İŞLETME ARAŞTIRMALARI DERGİSİ
JOURNAL OF BUSINESS RESEARCH-TURK
2026, 18(2), 1163-1183
https://doi.org/10.20491/isarder.2026.2228

Mobil Güvenlik Uygulamaları Kullanıcı Değerlendirmelerinin Karşılaştırmalı Analizi: McAfee, Avast ve AVG Örneği

Comparative Analysis of User Reviews of Mobile Security Applications: Evidence from McAfee, Avast and AVG

Tuğçe KARAYEL [a]

[a] Düzce Üniversitesi, İşletme Fakültesi, Yönetim Bilişim Sistemleri, Düzce, Turkiye. tugceaslan@duzce.edu.tr

MAKALE BİLGİSİ

Anahtar Kelimeler:
Siber Güvenlik Farkındalığı
Mobil Güvenlik Uygulamaları
Metin Madenciliği
Kullanıcı Yorumları
Yıldız Derecelendirmesi

Gönderilme Tarihi 31 Ağustos 2025
Revizyon Tarihi 15 Mayıs 2026
Kabul Tarihi 30 Mayıs 2026

Makale Kategorisi:
Araştırma Makalesi

ÖZET

Amaç – Bu çalışmanın amacı; Mcafee, Avast ve AVG uygulamaları ile ilgili yapılan kullanıcı yorumları ve yıldız derecelendirmelerini analiz etmektir.

Yöntem – Bu araştırmada metin madenciliği yöntemi tercih edilmiştir. Veri ve metin seti uygulama programlama arayüzü olan Apify yardımıyla oluşturulmuştur. Apify üzerinden Google Play platformundaki McAfee, Avast ve AVG android uygulamalarından kullanıcı yorumu, yorum tarihleri ve yorumlara ait yıldız derecelendirmeleri çekilmiştir. 2011 ile 2025 yılları arasındaki McAfee için 7015, Avast için 36679 ve AVG için 44480 adet kullanıcı yorumu çekilmiştir. Elde edilen veri ve metin seti, QDA Miner® ve WordStat® metin madenciliği yazılımları ile analiz edilmiş ve yorumlanmıştır.

Bulgular – Pozitif kullanıcı deneyimlerinin ortak göstergesi olarak her üç uygulamada "tavsiye ederim", "güzel bir," "iyi bir" ve "harika bir" gibi olumlu yargı içeren kalıpların yüksek frekanslarla yer aldığı görülmektedir. Bununla birlikte, Avast ve AVG uygulamalarında veri gizliliğine dair endişeleri ifade eden yorumlar da dikkat çekicidir. Yıldız derecelendirmeler incelendiğinde yıldız derecelerin azaldıkça yorum dilinin olumlu ifadelerden teknik eleştirilere ve memnuniyetsizlik bildirimlerine doğru kaydığı görülmektedir. 2020–2025 yılları arasında McAfee, Avast ve AVG uygulamalarına ilişkin kullanıcı yorumları incelendiğinde üç uygulama için de gözlemlenen ortak eğilim, erken dönemlerde duygusal ve genel değerlendirmelerin ön planda olması, ilerleyen yıllarda ise teknik ve işlevsel geri bildirimlerin artmasıdır.

Tartışma – Araştırma sonuçlarına göre kullanıcıların siber güvenlik farkındalığının arttığı ve güvenlik uygulamalarından yalnızca temel koruma değil, bütünleşik güvenlik çözümleri bekledikleri ortaya çıkmıştır. Ayrıca kullanıcıların lisans politikaları, yazılım sürekliliği ve deneyim sürekliliği gibi operasyonel konularda daha hassas oldukları görülmüştür. Çalışma, teorik olarak mobil güvenlik uygulamalarına ilişkin kullanıcı deneyimlerini çevrim içi kullanıcı yorumları üzerinden inceleyerek mevcut literatüre gerçek kullanıcı geri bildirimlerine dayalı ampirik kanıt sunmaktadır. Uygulamaya yönelik olarak ise mobil antivirüs uygulamalarına ilişkin gizlilik kaygıları, güven algısı ve kullanıcı beklentileri konusunda geliştiricilere ve politika yapıcılara uygulanabilir içgörüler sunmaktadır.

ARTICLE INFO

Keywords:
Cyber Security Awareness
Mobile Security Applications
Text Mining
User Reviews
Star Rating

Received 31 August 2025
Revised 15 May 2026
Accepted 30 May 2026

ABSTRACT

Purpose – The aim of this study is to analyze user reviews and star ratings related to the McAfee, Avast, and AVG applications.

Design/methodology/approach – This research employed the text mining method. The data and text set were compiled using Apify, an application programming interface (API). Through Apify, user reviews, review dates, and associated star ratings were retrieved from the Google Play platform for the McAfee, Avast, and AVG Android applications. Within the period between 2011 and 2025, a total of 7015 user reviews for McAfee, 36679 for Avast, and 44480 for AVG were collected. The resulting data and text set were analyzed and interpreted using the text mining software QDA Miner® and WordStat®.

Results – As a common indicator of positive user experiences, high-frequency occurrences of phrases with favorable connotations such as "highly recommend," "a great," "a good," and "wonderful" were observed across all three applications. Notably, in AVG and Avast, there were also reviews expressing concerns regarding data privacy. An examination of star ratings revealed that as ratings decreased, the tone of reviews shifted from positive expressions toward technical

ETİK ONAY: Bu çalışmada ikincil veriler kullanılmış olup etik kurul onayı gerektirmemektedir.

Önerilen Atıf/ Suggested Citation
Karayel, T. (2026). Mobil Güvenlik Uygulamaları Kullanıcı Değerlendirmelerinin Karşılaştırmalı Analizi: McAfee, Avast ve AVG Örneği, İşletme Araştırmaları Dergisi, 18 (2) 1163-1183.

Article Classification:
Research Article

criticisms and statements of dissatisfaction. Analysis of user reviews for McAfee, Avast, and AVG antivirus applications between 2020 and 2025 indicated a shared trend: while earlier reviews predominantly featured emotional and general evaluations, later reviews increasingly emphasized technical and functional feedback.

Discussion – The findings reveal that users' cybersecurity awareness has increased, and that they now expect not only basic protection but also integrated security solutions from such applications. Furthermore, users appear to be more sensitive to operational issues such as licensing policies, software continuity, and consistency in user experience. The study theoretically contributes to the existing literature by examining user experiences related to mobile security applications through online user reviews and providing empirical evidence based on real user feedback. From a practical perspective, it offers actionable insights for developers and policymakers regarding privacy concerns, trust perceptions, and user expectations toward mobile antivirus applications.

1. Giriş

Günümüzde akıllı telefonlar birçok kişi için bağımlılık noktasına ulaşmış ve bireylerin günlük yaşamlarında vazgeçilmez bir araç haline gelmiştir (Chen vd., 2017; Koyuncu & Pusatli, 2019). Akıllı telefonlar telefon görüşmelerinin yanı sıra birçok farklı amaç için kullanılmaktadır. Bunlar yalnızca e-posta gönderip almakla sınır değildir. Aynı zamanda Instagram, Facebook ve X gibi programları kullanarak sosyal medyada çevrimiçi kalmak ve elektronik finansal işlemler gerçekleştirmektir (Koyuncu & Pusatli, 2019).

Akıllı telefonların hızla yaygınlaşması, mobil güvenlik alanını önemli ölçüde etkilemiş ve kötü amaçlı yazılım saldırılarının yol açtığı benzeri görülmemiş zorlukları ortaya çıkarmıştır (Jin vd., 2025). Akıllı telefonlara yönelik kötü amaçlı yazılım, reklam yazılımı veya istenmeyen yazılımlar kullanılarak gerçekleştirilen siber saldırı sayısı her yıl artarak devam etmektedir. Örneğin Kaspersky mobil istatistik raporuna göre 2024 yılı tehditleri 2023 yılı tehditlerinden daha fazla sayıda çıkmıştır (Kaspersky, 2024). Bu oran 2025 yılı içinde benzer şekilde artmaya devam etmektedir. Büyüyen tehditler yaygın olarak kabul edilirken, akıllı telefon kullanıcılarının cihaz güvenliği için güvenlik yazılımlarını benimsemesi büyük oranda ihmal edilmektedir (Chenoweth vd., 2009; Lee vd., 2008). Kullanıcıların siber tehditlerden kendilerini korumanın yollarından biri, güvenlik yazılımları veya uygulamaları kullanmaktır (Toch vd., 2018). Güvenlik sağlayıcılarının önerilerine rağmen, mobil antivirüs kullanım oranları düşük düzeyde kalmaktadır (Jin vd., 2025). Bu düşük oranlar, giderek artan tehdit ortamı göz önüne alındığında endişe vericidir. Örneğin, Kaspersky'nin 2024 1. Çeyrek raporu, antivirüs yazılımları tarafından 10,1 milyon kötü amaçlı yazılım saldırısının önlendiğini belgelemiştir (Kaspersky, 2024). Tehditlerin arttığı yaygın olarak kabul edilirken, kullanıcıların gerçek dünya kullanımı sırasında antivirüs yazılımını nasıl algıladıkları ve deneyimledikleri konusunda kritik bir boşluk bulunmaktadır. Dahası, kullanıcıların mobil cihazlarda kendilerini koruma konusundaki farkındalıkları ve yetenekleri hala tartışmalıdır (Karayel & Saygılı, 2025; Koyuncu & Pusatli, 2019).

