönelik ek bir güvenlik katmanı sunmaktadır. Bu yöntem, kullanıcıya ait fiziksel bir donanım ya da yazılımsal bir öğe aracılığıyla gerçekleştirilmektedir. İkinci doğrulama faktörü; kullanıcıya ait biyometrik veriler (parmak izi, yüz tanıma vb.) ya da kısa mesaj (SMS) veya e-posta yoluyla iletilen tek kullanımlık şifreler (OTP) olabilir. Hem istemci tarafında hem de sunucu tarafında gerçekleşen işlem akışı, Şekil 2.1'de şematik olarak gösterilmiştir [15].



Şekil 2.1 İki faktörlü doğrulama şeması

Sistem mimarisi kapsamında, kullanıcılar ilk aşamada giriş sayfasına yönlendirilir. Burada, kullanıcı adı ve şifre bilgileri girildikten sonra, "Giriş" butonuna tıklanarak kimlik doğrulama isteği sunucuya iletilir. Sunucu tarafında, girilen bilgiler kontrol edilir ve doğruluğu teyit edildiğinde işlem bir sonraki aşamaya aktarılır. Ancak, bilgilerin hatalı olması durumunda süreç sunucu tarafından sonlandırılır. Kullanıcı bilgileri doğru olarak girildiğinde, kullanıcı iki faktörlü kimlik doğrulama (2FA) gerektiren arayüze yönlendirilir. Bu aşamada, kullanıcıdan zaman tabanlı tek kullanımlık parola (TOTP) veya SMS yoluyla iletilen doğrulama kodunu sisteme girmesi beklenir. Girilen doğrulama kodu sunucu tarafından doğrulanır; doğruysa kullanıcıya erişim izni tanımlanır. Ancak, tek kullanımlık şifre yanlış girildiğinde erişim izni verilmez ve kullanıcıya yeni bir doğrulama kodu gönderilerek sürecin tekrarlanması istenir.

Kullanıcıların verilerinin güvenli şekilde veri tabanlarında saklanması için kullanıcıların girmiş olduğu kritik verilerin veri tabanlarında özet fonksiyonu (Şekil 2.2) kullanılmış ya da şifreli şekilde saklanması gerekmektedir. Veri tabanlarına başarılı bir saldırı yapıldığı zaman kullanıcı verileri yine de güvenli kalmalıdır. Bunun için kullanılan Blowfish-based crypt, Argon2 Password Hashing Function, Secure Hash Algorithm 256-bit, Password-Based Key Derivation Function 2 gibi güvenli algoritmalar var.



Şekil 2.2 Kullanıcı girişinde özet fonksiyonu kullanımı

Kullanıcının kimlik doğrulama süreci, özet tabanlı bir yönteme dayanmakta olup, bu süreç kayıt ve giriş aşamaları olmak üzere iki aşamalı olarak gerçekleştirilmektedir. Kayıt aşamasında, kullanıcının girmiş olduğu kullanıcı adı ve şifre bilgileri, belirli bir özet fonksiyonu kullanılarak işlenir ve elde edilen özet değer (hash), veri tabanına kaydedilir. Giriş aşamasında ise kullanıcı, kullanıcı adı ve şifresini yeniden sisteme girer. Girilen şifre, kayıt aşamasında kullanılan aynı özet fonksiyonu aracılığıyla tekrar özetlenir. Elde edilen özet değerin, veri tabanında kayıtlı olan özet değeriyle eşleşmesi durumunda, kullanıcıya sisteme erişim izni verilir. Aksi takdirde, kimlik doğrulama başarısız olur ve kullanıcı sisteme giriş yapamaz.

Özet fonksiyonlarının kullanımı, özellikle düz metin şifrelerin veri tabanlarında saklanmasını engelleyerek güvenliği artırmayı amaçlamaktadır. Ancak bu yöntemin etkinliği, kullanılan özet algoritmasının kriptografik gücüne ve ek güvenlik önlemlerine bağlıdır. Bu bağlamda, "salt" adı verilen rastgele verilerin özetleme sürecine dahil edilmesi gibi ek önlemler, söz konusu yöntemin güvenliğini önemli ölçüde artırabilir. Aksi takdirde, özet fonksiyonları çeşitli saldırı türlerine (örneğin sözlük saldırıları veya gökkuşağı tablosu saldırıları) karşı savunmasız hale gelebilir.

Amerika Birleşik Devletleri'nde 2022-2024 yılları arasındaki veriler incelendiğinde, kullanıcıların çevrimiçi hesap şifrelerini yönetme alışkanlıklarında dikkate değer değişimler Tablo 2.1'de verilmiştir. "Şifremi ezberledim" seçeneğini tercih eden kullanıcıların oranı, bu dönemde artış göstererek %41'den %51'e yükselmiştir. Bununla birlikte, şifre yöneticisi uygulamaları kullanan bireylerin oranı da anlamlı bir artışla %21'den %36'ya çıkmıştır. Bu artış, dijital güvenlik alanında olumlu bir gelişme olarak değerlendirilse de hala ezberleme yöntemini tercih eden kullanıcı oranının gerisinde kalmaktadır.

Geleneksel yöntemlerden biri olan şifreleri kağıda yazma alışkanlığı ise düşüş eğilimi göstermektedir. Ancak, güvenli olmayan bu yöntemlerin yerine geçen bazı diğer alışkanlıklar da benzer riskler taşımaktadır. Örneğin, şifrelerin bilgisayar ya da mobil cihazlardaki not uygulamalarında saklanması oranı sırasıyla %25 ve %26 düzeylerinde artış göstermiştir.

Tablo 2.1 Kullanıcıların şifre yönetim alışkanlıklarının yıllara göre dağılımı [16]

Çevrimiçi hesap şifrelerinizi nasıl yönetiyorsunuz?	2022	2023	2024
Şifrelerimi ezberledim	%41	%41	%51
Bir şifre yöneticisi kullanıyorum	%21	%34	%36
Şifrelerimi tarayıcımda saklıyorum	%25	%27	%34
Bunları bilgisayarımda veya mobil cihazımda bir notta saklıyorum	%25	%25	%26
Bunları kağıda yazıyorum	%32	%30	%25
Tüm hesaplarımda aynı birkaç şifreyi kullanıyorum	%22	%21	%18
Bir güvenlik anahtarı veya başka bir fiziksel parola aygıtı kullanıyorum	-	%10	%10

Tüm hesaplarda aynı veya birkaç şifreyi kullanma alışkanlığında ise azalma gözlemlenmektedir. Bu durum, kullanıcıların dijital güvenlik konusunda daha bilinçli hareket etmeye başladıklarını ve daha güvenli şifreleme stratejilerine yöneldiklerini göstermektedir. 2023 yılında ölçülmeye başlanan fiziksel güvenlik anahtarı ya da cihaz kullanım oranı ise %10 seviyesinde sabit kalmıştır. Genel olarak, elde edilen veriler, kullanıcıların dijital güvenlik bilincinin arttığını ve daha güvenli, modern yöntemlere yönelmeye başladıklarını ortaya koymaktadır.

Şifre yöneticisi kullanmayan kişilerin ise kullanmama nedenlerine baktığımız zaman Tablo 2.2'de gösterilmiştir. Kullanıcıların şifre yöneticilerini kullanmama sebeplerine baktığımız zaman sadece %9'luk kullanıcı ücretle alakalı olarak kullanmadığı tespit edilmiştir. Geriye kalan değerlere baktığımızda insanların genel olarak ya şifre yöneticilerini kullanamayacağını düşündükleri için kullanmadıkları tespit edilmiştir bu değerlerin ise yükselmesi için kullanıcılar bu konular hakkında sık-sık bilgilendirilmelidir.

Tablo 2.2 Şifre yönetici kullanmama sebepleri [17]

Şifre yöneticisi kullanmamanızın temel nedeni nedir?	Kullanıcı olmayanların yüzdesi
Birine ihtiyacım olup olmadığından emin değilim	%37
Onların güvenli olduğuna inanmıyorum	%23
Nasıl çalıştıklarını bilmiyorum	%16
Çok pahalı olduklarını düşünüyorum	%9
Kurulumlarının çok zor olduğuna inanıyorum	%9

2.2. Şifre Yönetim Sistemleri

Günümüzde uygulama sayılarının artması ve kullanıcıların her platform için karmaşık çok fazla şifre belirleme ihtiyacı sebebiyle şifre yöneticilerinin kullanımı zorunlu hale gelmektedir. Şifre yöneticileri, kullanıcıların tüm şifrelerini tek bir platformda ana şifre ile saklayan hizmetlerdir. Kullanıcılar ana şifreyi kullanarak dijital platformlar için şifre üreterek veri tabanında şifreli bir şekilde kaydeder.

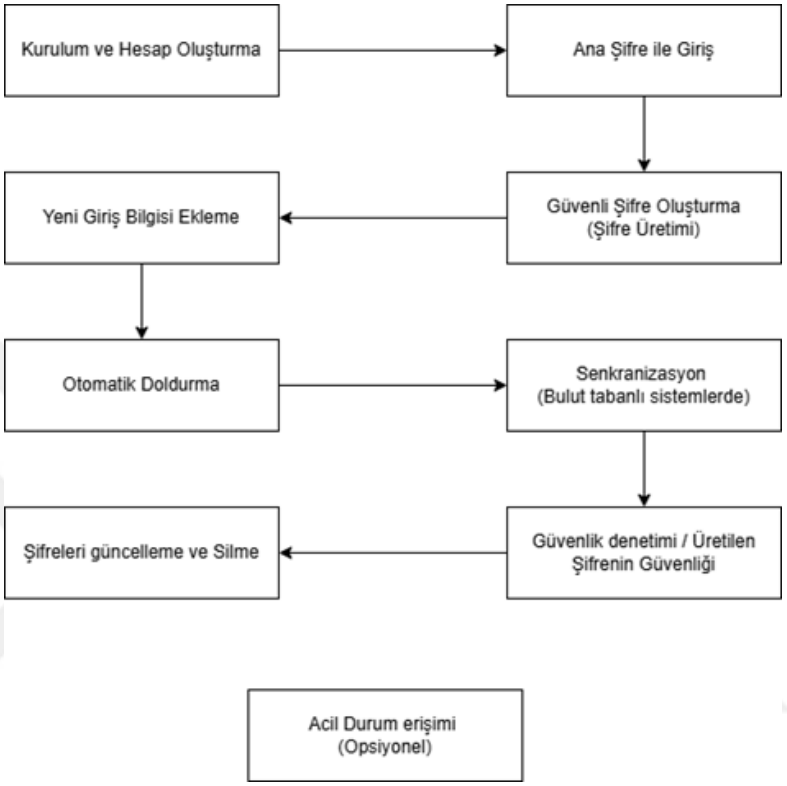
Bu araçların en büyük avantajları kullanıcılar için benzersiz ve güçlü şifreler oluşturabilmesidir. Bu sistemlerle her platform için farklı şifre üretilmesinin yanı sıra kullanıcıların her platform için üretilen bu şifreleri hatırlamasına gerek kalmamaktadır. Kullanıcının bu işlemler için sadece ana şifreyi hatırlaması yeterlidir.

2.2.1. Şifre Yöneticilerin Temel Özellikleri

Şifre yöneticileri hem kullanıcı deneyimini kolaylaştırmakta hem de dijital güvenliği artırmaktadır. Tipik bir parola yöneticisinin temel işlevsel süreci Şekil 2.3'te adım adım gösterilmektedir. Süreç, istemci tarafında gerçekleştirilen yazılım kurulumu ve kullanıcı hesabının oluşturulması ile başlamaktadır. Bunu, kimlik doğrulama mekanizması kapsamında ana parolanın girilmesiyle gerçekleşen oturum açma (authentication) adımı izlemektedir.

Oturum açma işleminin ardından, parola yöneticisi, kriptografik olarak güçlü parolaların üretilmesini sağlayan entegre parola jeneratörü aracılığıyla kullanıcıya yeni kimlik bilgileri oluşturma imkânı sunmaktadır. Bu kimlik bilgileri, güvenli veri

havuzlarında şifrelenmiş (encrypted) biçimde saklanmakta ve sistemin parola otomatik doldurma (autofill) modülü ile hedef web uygulamalarına entegre edilmektedir.



Şekil 2.3 Şifre yöneticisinin temel adımları

Ayrıca, parola yönetim sistemi, istemciler arası veri tutarlılığını sağlamak amacıyla bulut tabanlı senkronizasyon altyapısını kullanmakta; bu sayede çoklu cihazlar arasında gerçek zamanlı veri replikasyonu ve kimlik bilgisi senkronizasyonu mümkün hale gelmektedir. Sistem mimarisi, hem yerel (local) hem de uzak (remote) sunucu bileşenleri arasında şifreli iletişim protokolleri (örneğin TLS/SSL) üzerinden veri aktarımını güvence altına almaktadır.

2.2.2. Şifre Yöneticilerinin Avantajları ve Dezavantajları

Şifre yöneticisi tek başına kullanımında kullanıcıların şifrelerini tamamen güvenli hale getirmiyor [18]. Şifre yöneticilerinin avantajları şu şekilde sıralanabilir:

- Kullanıcıların şifrelerini kaybetmelerinin önüne geçer.
- Sistem politikalarına uygun şekilde güçlü şifreler oluşturulmasını sağlar.
- Kurtarma soruları ve cevaplarının güvenli biçimde saklanmasına imkân tanır.

- Üyelik kartları ile banka kartı gibi hassas verilerin güvenli notlar içerisinde saklanmasını mümkün kılar.
- Farklı cihazlar arasında güvenli iletişimi destekler.

Bununla birlikte bazı dezavantajları da söz konusudur:

- İşletim sistemi desteği sınırlı olabilir.
- Sadece belirli internet siteleriyle uyumlu çalışabilir.
- Ana anahtar (master key) kaybedildiğinde verilere erişim imkânsız hale gelebilir.
- Yetkisiz kullanıcılar tarafından yapılabilecek değişiklik riskleri mevcuttur.
- Uygulamanın çökmesi durumunda erişim sorunları yaşanabilir.
- Tek oturum açma (SSO) özelliğinin kullanımı bazı güvenlik risklerini beraberinde getirebilir.

Parola yöneticilerinin en önemli avantajlarından biri, şifre kaybını önleyerek kullanıcıya zaman kazandırmasıdır. Kullanıcılar her giriş yapmak istediklerinde şifrelerini unuttuğu için şifre yenilemek durumunda kalmamaktadır. Şifre yöneticileri sayesinde gerekli uygulama ya da site için önceden kaydedilmiş şifre kullanıcıya gösteriliyor ya da otomatik doldurma ile sisteme girişini sağlamaktadır. İkinci olarak her bir sistemin kendine özgün şifre politikası var. Bazı siteler kullanıcı tarafından 10 karakterli şifre talep ederken bazılar 15 karakterli şifre talep edebilmektedir. Kullanıcılar için ise şifre yöneticileri bu uygulamalar için onların politikalarına uygun olarak şifre üretebilmektedir. Eskiden daha yaygın olan güvenlik soruları ve cevapları az da olsa günümüzde de kullanılmaktadır. Burada bazı sorulara baktığımız zaman kendimiz hakkında sorular bulunmaktadır. Buradaki soruları doğru bir şekilde cevapladığımız zaman bize yakın olan kişiler tarafından bu soruların cevapları bulunabilmektedir. Bu sorulara cevap olarak farklı cevaplar yazıp ve bu soruları şifre yöneticilerinde kaydedersek bu sorunun önüne geçebiliyoruz. Şifre yöneticileri sadece kullanıcı adı ve şifreleri kaydetmekle kısıtlı değildir. Bazı şifre yöneticileri kullanıcılar için banka kartı, verilerini notları, özel kart bilgilerini de güvenli bir şekilde saklayabilmektedir. Kullanıcılar bu verileri bilgisayarlarında kaydettikleri zaman bu verilere anlık olarak mobil cihazlarından ya da başka cihazlarından güvenli bir şekilde erişebiliyor.

Şifre yöneticilerinin avantajları olduğu gibi dezavantajları da bulunuyor bunlardan ilki sistem entegrasyonları yani bazı şifre yöneticileri sadece Windows işletim sistemine destek verdiği zaman kullanıcılar bilgisayarlarında kaydettiği şifreleri Android cihazlarında kullanamıyor. Bu da şifre yöneticilerinin kullanımını azaltabilecek bir dezavantaj olabilir. Bir diğer dezavantajına baktığımız zaman bazı şifre yöneticilerinin sadece web siteleri için hizmet veriyor olmasıdır. Kullanıcılar yerel de çalıştırdıkları uygulamalar için kullanamamasıdır. En önemli sorunlardan biri ise kullanıcılara kayıt zamanı üretilmiş ya da kullanıcı tarafından seçilmiş ana şifre kaybolduğu zaman kullanıcının tüm verileri erişilemez hale gelmektedir. Bu da kullanıcıların tüm verilerinin kaybolması anlamına gelmektedir.

Şifre yöneticileri bazen işletim sistemi değiştirildiğinde ya da farklı cihazlar kullanıldığı zaman bazı ayarları otomatik olarak yetki almadan değiştirebilmektedir. Örneğin kullanıcının ön yükleme ve depolama şifrelerinin devre dışı bırakıldığı durumlar var [18]. Her uygulamada olduğu gibi şifre yöneticilerinin uygulamalarında da bazı yazılımsal sorunlar ortaya çıkabilmektedir. Bu gibi durumlarda kullanıcılar için sorunlar yaratabilmektedir. Kullanıcılar kısa ya da uzun süren bu gibi durumlarda şifrelerine ve özel verilerine ulaşamadığı için kayıtlı oldukları platformlara erişemiyor. Günümüzde bazı şifre yöneticileri tek oturum açma (SSO) teknolojisini kullanmaktadır [19]. Bu ise kullanıcının bir kez kimlik doğrulaması yaptıktan sonra tekrar tekrar kimlik doğrulama işleminin istenmemesi anlamına geliyor. Bu işlem kullanıcıların işlerini kolaylaştırsa da bazı güvenlik açıkları ortaya çıkarabilmektedir.

2.2.3. Popüler Şifre Yöneticileri ve Dikkat Edilmesi Gerekenler

Popüler şifre yöneticileri ve bu şifre yöneticilerinin avantajları ve dezavantajları Tablo 2.3'te gösterilmiştir [20]. Güçlü şifreleme ve güvenlik özelliklerine baktığımızda Bitwarden, Lastpass, Keeper gibi şifre yöneticileri AES-256 gibi güçlü şifreleme protokolleri kullanmaktadır. Bunun yanı sıra çok faktörlü kimlik doğrulama desteğinin olması kullanıcıların güvenliklerini artırmaktadır. Ayrıca Keeper gibi şifre yöneticileri karanlık web izleme gibi ek özelliklere sahiptir [20].

Tablo 2.3 Popüler şifre yöneticilerinin avantaj ve dezavantajları

Parola Yöneticileri	Avantajları	Dezavantajları
Lastpass	• AES-256 Kullanımı • MFA kullanımı • Parola paylaşımı ve senkron kullanımı	• Merkezi depolama kullanımı • Geçmişteki güvenlik açıkları • Bazı özelliklerin ücretli olması
1Password	• Kullanışlı arayüzü • Tarayıcılarla integrasyon • Güvenlik uyarıları ve özellikleri	• Ücretsiz sürümün sınırlı özellik • Merkezi veri depolama riski • Aboneliğin pahalı olması
Dashlane	• Güvenlik odaklı çalışıyor • VPN hizmeti de sunması	• Yeni kullanıcıların kullanım zorlukları • Yüksek abonelik ücretleri • Sistemde performans sorunları
Keepass	• Açık kaynaklı • Güvenlik odaklı çalışıyor • Bulut depolama hizmeti veriyor	• Otomatik senkronizasyon yok kullanıcı yapmalı • Daha az kullanıcı dostu arayüzünün olması
Bitwarden	• Çapraz platform desteği • Açık kaynaklı	• Performans sorunları • Bulut tabanlı güvenlik sorunları • Ücretsiz sürümün kısıtlı olması
RoboForm	• Basit arayüz • Güvenli paylaşım var • Otomatik doldurma	• Gelişmiş güvenlik özellikleri yok • Ücretsiz sürümün kısıtlı olması • İyi özelliklere abonelik talebi
Keeper	• Karanlık web izleme • Güçlü şifreleme özelliği • Güvenli dosya saklama	• Abonelik fiyatlarının pahalı olması • Sınırlı ücretsiz sürüm • Zayıf arayüz
Zoho Vault	• Diğer ürünler ile entegre • Güvenlik özellikleri • Uygun fiyatlandırma	• Çevrimdışı özellikler kısıtlı • Kısıtlı özellik • Karışık arayüzünün olması
Enpass	• Abonelik yok ücreti yok • Güçlü şifreleme özelliği • Yerel depolama özelliği	• Gelişmiş özelliklerin kısıtlı olması • Sınırlı bulut senkronizasyonu • Kullanıcı dostu olmayan arayüz
NordPass	• Basit arayüz • Güçlü güvenlik	• Sınırlı özelliklerinin olması • Abonelik tabanlı çalışması

1Password, RoboForm, NordPass gibi şifre yöneticileri ise kullanıcı dostu arayüz ile kullanıcı deneyimlerini artırmaktadır. Bu şifre yöneticilerinin tarayıcılar ile ve mobil cihazlar ile sorunsuz entegrasyonu, kullanıcılar için otomatik doldurma ve parola paylaşımı gibi özelliklerde bu yöneticilerin kullanım alışkanlıklarını artırmaktadır. Keepass ve Bitwarden gibi açık kaynaklı çözümler, özellikle teknik kullanıcılar için özelleştirile bilirlik sağlamaktadır. Enpass ise abonelik modeline dayanmayan yapısıyla dikkat çekmekte, tek seferlik lisanslama imkanı sunmaktadır. Bazı şifre yöneticileri ise merkezi bulut depolama sistemi kullandıkları için tekil saldırılı noktası oluşturabilmektedir. LastPass ise geçmişte veri ihlalleri bu yüzden yaşanmıştır. Bu da kullanıcı güvenliği açısından soru işaretleri yaratmaktadır. Aynı zamanda Bitwarden gibi yöneticilerde bulut tabanlı çözümleri de kullanıcılar için endişe yaratmaktadır.

Dashlane, Keeper ve 1Password gibi yöneticiler birçok gelişmiş özellikleri ücretli bir şekilde sunmaktadır bu da fiyat odaklı kullanıcıların bu yöneticileri seçmelerini zorlaştırmaktadır. Özellikle de kurumsal firmalar için yöneticilerin fiyatlandırma politikaları kurumsal kullanıcıları zorlamaktadır. Keepass, Zoho Vault ve Enpass gibi bazı yöneticiler, daha teknik ve kullanıcı dostu olmayan arayüzleri nedeniyle yeni kullanıcılar için erişim zorluğu yaratabilmektedir. Ayrıca bazı uygulamalarda (ör. Keepass) senkronizasyon işlemlerinin manuel yapılması kullanıcı deneyimini olumsuz etkileyebilmektedir. Bu durumlar göz önünde bulundurulduğu zaman popüler şifre yöneticilerinin değerlendirmesi Tablo 2.4'te gösterilmiştir.

Parola yöneticileri dijital güvenliğin yapı taşlarından biridir. Kullanıcılar seçimini yaparken ihtiyaçları ve öncelikleri doğrultusunda seçim yapmadıkları zaman yöneticiler tarafından istedikleri performansı almayabilir. Bu sebepten kullanıcılar seçim yaparken teknik düzeyleri, güvenlik özellikleri ve bütçeleri göz önünde bulundurulmalıdır.

Tablo 2.4 Kullanıcı profillerine göre parola yöneticisi önerileri ve gerekçeleri [20]

Kullanıcı Profili	Önerilen yöneticiler	Gerekçe
Temel, Yeni kullanıcılar	RoboForm, NordPass,1Password	Basit arayüz, otomatik doldurma, kolay kurulum
Teknik Kullanıcı, Geliştirici	KeePass, Bitwarden	Açık kaynaklı, güvenlik özellikleri, özelleştirilebilir
Yüksek güvenlik	KeePer, Dashlane	Vpn desteği, Gelişmiş şifreleme, karanlık web izleme
Bütçe odaklı	Enpass, Zoho Vault	Uygun maliyet, abonelik yok
Kurumsal kullanıcılar	1Password, Zoho Vault	Güvenlik politikaları, Ekip paylaşımı, entegrasyon

2.2.4. Şifre Yöneticisi Güvenliği

Şifre yöneticisinin uygulama tarafında alınması gereken güvenlik önlemleri var. Bu önlemler yedi başlıkta toparlanabilir [20].

- Veri şifreleme
- Anahtar Yönetimi
- Kimlik doğrulama ve yetkilendirme
- Sunucu güvenliği
- Veri bütünlüğü ve erişim kontrolü
- Yedekleme ve kurtarma
- Penetrasyon testleri ve güvenlik denetimi

Parola yöneticileri, kullanıcıların şifrelerini güvenli biçimde saklamak, senkronize etmek ve yönetmek üzere tasarlanmış kritik güvenlik araçlarıdır. Bu sistemlerin güvenliği, gelişmiş anahtar yönetimi süreçleri ve çok katmanlı kriptografik önlemlerle sağlanır. Anahtar yönetimi; anahtar üretimi, dağıtımı, sertifikalandırma, kimlik doğrulama, saklama, değiştirme ve silme gibi işlemleri içeren bütüncül bir güvenlik çerçevesini ifade eder. Parola yöneticilerinde, kullanıcı verilerinin gizliliğini sağlamak amacıyla şifreleme işlemleri istemci tarafında gerçekleştirilir. Sunucuya ulaşan hiçbir

parola düz metin olarak iletilmez; tüm veriler, istemci tarafında güçlü simetrik şifreleme algoritmalarıyla (örneğin AES-256) şifrelenmiş olarak gönderilir [21], [20]. Bu yapı, zero-knowledge mimarisi olarak adlandırılır; sunucu yalnızca şifreli veriyi saklar ve içeriğine erişemez [22].

Şifreleme anahtarları, kullanıcının ana parolasından türetilir. Bu türetme işlemi, PBKDF2, Argon2 gibi güçlü ve hesaplama açısından maliyetli fonksiyonlarla yapılır, böylece kaba kuvvet saldırılarına karşı direnç artırılır. Bu anahtarlar geçici olarak yalnızca istemci tarafında üretilir ve sunucu üzerinde hiçbir zaman depolanmaz. Kimlik doğrulama süreçlerinde ise, sadece parolayla yetinmek yetersizdir. Sistemler, iki faktörlü (2FA) veya çok faktörlü kimlik doğrulama (MFA) yöntemlerini desteklemeli ve zorunlu kılmalıdır. Erişim kontrolü jeton (token) tabanlı sistemlerle (JWT, OAuth 2.0) gerçekleştirilerek oturum güvenliği sağlanmalı; oturumlar belirli süreyle sınırlandırılmalı ve belirli aralıklarla yeniden kimlik doğrulama talep edilmelidir [23].

Parola yöneticisinin hizmet verdiği sunucu altyapısı da güvenlik açısından titizlikle korunmalıdır. Tüm veri iletimi HTTPS üzerinden şifreli yapılmalı, sunucular düzenli olarak güncellenmeli ve gereksiz portlar kapatılmalıdır. Hız sınırlaması (Rate limiting), kaba kuvvet koruması ve uygulama güvenlik duvarı (WAF) gibi ek güvenlik önlemleri uygulanarak sistem saldırılara karşı dayanıklı hale getirilmelidir. Kullanıcı verilerine sadece yetkili servislerin ve bireylerin erişimi sağlanmalı; bu erişimler de "minimum ayrıcalık" ilkesiyle sınırlandırılmalıdır. Kullanıcı parolaları bcrypt veya Argon2 gibi modern özet algoritmalarıyla işlenmeli, uygun şekilde salt uygulanmalı ve geriye dönük çözümlemelere karşı korunmalıdır. Ayrıca tüm yetkisiz erişim denemeleri kaydedilmeli ve analiz edilmelidir [23].

Parola kasalarının kaybolmasını ya da erişilemez hale gelmesini önlemek için düzenli, şifreli yedekleme politikaları uygulanmalı ve olası veri kaybı, sistem arızası veya siber saldırı senaryoları için kurtarma planları oluşturulmalıdır. Bu planlar belirli aralıklarla test edilmelidir. Sistemin güvenliği yalnızca mimariyle değil, aynı zamanda sürekli denetimle sağlanır. Bu kapsamda, bağımsız üçüncü taraflarca düzenli olarak penetrasyon testleri yapılmalı, sistemin OWASP Top 10 gibi bilinen güvenlik

açıklarına karşı dayanıklılığı değerlendirilmelidir. Özellikle kimlik doğrulama açıkları (Broken Authentication) ve hassas veri sızıntısı (Sensitive Data Exposure) gibi konulara özel önem verilmelidir [23].

Sonuç olarak, parola yöneticilerinin güvenliği; istemci taraflı şifreleme, sağlam anahtar yönetimi, güçlü kimlik doğrulama, sunucu güvenliği, erişim kontrolü, veri yedekleme ve sürekli denetim gibi bileşenlerin entegre biçimde uygulanmasına dayanır. Bu bütünsel yaklaşım, kullanıcı güvenliğini maksimum düzeyde sağlamayı ve gizliliği korumayı hedefler.

2.3. Siber Tehditler

Günümüzde siber saldırılar dünyada bireyler ve kuruluşlar için önemli bir tehdit haline gelmiştir. Siber saldırganlar bilgi güvenliğini tehlikeye atmak, hassas verileri çalmak, sistemlere ve ağlara zarar vermek için çeşitli teknikler kullanmaktadır. Siber tehdit yetkisiz erişim, imha, ifşa, bilgilerin değiştirilmesi ve/veya hizmet reddi yoluyla bir bilgi sistemi aracılığıyla kurumsal operasyonları (misyon, işlevler, imaj veya itibar dahil), kurumsal varlıkları, bireyleri, diğer kuruluşları veya Ulusu olumsuz etkileme potansiyeli olan herhangi bir durum veya olaylardır [24].

Mayur Jariwala'nın "Siber Güvenlik Yol Haritası: Daha Güvenli Bir Dijital Dünya İçin Siber Tehditler, Siber Yasalar ve Siber Güvenlik Eğitimine İlişkin Kapsamlı Bir Kılavuz" kitabında siber tehditleri kötü amaçlı yazılımlar, sosyal mühendislik saldırıları, ağ saldırıları, kablosuz saldırı ve ortak uygulama tehditleri olarak 5 farklı saldırı türüne bölüyor [25]. Kötü amaçlı yazılımlar karşı taraftaki bilgisayar sistemlerini, ağları ya da cihazları bozmak için veya zarar vermek için hazırlanmış yazılım olarak adlandırılmaktadır. Kötü amaçlı yazılımların türlerine bakacak olursak virüsler, truva atları, fidye yazılımları ve solucan yazılımlarıdır bunlar ise e-posta eklerinde, virüslü web sitelerinde bulunabilmektedir [25]. Kötü amaçlı yazılımların türleri Tablo 2.5'te gösterilmiştir.

Tablo 2.5 Zararlı yazılım türleri ve açıklamaları

İsimleri	Açıklaması
Virüs (virus)	Virüsler dosyaları kendi kopyalarıyla üzerine yazar. Bu yazılımlar eski teknikler olsa da en kolay tekniktir. Dosya üzerine yazılmış virüsler sistemden temizlenmez, enfekte dosyalar diskten sistemden silinmelidir [26].
Solucan (worm)	Solucan yazılımları bilgisayarın ve ağın normal işleyişini önemli ölçüde etkiler. Solucan yazılımı sistem kaynaklarını, ağ bant genişliğini, internet trafiğini de işgal eder [27].
Truva atı (trojan)	Truva atı saldırıları bilgisayar güvenliği için büyük tehditler yarata bilmektedir. Truva atı iki bölüme ayrılır sunucu ve istemci. En yaygın enfekte yolu e-posta ekleri olarak bilinir. Truva atı bilgisayara gizlice erişim alır, kullanıcıları izler ya da veri çala bilmektedir [28].
Reklam yazılımı (adware)	Reklam yazılımı, genellikle kullanıcı izni olmaksızın sistemlere entegre edilen ve reklam içerikleri sunarak gelir elde etmeyi amaçlayan yazılımlardır. Bu tür yazılımlar, çoğunlukla başka uygulamalarla birlikte gizli biçimde kurulur ve kullanıcıların çevrim içi davranışlarını izleyerek kişiselleştirilmiş reklamlar üretir. Reklam yazılımı, sistem performansını olumsuz etkileyebilmekte ve kullanıcı mahremiyetini tehdit eden veri toplama faaliyetlerinde bulunabilmektedir [29].
Casus yazılım (spyware)	Bir casus yazılım programının temel amacı belirlenmiş süre zarfında bilgisayara erişimin devam etmesini sağlamaktır. Bu yazılım belirli teknikler kullanarak bilgisayarda kullanılan güvenlik duvarları ve anti-virüs yazılımlarından saklanarak kendi görevlerini yapar [30].
Kök kullanıcı takımı (rootkit)	Kök kullanıcı takım, saldırganın sistemde yetkili erişimini gizlemesine ve kalıcılığını sürdürmesine olanak tanır. Dosyalar, işlemler, İletim Kontrol Protokolü (TCP) portları ve kayıt defteri gibi öğeleri gizlemek için kullanılır. Bu teknikler, mevcut antivirüs ve güvenlik sistemlerinin tespitten kaçınmasını sağlar, bu da kök kullanıcı takımları tespit edilmesi zor ve tehlikeli hale getirir. Bu nedenle, kök kullanıcı takımları siber güvenlik alanında önemli bir tehdit olarak değerlendirilir [31].
Tuş kaydedici (keylogger)	Tuş kaydedici, kullanıcının klavye üzerinden girdiği verileri gizlice kaydeden bir casus yazılım türüdür. Genellikle şifre ve kredi kartı bilgileri gibi hassas verileri ele geçirmek amacıyla kullanılır. Sistem kaynaklarına entegre olarak fark edilmeden çalışabilir, bu da onu ciddi bir siber güvenlik tehdidi haline getirir.

Sosyal mühendislik saldırılarına baktığımız zaman da bu saldırılar kendi aralarında farklılıklar göstermektedir. Sosyal mühendislik saldırıları sistemlerdeki ve yazılımlardaki açıkları ve zayıflıkları kullanmadan, kullanıcı manipülasyonuna dayanan siber tehdit biçimidir. Sosyal mühendislik saldırıları, hedeflenen bireyi manipüle etmek için güven, merak, korku ya da otoriteyi istismar ederek insan davranışının psikolojik yönlerini kullanır [25]. Sosyal mühendislik saldırılarının türlerine bakarsak kimlik avı (phishing), büyük balık avı (Whaling), Senaryo uydurarak kandırma (Pretexting) ve yemleme (baiting) gibi teknikler kullanılır [25]. Genellikle sosyal mühendislik saldırıları kullanıcıların kredi kartı bilgilerini, kullanıcı bilgilerini ve kişisel bilgileri gibi verileri sahte sitelere yönlendirerek, köprü metinleri taşıyan sahte e-postalar, anlık mesajlar göndererek kullanıcı verilerini çalmayı hedeflemektedir [32].

Ağ saldırılarının tanımına bakarsak bir bilgisayar ağına ya da bağlı olduğu sistemlere yönelik yetkisiz erişim sağlamak, çalışmakta olan hizmeti aksatmak veya bütünlüğü bozma amaçlı yapılan saldırılardır. Bilgi güvenliği kapsamında bu saldırılar gizlilik (confidentiality), bütünlük (integrity) ve erişebilirlik (accessibility) ilkelerini hedeflemektedir. Bu ise literatürde CIA ilkesi olarak geçmektedir. [33]. Ağ saldırılarına örnek olarak orta adam saldırısı (MITM), IP sahtekarlığı (IP spoofing), ARP sahtekarlığı (ARP spoofing), hizmet engelleme saldırısı (DOS) ve dağıtılmış hizmet engelleme (DDOS) gibi yöntemler de var. Bu yöntemlerin açıklamaları tablo 2.6'da verilmiştir.

Kablosuz ağlara yönelik saldırılar ise, doğrudan sistemlere müdahale edilerek ya da kullanılan yazılım ve donanımdaki güvenlik açıklarının istismar edilmesi yoluyla gerçekleştirilir; bu tür saldırılar genellikle yetkisiz veri erişimi sağlamak veya hedef sistem üzerinde zararlı etkiler oluşturmak amacı taşır. Bu saldırı ya da zafiyet kullanma teknikleri SQL enjeksiyon (SQL injection), XML Dış Varlık Saldırısı (XXE), Siteler Arası Komut Dosyası Çalıştırma (XSS) gibi teknikler kullanılmaktadır [25].

Tablo 2.6 Bazı ağ saldırıları kullanım amaçları

İsim	Açıklama
Ortadaki adam	Ortadaki adam saldırısı, iki tarafın arasında gerçekleşmekte olan iletişimin gizlice dinlenmesi, değiştirilmesi veya yönlendirilmesi yoluyla gerçekleştirilen bir saldırıdır. Saldırgan, kurban ile hedef sistem arasına sızarak veri trafiğini manipüle eder ve genellikle kimlik bilgileri ya da kullanıcının hassas verilerini çalar [34].
IP sahtekarlığı	IP sahtekarlığı, sahte IP adresleri kullanarak bir paketin kaynağını gizlemeye yönelik bir tekniktir. Bu yöntem genellikle güvenlik önlemlerini atlatmak veya hedef sistemin saldırganın gerçek konumunu tespit etmesini engellemek amacıyla kullanılmaktadır [34], [25].
ARP sahtekarlığı	ARP sahtekarlığı, yerel ağ üzerindeki ARP tablolarının sahte ARP mesajlarıyla zehirlenmesi yoluyla, saldırganın ağ üzerindeki trafiği kendisine yönlendirmesini sağlamakta olan bir tekniktir. Bu saldırı türü, genellikle ortadaki adam saldırısının bir alt basamağı olarak kullanılmaktadır [34], [25].
Hizmet engelleme	Hizmet engelleme saldırıları, bir sistemin veya servisin çoklu isteklerle aşırı yüklenerek kullanıcıların erişimine kapatılmasını amaçlamaktadır. Tek bir kaynaktan gelen bu saldırılar, hedef sistemin işlem gücünü ve bant genişliğini tüketerek hizmet kesintisine yol açmaktadır [25].
Dağıtılmış hizmet engelleme	Dağıtılmış hizmet engelleme saldırıları, birçok cihazdan hedef sisteme aynı anda saldırılar yapılarak hizmetin çökmesine neden olmasını sağlamaktadır. Dağıtılmış hizmet engelleme saldırıları, büyük ölçekli ağlar ve sistemler üzerinde ciddi kesintilere ve maddi zararlara yol açabilecek karmaşık saldırı türlerindendir [25].

2.3.1. Şifre Elde Etme Amaçlı Tehditler

Günümüzde dijital iletişim araçlarının yaygınlaşmasıyla bireylerin kişisel verileri, özellikle de çevrimiçi platformlarda kullanıcı kimliğini doğrulamak için kullanılan

parolalar güvenlik meselesi haline gelmektedir. Tablo 2.7'de "password" AND "attack type" ve "Threats to obtain passwords" kelimeleri ile literatürde tarama yapılmıştır. 10 farklı makale ve raporlarda şifreler için tehdit olduğu düşünülen saldırı türleri listelenmiştir. Bu literatür taraması hangi saldırıların şifreler için tehdit oluşturduğunun tespit edilmesi için yapılmıştır. Yapılan araştırma esnasında 4 ve üzeri kaynakta tehdit olarak bulunan saldırılar bu araştırmada şifreler için tehdit olarak kabul edilecektir.

Tablo 2.7 Parola güvenliğini tehdit eden saldırı teknikleri ve kaynaklar

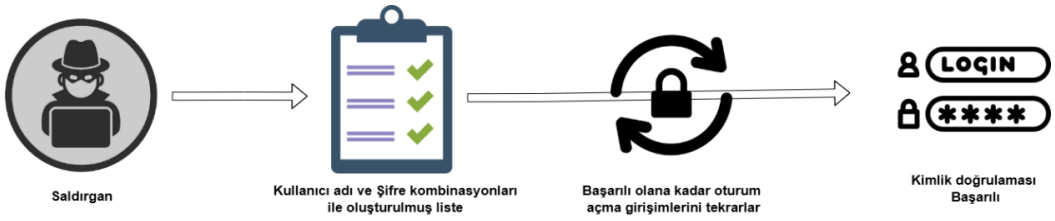
Saldırılar	Kaynaklar
Kaba Kuvvet saldırısı	[35],[36],[37],[38],[39],[40],[41],[42],[43],[44]
Oltalama saldırısı	[35],[36],[40],[41],[43],[44]
Sözlük saldırısı	[35],[36],[37],[38],[39],[40],[42],[44]
Tuş Kaydedici	[35],[36],[38],[40],[43]
Video kaydedici	[35],[37],[38]
Tekrar saldırısı	[35],[38],[41]
Omuz sörfü	[37],[38],[41]
Kimlik bilgisi doldurma saldırısı	[36],[40],[41]
Leke saldırısı	[37]
Casus yazılım	[37],[38]
Histogram	[38]
Harf frekans saldırısı	[39]
Markov model	[39]
Gökkuşağı Tablo saldırısı	[39]
Orta adam saldırısı	[37],[40],[43],[44]

Literatür taraması esnasında beş tane saldırı şifreler için tehdit olarak seçilmiş ve bu saldırılar kaba kuvvet saldırısı, oltalama saldırısı, sözlük saldırısı, tuş kaydedici ve orta adam saldırılarıdır.

2.3.1.1. Kaba Kuvvet Saldırısı

Kaba kuvvet saldırısının amacı kullanıcının ya da yöneticinin yetkisine erişim sağlamaktır [45]. Örneğin saldırgan uzak bilgisayara erişim sağlamak için kaba kuvvet

saldırısı yaparak yönetici erişimini elde edebilir bu sayede kullanıcının tüm ayarlarını değiştirebilir ya da kullanıcıya özel verileri elde edebilir [46]. Bunun yanı sıra kullanıcının dijital hesaplarına da kaba kuvvet saldırıları yapıla bilinir ama kullanıcı tarafında da bu saldırılara karşı önlemler alınmaktadır. Şekil 2.4'te kaba kuvvet saldırısının şeması gösterilmiştir.



Şekil 2.4 Kaba kuvvet saldırı şeması

Kaba kuvvet saldırısı saldırgan tarafından şifre ve kullanıcı adının bulunması için olası tüm harf, rakam, özel karakterler ile olası tüm kombinasyonlar kullanılarak kullanıcıya karşı saldırı başlatılır. Daha sonra ise olası bu kombinasyonlar kullanılarak giriş için denemeler yapılır. Bu saldırı türü bilgisayarlar donanımlarının güçlenmesi ile saldırıları süreleri azalmaktadır. Kaba kuvvet saldırı kullanılarak oluşturulmuş tüm şifreler bulunabilir sadece bu saldırı saldırgan için zaman almaktadır. Hivesystems tarafından oluşturulan 2024 senesindeki raporda kaba kuvvet saldırısı ile şifrelerin 12 tane RTX 4090 ekran kartı ile kırılma süreleri (Şekil 2.5) hesaplanmıştır.

Şekil 2.5 Kaba kuvvet saldırısı ile şifrelerin kırılma süresi [47]

Verilen zaman aralıkları donanım değişiklikleri ile arta ya da azala bilir. Şekil 2.5'te görüldüğü gibi sekiz haneli sadece rakamlardan oluşan bir şifre oluşturduğumuz zaman şifrenin bulunma süresi 37 saniye olarak hesaplanmıştır. Harf rakam ve sembollerin kullanımı bu süreyi yedi seneye yükseltmektedir.