Akıllı telefon güvenliği, akıllı telefonları kullanırken güvenlik uzmanları tarafından önerilen güvenli uygulamaları kullanmak ve güvenli davranışlara uymak olarak tanımlanmaktadır (Zhou vd., 2020). Bu, akıllı telefon güvenliğindeki en iyi uygulamaların farkında olmayı ve bu uygulamaları takip etmeyi içerir (Hong vd., 2022). Kullanıcılar güvenilir olmayan bir kaynaktan mobil uygulamalar indirdiğinde kötü amaçlı yazılım saldırıları ile karşı karşıya kalabilir (Malleswari vd., 2018). Siber suçlular, kötü amaçlı yazılım saldırıları yoluyla akıllı telefonlara yetkisiz erişim elde edebilir (BalaGanesh vd., 2018). Bu durum güvenlik ve gizlilik konularında zafiyetlere neden olabilmektedir. 2025 yılında Android kullanıcılarını hedef alan "GodFather" adlı mobil kötü amaçlı yazılım, sahte uygulamalar aracılığıyla kullanıcıların erişim izinlerini ele geçirerek mobil bankacılık uygulamalarına yönelik sahte arayüzler oluşturmuştur. Bu saldırılar, kullanıcı giriş bilgileri ve işlem verilerinin kötü niyetli aktörler tarafından izlenmesine neden olmuş; Türkiye'de yaygın kullanılan çeşitli bankacılık uygulamalarını da etkilemiştir (Akbaş, 2025). Bu tür gelişmiş mobil tehditler, kullanıcıların mobil güvenlik farkındalığı ve güvenli kullanım davranışlarının kritik önemini ortaya koymaktadır.

Akıllı telefonlara yönelik siber saldırıların önemli ölçüde arttığı günümüzde, etkili bir karşı önlem olarak yalnızca teknik güvenlik çözümlerinin değil, aynı zamanda kullanıcı davranışlarının ve farkındalığının da geliştirilmesi gerekmektedir. Mevcut literatür incelendiğinde, çalışmaların büyük ölçüde teknik güvenlik performansı, sistem mimarileri ve zararlı yazılım tespiti gibi konulara odaklandığı; buna karşın kullanıcı algıları, deneyimleri ve geri bildirimlerine dayalı analizlerin sınırlı kaldığı görülmektedir. Bu çalışmanın amacı; McAfee, Avast ve AVG uygulamaları ile ilgili yapılan kullanıcı yorumları ve yıldız

derecelendirmelerini analiz etmektir. Bu amaç doğrultusunda aşağıdaki araştırma sorularına cevap aranacaktır:

1. McAfee, Avast ve AVG uygulamaları ile ilgili yapılan kullanıcı yorumlarında sıklıkla geçen kelime ve kelime grupları nelerdir?
2. McAfee, Avast ve AVG uygulamalarına yönelik kullanıcı yorumlarında geçen tematik içerikler ile verilen yıldız derecelendirmeleri arasında nasıl bir ilişki vardır?
3. McAfee, Avast ve AVG uygulamalarına yönelik kullanıcı yorumlarında sıklıkla geçen kelimeler 2020–2025 yılları arasındaki nasıl bir değişim göstermiştir?

Araştırma sorularını yanıtlamak için, Google Play Store üzerinden McAfee, Avast ve AVG mobil uygulamalarına ait kullanıcı yorumları çekilmiştir. Elde edilen veri ve metin seti QDA Miner ve Word Stat programları aracılığıyla analiz edilmiştir. Bu kapsamda çalışmanın beklenen katkıları iki yönlüdür. Teorik açıdan, mobil güvenlik uygulamalarına yönelik kullanıcı algıları ve deneyimlerine odaklanarak literatürde ağırlıklı olarak ihmal edilen kullanıcı merkezli bakış açısını güçlendirmektedir. Uygulama açısından ise, kullanıcı yorumları ve derecelendirmeleri üzerinden elde edilen bulgular sayesinde, geliştiricilere uygulama performansı, kullanıcı beklentileri ve geliştirilmesi gereken alanlara ilişkin veri temelli öneriler sunulmaktadır. Ayrıca çalışma, kullanıcıların uygulamalardan beklentilerini, güncelleme farkındalıklarını ve memnuniyet düzeylerini ortaya koyarak gelecekteki uygulama geliştirme süreçlerine rehberlik etmektedir.

2. Literatür

2.1. Mobil Güvenlik Uygulamaları

Akıllı telefonların popülaritesi, küçük boyutları, gelişmiş işlem ve bağlantı yetenekleri, düşük maliyetleri ve çok işlevli üçüncü taraf uygulamaları barındırma kabiliyetlerinden kaynaklanmaktadır. Akıllı telefonlar, multimedya, sensör verileri, iletişim kayıtları, uygulamalar tarafından oluşturulan veya tüketilen veriler vb. gibi karışık veriler barındırır. Aynı cihaz hem iş hem de eğlence amaçlı kullanılabildiğinden, akıllı telefonlar genellikle değerli kişisel ve ticari verilerin bir birleşiminide içerir. Akıllı telefon kullanmanın birçok avantajı varken aynı zamanda birçok güvenlik tehdidi de barındırmaktadır (Karayel & Saygılı, 2025). Akıllı telefon kullanıcıları, cihazı gün boyunca birden fazla konumda taşır ve genellikle güvenli olmayan çeşitli ağlara bağlanabilir. Akıllı telefonlar iş çevresini genişletirken, mevcut güvenlik ve gizlilik çevresine yönelik mekanizmaları yetersizdir (Theoharidou vd., 2012). Bu sebeple kullanıcıların kendilerini güvenlik önlemleri açısından geliştirmesi gerekmektedir. Akıllı telefon kullanıcılarının siber suçlara maruz kalma riskini en aza indirmek için cihazlarını korumaları önemlidir. Bu koruma yöntemi mobil siber hijyen seviyelerini iyileştirerek olacağı gibi telefonlarında güvenlik uygulamalarının kullanılmasıyla da olabilmektedir.

Her yıl artan bir hızla yeni kötü amaçlı yazılım türleri gelişmektedir (Karayel, 2025; Pereira vd., 2025). Akıllı telefonlar, çeşitli yollarla yayılan kötü amaçlı yazılımlara karşı savunmasızdır. Kullanıcılar kimlik hırsızlığı ve kişisel bilgilerin sızdırılması da dahil olmak üzere mobil cihazlarının güvenliği ve gizliliği konusunda giderek artan endişeler yaşamaktadır (Clarke vd., 2016). Mobil tabanlı tehditlere karşı savunma mekanizmaları oluşturmanın ve bunları hızlı bir şekilde uygulamanın önemi zamanla artmaktadır. Akıllı telefonlar için güvenlik uygulamaları kullanmak artık bir tercih meselesinden çıkıp bir gereklilik ve zorunluluk halini almaktadır. Bu güvenlik uygulamaları dahilinde bir kategoride antivirüs uygulamalarıdır. Antivirüs uygulamaları, çeşitli kötü amaçlı yazılım türlerini önlemek, tespit etmek, aramak ve kaldırmak için kullanılan bir güvenlik programıdır. Bu uygulamalar, kullanıcının telefonunu potansiyel güvenlik tehditlerinden korumaya yardımcı olur, kötü amaçlı yazılımların yayılmasını sınırlar ve mobil güvenlik ekosistemi içinde kapsamlı koruma sağlar (Jin vd., 2025).