2.3.1.2. Oltalama Saldırısı

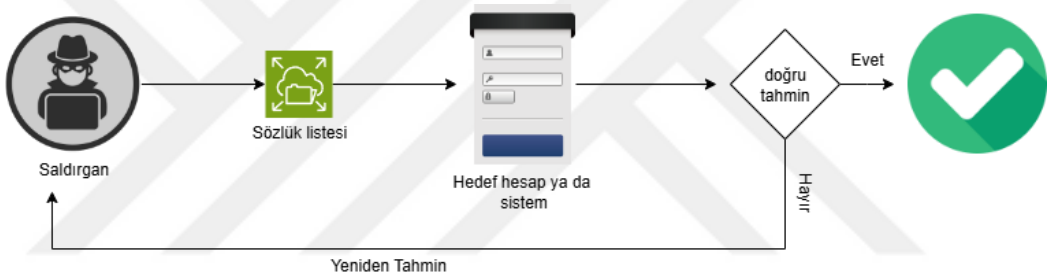
Oltalama saldırıları Klon oltalama (clone phishing), zıpkınla yemleme (spear phishing), telefonla oltalama (phone phishing) olarak üçe ayrılmaktadır [48]. Klon oltalama farklı güvenilir sitelerin klonları hazırlanarak kişileri bu sitelere çekerek kullanıcıya ait özel verileri bu yöntem ile elde etmektedir. İkinci tür ise "zıpkınla yemleme" (spear phishing) yöntemidir. Bu teknikte, belirli kişiler doğrudan hedef alınarak, .pdf, .txt, .docx gibi dosya formatlarında zararlı içerikler içeren dosyalar kullanıcıya gönderilmektedir [49]. Telefon oltalama saldırısındaysa saldırgan bankadan aramış gibi kullanıcıları manipüle ederek gönderilmiş sitede kullanıcıya banka kart numarasını şifresini gibi bilgileri girmeye zorluyor [50]. Her sene Anti-Phishing Working Group tarafından yayınlanan raporun 2025 yayınının verileri Tabloda 2.8'de gösterilmiştir. Aralık ayında oltalama saldırılarında bir artış eğilimi gözlemlenmektedir. Özellikle e-posta konularındaki çeşitlilik dikkat çekicidir. Web sitesi sayısındaki dalgalanma ve marka sayısındaki görece stabil seyir, saldırıların sadece hacimsel değil, içerik ve hedef bakımından da stratejik olarak şekillendiğini göstermektedir. Kurumların yıl sonlarında daha fazla oltalama saldırısına maruz kaldıkları gözükmektedir. Bunun için yıl sonlarına yaklaşırken oltalama farkındalığı daha da artırılmalıdır, e-posta güvenliği ve marka koruma stratejilerini gözden geçirmeleri önem taşımaktadır.

Tablo 2.8 Oltalama saldırı göstergeleri

	2024		
	Ekim	Kasım	Aralık
Tespit edilen benzersiz oltalama (phishing) web sitesi sayısı	345881	313288	329954
Benzersiz oltalama e-posta konuları	28327	27669	33899
Saldırıya uğrayan marka sayısını sayar.	315	333	309

2.3.1.3. Sözlük Saldırısı

Sözlük saldırıları, kaba kuvvet (brute-force) saldırılarından farklı olarak, tüm olası karakter kombinasyonlarını denemek yerine, saldırgan tarafından önceden hazırlanmış ya da internette bulunan büyük şifre listeleri kullanılarak gerçekleştirilir. Bu saldırı türünde, listedeki kullanıcı adı ve şifreler sırasıyla denenir ve doğru kombinasyon bulunana kadar süreç devam eder. Kaba kuvvet saldırıları uzun süreler alsa da kullanıcının şifresini bulabiliyor. Ama sözlük saldırılarında elde olan kombinasyon sayısı az olduğu için sözlük saldırıları daha az süre alır ama tüm şifreleri bulamaya bilir bu ise saldırganın ürettiği ya da bulduğu listeye göre değişiklik göstermektedir. Şekil 2.6'de göründüğü gibi saldırgan doğru tahmin edene kadar döngü devam eder listedeki parola biterse ve listede şifre olmazsa döngü başarısız bir şekilde biter.

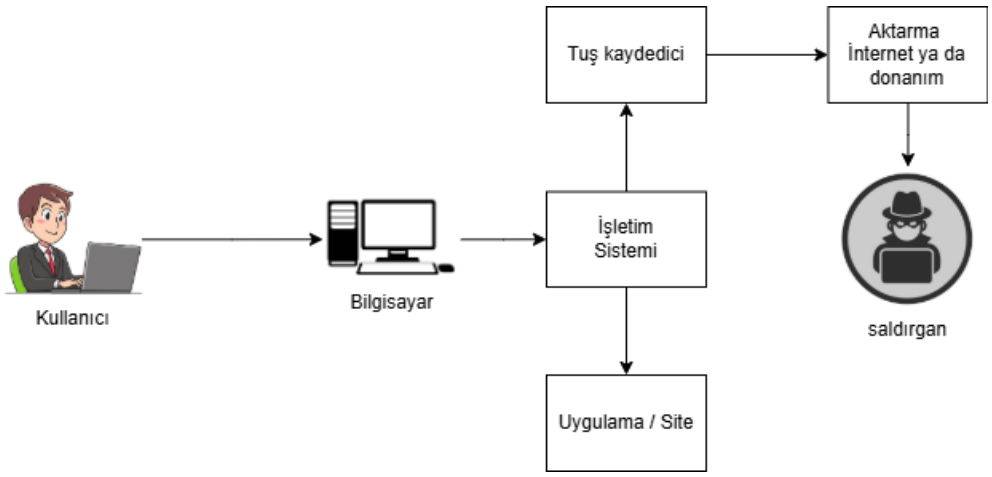


Şekil 2.6. Sözlük saldırısının şeması

2.3.1.4. Tuş Kaydedici

Tuş kaydedicileri bir kullanıcının tıkladığı klavye tuşlarını kaydederek saldırgana göndermektedir. Bu saldırı esnasında kullanıcının internet sitesine girdiği kullanıcı adı ve şifresini, kredi kartı bilgilerini, kişinin mesajlaşmalarını saldırgan ele geçirebilmektedir. Kullanıcılara bu yazılım sahte yazılımlarla, e-posta eklerine ve başka tekniklerle kullanıcı bilgisayarlarına sızabilmektedir [25].

Şekil 2.7'te gösterildiği üzere, kullanıcının bilgisayarda girdiği tuş kombinasyonları, işletim sistemi aracılığıyla aktif uygulamalarla birlikte işlenirken, bu veriler aynı zamanda tuş kaydedici (keylogger) yazılım tarafından kaydedilerek saldırgana iletilmektedir. Bu aktarım özel yazılımlar ile internet ile veya bilgisayara fiziksel olarak bağlanmış donanımlar ile de yapılabilmektedir.

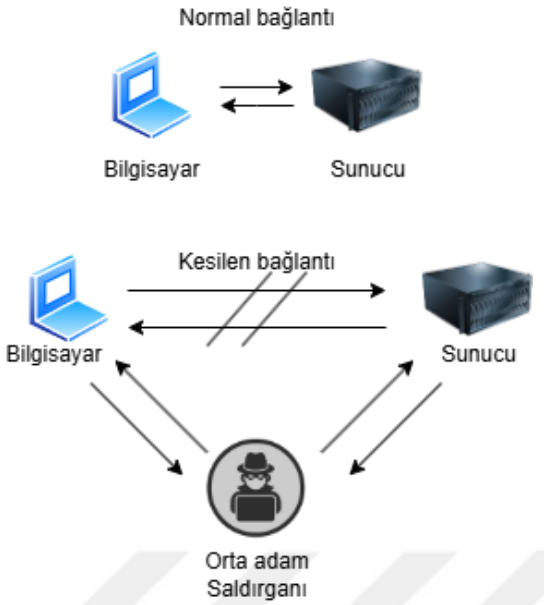


Şekil 2.7 Tuş kaydedici şeması

2.3.1.5. Orta Adam Saldırısı

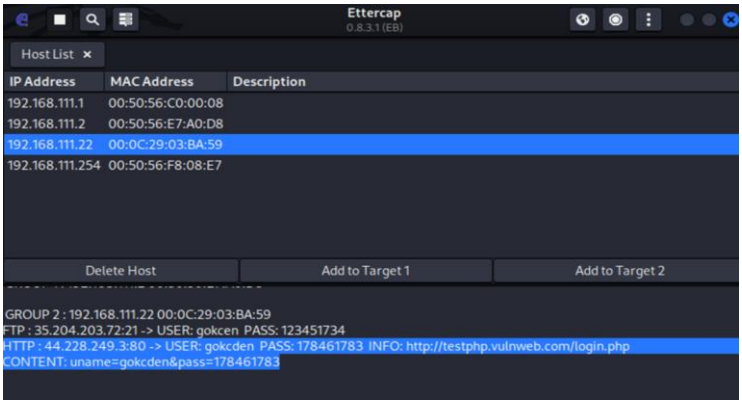
Ortadaki adam saldırıları, iki veya daha fazla bağlantı noktası arasındaki iletişimi izler ve bu iletişim kanalını gizlice ele geçiren bir siber saldırı türü olarak tanımlanmaktadır [50]. Bu tür saldırılarda saldırgan, hedeflenen kurbanın iletişimini yalnızca dinlemekle kalmamaktadır; aynı zamanda bu iletişimi kesme, değiştirme ya da manipüle etme gücüne de sahiptir. Dolayısıyla orta adam saldırıları, sadece pasif dinlemeyle sınırlı kalmamaktadır, bilgi güvenliğinin temel bileşenleri olan gizlilik, bütünlük ve erişilebilirlik (CIA) ilkelerini doğrudan tehdit etmektedir. Saldırgan, iletişimi izleyerek gizliliği ihlal edebilir, iletilen verileri değiştirerek bütünlüğü zedeleyebilir veya iletişimi kesintiye uğratarak erişilebilirliği engelleyebilmektedir. Bu sebepten, orta adam saldırıları bilgi güvenliğine yönelik çok yönlü tehditler oluşturmaktadır [50].

Orta adam saldırısının çalışma şeması Şekil 2.8'te gösterilmiştir. İlk örnekte bilgisayarla sunucu arasında hiçbir sorun yok yani normal bağlantı var ikinci örnekte ise bilgisayar ile sunucu arasında normal bağlantı kesilir ve saldırgan iki bağlantı arasına girer bilgisayar ile sunucu bağlantısı direkt saldırgan üzerinden iletilmektedir. Eğer kullanıcı HTTPS ve TLS protokollerini kullanmayan sitelere giriş yaparak burada kişisel bilgilerini girerse ve kullanıcıya karşı bir orta adam saldırısı varsa bu zaman saldırgan kullanıcının girmiş olduğu bilgileri şifresiz bir şekilde göre bilmektedir (Şekil 2.9).



Şekil 2.8 Orta adam saldırısının şeması

Şekil 2.9'da görüldüğü gibi kullanıcının HTTP olan siteye kullanıcı giriş yaparak kullanıcı adı ve şifre girişi yaptığı zaman kullanıcıya ait bilgiler saldırgan ekranında gözükmektedir. 'Http://testphp.vulnweb.com/login.php' sitesine kullanıcı giriş yapmış ve kullanıcı adı- 'gokcden' parola – '1784661783' olduğu gözükmektedir.



Şekil 2.9 Orta adam saldırısı bilgi elde etme [51]

2.3.2. Şifre Yönetim Sistemlerine Yönelik Tehditler

Parola yöneticisi kullanan kullanıcılar tüm şifrelerini bazı kullanıcılarsa banka kartı verileri gibi bilgilerini parola yöneticilerinde sakladığı için bu hizmetler ve uygulamalarda saldırılara maruz kalmaktadır. Bu bölümde literatürde taraması

yapılarak seçilmiş parola yöneticilerinin saldırılara karşı nasıl önlemler aldıkları gösterilecektir.

Petr Gallus ve arkadaşları [52] tarafından yapılan araştırmada 10 tane parola yöneticisi seçilerek 4 farklı testler yapılarak hangisinin daha güvenli olup olmadığı ve bu parola yöneticilerinden bilgi alınabiliyor mu? diye testler yapılmıştır. Bu çalışmada kaba kuvvet saldırıları, oltalama saldırıları, yedekleme güvenliği testleri ve bellek analizi gibi yöntemlerle parola yöneticileri değerlendirilmiştir. Araştırma sonuçlarına göre Bitwarden, ProtonPass ve Keeper gibi parola yöneticileri güçlü parola politikalarına sahip olup, kaba kuvvet saldırılarına karşı CAPTCHA kullanımı ve hesap kilitleme gibi güvenlik önlemleriyle korunmaktadır. 1Password ve LastPass gibi parola yöneticileri çok faktörlü doğrulama sistemini daha etkin olarak kullandıkları tespit edilmiştir.

Kimlik avı saldırısındaysa araştırma sonucunda Dashlane, LastPass, ProtonPass ve 1Password gibi yöneticiler otomatik doldurma işlemi zamanı sahte sitelerde otomatik doldurma özelliğini engelleyerek sahte siteye şifrenin girişini yapmamıştır. Ama KeePass'ın daha az etkili olduğu gözlemlenmiştir. Hatta KeePass gibi yerel ortamda çalışan yöneticiler sitelerin gerçek mi, sahtemi olduğunu tespit edememiştir. Bu da kullanıcı güvenliğini önemli ölçüde tehdit etmektedir [52].

Yedekleme güvenlik testinde AES-256 şifreleme tekniği kullanan Bitwarden, Keeper, ProtonPass gibi şifre yöneticileri güvenlik testinden geçerken araştırma sonucunda KeePass Google Password Manager gibi yöneticiler kullanıcıya güvenerek verileri ifşa edebilmektedir diye sonuç alınmıştır [52]. Bellek analizinde ise 1Password, Bitwarden ve Dashlane uygulamalar kullanım esnasında ana parolayı bellekte şifreli bir şekilde sakladığı bulunmuştur lakin KeePass ve NordPass kullanım esnasında metinsel olarak bellekte bulunduğu ya da parolaların bazı izlerinin bulunduğu tespit edilmiştir [52].

Michael Carr ve Siamak F. Shahandashti'nin parola yöneticilerinin açıkları ve saldırılara karşı ne kadar dayanıklı olduklarını test etmişler. Bu araştırmada 5 farklı parola yöneticisi test edilmiştir. Araştırmada İki Faktörlü Kimlik Doğrulama Tohum, Element Denetleme Güvenlik, Kayıt Keşfi Güvenlik, URL Uyuşmazlığı, HTTP(S)

Otomatik Doldurma Güvenlik ve Alt Alan Adlarını Yok sayma açıkları test edilmiştir. Bu testlerin sonuçları Tablo 2.9'de gösterilmiştir. Tablodaki (-) ismi geçen açıkların parola yöneticilerinde olduğunu, (+) ise bu açıkların bulunmadığını gösteriyor. İki faktörlü kimlik doğrulama tohum açığında beş parola yöneticisi de çaresiz durumda kalmaktadır. İki faktörlü kimlik doğrulama (2FA) tohum açığı karşısında, incelenen beş parola yöneticisi de savunmasız kalmaktadır. Bu testte, iki aşamalı doğrulama kurulurken güvenlik amacıyla kullanılan gizli bilginin (tohumun), ilişkilendirildiği internet adresinin (URL) kolaylıkla tahmin edilip edilemeyeceği değerlendirilmiştir. Diğer test olan eleman denetleme de ise başka bir kullanıcıya parolayı kullanma ama görememesi için yetkilendirme verildiğinde karşı taraf şifreyi ifşa ede biliyor mu diye test edilmiştir. Sonuç olarak 1Password ve RoboForm yöneticileri bu testten başarısız olarak geçmiştir [53].

Tablo 2.9 Parola yöneticilerinin açıklarının test sonuçları [53]

Açıklar	Parola Yöneticileri				
	Dashlane	LastPass	Keeper	1Password	RoboForm
İki Faktörlü Kimlik Doğrulama tohum	-	-	-	-	-
Element Denetleme Güvenlik	+	+	+	-	-
Kayıt Keşfi Güvenlik	+	-	-	-	-
URL Uyuşmazlığı	+	-	+	+	+
HTTP(S) Otomatik Doldurma	+	+	+	+	+
Güvenlik ve Alt Alan Adlarını Yok sayma	+	+	+	+	+

Kayıt keşif güvenliğinde ise bir kullanıcının sistemde kayıtlı olup olmadığını belirlemek amacıyla, kullanıcı arayüzü üzerinden yapılan doğrulama girişimlerinin analiz edilmesi. Bu süreçte, önce hatalı bir kullanıcı adı ve ardından hatalı bir parola kullanılarak oturum açma denemeleri gerçekleştirilir. Sistem tarafından verilen

tepkiler, hedeflenen kullanıcı adının sistemde mevcut olup olmadığına ilişkin dolaylı bir gösterge sağlayabilmektedir [53]. Bu testten ise sadece Dashlane yöneticisi başarılı bir şekilde geçmiştir. Sıradaki testte ise url uyuşmazlığı test edilmektedir kullanıcı verileri url uyuşmasa da şifreyi o sitede otomatik doldurma işleminin yapılıp yapılmadığı test edilmiş ve bu testten LastPass dışında tüm yöneticiler geçmiştir [53].

Gerçekleştirilen diğer iki test, HTTPS otomatik doldurma ve alt alan adlarını yok sayma zafiyetlerini ortaya koymuştur. HTTPS otomatik doldurma zafiyeti, tarayıcıların HTTPS protokolü üzerinden kaydedilmiş kimlik bilgilerini, HTTP protokolü üzerinden erişilen sitelerde de otomatik olarak doldurması nedeniyle, ortadaki adam (Man-in-the-Middle, MITM) saldırılarına karşı ciddi bir güvenlik açığı oluşturur. Alt alan adlarını yok sayma zafiyeti ise, farklı hizmetlerin barındırıldığı alt alan adları arasında kimlik bilgisi izolasyonunun sağlanamaması sonucunda, bir alt alan üzerinden diğer alt alanlara veya ana alan adına ait kullanıcı kimlik bilgilerinin ele geçirilmesine imkan tanımaktadır. Bu tür açıklar, özellikle çoklu alt alan adı kullanan şifre yöneticileri, üniversite portalları, forumlar ve blog platformları gibi sistemlerde önemli güvenlik riskleri yaratmaktadır [53]. Belirtilmiş bu açıklardan tüm yöneticiler başarılı bir şekilde geçmiştir.

2.4. Benzer Çalışmalar

Golla M. ve arkadaşları [7] tarafından yapılan araştırmada emojiler ile android cihazlara için kilit ekranı hazırlamışlar ve testler ile bu ekran kilidinin güvenilirliğini frekans testi, entropi testi, kullanıcılar tarafından parolaların hatırlanabilirlik testi gibi testler yapmışlar. Testler sonucunda üretmiş oldukları 20 emoji ile üretilmiş olan emoji ile ekran kilidi Android cihazlarda olan desenle kilit açmadan daha güvenli olduğu testler sonucunda tespit etmişler. Sonuç olarak uygulamanın üretmiş olduğu şifreler tahmin etme saldırılarına karşı dirençli bulunmuştur.

Zabidi ve arkadaşları [8] tarafından gerçekleştirilen bir çalışmada, emoji tabanlı ekran kilitleri ile geleneksel ekran kilidi yöntemleri karşılaştırmalı olarak analiz edilmiştir. Söz konusu çalışmada geliştirilen sistem, doğrudan emoji üretimine dayalı bir parola oluşturma yöntemi sunmamakta; bunun yerine kullanıcıların sisteme kaydolduktan

sonra bir görsel seçmeleri ve bu görsel üzerine dört farklı emojiyi sürükleyerek yerleştirmeleri esas alınmaktadır. Araştırma bulguları, grafiksel parola sistemlerinin kullanıcılar açısından daha dikkat çekici ve ilgi uyandırıcı olduğunu ortaya koymuştur. Ancak, uygulamada kullanılan sürükle-bırak tekniğinin bazı kullanıcılar için kullanım zorluğu yarattığı da tespit edilmiştir.

KSC Ayineni ve arkadaşları [9] tarafından yürütülen araştırmanın temel amacı, emoji tabanlı doğrulama yöntemini üç faktörlü kimlik doğrulama sistemlerinden biri olarak entegre etmektir. Çalışmada, bu yöntemin özellikle kaba kuvvet saldırıları, sosyal mühendislik saldırıları ve kimlik bilgisi doldurma (credential stuffing) saldırılarına karşı ek bir güvenlik katmanı sağlayarak sistemin direncini artırması hedeflenmiştir. Önerilen yöntemde, kullanıcıdan sisteme giriş esnasında sistem tarafından sunulan dokuz farklı emojiyi, önceden belirlediği sıraya göre dizmesi istenmektedir. Bu doğrulama adımının başarıyla tamamlanmasının ardından kullanıcı, kendi hesabına erişim sağlayabilmektedir.

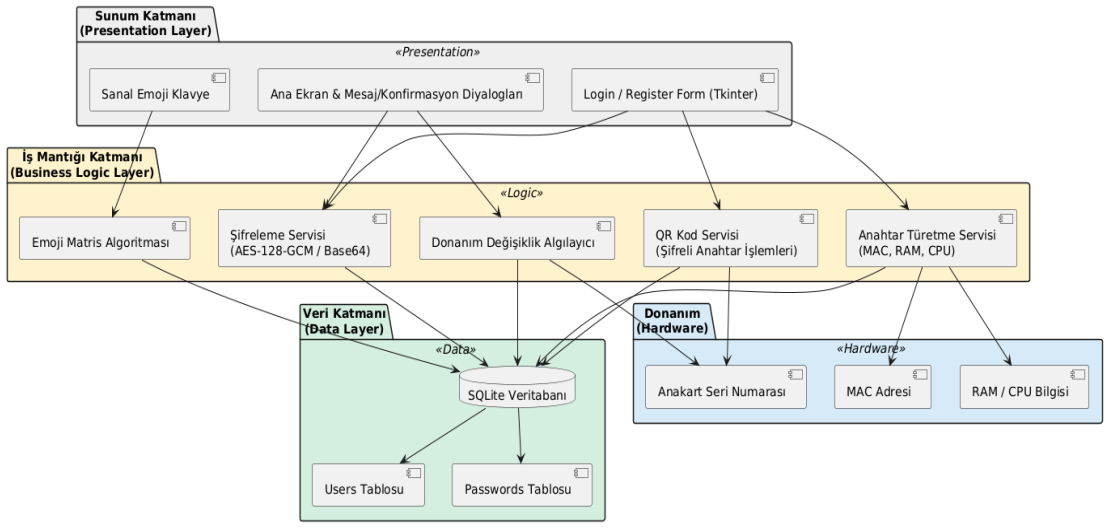
X. Nan [10] tarafından gerçekleştirilen çalışmada yalnızca emojiler değil, aynı zamanda ASCII karakter seti tarafından desteklenmeyen ancak Unicode standardı kapsamında yer alan karakterleri içeren özel klavyelerin oluşturulması ele alınmıştır. Geliştirilen bu klavyeler aracılığıyla, kullanıcıların şifre oluşturma politikalarına uygun biçimde, Unicode tabanlı karakterleri kabul eden platformlarda parola belirlemeleri mümkün hale getirilmiştir. Çalışma kapsamında elde edilen kullanıcı geri bildirimleri ilgili makalede detaylı bilgi verilmiştir. Bu geri bildirimlerin kullanıcı deneyimini olumlu yönde etkilediği, araştırmacı tarafından vurgulanmıştır.