Akıllı telefon güvenlik yazılımlarının benimsenmesiyle ilgili literatür incelendiğinde sınırlı sayıda çalışma yapıldığı görülmüştür. Al-ghaith (2016) Koruma Motivasyon Teorisi modelini genişleterek akıllı telefon antivirüs uygulamalarının benimsenmesinde öznel normların önemini bulmuştur. Lane ve Torri (2024), tarafından yapılan araştırmada iOS ve Android işletim sistemlerinde kullanılan antivirüs yazılımları araştırılmıştır. Araştırma sonuçlarına göre iOS işletim sisteminin Android işletim sisteminden daha güvenlik sistemine sahip olduğu ortaya koyulmuştur. Karayel ve Saygılı (2025) tarafından yapılan araştırmada ise akıllı telefonların da iOS ve Android işletim sistemi kullanan kullanıcılar arasında karşılaştırılmalı analiz

yapılmıştır. Araştırma sonuçlarına göre yanıt maliyetinin yalnızca iOS kullanıcıları arasında önemli bir etki gösterdiği ve algılanan yükün platforma göre değiştiği bulunmuştur. Christinne vd. (2021) tarafından yapılan araştırmada 360 Security ve CM Security uygulamalarının karşılaştırılmalı analizi yapılmıştır. Jin ve ark. (2025) akıllı telefon antivirüs yazılımlarının benimsenmesini ve kullanıcı algılarını araştırmıştır. Araştırma sonucunda, akran önerileri ve sosyal baskılar gibi sosyal normlar, akıllı telefon kullanıcıları için özellikle önemli olabilecek bir faktör olarak ortaya çıkmıştır.

2.2. Kullanıcı Değerlendirmeleri

Kullanıcılar, mobil uygulama mağazalarından uygulama indirebilir ve ardından uygulama incelemesi aracılığıyla deneyimlerini paylaşabilmektedir. Kullanıcılar uygulama ile etkileşime girdikten sonra, uygulama hakkındaki hislerini hızla ifade edebilmektedir. Kullanıcı yorumu, metin incelemesi ve yıldız derecelendirmesi içeren herkese açık bir değerlendirme olarak paylaşılmaktadır. Yıldız dereceleri bir en düşük, beş en yüksek şeklinde bir ölçekte kullanılmaktadır (Alismail & Albesher, 2023). En olumsuz görüşten en olumlu görüşe doğru yıldız sayısı artmaktadır. Beş yıldız ise en iyi görüşü ifade ederken üç yıldız orta derece bir görüşü, bir yıldız en kötü görüşü ifade etmektedir (Mudambi & Schuff, 2010). Kullanıcıların mobil uygulama değerlendirmeleri, kullanıcıların yaşadığı sorunlar hakkında değerli bilgiler içerir. Bu değerlendirmeler, yeni bir özellik isteği, hata raporu ve /veya gizlilik şikayeti gibi konular içerebilmektedir. Kullanıcılar, geliştiriciler ve uygulama mağazası sahipleri (örneğin Apple, Google) bu sorunları daha iyi anlamak için bu yorumlardan faydalanabilmektedir. Mobil uygulama geliştiricileri kullanıcıların endişelerini ve beklentilerini daha iyi anlayabilir, uygulama mağazası sahipleri anormal uygulamaları tespit edebilir ve kullanıcılar benzer uygulamaları karşılaştırarak hangilerini indireceklerine veya satın alacaklarına karar verebilmektedir (McIlroy vd., 2016).

Kullanıcıların mobil uygulamayı indirme kararları, yorumlar ve derecelendirmeler aracılığıyla diğer kullanıcıların deneyimlerinden etkilenir (Alhejji vd., 2022). Kullanıcılar aynı uygulama için çeşitli incelemeler yayınlayamazlar, ancak mevcut incelemelerini güncelleyebilmekte veya silebilmektedir. Kullanıcılar ayrıca başkalarının incelemelerine olumlu veya olumsuz oy verebilmektedir (Alismail & Albesher, 2023; Srisopha vd., 2020). Mobil uygulamalar, kullanıcıların uygulamayla ilgili deneyimlerini istedikleri yer ve zamanda rahatça değerlendirip yorumlamalarına olanak tanıyan platformlardır. Bu yorum kaynağı kullanıcıların mobil uygulamanın teknik yönlerine ilişkin değerlendirmelerini aynı zamanda genel kullanıcı deneyimini yansıtmaktadır (Li & Zhao, 2025). Bu herkese açık veriler, uygulamanın müşterilerin bakış açısından bütünsel bir değerlendirmesi olarak kabul edilir. Ancak, literatürde kullanıcıların mobil uygulamalardaki kullanıcı deneyimleri hakkında içgörüler elde etmek için bu metinsel veri kaynağını kullanan çalışmaların sınırlı kaldığı görülmektedir (Li & Zhao, 2025).

2.3. Kullanıcı Yorumlarıyla İlgili Çalışmaların İncelemesi

Outay vd.(2021) geliştiricilerin kullanıcı yorumlarına verdiği yanıtları incelemiştir. İHA mobil uygulamaları üzerine, Google Play Store'dan 162.250 değerlendirme/kullanıcı incelemesi içerik analizi yöntemi ile analiz edilmiştir. Hassan vd. (2018), Google Play Store'daki 2328 en popüler ücretsiz uygulama için 126.686 yanıt içeren 4,5 milyon yorumu içerik analizi yöntemi kullanarak incelenmiştir. Geliştiricilerin bir incelemeye yanıt vermesini neyin motive ettiğini anlamak için bir geliştiricinin bir incelemeye yanıt vermesini teşvik eden yedi faktör belirlenmiştir. Buna ek olarak, bir incelemeye yanıt vermenin, hiç yanıt vermemeye kıyasla bir kullanıcının puanını yükseltme olasılığını altı kata kadar artırdığı bulunmuştur.

McIlroy vd. (2017) tarafından Google Play Store'daki en iyi uygulamaların geliştiricilerinin bakış açısından uygulama incelemelerini ve incelemelere verilen yanıtları araştırmak için ampirik bir araştırma yapılmıştır. İki ay boyunca, Google Play Store'daki en iyi 10.713 uygulama için incelemeleri ve geliştirici yanıtları makine öğrenmesiyle analiz edilmiştir. Çalışma süresi içinde 111.099 incelemeye verilen yanıtlar manuel olarak etiketlenmiştir. Çalışma sonuçlarına göre, bir geliştirici yanıtından sonra, kullanıcıların puanlarını %38,7 oranında güncellediği ortaya çıkmıştır. Chen vd. (2021) tarafından mobil uygulamaların kullanıcı arayüzü zorluklarını değerlendirmek için derinlemesine bir ampirik araştırma yapılmıştır. Google Play Store'un 22.199 en iyi ücretsiz uygulaması ve 9380 en iyi ücretsiz olmayan uygulamasından 3 milyondan fazla kullanıcı değerlendirmesi incelenmiştir. Geri bildirimlere yanıt olarak kullanıcı arayüzünü düzenli olarak yükseltmenin, kullanıcıları mutlu etmek için kritik olduğu sonucuna ulaşılmıştır. Araştırma bulguları,

uygulama geliştiricilerinin kullanıcı arayüzü kalitesini yükseltmek ve kullanıcıların kullanıcı arayüzlerinden memnuniyetini artırmak için kullanıcılarla aktif olarak etkileşim kurmaları gerektiğini göstermektedir.

Bailey vd. (2019), geliştiricilerin bir kullanıcının incelemesine yanıt verdiğinde oluşan geri bildirim döngülerine odaklanmıştır. Çalışma için, 30.875 sürüm notu ve 806.209 uygulama incelemesi içeren App Store'dan 1752 farklı uygulamayı değerlendirmek üzere denetimli ve denetimsiz algoritmalar kullanılmıştır. Ayrıca, destek vektör makinesi sınıflandırıcıları ve incelemelere dayalı duygu analizi kullanılarak geri bildirim döngüleri otomatik olarak analiz edilmiştir. Vu vd. (2019a) Google Play Store'dan seçilen 22 uygulamadan 35.240 yorum makine öğrenmesi teknikleri ile analiz edilmiştir. Araştırma bulgulara dayanarak, mobil uygulama geliştiricilerinin kullanıcı incelemelerine daha başarılı bir şekilde yorum yazmalarına yardımcı olmak için yarı otomatik bir araç önerilmiştir. Srisopha vd. (2020), Google Play Store'daki en popüler 1600 ücretsiz indirilebilir uygulama için kullanıcı derecelendirmelerinde ve geliştirici yanıtlarındaki değişiklikler incelenmiştir. Analiz olarak rastgele orman algoritması kullanılmıştır. Alismail ve Albesher (2023) Suudi Arabistan ve Amerika Birleşik Devletleri'ndeki bankacılık uygulamalarına yönelik geliştirici yanıtlarını incelemiştir. Araştırmanın en temel bulgusu, ABD'li banka uygulama geliştiricilerinin hem yanıt sayısı hem de yanıt kalitesi açısından Suudi Arabistan 'daki geliştiricilerden belirgin şekilde daha iyi performans göstermesidir.

Tablo 1 literatürdeki mobil uygulama yorumları ile ilgili yapılan çalışmaların özetini sunmaktadır. Bu tabloya göre kullanıcı değerlendirmeleri, Google Play Store ve iTunes App Store gibi mobil uygulama mağazalarında en popüler, en iyi ücretsiz, ücretli veya belirli bir alana odaklı uygulamalar üzerinde gerçekleştirilmiştir. Kullanıcı yorum sayıları ise yüzler ile milyonlar arasında değişmektedir. Analiz yöntemleri içerik ve makine öğrenimi algoritmalarına (rastgele orman), denetimli/denetimsiz sınıflandırmalardan deneysel çalışmalara kadar çeşitlilik göstermektedir.

Tablo 1. Kullanıcı Değerlendirmelerine Yönelik Yapılan Çalışmalar

Yazar	Platform	Uygulama Türü	Yorum Sayısı	Analiz
McIlroy vd. (2017)	Google Play Store	En iyi	111.099	Makine Öğrenmesi
Hassan vd. (2018)	Google Play Store	En popüler ücretsiz	4,5 milyon	İçerik Analizi
Bailey vd. (2019)	iTunes App Store	Çeşitli	806.209	Makine Öğrenmesi
Vu vd. (2019a)	Google Play Store	Çeşitli	35240	İçerik Analizi
Vu vd. (2019b)	Google Play Store	Çeşitli	649.645	İçerik Analizi
Srisopha vd. (2020)	Google Play Store	En popüler ücretsiz	228.274	Makine Öğrenmesi
Outay vd. (2021)	Google Play Store	İHA (İnsansız Hava Aracı)	162.250	İçerik Analizi
Savarimuthu vd. (2021)	Google Play Store	En iyi	24.407	İçerik Analizi
Chen vd. (2021)	Google Play Store	En iyi ücretsiz + En iyi ücretli	3+ milyon	Makine Öğrenmesi
Alismail ve Albesher (2023)	Apple App Store ve Google Play Store	Mobil Bankacılık	87174	İçerik Analizi
Bu çalışma	Google Play Store	Mobil Güvenlik	88174	Metin Madenciliği

3. Yöntem

3.1. Araştırma Yöntemi

Bu çalışmanın amacı, McAfee, Avast ve AVG uygulamaları ile ilgili yapılan kullanıcı yorumları ve yıldız derecelendirmelerini analiz etmek olduğu için metin madenciliği yöntemi tercih edilmiştir. Metin madenciliği, veri madenciliğinin özel bir türü olarak değerlendirilmektedir (Akbıyık, 2019). Metin madenciliği, metin tabanlı verilerden gizli ya da örtük bilgilerin ortaya çıkarılmasına yönelik bir süreç olarak

tanımlanmaktadır (Feldman & Sanger, 2007). Metin madenciliği süreci, veri toplama ile başlayıp veri dönüştürme ve modelleme aşamalarına kadar uzanan çok aşamalı ve döngüsel bir yapıya sahiptir. Bu süreçte ilk olarak dokümanlar, internet sayfaları ve kullanıcı yorumları gibi farklı kaynaklardan elde edilen yapılandırılmamış veya yarı yapılandırılmış metin verisi, ön işleme aşamasında doğal dil işleme teknikleri kullanılarak anlamlı bir forma dönüştürülmektedir. Bu kapsamda metinler en küçük birimlere ayrılmakta, cümle öğeleri belirlenmekte, kök bulma (stemming/lemmatization), durak kelime çıkarma ve normalizasyon işlemleri gerçekleştirilmektedir. Ardından metin filtreleme aşamasında analizle ilgisiz veya düşük frekanslı kelime ve kelime öbekleri belirli kriterlere göre veri setinden çıkarılmaktadır. Veri dönüştürme aşamasında ise kelime sıklıkları ve birlikte görülme olasılıkları dikkate alınarak metinler sayısallaştırılmakta ve kelime-doküman matrisi gibi yapılar oluşturulmaktadır. Bu yapılandırılmış veri üzerinden gerçekleştirilen metin madenciliği aşamasında konu modelleme, kümeleme, sınıflandırma ve bağlantı analizi gibi yöntemler uygulanmaktadır (Akbıyık, 2019).

3.2. Araştırma Soruları

Çalışmanın amacı doğrultusunda aşağıdaki araştırma sorularına cevap aranacaktır:

1. McAfee, Avast ve AVG uygulamaları ile ilgili yapılan kullanıcı yorumlarında sıklıkla geçen kelime ve kelime grupları nelerdir?
2. McAfee, Avast ve AVG uygulamalarına yönelik kullanıcı yorumlarında geçen tematik içerikler ile verilen yıldız derecelendirmeleri arasında nasıl bir ilişki vardır?
3. McAfee, Avast ve AVG uygulamalarına yönelik kullanıcı yorumlarında sıklıkla geçen kelimeler 2020–2025 yılları arasındaki nasıl bir değişim göstermiştir?

3.3. Evren ve Örneklem

Araştırma evrenini Google Play Platformu'ndaki aktif olarak çalışan mobil güvenlik uygulamaları oluşturmaktadır. Fakat tüm evrene ulaşılması zaman ve analiz kısıtları nedeniyle mümkün olamadığından örnekleme yoluna gidilmiştir. Bu doğrultuda, çalışmanın örneklemi AVG, McAfee ve Avast olmak üzere üç mobil antivirüs uygulaması ile sınırlandırılmıştır. Bu uygulamaların seçilmesinde Google Play Store üzerinde yaygın biçimde erişilebilir olmaları, yüksek indirme sayılarına sahip bulunmaları, geniş kullanıcı tabanlarına hitap etmeleri ve mobil güvenlik alanında küresel ölçekte bilinen markalar olmaları etkili olmuştur. Ayrıca söz konusu uygulamalar, kullanıcı yorumları bakımından zengin veri sunmaları nedeniyle karşılaştırmalı metin madenciliği analizleri için uygun bir araştırma zemini sağlamaktadır.

3.4. Veri Toplama Aracı

Veri ve metin seti bir uygulama programlama arayüzü olan Apify yardımıyla oluşturulmuştur. Apify web sayfası üzerinden Google Play platformundaki McAfee, Avast ve AVG android uygulamalarından maksimum miktardaki kullanıcı yorumu, yorum tarihleri ve yorumlara ait yıldız derecelendirmeleri çekilmiştir. Tarih aralığı olarak 2011 ile 2025 yılları arasındaki McAfee için 7015, Avast için 36679 ve Avg için 44480 adet kullanıcı yorumu çekilmiştir. Bu çalışmada kullanılan veriler, kamuya açık olarak paylaşılan kullanıcı yorumlarından elde edilmiştir. Veri toplama sürecinde herhangi bir kişisel tanımlayıcı bilgi (isim, kullanıcı kimliği vb.) analiz kapsamına dahil edilmemiş ve tüm veriler anonimleştirilerek değerlendirilmiştir. Araştırma kapsamında yalnızca kullanıcıların uygulamalara yönelik görüş ve değerlendirmeleri analiz edilmiş olup, bireylerin kimliğini ortaya çıkarabilecek herhangi bir işlem gerçekleştirilmemiştir.