3. MALZEME VE YÖNTEM

Bu çalışmada kullanıcılar için her seferinde benzersiz emoji tabanlı bir şifre üreten ve bu şifreleri yerel ortamda şifreli bir şekilde kaydeden daha sonra ise üretilmiş şifreye kullanıcının istediği zaman ulaşabildiği bir uygulama geliştirilmiştir. Uygulama Windows 11 işletim sistemi için Python programlama dilinde yazılmış ve veri tabanı olarak SQLite kullanılmıştır.

3.1. Uygulama Mimarisi ve Bileşenleri

Uygulamanın veri katmanı, iş mantığı katmanı ve sunum katmanı olmak üzere üç temel katmanı var. Uygulama mimarisi Şekil 3.1'de gösterilmiştir. Uygulamanın veri tabanında tüm veri yönetimini üstlenen "users" ve "passwords" tabloları bulunmaktadır. Bu katman python'un yerleşik modülü olan SQLite3 aracılığıyla veri tabanı bağlantısı sağlamakta ve oluşturma (Create), okuma (Read), güncelleme (Update) ve silme (Delete) sözlerinin baş harfleri olarak bilinen CRUD güvenli bir şekilde sağlanmaktadır.



Şekil 3.1 Uygulama mimarisi

İkinci katman, yani iş mantığı katmanı, tüm şifreleme, anahtar türetme ve donanım algılama süreçlerini kapsar. Bu katmanda, simetrik şifreleme işlemleri Gelişmiş Şifreleme Standardının 128 bitlik Elektronik Kod Bloğu (AES-128-GCM) modu ve dolaylı olarak Açık Anahtarlı Kriptografi Standardı (PKCS#7) kullanılarak gerçekleştirilir; şifreleme ve şifre çözme işlemlerine ek olarak temel güvenlik fonksiyonları da bu standartlar çerçevesinde tasarlanmıştır. Veri taşımayı kolaylaştırmak amacıyla, şifreleme öncesi ve sonrasında Base64 kodlama ve çözme adımları uygulanmaktadır.

Anahtar türetme mekanizması, her bilgisayara özgü olarak analiz edilen MAC adresi, bellek (RAM) ve işlemci (CPU) bilgileri temel alınarak oluşturulur. Buna ek olarak, şifre güvenliğini artırmak amacıyla emoji tabanlı beş × beş matris modeline dayalı bir bit işleme algoritması entegre edilmiştir. Uygulama, internet bağlantısı olmaksızın yerel ortamda çalışacak şekilde tasarlanmıştır. Donanım bileşenlerinde yapılacak herhangi bir değişiklik, doğrulama sürecinin başarısız olmasına neden olacağından, ek bir güvenlik katmanı olarak kullanıcı kaydı sırasında oluşturulan AES-128 anahtarı, bilgisayarın anakart seri numarası ile şifrelenerek karekod (QR kod) hâline dönüştürülür. Donanım değişikliği gerçekleştiğinde kullanıcı, söz konusu QR kodu kullanarak eskiden ürettiği şifreleri geri alabilmektedir.

Üçüncü katman olan sunum katmanı kullanıcı ile etkileşimi yöneten grafiksel kullanıcı arayüzünü kapsamaktadır. Giriş ve kayıt formları, ana ekran ve sanal emoji klavye bileşenleri Tkinter kütüphanesi ile hazırlanmıştır. Bunun yanı sıra fiziksel klavyenin devre dışı bırakılması ve mesaj ve onay ekranlarının olması da hem kullanıcı deneyimini zenginleştirmektedir hem de kaba kuvvet saldırıları zamanı saldırganın şifre denemeleri yapmasını engellemektedir.

Uygulamanın geliştirilmesinde; veri yönetimi, kriptografik işlemler, donanım bilgilerinin alınması, arayüzün oluşturulması ve QR kod entegrasyonu gibi farklı özelliklerin kullanılabilir olması için Tablo 3.1’ de verilen çeşitli python kütüphaneleri kullanılmıştır.

Tablo 3.1. Kullanılan kütüphaneler ve işlevleri

Kütüphaneler	Kullanım alanı
Sqlite3	Yerel veri tabanı işlemlerinde kullanılmıştır.
Cryptography	AES-128-GCM şifreleme ve PKCS7 dolgu işlemleri bu kütüphane üzerinden sağlanmıştır.
Hashlib	Kimlik doğrulama işleminin güvenliğinin artırılması için Güvenli Özet Algoritması-256 (SHA-256) tabanlı özet üretimi ile kimlik doğrulama işlemi yapılmıştır
Platform, uuid, psutil	Sistem bilgilerinin toplanması için ve donanım değişikliğinin tespiti için kullanılmıştır.
Qrcode, cv2 (OpenCv),	Karekod'un oluşturulması ve okunması için kullanılmıştır.
Tkinter	Grafiksel kullanıcı arayüzünün tasarımı için kullanılmıştır.
Emoji, random, string	Emoji destekli şifre üretim algoritmasının rastgelelik ve karakter seçimi ihtiyaçları için kullanılmıştır.
Shutil, os, csv	Dosya ve dizin yönetimi ile geçici veri saklama işlevleri için kullanılmıştır

3.2. Şifreleme Yapısı

Gelişmiş Şifreleme Standardı (AES), veri güvenliği sağlamak amacıyla geniş çapta benimsenmiş, blok şifreleme tabanlı bir simetrik şifreleme algoritmasıdır. 2001 yılında ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından Rijndael algoritmasının seçilmesiyle standartlaştırılmıştır. AES, 128-bit blok boyutunda veri işleyerek 128, 192 veya 256 bit uzunluğunda anahtarlar kullanabilir. Algoritma, şifreleme ve çözme işlemlerini belirli sayıda tur (10, 12 veya 14) üzerinden gerçekleştirir; bu turlar Alt baytlar, Satır Kaydırma, Sütun Karıştırma ve Tur Anahtarı Ekleme gibi temel işlemlerden oluşur. Güçlü matematiksel yapısı, yüksek performansı ve donanım/yazılım ortamlarına uyumluluğu sayesinde hem kamu hem de özel sektörde yaygın olarak kullanılmaktadır. Ayrıca, günümüzün kuantum öncesi kriptanaliz tekniklerine karşı dayanıklı olması, AES'in modern kriptografideki merkezi rolünü pekiştirmektedir.

Uygulamada AES anahtarı sistem bilgileri bazı işlemlerden geçer ve elde edilen bir dizi (string) üretiliyor. Bu dizi daha sonra UTF-8 formatında baytlara dönüştürülerek 16 baytlık yani 128 bitlik AES anahtarı olarak kullanılmaktadır. Bu anahtar AES-GCM modülü kullanılarak hem şifreleme işlemini hem de kimlik doğrulama işlemi için kullanılmaktadır. Şifreleme işlemi sürecinde her şifreleme sırasında 12 bayt (96 bit) uzunluğunda rastgele başlangıç vektörü (IV) üretilmektedir. Bu vektör AES-128 algoritmasının sayaç modunda şifreleme işlemini başlatır ve GHASH tabanlı kimlik doğrulama etiketi oluşturmak için kullanıyor. Kod içerisinde şifrele metodu çağırılarak algoritma tarafından üretilen parolanın bayt dizisini AES-CTR ile şifreleyerek GHASH fonksiyonu ile 16 baytlık kimlik doğrulaması etiketini hesaplıyor. Elde edilen şifrelenmiş veri ve etiket birleşimi, vektör ile birleştiriliyor ve Base64 formatına dönüştürülerek şifreli metin üretilerek veri tabanında saklanıyor.

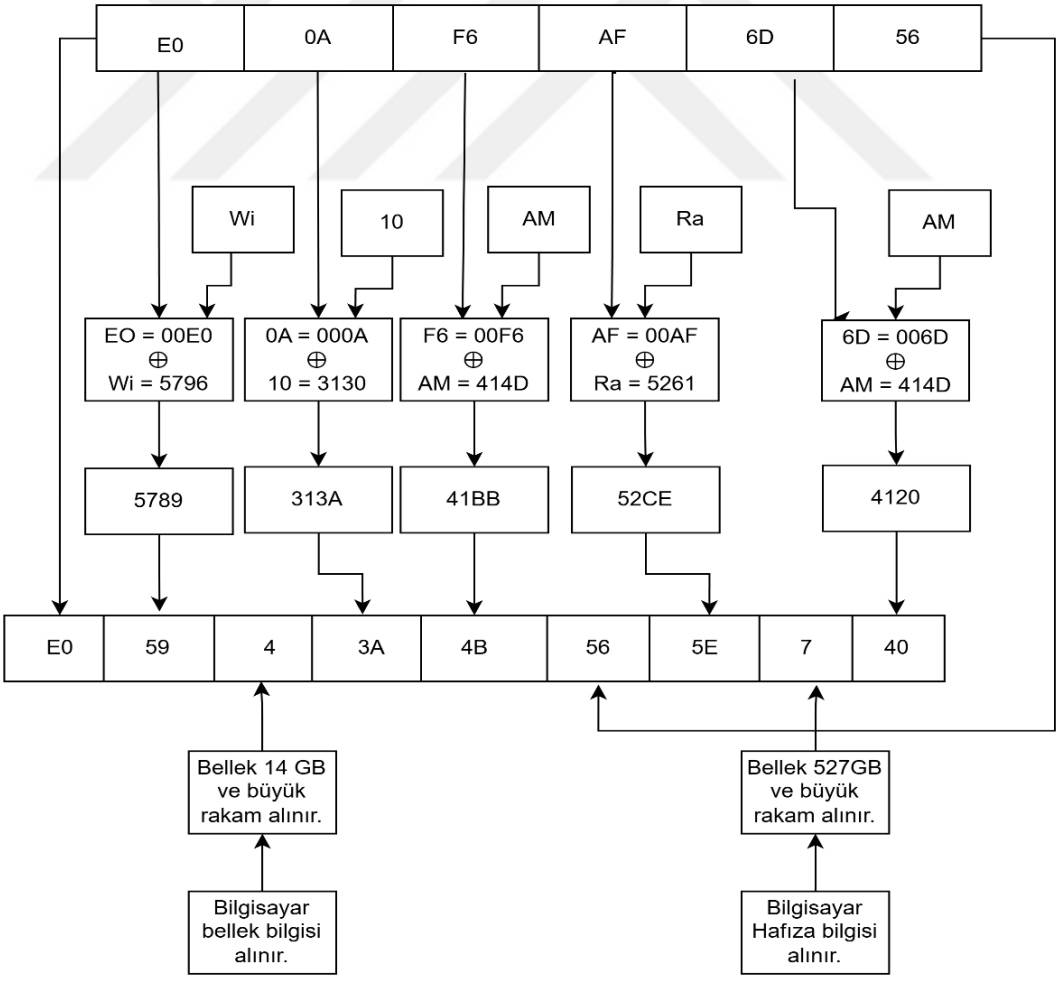
Bunun tam tersi işlem olan çözme işleminde ise kullanıcı uygulamaya giriş yaptığı zaman ilk önce Base64 formatındaki şifreli metin çözülerek ikilik veriye dönüştürülüyor. İlk 12 bayt rastgele başlangıç vektörü olarak ayırılıyor geriye kalan kısım da ise şifreli metin ile kimlik doğrulaması için eklenmiş olan etiketin birleşimi kalıyor. Sıradaki adımda ise şifre çözme metodu çağırılarak rastgele başlangıç vektörü ve şifrelenmiş veri kullanılarak GHASH tabanlı etiket ile kullanıcı doğrulama işlemi yapılıyor. Eğer etikette eşleşme olursa AES-CTR akışı tersine uygulanarak düz metin elde edilerek kullanıcının arayüzünde gösteriliyor.

3.3. Geliştirilen Anahtar Üretim Mekanizması

Kullanıcı için üretilen anahtar, kullanıcı adı kaydolduğu ya da şifresini değiştirmek istediği uygulamanın ya da sitenin adı bu algoritma ile şifrelenmektedir. AES-128 standardı, metin verisinin güvenli bir biçimde şifrelenebilmesi için 128 bit (16 bayt/karakter) uzunluğunda bir anahtar kullanımını zorunlu kılar. Anahtar oluşturma sürecinde, sistemin işletim sistemi sürümü, işlemci kimliği, bellek modülleri ve diğer donanım bileşenlerinin benzersiz tanımlayıcı bilgileri bir araya getirilerek kriptografik anahtarın türetilmesi sağlanmıştır. Bu yöntem hem anahtarın kullanıcıya özgü olmasını hem de olası tersine mühendislik saldırılarına karşı ek bir güvenlik katmanı oluşturmasını mümkün kılmaktadır.

Geliştirilen anahtar üretim mekanizması dokuz adımdan oluşmaktadır. İlk önce uygulama kullanılan ortamdan işletim sisteminin adı, işletim sisteminin sürüm numarası, CPU ismi, kullanıcı adı ve makine adı gibi bilgileri almaktadır. Adımların anlatılmasında kullanılacak örnek bilgisayar verileri aşağıda verilmiştir ve örnek üzerinden çalışma mekanizması Şekil 3.2'de gösterilmiştir.

- İşletim sistemi adı: Windows
- İşlemci ismi: AMD
- İşletim sistemi sürüm: 10.0.0.2691297
- Kullanıcı adı: RashadM
- Makine adı: AMD FAMILY
- MAC adresi: E0:0A:F6:AF:6D:56
- Bellek (RAM): 14 GB
- Hafıza – 527 GB



Şekil 3.2 Anahtar üretim mekanizmasının gerçek veri örneği

Adım 1: Anahtarın ilk iki değeri için MAC adresinin ilk parçasını yani E0 alınıyor (Anahtar: E0).

Adım 2: Önce işletim sisteminin adının ilk iki karakteri (“Wi”) alınır. ASCII tablosunda bu karakterlerin on altılık karşılıkları sırasıyla w için 0x57, i için 0x69 şeklinde belirlenir ve birleştirilerek iki baytlık 0x5769 değeri elde edilir. Ardından bu değer, MAC adresinin birinci kısmı olan 0xE0 ile, öncelikle 16 bitlik biçimde (0x00E0) hizalanarak, Tablo 3.2’de gösterildiği gibi bit düzeyinde eXclusive OR (XOR) işlemine tabi tutulur ve 0x5789 sonucu alınıyor. Buradaysa ilk ve son değer alınır sonuç olarak “59” değeri anahtar dizisine eklenir (Anahtar: E059).

Tablo 3.2 Algoritmada kullanılan eXclusive OR işlem sonuçları

16-lık değerler	2-lik değer				Seçilen değer
5769	0101	0111	0101	1001	59
00E0	0000	0000	1110	0000	
5789	0101	0111	1000	1001	

Adım 3: Bilgisayarın belleği Gb cinsinden alınır ve burada en büyük rakam alınır. Bellek 14 GB olduğu için büyük rakam 4 seçiliyor ve anahtarın sıradaki değeri olarak atanıyor. (Anahtar: E0594).

Adım 4: İşletim sisteminin sürüm numarası alınır ve sayının ilk iki basamağı tespit edilir; örnekte bu değer “10” olarak belirlenmiştir. Daha sonra, ASCII karşılıklarına göre karakter “1” için 0x31 ve karakter “0” için 0x30 değeri elde edilir. Bu iki bayttan oluşan 0x3130 verisi, MAC adresinin ikinci kısmı olan 0x0A ile bit düzeyinde XOR işlemine tabi tutulur. Elde edilen 0x313A değerinin ilk ve son baytı (“3A”) anahtara dizinine eklenir (Anahtar: E05943A).

Adım 5: Makine adının ilk iki karakteri alınır ve bu karakterlerin ASCII karşılıkları on altılık sayı değerlerine dönüştürülür. Örneğin “A” karakteri 0x41’e, “M” karakteri 0x4D’ye karşılık gelir ve birleştirilerek 0x414D değeri elde edilir. Daha sonra, MAC adresinin üçüncü parçası olan 0xF6, 16 bitlik biçimde 0x00F6 olarak hizalanır ve 0x414D değeri ile XOR işlemine Tablo 3.2’de olduğu gibi tabi tutulur. Elde edilen

sonuç 0x41BB'dir. Daha sonra değerinin ilk ve son baytı ("4B") anahtara dizinine eklenir (Anahtar: E05943A4B).

Adım 6: Mac adresinin son parçası "56" anahtar dizinine eklenir (Anahtar: E05943A4B56).

Adım 7: Kullanıcı adının ilk iki karakteri ("Ra") seçilir ve bu karakterlerin ASCII karşılıkları on altılık sayı biçimde yazılır: "R" için 0x52, "a" için 0x61; bu iki bayt birleştirilerek 0x5261 değeri elde edilir. Ardından, MAC adresinin dördüncü parçası 0xAF, 16 bitlik biçimde 0x00AF olarak hizalanır ve bit düzeyinde XOR işlemi Tablo 3.2'deki gibi uygulanır. Elde edilen 0x52CE on altılık sayı değerinin ilk baytı ("5") ve son baytı ("E") seçilerek yan yana yazılır ve "5E" değeri anahtar dizisine eklenir (Anahtar: E05943A4B565E).

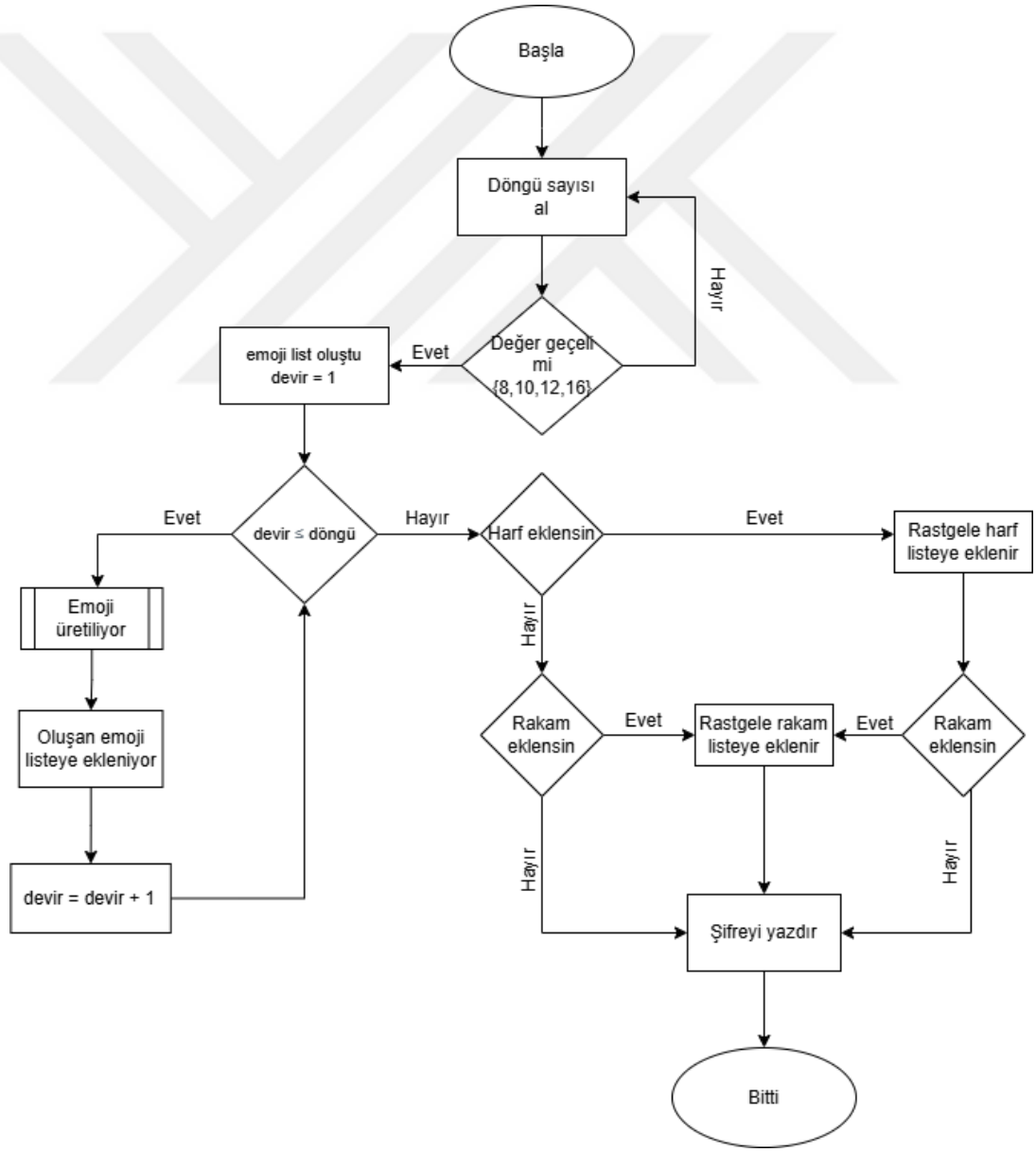
Adım 8: Bilgisayarın hafıza bilgisi alınarak en büyük değeri alınmaktadır. Verilen bilgilerde hafıza 527 GB ve en büyük değer olan 7 alınarak anahtar dizinine eklenir (Anahtar: E05943A4B565E7).

Adım 9: İşlemci isminin ilk iki karakteri alınır ve ASCII tablosundaki on altılık sayı değeri karşılıkları elde edilir. Örneğin "A" karakteri 0x41'e, "M" karakteri 0x4D'ye karşılık gelir; bu değerler birleştirilerek 0x414D sonucu elde edilir. Ardından, MAC adresinin beşinci parçası olan 0x6D, 16 bitlik biçimde 0x006D hizalanır ve XOR işlemine Tablo 3.2'de olduğu gibi tabi tutulur. Elde edilen 0x4120 on altılık sayı değerinin ilk baytı ("4") ile son baytı ("0") seçilerek yan yana yazılır; böylece "40" değeri anahtar dizisine eklenir (Anahtar: E05943A4B565E740).

Adımların tamamlanmasının ardından AES-128 şifreleme standardı için gereken 16 bayt uzunluğundaki anahtar elde edilmiş olur. Verilen örnekte bu anahtar "E05943A4B565E740" olarak belirlenmiş oluyor. Daha sonra ise bu anahtar ile şifreleme sürecine geçiliyor. Anahtar, hiçbir kalıcı depolama ortamında saklanmaksızın; kullanıcı her oturum açma işleminde sistem tarafından otomatik olarak donanım bileşenlerine ait veriler toplanarak yeniden türetilir ve aynı algoritmik adımlar izlenerek şifre çözme işlemi gerçekleştirilir.

3.4. Emoji ile Güçlendirilmiş Şifre Üretim Algoritması

Şifre oluşturmak için kullanıcının belirlediği kısıtlar doğrultusunda Şekil 3.3'te gösterilen şifre üretim algoritması geliştirilmiştir. Burada ilk önce kullanıcıdan şifre uzunluğu isteniyor kullanıcı bu veriyi girdiyi zaman kullanıcının girmiş olduğu değer kontrol edilerek bir döngü başlıyor ve her döngüde uygulama bir emoji üreterek liste içerisine ekleme yapıyor. Kullanıcıdan son olarak harf ya da rakam isteyip istemediği bilgisi alınarak nihai şifreyi oluşturuyor. Kullanıcı harf ya da rakam eklenmesini isterse şifrenin rastgele bir kısmına harf ve rakamlar da eklenmektedir.



Şekil 3.3 Emoji ile güçlendirilmiş şifre üretim algoritmasının akış şeması

Uygulamanın şifre üretim kısmında uygulama ilk önce Unicode tablosunda olan 3 tane karakter istemektedir. Bu karakterler girildikten sonra uygulama kullanıcı için özgün bir parola üretmeye hazır hale gelmektedir. Algoritmanın anlatılması için “A”, “B”, “C” olarak 3 karakter seçildiği zaman uygulama bu karakterleri 25 farklı işlemden geçirerek 5 x 5 boyutlu bir matris oluşturuyor. Bu matrisin oluşturma aşamasında toplama, çarpma, kaydırma, XOR ve mod alma gibi işlemler yapılmaktadır. İşlemlerin sonucunda algoritmanın oluşturduğu ilk matrisi Tablo 3.3’te verilmiştir.

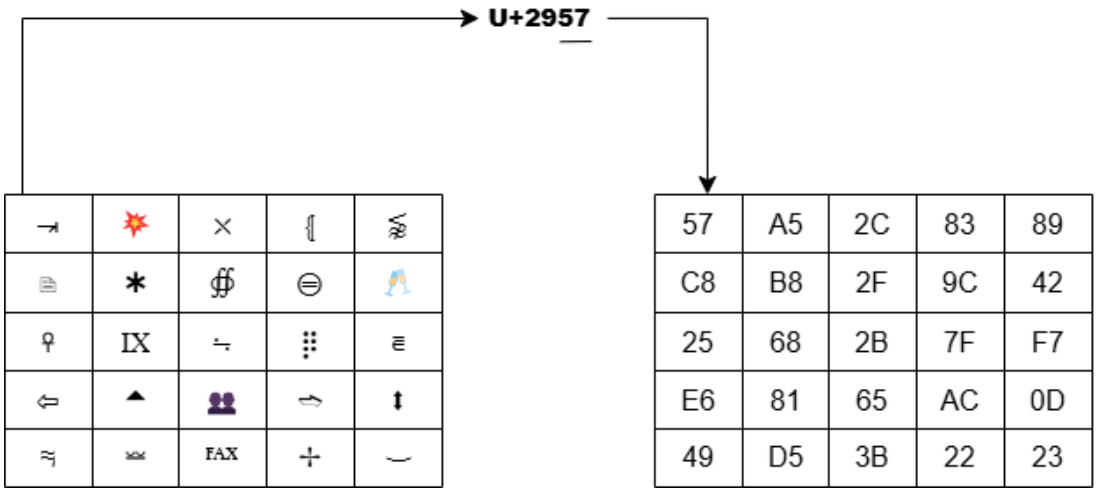
Tablo 3.3 Algoritmanın ürettiği ilk matris

03	03	0F	02	02
03	05	0A	04	0A
00	04	06	03	02
05	04	08	09	06
01	0F	01	00	0F

Üretilmiş olan ilk matrisin her ikinci baytı alınarak bit değerleri bulunarak genişletme işlemi yapılıyor bu işlemde ilk bit 1 olduğu halde beşinci bite 0 ekleniyor eğer bit 0 ise 1 eklenerek 8 bitlik bir dizin elde edilmektedir. Matrisin ilk hücresindeki değere baktığımız zaman 0011 genişletilerek 00111100 olarak genişletiliyor. Sıradaki adımda bit değerleri 16-lık sisteme dönüştürülerek “3C” değeri bulunuyor. Bu işlem matristeki tüm hücrelere uygulanarak Tablo 3.4’te verilen yeni bir matris oluşturuluyor.

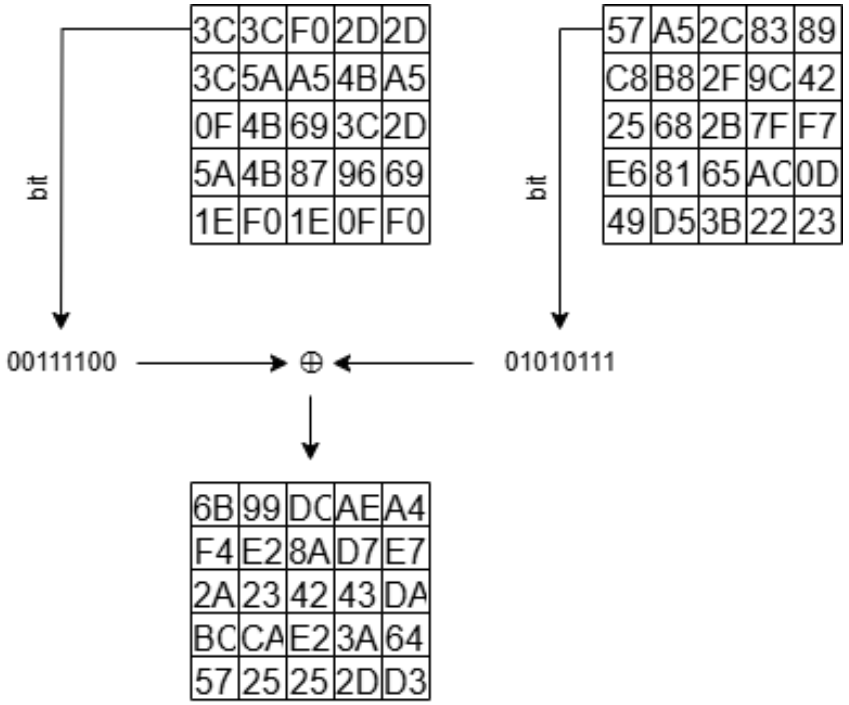
Tablo 3.4 Algoritmanın bayt matrisi

3C	3C	F0	2D	2D
3C	5A	A5	4B	A5
0F	4B	69	3C	2D
5A	4B	87	96	69
1E	F0	1E	0F	F0



Şekil 3.4 Emojilerin on altılık sayı değerine dönüşümü

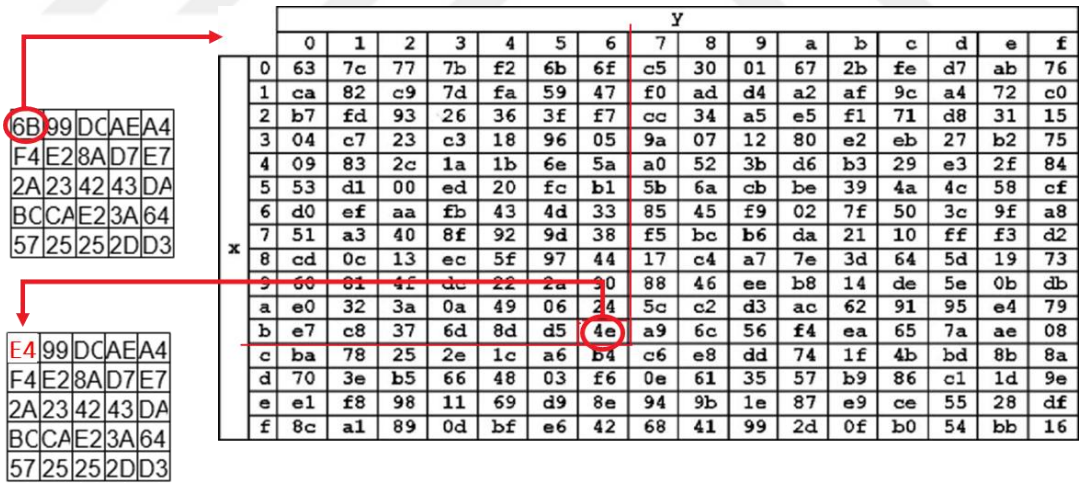
Sıradaki adımda toplam 4694 emoji ve işaretten Windows 11'in desteklemediği 487 emoji devre dışı bırakılarak emoji ve randint kütüphanesi kullanılarak Windows 11'in desteklediği 4207 emoji arasından rastgele bir şekilde 25 emoji seçilerek Şekil 3.4'te sol tarafta yer alan matris oluşturuluyor. Ardından oluşturulmuş emojilerin unicode tablosundaki 16'lık karşılıklarının son iki değeri alınarak Şekil 3.4'te sağ taraftaki yeni matris oluşturuluyor.



Şekil 3.5 Kriptografik matris güncelleme

Şekil 3.4'te üretilen matris ile Tablo 3.5'teki matris bit düzeyine dönüştürülerek hücreler arasında karşılıklı şekilde XOR işlemi yapılıyor. Elde edilen sonuçlar tekrar on altılık (16'lık) sayısal sisteme çevrilerek yeni bir matris oluşturuluyor. Bu yöntem, orijinal verinin yapısal bütünlüğünü korurken aynı zamanda kriptografik dayanıklılığı ve veri gizliliğini artırmak amacıyla yapılmıştır.

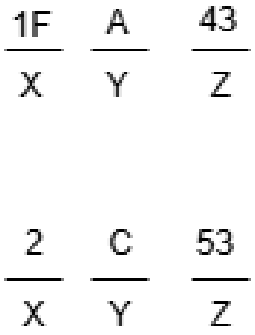
Sıradaki aşamada, Şekil 3.5'te elde edilen son matriste yer alan her bir hücre, AES yer değiştirme kutusu (S-kutu) kullanılarak yer değiştirme işleme tabi tutuluyor ve yeni bir matris oluşturulur. Örneğin, orijinal matrisin ilk hücresindeki "6" değeri, S-kutu tablosunda sütun indeksi; "B" değeri ise satır indeksi olarak kullanılıyor. Bu iki indeksin kesiştiği konumda bulunan değer, Şekil 3.6'te gösterildiği gibi yeni matristeki aynı hücreye baytların yeri değiştirilerek atanıyor. Aynı yöntem, matrisin tüm hücreleri için tekrarlanarak işlem bitiyor. Böylelikle, S-kutu tablosundaki dönüştürme işlemi sonucu elde edilen değerlerin baytları değiştirilerek, yeni matris üzerine ekleniyor. Daha sonra oluşturulmuş olan matristen rastgele bir şekilde bir hücre seçilmektedir (örneğin "BC").



Şekil 3.6 Yer değiştirme işlemi

Tüm emoji aralıkları 0x1F300 ile 1FAF8, 0x2100 ile 0x2426 ve 0x2460 ile 0x2B95 olarak bulundu. Ardından Windows 11 işletim sisteminin desteklemediği aralıklar "unsupport_emoji" olarak koda eklendi. Üretilecek olan her bir emojinin on altılık sistemde bir karşılığı var. Bu kodların ise 0x1F ve 0x2 ile başlayan iki türü bulunuyor. Uygulamanın geliştirme aşamasında emojilerin üretilmesi için emojilerin kodları 3

parçaya bölünerek işlenmiştir. Bu parçalar X, Y, Z olarak adlandırılmıştır Şekil 3.7'da örnekleri verilmiştir.



Şekil 3.7 Emojilerin on altılık sistemde kod parçaları

Bu algoritmada, Y bileşeninin seçimini gerçekleştirmek amacıyla on altılık (hexadecimal) sistemde 1'den F'ye kadar olan değerleri kapsayan bir döngü oluşturuluyor. Her döngü adımında, X parçasının belirlenmesi için rastgele bir şekilde 0 veya 1 üretilir. Üretilen değer 0 ise, ilgili döngü adımına karşılık gelen kodun başlangıç kısmı "1F" olarak sabitlenir. Eğer 0 yerine bir seçilseydi bu zaman kod 1F değil 2 ile başlardı. Z bileşeni ise Şekil 3.6'da S-kutu kullanılarak elde edilen matris içindeki seçilen hücrenin değerini ifade eder. Örnek vermek gerekirse; döngü ilk adımda Y bileşenine 1 değerini atadığında ve X bileşeni için üretilen rastgele değer 0 ise, ortaya çıkan kod "1F1BC" olarak belirlenir. Bu koda karşılık gelen bir emoji mevcutsa, söz konusu emoji listeye eklenir. Daha sonra döngü, Y bileşeni F değerini alana kadar devam eder her adımda X bileşeni için yeniden 0 veya 1 değeri üretilir ve elde edilen Z bileşeni koda ilave edilir. Döngü tamamlandığında, oluşturulan tüm kodlara karşılık gelen emojiler tek bir listede toplanır ve bu listeden rastgele bir emoji seçilir.

Sonuç olarak, kullanıcının tercihlerine veya kaydolacağı platformun parola uzunluğu gereksinimlerine (örneğin 8, 10, 12 veya 16 adımlık bir süreç) bağlı olarak algoritma, her döngü adımında bir emoji seçip birleştirerek nihai şifreyi üretmektedir.

Hazırlanmış uygulama içerisine 18 farklı platformun şifre gereksinimleri eklenmiştir. Ama bazı platformlar yalnız emoji olarak şifre kabul ederken bazı platformlar harf rakam eklenmesini talep etmektedir bazıları ise emoji ile şifre kabul etmemektedir.

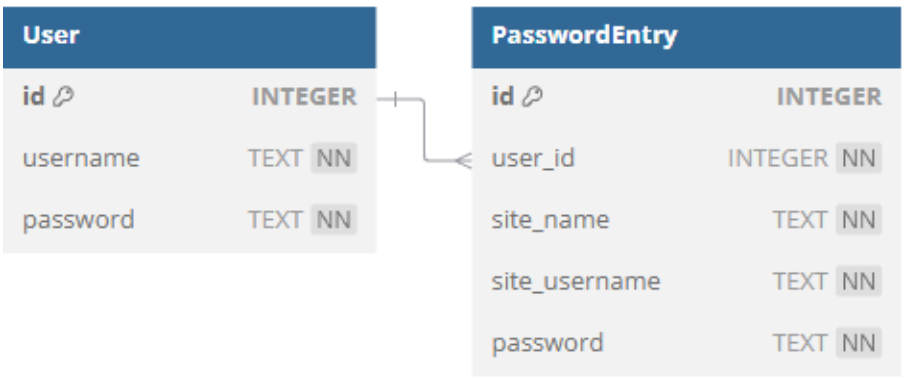
Uygulama geliştirilirken Tablo 3.5'te yer alan uygulamalar dikkate alınmış ve bu platformlar için emojiler ASCII karakterlerine otomatik olarak uygulama tarafından dönüştürülmektedir.

Tablo 3.5 Platformların emoji ile parola destekleri

Sadece emoji	Emoji, harf, rakam	Emoji ve harf	Sadece ASCII
Linkedin	Spotify	Ebay	Google
Facebook	Zoom		Outlook
Icloud	Turnitin		Steam
Github			Yahoo
Twitter (X)			Twitch
Steam			
Reddit			
Netflix			
Amazon			

3.5. Veri Tabanı Tasarımı ve Yönetimi

Bu çalışmada, kullanıcı verilerinin saklanması ve belirli verilerin karşılaştırılması amacıyla SQLite tabanlı bir veri tabanı yönetim sistemi tercih edilmiştir. SQLite, sunucusuz ve dosya tabanlı yapısı sayesinde hem kurulum açısından basitlik hem de kullanım açısından yüksek derecede esneklik sunmaktadır. Bununla birlikte, Python programlama dili ile doğal ve doğrudan entegrasyon yeteneğine sahip olması, SQLite'ı bu proje kapsamında veri işleme ve yönetim süreçleri için uygun bir çözüm haline getirmiştir.



Şekil 3.8 Veri tabanı tasarımı

Veri tabanı “users” ve “passwords” olmak üzere iki tablodan oluşmaktadır (Şekil 3.8). “Users” tablosu kayıt esnasında her kullanıcıya birbirinden farklı kimlik numarası atıyor ve kullanıcı uygulamaya kaydolurken girdiyi kullanıcı adı ve şifresini özet fonksiyonuna tabi tutularak bu tabloya ekliyor. “Users” tablosundaki kullanıcı adı ve parola SHA-256 ile özetlenerek veri tabanına eklenmektedir.

“Passwords” tablosunda ise kullanıcının teyit edilmesi için “Users” tablosundaki kimlik numarasını almaktadır. Ardından o kullanıcıya ait olan bilgileri arayüze yansıtmaktadır. Bu bilgiler ise “Passwords” tablosundaki site ismi, platforma kaydolduğu kullanıcı adı ve uygulamanın ürettiği parola kaydedilmektedir. Uygulamaya kaydolmuş bir kullanıcı istediği kadar şifre üretebilir ve veri tabanına kaydedilir.

3.6. Kimlik Doğrulama ve Güvenlik Önlemleri

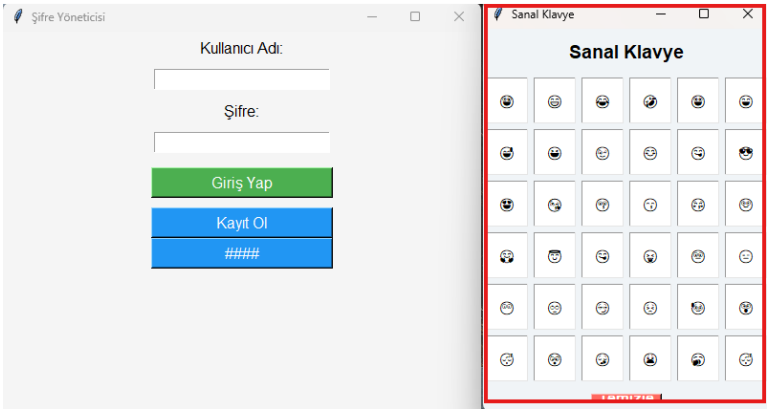
Bu projede, kullanıcı kimliği doğrulama ve güvenliği için bir dizi önlem entegre edilmiştir. Sisteme erişim, kullanıcı adı ve şifre doğrulaması ile sınırlanmıştır. Şifreler, veri tabanında düz metin olarak saklanmak yerine, geri dönüştürülemez bir biçimde korunmak amacıyla SHA-256 özet algoritmasıyla özetlenerek kaydedilmektedir. Bu yöntem, veri sızıntılarının önlenmesi ve şifrelerin güvenliğinin sağlanması açısından kritik bir güvenlik önlemi sunmaktadır.

Uygulamanın şifreleme algoritması seçimi zamanı Blowfish, RSA ve AES arasında seçim yapabilmek için literatür taraması ve uygulama hazırlık aşamasında başı testlere tabi tutulmuştur. Blowfish algoritması simetrik şifreleme algoritmasıdır. Bu şifreleme algoritması 64 bitlik bloklar kullanarak şifreleme yapmaktadır. Blowfish algoritması şifreleme ve şifre çözme işleminin hızlı bir şekilde donanımı kullanarak yapmaktadır. İki taraf arasında iletişim çok gizli bir şekilde saklanabilmesi de bu algoritmanın güvenilirliğini göstermektedir. Ama bu avantajlarının yanı sıra dezavantajları da bulunmaktadır. Bu dezavantajlardan birisi anahtarın güvenli bir şekilde saklamasının zorluğudur.

RSA şifreleme algoritması iki farklı anahtar ile şifreleme ve çözme işlemi yapmaktadır. Bu şifreleme algoritması asimetrik şifreleme algoritmasıdır. Şifreleme ve çözme işleminde özel anahtar ve açık anahtar ile bu işlemi yapmaktadır. Bu algoritmanın da avantajları ve dezavantajları var. Bunlara baktığımızda RSA algoritması güvenli bir algoritma olarak tanımlanmaktadır. Kullanıcılar veri iletimi esnasında bu algoritma güvenli bir şekilde kullanılmaktadır. Genellikle güvenli olarak bilindiği için bu algoritma internet bankacılığında ve e-ticaret uygulamalarında yaygın olarak kullanılmaktadır. Dezavantajları ise bu algoritmanın diğer algoritmalar gibi hızlı çalışmaması, yan kanal saldırılarına karşı güvenlik açığının olması yani saldırgan radyasyon, güç tüketimi, zaman verileri, işlemci ve ram bilgileri gibi veriler kullanarak özel anahtarı bula bilmesi için ipuçları bulabilmektedir [54]. Bu algoritmada da özel anahtarın güvenli bir şekilde saklanması bazı durumlarda zorluklar yaşatmaktadır.

Ek olarak, bazı hassas veriler AES-128 şifreleme algoritması (GCM modu) kullanılarak şifrelenmektedir. Bu simetrik şifreleme tekniği, verilerin gizliliği ve bütünlüğü konusunda ek bir güvenlik katmanı sağlayarak, sistemin genel güvenlik düzeyini artırmaktadır. Kullanıcı doğrulama süreci, girilen parolanın aynı algoritmalarla işlenmesi ve veri tabanındaki karşılığıyla karşılaştırılması esasına dayanmakta, yalnızca doğru eşleşmelerde sisteme erişim izni verilmektedir.

Sistemde, tuş kaydedici gibi kötü niyetli yazılımlara karşı alınan bir diğer önlem ise sanal klavye ara yüzüdür (Şekil 3.9). Bu sayede kullanıcılar, fiziksel klavye kullanmadan parola girişi gerçekleştirebilmektedir, bu da şifrelerin üçüncü şahıslar tarafından ele geçirilme riskini önemli ölçüde azaltmaktadır.