3.5. Verilerin Analizi

Veri analiz sürecinden önce kapsamlı bir veri temizleme ve ön işleme süreci yürütülmüştür. Bu kapsamda yinelenen yorumlar, anlamsız içerikler, yalnızca sembol veya sayıdan oluşan kayıtlar ile analiz açısından yetersiz görülen kısa yorumlar veri setinden çıkarılmıştır. Ayrıca dil filtrelemesi uygulanarak analiz kapsamına uygun yorumlar seçilmiş, yazım farklılıkları, büyük-küçük harf uyumsuzlukları ve gereksiz karakterler standartlaştırılmıştır. Son aşamada metin verileri, içerik analizi ve metin madenciliği yöntemlerine uygun hâle getirilerek analiz sürecine dâhil edilmiştir. Elde edilen veri ve metin seti, QDA Miner® ve WordStat® metin madenciliği yazılımları ile analiz edilmiş ve yorumlanmıştır. Çalışmada veri setine dair tanımlayıcı istatistikler yüzde dağılımı seklinde bir Tablo 2 ve Tablo 3'te sunulmaktadır. Ayrıca mobil uygulamalara ilişkin yorumlarda sıkça geçen kelime öbekleri, frekans dağılımları ve kelime bulutu

görselleştirmeleri sunulmuştur. Ardından, yorumlar üzerinde faktör analizi uygulanarak tematik yapılar belirlenmiş ve bu temaların dağılımı ortaya konmuştur. Elde edilen kelime gruplarının uygulama türlerine, yıllara ve yıldız puanlarına göre dağılımı ise grafiklerle görselleştirilmiştir.

Tablo 2. Yıldız Derecelerine Göre Tanımlayıcı İstatistikler

	Yıldız Derecesi	Mutlak Frekans	Oransal Frekans		Yıldız Derecesi	Mutlak Frekans	Oransal Frekans		Yıldız Derecesi	Mutlak Frekans	Oransal Frekans
MCAFEE	1	816	11,63	AVAST	1	2450	6,68	AVG	1	3148	7,08
	2	164	2,34		2	526	1,43		2	699	1,57
	3	331	4,72		3	1615	4,40		3	1703	3,83
	4	681	9,71		4	3532	9,63		4	3947	8,87
	5	5023	71,60		5	28556	77,85		5	34983	78,65
	Toplam	7015	100		Toplam	36679	100		Toplam	44480	100

Tablo 3. Yıllara Göre Tanımlayıcı İstatistikler

	Yıl	Mutlak Frekans	Oransal Frekans		Yıl	Mutlak Frekans	Oransal Frekans		Yıl	Mutlak Frekans	Oransal Frekans
MCAFEE	2011	2	0,03	AVAST	2011	10	0,03	AVG	2011	36	0,08
	2012	43	0,61		2012	727	1,98		2012	444	1,00
	2013	341	4,86		2013	1759	4,80		2013	2387	5,37
	2014	870	12,40		2014	3495	9,53		2014	6092	13,70
	2015	1043	14,87		2015	5497	14,99		2015	13053	29,35
	2016	895	12,76		2016	2544	6,94		2016	4510	10,14
	2017	591	8,42		2017	1200	3,27		2017	2938	6,61
	2018	518	7,38		2018	1226	3,34		2018	1285	2,89
	2019	588	8,38		2019	2210	6,03		2019	1357	3,05
	2020	683	9,74		2020	5474	14,92		2020	3052	6,86
	2021	790	11,26		2021	4864	13,26		2021	3209	7,21
	2022	236	3,36		2022	3041	8,29		2022	2493	5,60
	2023	135	1,92		2023	1967	5,36		2023	1868	4,20
	2024	214	3,05		2024	1766	4,81		2024	1328	2,99
	2025	66	0,94		2025	899	2,45		2025	428	0,96
	Toplam	7015	100		Toplam	36679	100		Toplam	44480	100

4. Bulgular

Bu bölümde QDA Miner® ve WordStat® yazılımları aracılığıyla kullanıcıların McAfee, Avast ve AVG mobil uygulamalarına yaptıkları yorum ve değerlendirmelerinde; en sık kullanılan kelimeler, kelime grupları, yıldız derecelendirmeleri ve yorumlara yönelik yıl bazlı analizler gerçekleştirilmiştir. Veri ve metin seti üzerinde yapılan analizler neticesinde elde edilen bulgular ortaya konulmuş ve yorumlanmıştır. Bölüm üç ana başlık altında gruplandırılmıştır. Birinci başlıkta sık kullanılan kelime ve kelime gruplarına, ikinci başlıkta yıldız derecelendirme düzeylerine göre kullanılan kelimelere ve üçüncü başlıkta spesifik kelimelerin yıllara göre dağılımlarına değinilmektedir.

4.1. Sık Kullanılan Kelime ve Kelime Grupları

Şekil 1, 2 ve 3 frekansı en yüksek olan kelimeleri ve kelime gruplarını göstermektedir. Bu şekillere bakıldığında yapılan yorumlar içerisinde en sık kullanılan kelimelerin "güzel, iyi, tavsiye, kişisel, antivirüs, süper, mükemmel" gibi kelimeler olduğu görülmektedir. Kelime bulutları, McAfee, Avast ve AVG mobil güvenlik uygulamalarına yönelik kullanıcı yorumlarında belirgin biçimde pozitif bir algının hâkim olduğunu göstermektedir. Üç uygulama için de en baskın ifadeler olan "güzel", "iyi", "mükemmel" ve "harika" gibi olumlu nitelikler, kullanıcı memnuniyetinin yüksekliğine işaret etmektedir. Ayrıca "tavsiye ederim" ifadesinin her üç görselde de öne çıkması, kullanıcıların uygulamaları başkalarına önermeye istekli olduklarını ve marka sadakatinin güçlü olduğunu ortaya koymaktadır. Avast ve AVG'de görülen "TC

kimlik", "kişisel veriler", "iznim yoktur" gibi ifadeler ise veri gizliliği ve kişisel bilgi güvenliği konularında farkındalığın yüksek olduğunu yansıtmaktadır. McAfee'de ise memnuniyet ve kullanım kolaylığına ilişkin ifadeler daha baskın görünmektedir. Bu bulgular, mobil güvenlik uygulamalarının yalnızca zararlı yazılımlara karşı koruma sağlamada değil, aynı zamanda kullanıcı güveni ve tavsiye davranışını teşvik etmede de etkili olduğunu göstermektedir.

Şekil 1. McAfee Mobil Uygulaması Yorumları Kelime Bulutu

Şekil 2. Avast Mobil Uygulaması Yorumları Kelime Bulutu

Şekil 3. AVG Mobil Uygulaması Yorumları Kelime Bulutu

Tablo 4 sık kullanılan kelime gruplarını göstermektedir. Kullanıcı yorumlarının metin madenciliği ile incelenmesi sonucunda, McAfee, AVG ve Avast uygulamalarına yönelik değerlendirmelerde sık tekrar edilen ifadeler, hem içerik hem de ayırt edicilik düzeyinde anlamlı farklılıklar göstermektedir. Tüm uygulamalarda "Tavsiye ederim", "Güzel bir" ve "Çok iyi" gibi olumlu yargılar öne çıkarken, TF-IDF skorları bu ifadelerin uygulamalara özgü farklılıklarını ortaya koymaktadır. AVG yorumlarında ise "AVG Antivirüs" ve "Güzel bir uygulama" ifadeleri yüksek TF-IDF skorlarıyla dikkat çekerken, "İznim yoktur" ifadesinin sıkça kullanılması

(690) ve yüksek ayırt ediciliği (TF-IDF: 1254,6), kullanıcıların veri gizliliğine dair endişelerini ortaya koymaktadır. Avast kullanıcıları ise "Çok güzel", "Avast Antivirüs" ve "Herhangi bir" gibi ifadelerle hem uygulamaya yönelik memnuniyetlerini hem de genel değerlendirmelerini daha yoğun biçimde dile getirmiştir. Ayrıca Avast yorumlarında yer alan "TC kimlik" ve "İznim yoktur" gibi ifadelerin göreli sıklığı, bu uygulamaya özgü bir veri güvenliği algısını da işaret etmektedir. Bu sonuçlar, kullanıcıların sadece uygulama performansına değil, aynı zamanda veri güvenliği, gizlilik ve kişisel bilgilere ilişkin hassasiyetlerine de yorumlarında yer verdiklerini göstermektedir.

Tablo 4. Sık Kullanılan Kelime Grupları

	Kelime Grupları	**Frekans**	**Vaka (%)**	**Tf • Idf**
MCAFEE	Tavsiye Ederim	365	5,16	469,9
	Güzel Bir	236	3,36	347,7
	Bir Program	190	2,65	299,5
	Herkese Tavsiye Ederim	91	1,28	172,2
	Harika Bir	86	1,21	164,8
	Google Play	81	1,07	159,6
	İyi Bir	71	1,01	141,6
	Teşekkür Ederim	70	1,00	140,1
	En İyi	66	0,93	134,2
	Google Play Store	61	0,80	128,0
AVAST	Tavsiye Ederim	1659	4,50	2235,0
	Çok Güzel	1619	4,34	2205,4
	Avast Antivirüs	1617	4,07	2247,7
	Çok İyi	1477	3,92	2077,2
	Google Play	1417	3,77	2016,8
	Play Store	1389	3,75	1981,3
	Herhangi Bir	1111	2,80	1724,7
	Ve Avast	919	2,49	1474,5
	Güzel Bir Uygulama	889	2,41	1438,4
	Bu Uygulamayı Tarihinde	785	2,14	1310,6
AVG	Tavsiye Ederim	2202	4,93	2877,9
	AVG Antivirüs	1055	2,03	1785,6
	Güzel Bir Uygulama	1026	2,29	1682,2
	Play Store	925	2,05	1562,4
	İznim Yoktur	690	1,52	1254,6
	Çok Guzel	615	1,38	1143,5
	Çok İyi	600	1,35	1122,4
	Bir Uygulama	470	1,05	930,5
	Google Play Store	459	1,03	912,6
	Güzel Uygulama	447	1,00	893,5
	Tavsiye Ederim	2202	4,93	2877,9
	AVG Antivirüs	1055	2,03	1785,6

4.2. Yıldız Derecelendirme Düzeylerine Göre Kullanılan Kelimeler

Tablo 5 uygulamalara yönelik kullanıcı değerlendirmelerinin yıldız derecelerine göre nasıl değiştiğine dair önemli bilgiler sunmaktadır. McAfee, Avast ve AVG uygulamaları için yapılan incelemede, 5 yıldızlı yorumlarda olumlu duygu yüklü ifadelerin ("güzel", "iyi", "harika", "süper", "tavsiye") yüksek frekanslarla kullanıldığı görülmektedir. Özellikle McAfee'de "güzel" (827) ve "iyi" (580) kelimeleri öne çıkarken, AVG'de "güzel" kelimesi 5504 kez kullanılarak kullanıcı memnuniyetinin en açık göstergesi olmuştur. Benzer şekilde, Avast kullanıcıları da 5 yıldızlı yorumlarda "güzel" (4506), "iyi" (3934) ve "tavsiye" (1906) gibi olumlu nitelendirmelere sıklıkla başvurmuştur. Ancak yıldız derecesi azaldıkça kullanılan kelimelerde belirgin bir dönüşüm göze çarpmaktadır. Özellikle 1 yıldızlı yorumlarda AVG ve Avast kullanıcılarının "virüs", "yok", "para", "hiç" ve "kişisel" gibi daha olumsuz ya da eleştirel ifadeleri tercih ettiği, veri güvenliği ve uygulama işlevselliğine ilişkin rahatsızlıkları vurguladığı gözlemlenmektedir. McAfee'de ise 1 yıldızlı yorumlarda "VPN", "yok" ve "telefon" gibi teknik veya işlevsel sorunlara gönderme yapan ifadeler dikkat çekmektedir. Bu durum, düşük puan veren kullanıcıların daha çok gizlilik, veri kullanımı ve beklenti karşılamama gibi

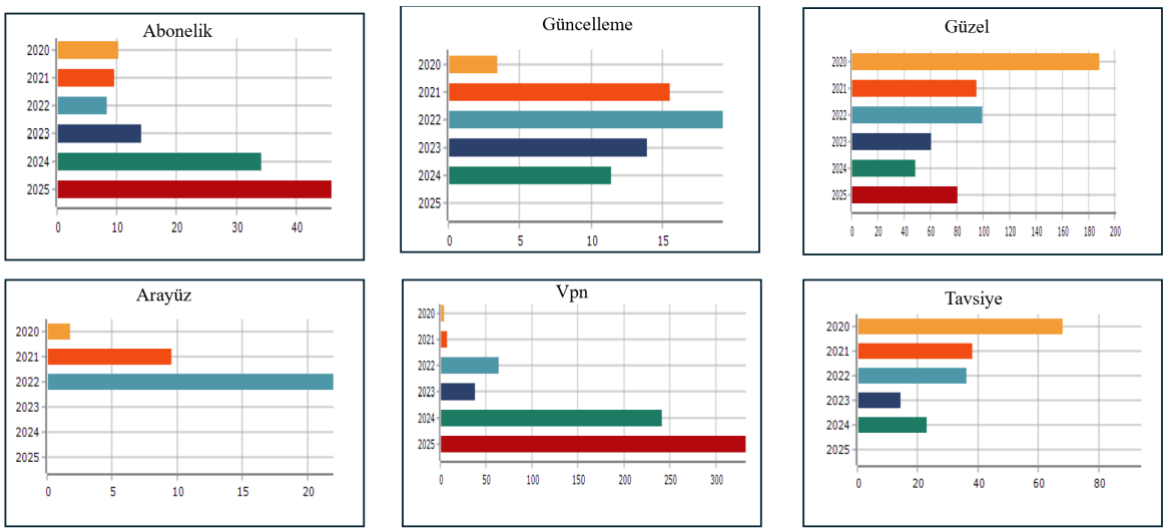
konulara odaklandığını göstermektedir. Özetle, olumlu yıldız puanlarında duygusal ve genel memnuniyet belirten ifadeler ön plana çıkarken; düşük puanlı yorumlar, teknik sorunlara, hizmet memnuniyetsizliğine ve kişisel veri hassasiyetine odaklanmaktadır.

Tablo 5. Yıldız Derecelendirme Düzeylerinde En Sık Kullanılan Kelimeler

	5 Yıldız Kelimeler		4 Yıldız Kelimeler		3 Yıldız Kelimeler		2 Yıldız Kelimeler		1 Yıldız Kelimeler	
MCAFEE	**Kelime**	**Frekans**	**Kelime**	**Frekans**	**Kelime**	**Frekans**	**Kelime**	**Frekans**	**Kelime**	**Frekans**
	Güzel	827	Güzel	140	İyi	38	Telefon	18	VPN	82
	İyi	580	İyi	122	McAfee	35	McAfee	16	Yok	81
	Tavsiye	393	Uygulama	43	Var	35	Yok	13	Sonra	73
	Harika	381	Program	42	Sonra	32	VPN	13	Var	66
	Süper	320	McAfee	37	Yok	31	Güzel	13	Para	62
	Program	290	Tavsiye	35	Uygulama	30	Var	12	Telefon	61
	Mükemm	271	Play	34	VPN	28	Sonra	12	Uygulama	55
AVAST	**5 Yıldız Kelimeler**		**4 Yıldız Kelimeler**		**3 Yıldız Kelimeler**		**2 Yıldız Kelimeler**		**1 Yıldız Kelimeler**	
	Kelime	**Frekans**	**Kelime**	**Frekans**	**Kelime**	**Frekans**	**Kelime**	**Frekans**	**Kelime**	**Frekans**
	Güzel	4506	Kişisel	610	Kişisel	388	Kişisel	91	Virüs	298
	İyi	3934	Güzel	541	İndirdim	327	İndirdim	75	Para	164
	Tavsiye	1906	Antivirüs	473	Antivirüs	277	Tarihinde	54	İndirdim	163
	Virüs	1517	İndirdim	467	Sorumlud	257	Antivirüs	53	Hiç	162
	Harika	1480	Sorumludu	452	Tarihinde	249	Sorumlud	51	Kişisel	152
	Süper	1415	İyi	443	Kimlik	179	Virüs	47	Antivirüs	147
	Antivirüs	1415	Tarihinde	420	Herhangi	178	Herhangi	43	Yok	141
AVG	**5 Yıldız Kelimeler**		**4 Yıldız Kelimeler**		**3 Yıldız Kelimeler**		**2 Yıldız Kelimeler**		**1 Yıldız Kelimeler**	
	Kelime	**Frekans**	**Kelime**	**Frekans**	**Kelime**	**Frekans**	**Kelime**	**Frekans**	**Kelime**	**Frekans**
	Güzel	5504	Güzel	646	AVG	295	AVG	92	Virüs	276
	İyi	4238	İyi	558	Uygulama	238	İndirdim	74	AVG	231
	Tavsiye	2453	AVG	490	Kişisel	224	İçin	69	Yok	229
	Süper	2156	Uygulama	383	İndirdim	209	Uygulama	64	Uygulama	215
	Harika	2111	Kişisel	383	İçin	187	Play	59	İçin	205
	Çok	2087	İçin	323	Antivirüs	185	Antivirüs	56	İyi	183
	Program	1861	Antivirüs	316	Play	183	İyi	54	Program	168