Şekil 3.9 Sanal Klavye

Ayrıca, donanımsal güvenlik denetimi de uygulamaya dahil edilmiştir. Kullanıcının cihazında herhangi bir donanımsal değişiklik tespit edildiğinde ve bu değişiklik, kullanıcı tarafından QR kod aracılığıyla doğrulanmadığında, veri tabanı güvenlik amacıyla otomatik olarak silinmektedir. Ardından, veriler şifrelenmiş bir biçimde kullanıcının cihazına aktarılmaktadır. Bu yaklaşım, cihaz manipülasyonlarına karşı kritik verilerin korunmasını sağlamayı hedeflemektedir.

4. UYGULAMA TEST SONUÇLARI

Algoritmanın üretmiş olduğu şifrelerin güvenli ve hızlı bir şekilde şifrelendiğinin test edilmesi amacıyla farklı şifreleme algoritmaları ile de uygulama hazırlanmıştır. Hem simetrik hem de asimetrik algoritmalar test edilebilmesi için bir asimetrik şifreleme algoritması olan RSA algoritması ve iki tane ise simetrik şifreleme algoritması olan AES ve Blowfish seçilmiştir. Bu algoritmaların seçilmesinin bir diğer nedeni yapılan literatür taramasında şifre yöneticileri için kullanılan algoritmalar ve [55], [56], [57] çalışmalarında tavsiye edilen algoritmalar olmasıdır. İlk önce uygulama AES-128 şifreleme algoritması kullanılarak geliştirilmiş ve tüm testler yapılmıştır. Daha sonra şifreleme algoritması Blowfish ve RSA ile değiştirilerek aynı testler yapılmıştır.

İlk önce bu algoritmaların büyük ve küçük harf, rakam ve emoji içeren 12 karakterlik şifreyi güvenlik saklamak için şifreleme işlemleri için geçen süresi hesaplanmıştır. Tablo 4.1'de görüldüğü gibi AES-128 simetrik şifreleme algoritması RSA ve Blowfish algoritmalarına kıyasla daha hızlı şifreleme ve çözme işlemi yapmaktadır. Tablo 4.1'deki süreler uygulama çalışırken şifreleme ve şifre çözme sürelerini göstermektedir. Uygulama çalışırken bu sürelerin hesaplanması uygulamanın kendisinin de belleği ve işlemciyi yorduğu için süreyi uzatabilmektedir. Her üç algoritmanın da şifreleme ve şifre çözme işlemi aynı şartlarda hesaplanmıştır. Yapılan test sonuçları gösteriyor ki en hızlı algoritma AES şifreleme algoritması olmuştur.

Tablo 4.1 Algoritmaların şifreleme süresi

Algoritma	Şifreleme (saniye)	Şifre Çözme (saniye)	Toplam (saniye)
AES	1.74	2.23	3.96
RSA	2.44	2.95	5.39
Blowfish	1.81	3.21	5.02

4.1. Algoritma için NIST SP 800-22 Test Sonuçları

Süre ölçümünden sonra algoritmanın üretmiş olduğu şifreler NIST SP 800-22 ile test edilmiştir. Bu test algoritmanın üretmiş olduğu şifrelerin bit bazında rastgele olup olmadığını test etmek amacıyla yapılmıştır. NIST SP 800-22 içerisinde yer alan Frekans, Blok Frekansı, Kümülatif toplamalar, Koşu, Matris sıra, Hızlı Fourier Dönüşümü, Doğrusal Karmaşıklık ve Seri (Alt Dizi Sıklığı) testler ile uygulama tarafından üretilmiş farklı şifreler test edilmiş ve sonuçları Tablo 4.2'de verilmiştir.

Tablo 4.2 NIST SP 800-22 test sonuçları

Testler	Sonuçlar
Frekans	78/100
Blok Frekans	70/100
Kümülatif Toplamalar	78/100
Koşu	82/100
Matris Sıra	100/100
Hızlı Fourier Dönüşümü (FFT)	89/100
Doğrusal Karmaşıklık	96/100
Seri (Alt Dizi Sıklığı)	76/100

Frekans Testi: İlk test olan frekans testi algoritmanın üretmiş olduğu şifrelerin bit bazında analizini yapmaktadır. Burada bitlerin yani 0 ve 1'lerin birbirine eşit olup olmadığını kontrol etmektedir. Yani test n uzunluğundaki bit diziliminde 1 sayısının n / 2'ye yakın olup olmadığını test eder. Test sonucunda frekans testi 100 kez yapılmış ve 100 testin 78'inde bitlerin sayıları birbirine neredeyse eşit olarak testten geçmiştir.

Blok Frekans Testi: Blok frekans testinde ise örnek olarak bit dizinlerini 100'lük bloklara ayırarak her bloğun içerisindeki 1'lerin oranını hesaplayarak tüm blokların oranları bir birisine benzer mi? diye kontrol etmektedir. Bu testin sonucunda 100 testin 70'i tam başarılı şekilde geçmiştir.

Kümülatif Toplamalar Testi: Kümülatif toplama testinde ise üretilmiş şifrenin bitlerinde 0 ve 1'lerin dağılımında aşırı sapma (bias) var mı? diye kontrol etmektedir.

Her 1 için +1, her 0 için ise -1 eklenir. Bit dizininin sonuna kadar devam edecek bir şekilde yürüyüş oluşturulmakta ve burada denge var mı? yoksa hızlı bir sık sık eksi ve artı ya inip çıkmalar oluyor mu? diye kontrol edilmektedir.

Koşu Testi: Sıradaki test olan koşu (runs) testinde ise 0 ile 1'lerin arka arkaya gelip gelmediğini kontrol etmektedir. Örneğin sık sık "0000", "1111" bitleri arka arkaya gelip gelmediğini kontrol etmektedir. Bu test sonucunda algoritmanın test sonucunda 100 testin 82'si başarılı bir şekilde geçmiştir.

Matris Sıra Testi: Matris (Rank) testinde ise bit dizininden matris oluşturularak doğrusal bağımlılığı test edilir. Rank Testi, bit dizisinden oluşturulan matrislerdeki doğrusal bağımsızlığı ölçerek dizide yapısal veya tekrar eden desenler olup olmadığını tespit eder. Amaç, dizinin rastgele olup olmadığını anlamak için matrislerin sıralarının (rank) beklenen değerlere ne kadar yakın olduğunu analiz etmektir. Bu testte 100 kez tekrarlandı ve sonuçta 100 testte başarılı bir şekilde tamamlandı.

Hızlı Fourier Dönüşümü (FFT) Testi: Bit dizininin tekrarlanan bit kombinasyonlarının olup olmadığını test etmektedir. Bu testin sonucunda 89'u başarılı bir şekilde geçmiştir.

Doğrusal Karmaşıklık Testi: Bir bit dizisini üretebilecek en kısa lineer geri beslemeli kaydırma kaydının (LFSR) uzunluğunu belirleyerek dizinin tahmin edilebilirliğini ölçer. Amaç, rastgele bir dizinin yüksek yapısal karmaşıklığa sahip olup olmadığını kontrol ederek, kolayca üretilebilecek veya tahmin edilebilecek dizileri tespit etmektedir. Bu testin sonucunda da 100 testten 96'sı başarılı bir şekilde geçmiştir.

Seri Test: Bir bit dizisinde belirli uzunluktaki alt dizilerin (örneğin 00, 01, 10, 11) ne sıklıkta tekrarlandığını analiz ederek desen tekrarlarını kontrol eder. Amaç, tüm olası alt dizilerin eşit olasılıkla ortaya çıkıp çıkmadığını test ederek dizinin istatistiksel rastgeleliğini değerlendirmektir. Bu testten de 76'sı başarılı bir şekilde tamamlanmıştır.

Tablo 4.3'te gösterildiği gibi tüm testler bir kez yapıldığında hepsi için p değeri hesaplanmıştır. Test sonuçlarının başarılı olması için aldığı p değerleri 0.01'den yüksek olmalıdır. Uygulamanın üretmiş olduğu şifreler ile yapılan testlerin p değerlerine göre sistem başarılı olmuştur.

Tablo 4.3 NIST SP 800-22 test başarı oranları

Testler	Değerler (P_değerleri)	Sonuçlar
Frekans	0.114107	Başarılı
Blok Frekans	0.013115	Başarılı
Kümülatif Toplamalar	0.125771	Başarılı
Koşu	0.503797	Başarılı
Matris Sıra	0.587007	Başarılı
Hızlı Fourier Dönüşümü (FFT)	0.358795	Başarılı
Doğrusal Karmaşıklık	0.945039	Başarılı
Seri (Alt Dizi Sıklığı)	0.031761	Başarılı

4.2. Entropi Test Sonuçları

Uygulamanın üretmiş olduğu 12 karakter uzunluğundaki emojilerden oluşan şifreler ile 12 karakterli günlük kullanılan büyük, küçük ve rakamlardan oluşan şifrelerin entropileri hesaplanmıştır. Bu testin amacı sayı ya da parola üreticilerinin ne kadar rastgele ya da ne kadar ön görülemez olduğunu ölçmek için yapılır. Bu test sonucunda entropi bit değeri yüksek olan şifrelerin kaba kuvvet saldırılarına karşı daha dayanıklıdır. Shannon entropisi Denklem (4.1) ile hesaplanmaktadır.

$$H = -\sum_{i=1}^{n} p_i log_2 p_i \tag{4.1}$$

Bu denklemi kullanarak 12 karakterlik sadece emoji şifresi, büyük/küçük harf ve rakamdan oluşan şifre ve emoji, harf ve rakamdan oluşan şifrelerin entropisi hesaplandı. İçeriğinde harf olan şifreler 1 büyük harf içermektedir (Tablo 4.4). Emojiler ise Windows 11'in desteklediği 4207 emoji ile üretilmiştir.

Tablo 4.4 Şifre türlerine göre entropi sonuçları

Şifre türleri	Şifreler	Entropi bit	Shannon bit
Emoji (12 emoji)	⊃∈✱⁖┬♡▽❋⁞□▵↜🐊	144.5 bit	43.0 bit
Emoji, harf ve rakam (1 büyük, 1 küçük harf, 1 rakam ve 9 emoji)	w😊🈂4😾🏪⇌⑹🐊Z⋞	131.5 bit	43.0 bit
Harf ve rakam (1 büyük, 10 küçük harf ve 1 rakam)	7gczhkMwjhpj	71.45 bit	39.0 bit

Bu sonuçlara baktığımız zaman emoji ya da emoji, harf ve rakam kombinasyonları daha güvenli olarak gözüküyor. Yüksek güvenlik için harf ve rakam diğerlerinden daha zayıf olarak gözükmektedir. Üretilen parola 112 bitten az olmamalı ve üretilen şifre salt (tuz) işlemi yapılarak depolanmalıdır [58]. Bu sebepten uygulama üretilirken salt işlemi de uygulanarak şifre güvenli şekilde saklanmaktadır. Tablo 4.4'te görüldüğü gibi sadece emojilerden oluşmuş şifrelerin entropi değeri daha yüksektir. Hibrit şifrelerin ise entropi değerleri emoji sayısı azaldıkça entropi değeri de azalmaktadır. Entropi değerlerinde sadece emojiden ibaret aynı karakter uzunluğundaki sadece emoji parolalarının entropi bit değeri yüksek ve tahmin edilmesinin zor olduğu gözüküyor ama emoji ve emoji harf kombinasyonunda Shannon bit değerleri aynı olarak görünüyor. Sadece harf ve rakam kombinasyonunda ise bit değeri diğerlerinden az olduğu Tablo 4.4'te verilmiştir. Tabloda gösterilen harf ve rakamdan ibaret şifre Avast'ın şifre üretim uygulaması ile diğer şifreler ise hazırlanmış olan algoritma ile üretilmiştir.

4.3. Kaba Kuvvet Saldırısı Testi

Algoritma ile üretilmiş şifrelerin kaba kuvvet saldırılarına karşı ne kadar dayanıklı olduğu test edilmiştir. Bu test 12 tane RTX – 4090 ekran kartı kullanılarak üretilmiş şifrenin bulunma süreleri hesaplanmıştır. Şifrelerin kaba kuvvet saldırıları ile bulunma süreleri Tablo 4.5'te gösterilmiştir. Emoji ile oluşturulmuş şifrelerin, klasik karakter

setlerine kıyasla çok uzun kırma sürelerine sahip olduğu görünmektedir. Örneğin 8 karaktere sahip emoji şifresi için $1{,}4\times10^{15}$ yıl hesaplanmıştır. Bu ise pratikte imkansız olarak gözükmektedir. Emoji kullanımı, hem karakter çeşitliliğini (N = 4207) hem de kullanıcı deneyimini zenginleştirirken güvenliği katbekat artırıyor. Geleneksel harf, rakam veya sembol setleriyle aynı uzunlukta şifreler bile daha kolay kırılabilirken, emojiyle aynı uzunlukta bir şifrenin kaba kuvvet saldırısı ile kırılması çok daha zor hale geldiği gözüküyor. Bunun yanı sıra sadece kullanıcıların bir tip karakter kullanması da şifrelerini daha sonra hatırlayabilmelerini kolaylaştırmaktadır.

Tablo 4.5 Kaba kuvvet saldırısı ile şifre bulma süreleri

	8 karakter	10 karakter	12 karakter	16 karakter
Rakam	45 saniye	1 saat	5 gün	140 yıl
Küçük harf	1 gün	2 yıl	1000 yıl	6.26×10^{8} yıl
Büyük ve küçük harf	280 gün	2 bin yıl	5.61×10^{6} yıl	4.10×10^{13} yıl
Harf ve rakam	3 yıl	12 bin yıl	4.63×10^{7} yıl	6.85×10^{14} yıl
Büyük harf, küçük harf ve rakam	87 yıl	7×10^{5} yıl	6.83×10^{9} yıl	5.34×10^{17} yıl
Emoji	1.4×10^{15} yıl	2.49×10^{22} yıl	4.41×10^{29} yıl	1.38×10^{44} yıl

4.4. Üretilen Şifrelerin Dayanıklılığı

Geliştirilen algoritma aracılığıyla, 2 karakterden başlayarak 15 karaktere kadar farklı uzunluklarda emoji tabanlı şifre kombinasyonları üretilmiştir. Elde edilen bu kombinasyonların her biri için entropi değerleri hesaplanmış ve ilgili kombinasyonların uygulama tarafından oluşturulma süreleri tespit edilerek Tablo 4.6'da sunulmuştur.

Tablo 4.6 Emoji tabanlı şifrelerin entropi ve üretim süresi analizi

Emoji	Uzunluk	Şifre türü	Entropi değerleri	Üretim süreleri (Milisaniye)	Ortalama süreleri (Milisaniye)
❼	1	Emoji	13	2.2	2.2
👌	1	Emoji	13	1.8	
⩛	1	Emoji	13	1.9	
◪	1	Emoji	13	2.5	
✹	1	Emoji	13	2.0	
-- 🚪	2	Emoji	25	4.0	5.5
📷🡐	2	Emoji	25	3.1	
∈⁞	2	Emoji	25	7.8	
🎧◺	2	Emoji	25	6.2	
✒️▻	2	Emoji	25	6.5	
∑❄🧘	3	Emoji	37	6.6	6.5
‿👓⇪	3	Emoji	37	3.5	
🚰— ˪	3	Emoji	37	7.0	
➞☿💬	3	Emoji	37	7.8	
⇂↘⁖	3	Emoji	37	7.9	
⎚ℍb 🔮□	4	Emoji	49	5.9	8.4
⬛〉≅ⓤ	4	Emoji	49	9.3	
⍭📲♮😈	4	Emoji	49	8.9	
🏰♦♪🔰	4	Emoji	49	9.6	
≠①⊸ⓤ	4	Emoji	49	8.3	
🚩🐿️🚮⩛🚱	5	Emoji	61	8.5	7.8
⍞▫⎢ ▢◻	5	Emoji	61	4.6	
⩛🧱😋ϕ◇	5	Emoji	61	7.5	
☌⑳🖃⧫	5	Emoji	61	9.7	
≇⍭♜⎢ ⅄	5	Emoji	61	8.8	
⣿👽:}🥶🕶️	6	Emoji	73	9.7	8.8
🗺▢⊊⑰ʃ▬	6	Emoji	73	8.6	
ʃ▬⇔💍≋⍭	6	Emoji	73	8.5	
⥱✉☞🔑⁖👴①	6	Emoji	73	9.6	
⊁ω🥪🍦⍭🍔	6	Emoji	73	7.6	
🔎⚔🎬⁖=:⁖▫	7	Emoji	85	8.1	8.4
③15.ᔑ↬🤘⇄🧈	7	Emoji	85	9.8	
⌴🔋🍆⍿🎺†	7	Emoji	85	8.7	
↘🕹️👂◻✙🚁	7	Emoji	85	8.2	
🥎⟨😂↑□🔒◻	7	Emoji	85	7.5	
💂⍿⍈⍈⋄ʅ”	8	Emoji	97	8.3	9.2
😚†🕳⊁☝🕹⎚	8	Emoji	97	7.3	

😝🕐🕳☛🤩📑┤	8	Emoji	97	10.9	
≅➽(4)🏭⏮⇐🚷◣	8	Emoji	97	9.2	
⑮🙏❓↘🔃▽⬟🤡	8	Emoji	97	10.6	
]🔟🦷🌱🛌↞🥜::	9	Emoji	109	9.5	10.6
🫀└⌐🍗✕)ᓚ2.⋊	9	Emoji	109	9.1	
⏸Ⓦ🐅🦡🈂🧘♌⛑🍎	9	Emoji	109	11.1	
::🐅ω◡🌑.🍺ʕ↰	9	Emoji	109	11.9	
⣿⑩⓪🟦🪱::🐮ʕP	9	Emoji	109	11.8	
⟳♫⊣🚓◊❍(h)⊡❷↙	10	Emoji	121	10.6	11.1
⇆→⠿≎♓⍟⌥🏇🦊ᓚ	10	Emoji	121	11.8	
◂🕶╳≦❗⊒∫∫vii🏘┛	10	Emoji	121	10.4	
⊭☦▶:☒ϒ🏦+🍊⌄	10	Emoji	121	11.7	
🈂🔶⧗ㅋ▨Ⓝ⇤⏱ᔕ♪≫	10	Emoji	121	11.2	
🦖.≼🦊⠿:•⊶ש🗿a…ш	11	Emoji	133	10.5	11.2
⅑❒⑧≧🚴📠↖▲♂〉🚣	11	Emoji	133	10.7	
🈸🏓❯🧃✻☆🦡⑭≧↘▣	11	Emoji	133	11.2	
□▢⋈≤🚲:🌈⩾🧯😁🪒	11	Emoji	133	10.7	
\🎆└≼⧧🏊+♪✪⇒↠	11	Emoji	133	13.7	
🖋➥🕮🐡⇄🚮⭘🚰✈≏i☼	12	Emoji	145	10.9	11.7
🌈🟡🌐ᘐ𝟎𝟎𝟎☿▀⌐🐰↖♍	12	Emoji	145	12.4	
⠿🗁↩Ö⊭✻♠👂⠿◗卌Ш	12	Emoji	145	12.8	
🔗∆❶☆¬⊐ᕗ∫✚🧅🔍☆	12	Emoji	145	12.0	
❗➢⏣〉≦≪∪❼🕳┬⋮⩾	12	Emoji	145	10.7	
🧠⇢⇐🔃˙🍱😅✷⑨⑹ⓔ׀⛨	13	Emoji	157	12.3	12.9
▯☆ᖘ⎹⊩≒ᛝ🏷🌈⇀∴ℰ🛦	13	Emoji	157	13.8	
∴🕹◣🐬⛪↾┓😇ஸ꜀ᅮ➉	13	Emoji	157	11.6	
⧈☿⣿≤⁻🕑🍾◻⧫⋮➦✹+	13	Emoji	157	13.9	
8.]⌘⍜∩🚋⊳ʘ⌐◇△🌔↾	13	Emoji	157	13.0	
😳¨④👑🦹◦⌐✷↧⑪Ⓚ⊓💋🚷	14	Emoji	169	13.7	13.1
∅˙✙⊢⅊ᾒ❑🟧◻↻⊞⇄🍐✠	14	Emoji	169	10.7	
✷⊢ㅅ😊🧯○⇳⑮┬↣ᙢ🐮▽⩾	14	Emoji	169	12.9	
🏮🌞■∪(j)□🤠◎🧯≲🧘(x)⬎┘	14	Emoji	169	14.5	
↙🚨⁝∵⊢⋈⓵⚑☝←🩺⇦🍉🌄	14	Emoji	169	13.8	
_[🎆↭🕑┘🏞♪ⓦⓖ┼e☀ς☾	15	Emoji	181	14.7	14.4
⋐⠿🦉⎣╳🍩ᯤ🖤⠿🖫⇨☑☼⁝❦	15	Emoji	181	13.3	
⋮❀🄿.🦶:╕(t)~❸╾🤳👕⇂┽	15	Emoji	181	15.4	
╔↘ᗅ⋮↾🗑🚣🚋⊜\🍾🦸ↄ⓲ㄴ	15	Emoji	181	15.4	
┘↕⇆↓❼%→☁⛉(a)↦Ƿ≠◑💔	15	Emoji	181	13.4	

Şifre uzunluğundaki artışla birlikte entropi değerlerinin de düzenli bir şekilde arttığı gözlenmektedir. Örneğin, 1 karakterden oluşan emoji şifrelerinin entropi değeri ortalama 13 bit iken, 15 karakterden oluşan şifrelerde bu değer yaklaşık 181 bit'e ulaşmaktadır. Bu durum, şifre güvenliğinin karakter sayısına bağlı olarak doğrusal biçimde arttığını göstermektedir. Bu artış, teorik olarak beklenen bilgi karmaşıklığı artışıyla tutarlıdır.

Yüksek entropi değerleri genellikle daha uzun üretim süreleri ile ilişkilendirilse de bu ilişki her zaman doğrusal değildir. Örneğin, entropisi yüksek olan bazı kombinasyonlar daha kısa sürede üretilebilmiştir. Bu durum, algoritmanın içsel verimliliği kadar, emoji karakterlerinin sisteme işlenme süresi gibi dışsal faktörlerin de önemli rol oynadığını göstermektedir.