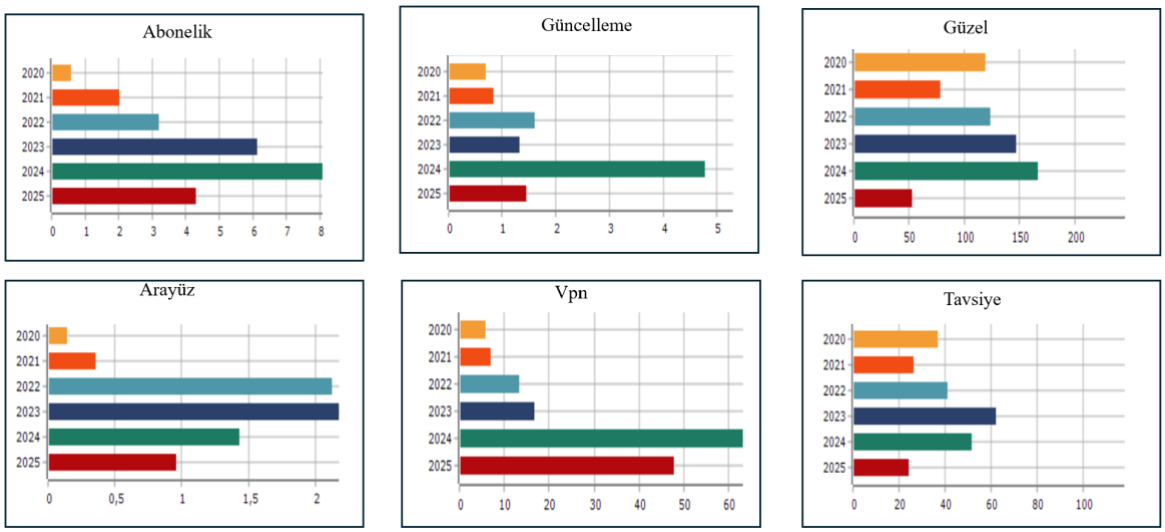
4.3. Spesifik Kelimelerin Yıllara Göre Dağılımları

Şekil 4 McAfee kullanıcı yorumlarının yıllara göre içerik dağılımını göstermektedir. Şekil 4'e göre, uygulamaya yönelik algının zaman içinde nasıl bir dönüşüm geçirdiği görülmektedir. 2020–2025 yılları arasında belirli anahtar kavramların kullanım sıklığına bakıldığında, kullanıcıların ilk yıllarda daha çok duygusal değerlendirmelere odaklandığı; ilerleyen yıllarda ise daha teknik ve işlevsel konulara yöneldiği gözlemlenmektedir. Örneğin, 2020 yılında en sık kullanılan ifadelerden biri olan "güzel", bu yıl yaklaşık 180 kez kullanılmışken, bu sayı 2025'te 80'nin altına düşmüştür. Benzer şekilde, "tavsiye" ifadesi de 2020'de en yüksek seviyedeyken, sonraki yıllarda düzenli bir azalma göstermektedir. Bu durum, kullanıcı memnuniyetinde bir azalma yaşandığını ya da yorumların duygusal ifadelerden işlevsel geri bildirimlere kaydığını göstermektedir. Nitekim 2025 yılında "abonelik" ve "VPN" gibi teknik terimlerin kullanımı en yüksek seviyeye ulaşmıştır. Özellikle "VPN" ifadesinin 2025 yılında 300'ü aşan frekansla öne çıkması, bu özelliğe yönelik kullanıcı ilgisinin arttığına işaret etmektedir. Ayrıca 2022 yılında "arayüz" kelimesinin dikkat çekici biçimde artması, bu dönemde yaşanan tasarımsal değişikliklerin kullanıcılar tarafından fark edildiğini ve yorumlara yansıdığını göstermektedir. Ancak bu ifadenin 2023, 2024 ve 2025 yıllarında kullanıcı yorumlarında anlamlı bir şekilde yer almaması, söz konusu tasarım değişikliklerinin sonraki yıllarda kullanıcı beklentilerine uyum sağladığını düşündürmektedir. Güncelleme kelimesinin yıllar içindeki dağılımına bakıldığında, 2020–2024 döneminde belirli bir sıklıkta yer aldığı, ancak 2025 yılı yorumlarında geçmediği görülmektedir.



Şekil 4. McAfee- Yıllara Göre Spesifik Kelime Analizi

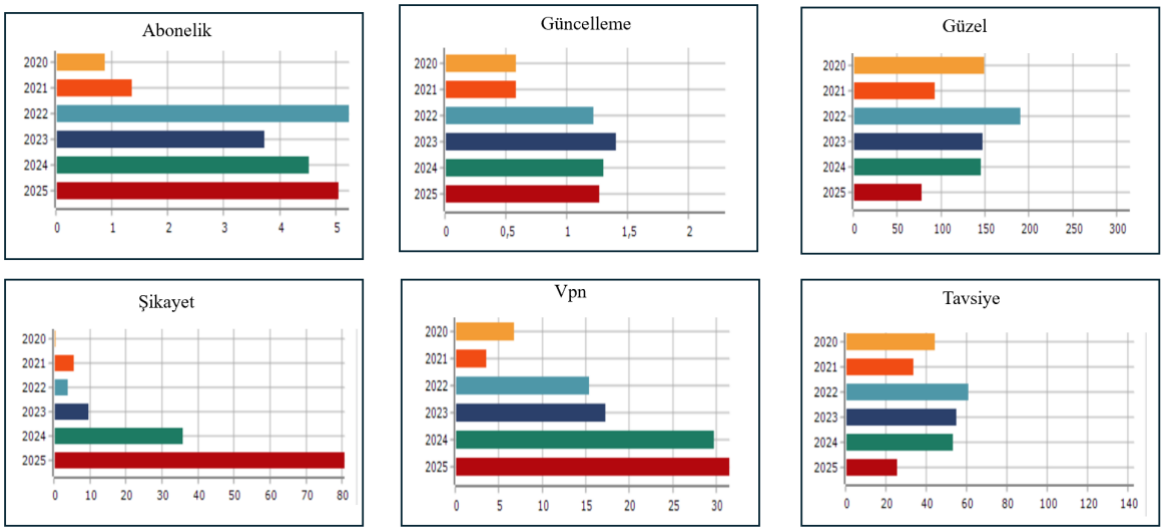
Şekil 5 Avast uygulamasına ilişkin kullanıcı yorumlarının yıllık dağılımını, kullanıcıların algısındaki değişimi ve metin içeriklerinin tematik dönüşümünü göstermektedir. 2020–2025 arası dönemde "güzel" ve "tavsiye" gibi olumlu duygular içeren ifadelerin frekansı, özellikle 2020–2023 yılları arasında görece yüksek seyretmiş, ancak 2024 ve 2025 yıllarında belirgin biçimde azalmıştır. Örneğin, "güzel" ifadesi 2024'de en yüksek seviyeye ulaşmışken, 2025'te frekansı yarıdan daha aza düşmüştür. Benzer şekilde "tavsiye" kelimesi 2023'te zirveye ulaşmış ve ardından azalmıştır. Nitekim "abonelik" ve "güncelleme" gibi işlevsel konulara ilişkin yorumların özellikle 2024 yıllında artış göstermesi, kullanıcıların kullanım sürecinde yaşadıkları deneyimlere dair daha somut geri bildirim sunduklarını göstermektedir. Özellikle "VPN" ifadesinin 2024 ve 2025 yıllarında en yüksek seviyelere ulaşması, bu özelliğin kullanıcılar açısından önemli hâle geldiğini göstermektedir. Ayrıca 2023 yılında "arayüz" kelimesinin frekansında görülen zirve, olası bir tasarım değişikliğine kullanıcıların doğrudan tepki verdiklerini düşündürmektedir.