Tablo 4.6'da ve Tablo 4.7'de şifre uzunluğu arttıkça entropi değerlerinin paralel olarak arttığı gözlemlenmektedir. Yalnızca emoji içeren şifrelerde entropi değerleri 1 karakter için yaklaşık 13 bit'ten başlamakta ve 15 karakterde 181 bit'e kadar ulaşmaktadır. Buna karşılık, emoji, harf ve rakam içeren karma şifrelerde entropi değerleri 8 karakterde 69–75 bit arasında değişiklik göstermektedir. Karakter uzunluğu 15 olan parolalarda ise 150–151 bit seviyesinde olduğu gözlemlenmiştir. Bu durum, karakter kümesinin genişlemesinin entropiyi olumlu yönde etkilediğini, ancak sadece emojilerle oluşturulan uzun şifrelerin daha yüksek güvenlik düzeyi sunabileceğini gösterilmektedir.

Tablo 4.7 Karma şifrelerin entropi sonuçları

Şifre	Uzunluk	Şifre türü	Entropi (bit)
⧹d↢S⧽🟥⁄2	8	Emoji, küçük ve büyük harf, rakam	75
5🏰tD🥣l↦↹	8	Emoji, küçük ve büyük harf, rakam	69
h⊥🖫R🤩ꕥ🐣8⇀	10	Emoji, küçük ve büyük harf, rakam	99
🚻⌓V🎙d1t◈J🧱	10	Emoji, küçük ve büyük harf, rakam	87
⋙6R▀▄l⓻🤷⊊A✊🫐k	12	Emoji, küçük ve büyük harf, rakam	111
3w✹⍤(a)⏀💉⤓==🚭H9	12	Emoji, küçük ve büyük harf, rakam	115
⚔⚌9🕯8🥈jU⩛p┌🚹⑼H	14	Emoji, küçük ve büyük harf, rakam	126
⁚g┣N⣿7👜❑⊑◍△⚭2┣	14	Emoji, küçük ve büyük harf, rakam	139
ᵇ₅4⑰9viin⦚🤷‍♀️♒(x)ϡ|⊟◺⟲	15	Emoji, küçük ve büyük harf, rakam	151
✶⊥🏙♿▨6◺▤⊏yj6EE↻	15	Emoji, küçük ve büyük harf, rakam	150

Tablo 4.8'de yer alan şifreler, yalnızca küçük harf, büyük harf ve rakamlardan oluşan klasik şifrelerdir. Tabloda yer alan şifreler Avast'ın şifre üretim uygulaması tarafından oluşturulmuştur. Şifre uzunlukları 8 ile 15 karakter arasında değişmekte olup, entropi değerleri ise 39 bit ile 84 bit arasında sınırlı kalmaktadır. Aynı uzunluktaki şifrelerin entropi düzeylerinde gözle görülür farklılıklar bulunmakta, bu da şifredeki karakter çeşitliliği ve dağılımının bilgi yoğunluğu üzerinde etkili olduğunu göstermektedir. Özellikle 14–15 karakterlik uzunlukta dahi bazı şifrelerin entropi değerlerinin 70 bitin altında kalması, bu karakter kümesinin yüksek güvenlik düzeyine ulaşmakta yetersiz olabileceğini ortaya koymaktadır.

Tablo 4.8 Harf ve rakam şifrelerin entropi sonuçları

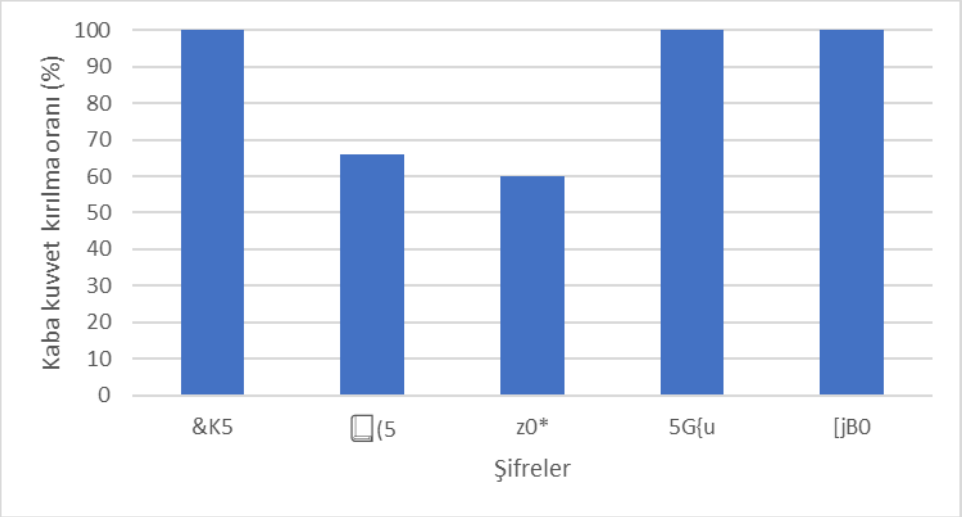
Şifre	Uzunluk	Şifre türü	Entropi (bit)
w3C95TPg	8	Küçük, büyük harf ve rakam	39
Qyoo66lM	8	Küçük, büyük harf ve rakam	41
dKFX5AX381	10	Küçük, büyük harf ve rakam	48
7vbMga9Exv	10	Küçük, büyük harf ve rakam	53
rBpmg5zWOizF	12	Küçük, büyük harf ve rakam	67
BjKiXw4yVdew	12	Küçük, büyük harf ve rakam	67
R63G3qHQ6DZor3	14	Küçük, büyük harf ve rakam	68
DjOC05bGE6VcQH	14	Küçük, büyük harf ve rakam	73
Vg79d4F29383kr5	15	Küçük, büyük harf ve rakam	65
tI3SwHZluksJhng	15	Küçük, büyük harf ve rakam	84

Karma şifreler ile yalnızca emoji içeren şifreler karşılaştırıldığında, Tablo 4.8'de yer alan klasik şifrelerin entropi değerlerinin belirgin biçimde daha düşük olduğu gözlemlenmektedir. Örneğin, 15 karakterli karma şifrelerde entropi değerleri 150 bit düzeyine ulaşırken, yalnızca harf ve rakam içeren 15 karakterli şifrelerde entropi en fazla 84 bit olarak ölçülmüştür. Bu sonuç, karakter kümesinin çeşitliliği arttıkça şifre güvenliğinin (entropisinin) anlamlı biçimde yükseldiğini göstermektedir dolayısıyla daha geniş karakter kümesi kullanımının kriptografik güvenlik açısından kritik olduğunu ortaya koymaktadır.

Emoji karakteri içeren ve içermeyen bazı örnek şifrelerin kaba kuvvet saldırısı simülasyonuna göre başarı oranları Şekil 4.1'de gösterilmiştir. Simülasyon sonuçlarına göre, sadece ASCII karakterlerinden oluşan şifrelerin (örn. "&K5", "5Gζu", "jB0") %100 oranında doğru şekilde tahmin edildiği görülmektedir. Ancak emoji karakteri içeren "■(5" ve "z0*" gibi şifrelerde başarı oranının sırasıyla %66 ve %60 seviyelerinde kaldığı gözlemlenmiştir.

Bu sonuç, emoji karakterlerinin kaba kuvvet saldırılarında olasılık kombinasyonlarını önemli ölçüde artırdığını göstermektedir. Unicode tabanlı emoji karakterlerinin büyük çeşitliliği sayesinde, saldırganın doğru şifreyi tahmin etme süresi uzamakta ve başarı

oranı düşmektedir. Dolayısıyla, şifrelerde emoji kullanımı, sadece entropiyi artırmakla kalmamakta, aynı zamanda saldırıların başarı oranını da azaltarak güvenliği güçlendirmektedir.



Şekil 4.1 Emoji karakterlerinin kaba kuvvet saldırılarına etkisi

Tablo 4.9'da simülasyon sonuçları, farklı karakter kümelerine sahip parolaların kaba kuvvet saldırılarına karşı dayanıklılığını ortaya koymaktadır. Özellikle yalnızca emoji karakterlerinden oluşan parolalarda (%100 oranla) hiçbir şifrenin tahmin edilemediği ve "en iyi tahmin" kısmının tamamen boş kaldığı dikkat çekmektedir. 8, 10, 12 ve 15 karakter uzunluğuna sahip tüm emoji şifreleri için başarı oranı %0.00 olarak kaydedilmiştir. Bu durum, emoji karakterlerinin Unicode sisteminde yer alması ve olası kombinasyon sayısını katbekat artırması nedeniyle saldırganlar açısından tahmin sürecini ciddi şekilde zorlaştırdığını göstermektedir.

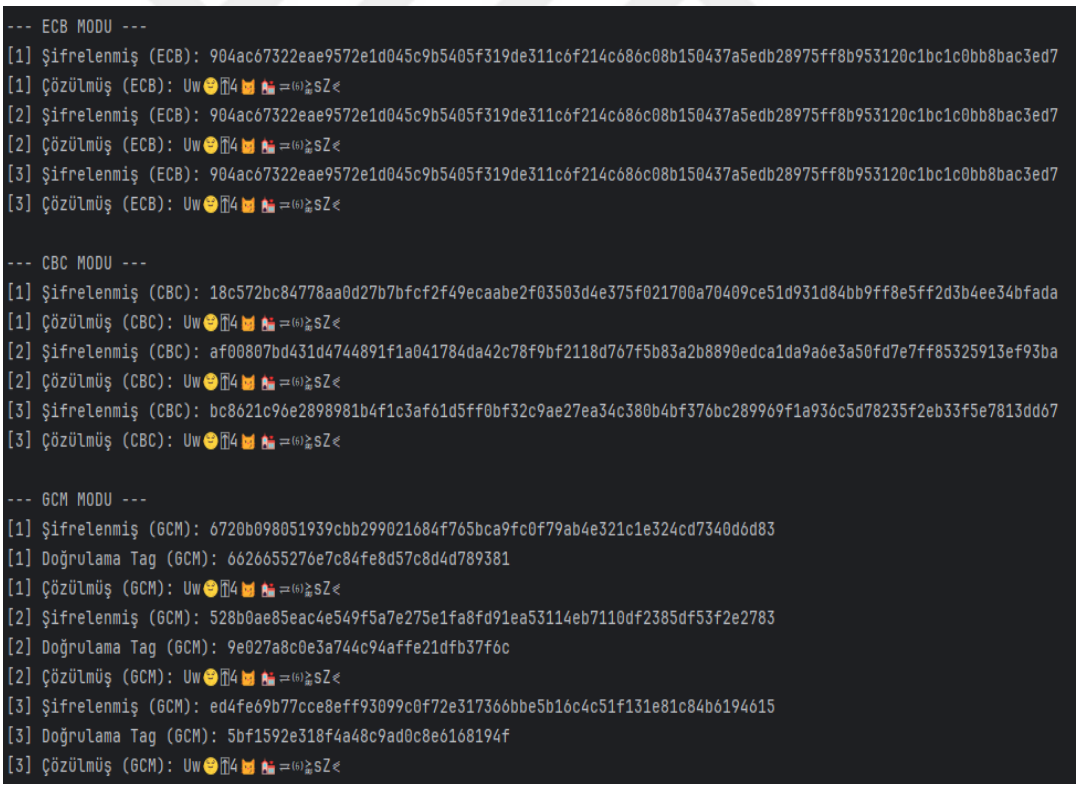
Tablo 4.9 Kaba kuvvet saldırısına karşı direnç sonuçları

Hedef Parola	Uzunluk	Karakter Kümesi	Parola bulundu mu?	Deneme sayısı	Süre (saat)	En iyi tahmin	Skor
💂‍♀️🤚⁝⊟∋◊ʅ”	8	Emoji	Hayır	10138071192	6	-	%0.00
\d↢S🟥/2	8	Emoji ,harf ve rakam	Hayır	9366565145	6	aaaaadS2	%37.50
w3C95TPg	8	Harf ve rakam	Hayır	10660710628	6	aaawCTPg	%62.50
⇆→⁝≎♓⌯⌥🏇🤽♌	10	Emoji	Hayır	18095335776	6	-	%0.00
🚻⌓V🎙d1t◈J🧱	10	Emoji, harf ve rakam	Hayır	10781617453	6	aaaaaVd1tJ	%50.00
7vbMga9Exv	10	Harf ve rakam	Hayır	10179560902	6	aaaaba9Exv	%60.00
🌈🟡🌐⌯ϑϑϑ☿▀⊣🔮⋋♍	12	Emoji	Hayır	8924195896	4	-	%0.00
3w✹⌯(a)⏀🖌⤓==⛒H9	12	Emoji ,harf ve rakam	Hayır	5789097920	4	aaaaaaaa3wH9	%33.33
BjKiXw4yVdew	12	Harf ve rakam	Hayır	5089634419	6	aaaaaaaiwdew	%41.67
╔↘⩓.:1⍑🏊🚎⛀\🍡🤷⊃18ㄴ	15	Emoji	Hayır	11310947987	4	-	%0.00
␡4⑰9viin}🤷‍♂️♒(x)ϒ๑lㅂ⊵ↄ	15	Emoji ,harf ve rakam	Hayır	7397107154	4	aaaaaaaaaa49nI	%26.67
Vg79d4F29383kr5	15	Harf ve rakam	Hayır	18047383870	6	aaaaaaaadF2kr5	%40.00

Öte yandan, harf ve rakam içeren parolalarda sistem, belirli ölçüde doğru tahminlerde bulunabilmiş ve skorlar %41,67 ila %62,50 arasında değişmiştir. Emoji + harf + rakam kombinasyonu ise, tahmin edilebilirlik açısından orta düzeyde direnç göstermiştir; bu tür şifrelerde skor %26,67 ile %50.00 aralığında kalmıştır. Bu sonuçlar, yalnızca ASCII tabanlı karakterlerin kullanıldığı şifrelerin daha yüksek oranda tahmin edilebildiğini, emoji eklenmesinin ise entropiyi artırarak hem tahmin süresini uzattığını hem de başarı oranını düşürdüğünü ortaya koymaktadır. Dolayısıyla, tezde geliştirilen sistemde emoji kullanımının, kaba kuvvet saldırılarına karşı önemli bir güvenlik katkısı sunduğu açıkça görülmektedir.

4.4. AES-128 için GCM, ECB ve CBC Mod Karşılaştırma

Uygulama tarafından üretilmiş şifre, site ismi ve kullanıcı adı sistem tarafından üretilen anahtar ile AES-128'in sayaç modu kullanılarak şifrelenmektedir. Bu mod seçilmeden önce ECB ve CBC modları da kullanılmış ve bu modların güvenlik açısından zayıf olduğu belirlenmiştir. AES-GCM (Galois/Counter Mode), simetrik anahtar şifrelemede hem veri gizliliğini hem de veri bütünlüğünü sağlayan kimlik doğrulama adımını da içeren bir şifreleme modudur. Şifreleme işlemini sayaç (CTR) modunda gerçekleştirirken, doğrulama etiketi üretmek için Galois alanı işlemlerinden yararlanıyor. Bu sayede de iletilen veriler üzerinde tüm yetkisiz değişiklikler tespit edilebiliyor ve güvenli iletişim sağlıyor. Bundan başka AES-128-GCM modunda olan kimlik doğrulama özelliğine sahip değil. Buda aynı anahtara sahip olan başka bir kullanıcı şifrelenmiş veriyi çözebilmektedir [59].



Şekil 4.2 AES-128 modları karşılaştırma

Şekil 4.2'de algoritma tarafından üretilmiş 13 karakterlik şifreye her mod ile üç kez şifreleme ve çözme işlemi yapılıyor ve sonuçta GCM ve CBC modunun ECB modundan önemli farkı ECB modunda bir veri her seferinde aynı şekilde

şifrelemektedir. GCM'de ise diğerlerinden farklı olarak doğrulama işlemi yapıyor bunu ise doğrulama etiketi oluşturarak yapmaktadır. Bu modların sürelerinin karşılaştırılması için üretilmiş şifreler ile süreler milisaniye olarak hesaplanmıştır. Bu süreler donanıma göre farklılıklar gösterebilir.

Algoritma tarafından üretilen bu şifrenin AES şifreleme algoritmasının farklı modlarının şifreleme ve şifre çözme süreleri hesaplanmıştır. Tablo 4.10'da görüldüğü gibi GCM modu en uzun şifreleme ve şifre çözme süresine sahip moddur. Lakin bu modlar arasında en güvenlisi GCM olduğu için uygulama üretimi zamanı bu mod seçilmiştir.

Tablo 4.10 Modların şifreleme ve çözme süreleri

Modlar	Şifre	Şifreleme süresi (ms)	Şifre çözme süresi (ms)	Toplam süre (ms)
ESB	Uw😊🀆4😼🏪⇌⑹⧛sZ⩽	3.48	0.03	3.51
CBC	Uw😊🀆4😼🏪⇌⑹⧛sZ⩽	3.12	0.03	3.15
GCM	Uw😊🀆4😼🏪⇌⑹⧛sZ⩽	13.7	0.24	13.94

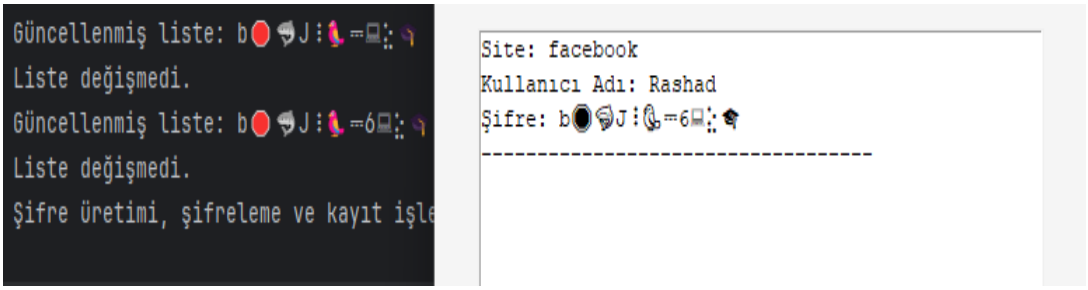
4.5. Birim Testi

Uygulamanın fonksiyonlarının veya sınıfın bağımsız olarak doğru çalışıp çalışmadığını kontrol etmek için birim testleri yapılmıştır. Tablo 4.11'de verilen sekiz tane birim testi yapılmış ve tüm birim testlerinden uygulama başarılı bir şekilde geçmiştir. Bu testler "unittest" kütüphanesi kullanılarak yapılmıştır.

Tablo 4.11 Birim test sonuçları

Test ismi	Ne test edildi?	Sonuç
Şifreleme çözme döngüsü	Şifreleme ve çözme doğru çalışıyor mu?	Başarılı
Her seferinde farklı şifreleme	Her şifreleme farklı mı?	Başarılı
Geçersiz şifre çözmede hata	Geçersiz şifre çözümünde hata dönüyor mu?	Başarılı
Şifre base64 formatında oluşturuluyor mu?	Çıktı geçerli bir Base64 mi?	Başarılı
Hash tutarlılık ve biçim	Hash sabit mi, doğru formatta mı?	Başarılı
Giriş yapan kullanıcı id tipi	Giriş ID tipi uygun mu?	Başarılı
Giriş sorgusu doğru mu?	Giriş sorgusu ve mesaj doğru mu?	Başarılı
Hatalı giriş bilgilendirmesi	Hatalı girişte uyarı veriliyor mu?	Başarılı

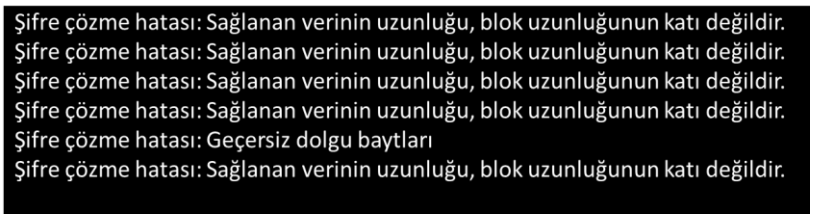
Yapılan ilk birim testi ile şifreleme ve şifre çözme fonksiyonlarının veri bütünlüğünü sağlayıp sağlamadığını denetlemektedir. Şifrelenen bir veri çözüldüğünde orijinal haline eksiksiz dönüp dönmediğini test etmektedir. Uygulama bu testten başarılı bir şekilde geçmiştir. Uygulama çözme işlemini kullanıcı her uygulamaya giriş yaptığında başlatıyor. Şekil 4.3'te görüldüğü gibi üretilmiş şifre ile çözme işlemini sonundaki çıktıların aynı olduğu gözükmektedir.



Şekil 4.3 Birim testi- şifreleme ve çözme

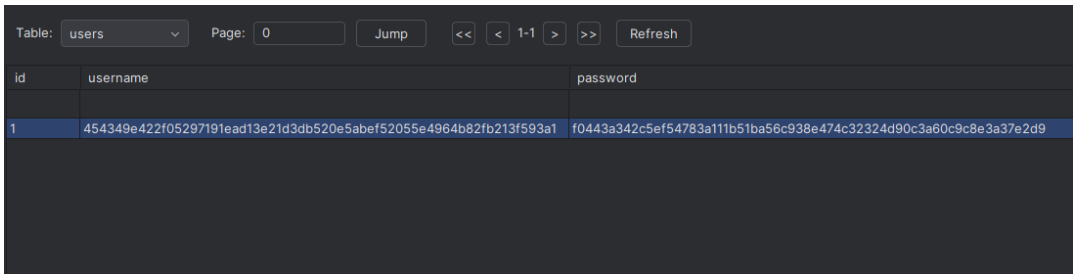
Sıradaki birim testi ise Şekil 4.4'te görüldüğü gibi aynı veri her şifrelemede farklı sonuç verip vermediği kontrol ediyor. Bu durum, nonce (tekil rastgelelik) kullanımının aktif olduğunu ve kriptografik güvenliğin sağlandığını gösteriyor. Şifreleme

algoritmasında GCM modu kullanıldığı için uygulama bu testten de başarılı şekilde geçmiştir.



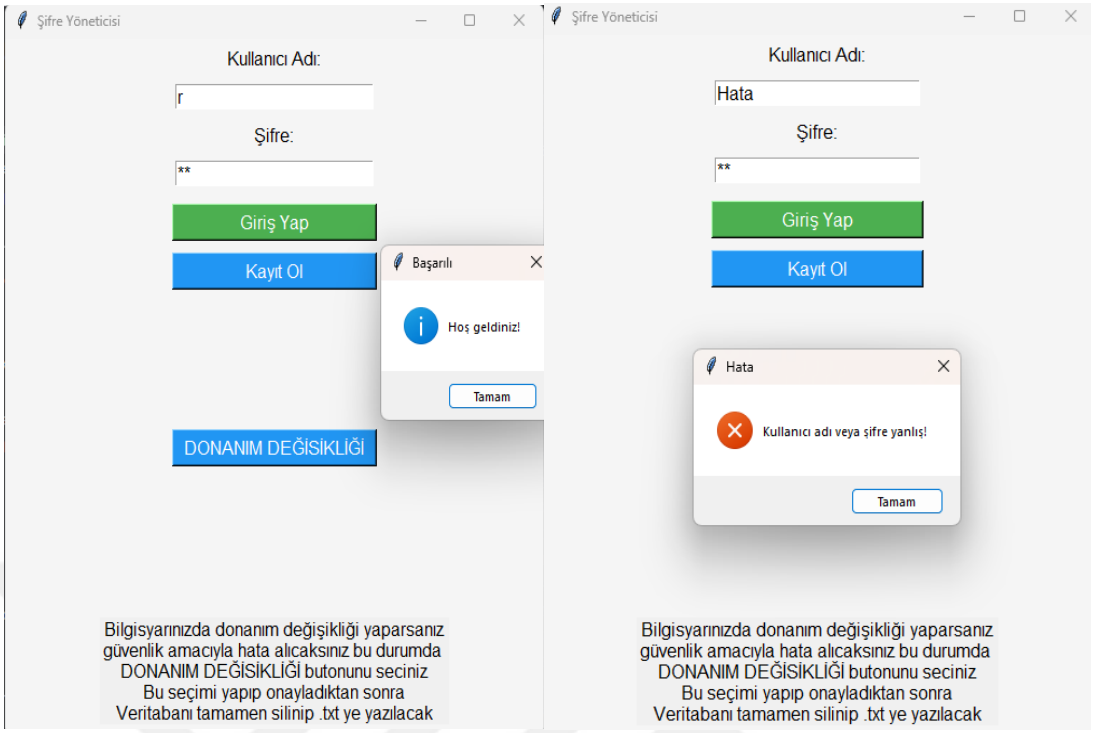
Şekil 4.4 Farklı anahtar ile çözme işlemi sonucu

Şifreleme işleminin sonucunda oluşan verinin Base64 standardına uygun formatta olup olmadığı bu test ile doğrulandı ve bu test sonucu başarılı oldu. Şifreli verinin güvenli biçimde aktarılabilirliğini ve saklana bilirliğini belirlemek için bu test yapıldı. Sıradaki testte aynı verinin her zaman aynı, farklı verilerin farklı özet değeri üretip üretmediği denetlenir. Ayrıca, çıktının SHA256 standardına uygun 64 karakterlik on altılı sayı biçimde olması beklenir. Sonuçta bu testler de başarılı olmuştur (Şekil 4.5). Uygulamada oturum açmış kullanıcının kimlik numarasının "int" ya da "None" tipinde dönüp dönmediği kontrol edilir. Bu, oturum yönetiminin türsel güvenilirliğini sağlamaya yönelik bir testtir.



Şekil 4.5 Özet değer birim testi sonucu

Verilen kullanıcı adı ve şifre ile sistemin doğru SQL sorgusunu oluşturup çalıştırdığı ve başarılı durumda kullanıcıya bilgi mesajı gösterdiği test edilmiştir. Bu sayede kimlik doğrulama sürecinin işlevselliği de test edilmiştir. Bunun yanı sıra geçersiz giriş bilgileriyle sistemin kullanıcıya uygun hata mesajı gösterip göstermediği de test edilmiş. Bu test, kullanıcı deneyimi ve doğrulama güvenliğinin tutarlı şekilde işleyip işlemediğini test etmektedir. Şekil 4.5'te verilen örneklerde görüldüğü gibi uygulama bu testlerde de olumlu sonuçlar vermiştir.



Şekil 4.6 Başarılı ve başarısız giriş denemeleri

Geçersiz şifre çözümünde hata dönüp dönmediğinin de kontrolü yapılmıştır. Geçersiz biçimli şifreli veri çözüldüğünde sistemin güvenli şekilde hata döndürüp döndürmediği test edilmiştir. Bu, hatalı veri girişine karşı yazılımın sağlamlığını ve istikrarını ölçer. Uygulama hatalı girişleri engellemede başarılı olmuştur (Şekil 4.6). Burada farklı anahtar ile algoritmanın üretmiş olduğu parola çözülmeye çalışıldığında hata mesajları alınıyor.

5. SONUÇ

Bu tez kapsamında geliştirilen uygulama, kullanıcıların güvenli, çeşitli ve hatırlanabilir şifreler oluşturmasını sağlamak amacıyla emoji karakterleri ile güçlendirilmiş bir şifre yönetim sistemidir. Uygulama, Windows 11 üzerinde Python ve SQLite kullanılarak geliştirilmiş olup; şifre üretiminde AES-128-GCM şifreleme algoritması, anahtar türetmede donanım bilgisi ve emoji matrisleri kullanmaktadır. Kullanıcı arayüzü, Tkinter üzerinden sanal emoji klavyesi ve görsel geri bildirimlerle desteklenmiştir. Üretilen şifreler 8, 10, 12 ve 16 karakter uzunluğunda olup, ASCII ve emoji karakterlerinin kombinasyonu ile oluşturulmaktadır. Sistem, NIST SP 800-22 testleri, birim testleri ve entropi analizleriyle başarıyla değerlendirilmiş; sonuçlar, emojilerin şifre güvenliğini ve çeşitliliğini anlamlı şekilde artırdığını ortaya koymuştur.

Uygulamanın test aşamasında RSA ve Blowfish şifreleme algoritmalarını AES şifreleme algoritmasına kıyasla daha geç şifreleme ve çözme işlemi yaptığı tespit edildi. Bundan başka literatür taraması zamanı RSA ve Blowfish algoritmalarının anahtarını güvenli bir şekilde saklanmasının zor olduğu ve kaba kuvvet ve yan kanal saldırıları kullanılarak bu algoritmalarda anahtar bilgilerinin bulunabilmesi sebebi ile AES-128 şifreleme algoritması kullanılmıştır. Bu algoritma ile hazırlanmış uygulamanın üretmiş olduğu parolalar üzerinde NIST tarafından hazırlanmış testler yapılmış ve bu testlerden uygulamanın üretmiş olduğu parolalar başarılı bir şekilde geçmiştir.

Entropi testinde sadece emoji kullanılmış şifreler, emoji, harf ve rakam ile oluşturulan şifreler ve standart harf ve rakam ile oluşturulan şifreler olmak üzere üç farklı şifre oluşturma türü test edildi. Entropi testinin sonucunda en güvenli şifre türü sadece

emojiler kullanılarak üretilmiş olan şifreler oldu. En az entropiye sahip şifreler ise standart kullanılan harf ve rakam kombinasyonlu şifreler oldu. Standart şifrelerin entropileri 71.45 bit iken emoji ile oluşturulmuş şifrelerin entropisi 144.5 bit olduğu tespit edilmiştir.

Uygulamada veri güvenliği için kullanılan AES-128 için kullanılan ECB, CBC ve GCM modlarının seçilmesi içinde testler yapıldı. ECB modu en kısa sürede şifreleme ve çözme işlemi yapan modlardan birisi bu mod toplamda 13 karakterlik bir veriyi şifreleme ve çözme işlemini 3.51 milisaniye de yapıyor. Lakin bu mod bir veriyi her seferinde aynı şekilde şifrelediği için bu mod seçilmedi. CBC modu ise her seferinde farklı şekilde şifreleme işlemi yapmaktadır ama aynı anahtara sahip olan farklı kullanıcı şifrelenmiş veriyi çözebildiği için bu modda uygulamada kullanılmamıştır. GCM modu şifreleme ve çözme işlemini toplamda 13.94 milisaniyede yapmakta ve diğer modlara göre daha uzun süreye ihtiyaç duymaktadır ama hem her kullanıcı için farklı etiket ile kullanıcıyı doğruladığı için uygulamada GCM modu kullanılmıştır.

Şifrelerde emojilerin kullanılması saldırganların kaba kuvvet saldırılarında başarılı olma sürelerini ciddi oranda arttırdığı testler sonucunda tespit edildi. Kullanıcılar tarafından kullanılan 8 karakterli harf ve rakam parolalarının bulunma süresi sistem donanımlarına göre farklılık gösterse de bu çalışmada test için seçilmiş 12 adet RTX 4090 ekran kartları kullanılarak bulunma süresi 87 yıl olduğu hesaplandı lakin aynı hesaplama 8 karakterlik emoji şifreleri için yapıldığında bu süre 1.4 x 10^{15} olarak hesaplandı.

Sonuç olarak, günümüzde bilgisayar korsanlarının, emoji kullanılarak güçlendirilmiş şifreleri deneme yanılma yoluyla elde etmeleri, emoji karakter kümesinin oldukça büyük olması nedeniyle son derece güçleştirmektedir. Ayrıca, şifre kırma amacıyla kullanılan sözlük tabanlı ve diğer saldırı araçlarının çoğunlukla yalnızca kelime, rakam ve işaretler üzerine odaklanması, bu tür şifrelerin bulunma ihtimalini daha da azaltmaktadır. Bu durum, şifre güvenliği açısından emoji kullanımının önemini ve geleneksel şifre kırma tekniklerine karşı sağladığı ek bir koruma katmanını açıkça ortaya koymaktadır.

6. TARTIŞMA

Yapılan literatür taraması sonucunda, parolaların emoji kullanılarak oluşturulmasına ilişkin çalışmaların sınırlı olduğu görülmüştür. Günümüzde parola güvenliği giderek daha önemli bir gereklilik haline geldiğinden yalnızca harf ve rakamlardan oluşan şifrelerin yanı sıra, emojilerin de şifre oluşturma sürecine dâhil edilmesi gerektiği yapılan testlerle kanıtlanmıştır. Bu çalışmada emoji ile güçlendirilmiş şifre yönetimi sistemi geliştirilmiş ve mevcut sistemlerin güvenlik zafiyetlerine yönelik çeşitli çözümler sunulmuştur. Elde edilen bulgular, emoji tabanlı şifrelerin hem kullanıcı dostu bir deneyim sağladığını hem de kaba kuvvet ve sözlük saldırılarına karşı dirençli olduğunu göstermektedir.

Çalışmanın bazı sınırlamaları ve gelecekte yapılabilecek araştırmalar için ilk öneri yapılmış bu çalışmada uygulama geliştirilmiş ve kullanıcı deneyimi açısından teorik olarak avantajlar sunsa da gerçek kullanıcı grubunda ortam testleri yapılmamıştır. Gelecek çalışmalar farklı yaş ve teknoloji okuryazarlığına sahip olan kullanıcı gruplarında sistem kullanılabilirliği ve benimseme oranları gibi parametreler analiz edilebilir. Sistemin güvenli anahtar yönetimi için Hiyerarşik Anahtar Yönetimi (HKM) veya Donanımsal güvenlik modülü (HSM) entegrasyonu değerlendirilebilir. Ayrıca kullanıcı şifre kasalarının düzenli ve şifreli yedeklemeleri yapılabilir. Olası veri kaybı senaryoları için yedekleme-kurtarma stratejileri geliştirilebilir.

Bu çalışma kapsamında hazırlanmış olan uygulama internet erişimi gerektirmeksizin yerel sunucuda çalışacak şekilde hazırlanmış ve testler buna göre yapılmıştır. Yapılacak yeni çalışmalarda emoji ile şifre üreten şifre yöneticileri bulutta çalışacak şekilde geliştirilebilir.

7. KAYNAKÇA

[1] LastPass. (2025). LastPass Security Report. www.lastpass.com/-/media/beb98dc9fd9a45b8b959f31cee59afc9.pdf 19.04.2025

[2] NordPass. (2024). Top 200 Most Common Passwords. NordPass. https://nordpass.com/most-common-passwords-list/ 19.04.2025

[3] Çeken, B., Arslan, A. A., & Tuğrul, D. (2017). İletişimde Emojilerin Kullanımı ve İncelenmesi. 21. Yüzyılda Eğitim Ve Toplum, 6(16), 91-106.

[4] Neskey, C. (2023). Are your passwords in the green. Hive Systems, 18.

[5] Vidojevic, A. (2025). Emojis in Business Communication: 2025 Statistics. https://pumble.com/learn/communication/emoji-statistics-internal-communication/ 05.05.2025

[6] Unicode Consortium. (2025). About emoji. https://home.unicode.org/emoji/about-emoji/ 19.04.2025

[7] Golla, M., Detering, D., & Dürmuth, M. (2017). EmojiAuth: quantifying the security of emoji-based authentication. In Proceedings of the usable security mini conference (USEC).

[8] Zabidi, N. S., Norowi, N. M., & Rahmat, R. W. O. (2018). A usability evaluation of image and emojis in graphical password. Int J Eng Technol, 7(4.31), 400-407.

[9] K. S. Charan Ayineni, P. M. V. Pranav and A. V. Vasanth, "Enhancing Authentication Security: Emoji based Graphical Passwords in Universal Three-Factor Authentication Systems," 2024 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2024, pp. 2152-2159

[10] Nan, X. (2024). Password Security Reinforcement via Combining Unicode Character Set (Doctoral dissertation, Waseda University).

[11] Öztürk, G. (2024). Uzaktan eğitim uygulamalarında veri güvenliği. In Y. Değirmenci (Ed.), Eğitim bilimlerinde öncü ve yenilikçi çalışmalar (pp. 59–80). All Sciences Academy.

[12] International Organization for Standardization [ISO] (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:isoiec:27000:ed-5:v1:en:term:3.28 23.04.2025

[13] Google Security Blog. (2019). New research: How effective is basic account hygiene at preventing hijacking https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html?utm_source 23.04.2025

[14] Simon, J., Watson, S. J., & van Sintemaartensdijk, I. (2025). Response-efficacy messages produce stronger passwords than self-efficacy messages… for now: A longitudinal experimental study of the efficacy of coping message types on password creation behaviour. Computers in Human Behavior Reports, 100615.

[15] Huseynov, E., & Seigneur, J. M. (2015). WiFiOTP: Pervasive two-factor authentication using Wi-Fi SSID broadcasts. In 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015) (pp. 1-8). IEEE.

[16] Cruz, B. (2024) Password Manager Industry Report and Statistics. https://www.security.org/digital-safety/password-manager-annual-report 03.05.2025

[17] Cruz, B. (2025). Password manager industry report and statistics. https://www.security.org/digital-safety/password-manager-annual-report/ 28.04.2025

[18] Grimes, R. A. (2018). Using a password manager: 7 pros and cons. https://www.proquest.com/trade-journals/using-password-manager-7-pros-cons/docview/2150931117/se-2

[19] Khan, S., Mumtaz, M., & Butt, S. K. (2025). Advance Password Manager (APM). MCS.

[20] Gallus, Petr & Stanek, Dominik & Klaban, Ivo. (2025). Security Evaluation of Password Managers: A Comparative Analysis and Penetration Testing of Existing Solutions. International Conference on Cyber Warfare and Security. 20. 105-113.

[21] Nair, V., & Song, D. (2023). MFDPG: Multi-Factor Authenticated Password Management With Zero Stored Secrets. arXiv preprint arXiv:2306.14746.

[22] Bitwarden Inc. (2025). How end-to-end encryption paves the way for zero knowledge – White paper. https://bitwarden.com/resources/zero-knowledge-encryption-white-paper/ 02.05.2025

[23] Fumy, W., & Landrock, P. (1993). Principles of key management. IEEE Journal on selected areas in communications, 11(5), 785-793.

[24] Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. NIST special publication, 800(150), 35.

[25] Mayur Jariwala. (2023). The Cyber Security Roadmap: A Comprehensive Guide to Cyber Threats, Cyber Laws, and Cyber Security Training for a Safer Digital World [eBook]. Baywood Hotels. ISBN: 978-93-5967-628-9

[26] Al Daoud, E., Jebril, I. H., & Zaqaibeh, B. (2008). Computer virus strategies and detection methods. Int. J. Open Problems Compt. Math, 1(2), 12-20.

[27] Wang, S. Y. (2009). Early warning technology of network worm virus in campus network environment https://www.proquest.com/dissertations-theses/early-warning-technology-network-worm-virus/docview/1870564292/se-2

[28] Al-Saadoon, G., & Al-Bayatti, H. (2011). A comparison of trojan virus behavior in linux and windows operating systems. Ithaca https://www.proquest.com/working-papers/comparison-trojan-virus-behavior-linux-windows/docview/2086783719/se-2

[29] Yilmaz, S., & Zavrak, S. (2015). Adware: a review. International Journal of Computer Science and Information Technologies, 6(6), 5599-5604.

[30] Wieslander, J., Boldt, M., & Carlsson, B. (2003). Investigating Spyware on the Internet. In Proceedings of the Seventh Nordic Workshop on Secure IT Systems.

[31] Ma, S. H. (2010). Windows hidden virus detection technology explore https://www.proquest.com/dissertations-theses/windows-hidden-virus-detection-technology-explore/docview/1868798817/se-2

[32] Chanti, S., & Chithralekha, T. (2022). A literature review on classification of phishing attacks. International Journal of Advanced Technology and Engineering Exploration, 9(89), 446-476.

[33] Popescul, D. (2011). The confidentiality–integrity–accessibility triad into the knowledge security: a reassessment from the point of view of the knowledge contribution to innovation.

[34] Tuğal, İ., Almaz, C., & Sevi, M. (2021). Üniversitelerdeki siber güvenlik sorunları ve farkındalık eğitimleri. Bilişim Teknolojileri Dergisi, 14(3), 229–238.

[35] Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. World applied sciences journal, 19(4), 439-444.

[36] Sechard. (2025). Most common types of password attacks and how to prevent them. https://sechard.com/blog/most-common-types-of-password-attacks-and-how-to-prevent-them/ 04.05.2025

[37] Por, L. Y., Ng, I. O., Chen, Y. L., Yang, J., & Ku, C. S. (2024). A systematic literature review on the security attacks and countermeasures used in graphical passwords.

[38] Saadi, Z. M., Sadiq, A. T., Akif, O. Z., & Farhan, A. K. (2024). A Survey: Security Vulnerabilities and Protective Strategies for Graphical Passwords. Electronics, 13(15), 3042.

[39] Gautam, T. (2024). Study of password cracking methodologies. Internafional Journal of Fuzzy Logic and Design, 9(1), 26-36.

[40] OneLogin. (2025). 6 types of password attacks. https://www.onelogin.com/learn/6-types-password-attacks 16.04.2025

[41] Wang, X., Yan, Z., Zhang, R., & Zhang, P. (2021). Attacks and defenses in user authentication systems: A survey. Journal of Network and Computer Applications, 188, 103080. https://doi.org/10.1016/j.jnca.2021.103080

[42] Taşçı, H., Gönen, S., Barışkan, M. A., Karacayılmaz, G., Alhan, B., & Yılmaz, E. N. (2021). Password attack analysis over honeypot using machine learning password attack analysis. Turkish Journal of Mathematics and Computer Science, 13(2), 388-402.

[43] SSH Academy. (2025). Types of password attacks and how to prevent them. https://www.ssh.com/academy/types-of-password-attacks-and-how-to-prevent-them/ 03.05.2025

[44] Endut, N. A., Azam, N. A. A., & Zulkafli, A. S. A. (2024). A Comparative Analysis of Offline and Online Password Cracking Tools. International Journal of Academic Research in Business and Social Sciences, 14(9), 1894–1906. doi.org/10.6007/IJARBSS/v14-i9/22996

[45] Loesch, H. J., & Remscheid, A. (1990). Brute force in molecular reaction dynamics: A novel technique for measuring steric effects. The Journal of chemical physics, 93(7), 4779-4790.

[46] KARA, İ. (2019). Detection, Technical Analysis of Brute Force Attack. Sakarya University Journal of Computer and Information Sciences.

[47] Hive Systems. (2025). Password solutions overview. Hive Systems. https://www.hivesystems.com/password 05.05.2025

[48] Hekim, H. (2015). Oltalama (Phishing) Saldirilari. Retrieved from academia: http://www. academia.edu/35136881/Oltalama_Phishing_Saldirilari.

[49] Dewan, P., Kashyap, A., & Kumaraguru, P. (2014, September). Analyzing social and stylometric features to identify spear phishing emails. In 2014 apwg symposium on electronic crime research (ecrime) (pp. 1-13). IEEE.

[50] Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE communications surveys & tutorials, 18(3), 2027-2051.

[51] İnönü Üniversitesi Siber Güvenlik Merkezi. (2025). Man-in-the-middle (MITM) saldırısı nedir, nasıl gerçekleştirilir? https://siber.inonu.edu.tr/man-in-the-middle-mitm-saldirisi-nedir-nasil-gerceklestirilir/ 05.05.2025

[52] Gallus, Petr & Staněk, Dominik & Klaban, Ivo. (2025). Security Evaluation of Password Managers: A Comparative Analysis and Penetration Testing of Existing Solutions. International Conference on Cyber Warfare and Security. 20. 105-113.

[53] Carr, M., & Shahandashti, S. F. (2020). Revisiting security vulnerabilities in commercial password managers. In ICT Systems Security and Privacy Protection: 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia, September 21–23, 2020, Proceedings 35 (pp. 265-279). Springer International Publishing.

[54] Geeksforgeeks. (2025). RSA Algorithm in Cryptography. https://www.geeksforgeeks.org/rsa-algorithm-cryptography/ 31.05.2025

[55] K. Chad. (2023). Types of Encryption, Methods & Use Cases. https://www.esecurityplanet.com/trends/types-of-encryption/ 01.06.2025

[56] R. Sheldon. (2024). Data security and privacy https://www.techtarget.com/searchsecurity/definition/encryption 01.06.2025

[57] Kaspersky. Veri şifreleme nedir? Tanım ve açıklama. https://www.kaspersky.com.tr/resource-center/definitions/encryption 01.06.2025

[58] Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., ... & Theofanos, M. F. (2016). Draft nist special publication 800-63b digital identity guidelines. National Institute of Standards and Technology (NIST), 27.

[59] B. Enes. (2021) BLOWFISH ŞİFRELEME ALGORİTMASI https://en3s.medium.com/1-blowfish-şifreleme-algoritması-özet-3d09a7f2f3cd 31.05.2025