Şekil 5. Avast- Yıllara Göre Spesifik Kelime Analizi

Şekil 6 AVG uygulamasına ait kullanıcı yorumlarındaki yıllık kelime kullanım sıklığını göstermektedir. Ayrıca, farklı temaların zaman içinde nasıl değişim gösterdiği görülmektedir. "Abonelik" teması, 2020'den 2025'e kadar istikrarlı bir artış sergilemiştir. Bu durum, kullanıcıların abonelik politikalarına yönelik farkındalığının kullanıcı yorumlarında her yıl sıklıkla geçtiğini düşündürmektedir. "Güzel" kelimesi, kullanıcı memnuniyetini yansıtan bir ifade olarak değerlendirildiğinde, 2020'den 2025'e kadar benzer düzeyde kalmıştır. "Şikayet" kelimesindeki çarpıcı artış, özellikle 2024 ve 2025 yıllarında belirginleşmiştir. Bu, son dönemde kullanıcı memnuniyetsizliğinin kayda değer biçimde arttığına işaret edebilir. Benzer şekilde

"VPN" kelimesi de zamanla daha sık kullanılmaya başlanmış ve 2025'te maksimum seviyeye ulaşmıştır. Bu artış, kullanıcıların VPN işlevselliğiyle daha fazla ilgilendiğini veya bu konudaki sorunları daha çok dile getirdiğini gösterebilir. Son olarak, "Tavsiye" kelimesi, 2020-2025 yılları arasında görece dengeli seyretmiştir. AVG uygulamasına ait kullanıcı yorumlarında "arayüz" ifadesinin 2020-2025 yılları arasında hiç yer almadığı için grafiği oluşmamıştır. Bu sebeple şekil 6' ya eklenememeştir. Bu durum birkaç olasılıkla açıklanabilir. İlk olarak, kullanıcıların arayüzle ilgili memnuniyetsizlik ya da övgü belirtme ihtiyacı duymamış olmaları, arayüz tasarımının artık beklentileri karşılayan, istikrarlı ve alışılmış bir düzeye ulaştığını gösterebilir. Diğer yandan, uygulamanın son yıllarda arayüz açısından kayda değer bir değişiklik sunmaması da yorumlarda bu temanın gündeme gelmemesine neden olmuş olabilir. Sonuç olarak, "arayüz" temasının yorumlarda yer almaması, kullanıcı deneyiminde bu unsurun artık sorun yaratmadığını ya da dikkat çekici bir yenilik içermediğini düşündürmektedir.



Şekil 6. AVG- Yıllara Göre Spesifik Kelime Analizi

4.4. Yorumlara Yönelik Faktör Analizi

WordStat yazılımında konu çıkarımı sürecinde temel istatistiksel yöntem olarak faktör analizi kullanılmıştır. Veri setinde yer alan tematik yapıların belirlenmesi amacıyla uygulanan bu analizde, Varimax rotasyon yöntemi tercih edilmiş ve faktör yükü eşik değeri 0.20 olarak belirlenmiştir. Yorumlarda birlikte geçen kelimeler arasındaki ilişkiler dikkate alınarak oluşturulan faktör yapısı toplamda 10 boyut altında toplanmıştır.

Tablo 6, McAfee uygulamasına ait toplam 7015 kullanıcı yorumunun tematik olarak 10 boyut altında toplandığını göstermektedir. Birinci sırada yer alan boyutun, kullanıcıların uygulamayı indirirken ve kullanırken kişisel verilerinin üçüncü şahısların eline geçmesine yönelik endişelerini yansıttığı görülmektedir. Bu boyutta, iletişim bilgileri, kimlik verileri ve banka bilgilerinin paylaşılması ya da ele geçirilmesi riskine ilişkin ifadeler öne çıkmaktadır. İkinci sıradaki boyut, benzer şekilde kullanıcıların kişisel verilerinin üçüncü şahıslarla paylaşılması durumunda oluşabilecek risklere ve sorumluluklara ilişkin algılarını kapsamaktadır. Üçüncü sıradaki boyutun, kullanıcıların veri güvenliği ihlallerine karşı hukuki yaptırımlara atıfta bulunduğu görülmektedir. Dördüncü sıradaki boyut, kullanıcıların uygulama satın alma, abonelik ve teknik destek süreçlerine ilişkin deneyimlerini içermektedir. Beşinci sıradaki boyut, kullanıcıların kişisel verilerinin izinsiz paylaşılmasına yönelik açık bir karşı duruş sergilediğini göstermektedir. Bu boyutta, kullanıcıların veri gizliliği, izin mekanizmaları ve kişisel güvenlik konularında hassasiyet taşıdığı görülmektedir. Altıncı sıradaki boyut, kullanıcıların uygulamayı Google Play Store üzerinden indirirken veri güvenliği ve olası zararlardan kimin sorumlu olduğuna ilişkin algılarını yansıtmaktadır. Yedinci sıradaki boyut, kullanıcıların uygulamayı cihazlarını virüslerden koruma amacıyla indirdiklerini ve kullanım bağlamını ifade eden yorumları içermektedir. Sekizinci sıradaki boyut, kimlik bilgileri, banka verileri ve diğer hassas kişisel bilgilerin korunmasına yönelik kullanıcı endişelerini kapsamaktadır. Dokuzuncu sıradaki boyut, kullanıcıların olası veri ihlalleri durumunda yasal haklarını kullanacaklarını ifade ettikleri yorumları

içermektedir. Onuncu ve son boyut ise, kullanıcıların uygulamaya yönelik olumlu değerlendirmelerini içermektedir.

Tablo 6. McAfee- Faktör Analizi

Nu	Faktör Adı	Anahtar Kelimeler	VAR %	Frekans	Vaka	Vaka%
1	Kurduğum	kurduğum; kişilerin; geçmesi; iletişim; konum; eline; şahıs; kartı; sorumlusu; arama; verilerin; LLC; üçüncü; banka; fotoğraf; kaydı; ses; sorumludur; Store; kimlik; vb.; Play; mesaj; Google; benim; TC benim ve iletişim kurduğum kişilerin; indirdim benim; üçüncü şahıs kişilerin eline geçmesi	*0,798*	183	76	1,08
2	Şahıslarla	şahıslarla; olacağını; sorumlu; mesajlarım; ikinci; paylaşılması; kart; üçüncü; bulunan; bilgilerim; durumunda; kimlik; LLC; fotoğraflarım; Play; Google; Store; bildiririm; security; cihazımda; herhangi; mobile; olan; saati; kişisel; sorumludur; McAfee; uygulaması; bilgilerin; banka; cihazıma; geçmesi; verilerimin; TC; vb.; ile; şahıs; Türkiye; kişilerin; ses kart bilgilerim; kimlik bilgilerim; cihazıma yükledim	*0,743*	567	175	2,49
3	Türk Ceza Gereği	ceza; gereği; maddesi; aktarılması; hukuki; işlem; kullanılması; bilgilerimin; Türk; yasal; durumunda Türk Ceza Kanunu'nun maddesi gereği; Türk ceza; maddesi gereği	0,789	117	44	0,63
4	Satın Aldım; Sonra	aldım; sonra; diyor; yardımcı; satın; iptal; müşteri; istiyorum; kodu; olursanız; kullanamıyorum; abonelik; mail; VPN özelliği; sonra tekrar; devam edelim; PIN kodu; yardımcı olur musunuz; hata veriyor; tekrar yükledim; satın aldım; giriş yapamıyorum; bir süre sonra; para iadesi; bir süre; Türk Telekom	0,225	10	29	0,14
5	İznim Yoktur	iznim; yoktur; paylaşılmasına; rehber; ses; kaydı; fotoğraf; banka; verdiğim; indiriyorum; video; hesap; fotoğraflar; bilgiler; bilgileri; kimlik; verilerimin; sorumludur; kişisel; güvenliği; TC; durumda; bilgilerim; Store; numaraları; özel; numaram; vb.; kapalı; geçmesi; LLC; tüm; Samsung Galaxy; konum; Play; indirdiğim	0,685	369	121	1,72
6	Google Play; Sorumludur	sorumludur; Play; Store; mobile; Google; bilgilerin; security; halinde; korumak; saat; ait; indirdim; tarafıma; zararlı; tarihinde; telefonumu; virüslerden; sızdırılması; uygulamayı; kişisel; kişisel; kullanılmasını; TC; banka; kimlik; numaram; veya tarafıma ait	0,712	567	175	2,49
7	Türkiye; Cihazımı	Türkiye; cihazımı; virüsler; civarında; saati; tarihinde; indirdim; korumak; uygulamayı; şahıs; saatiyle; saat; virüslerden; üçüncü; casus; ile; cihazıma; uygulamayı tarihinde Türkiye saati ile	0,636	219	128	1,82
8	Tc Kimlik; Kimlik	TC; kimlik; bilgileri; vb.; kartı; bilgim; kredi; kişisel; posta; işlemleri; banka; amaçlı; kullanılmasını; dışında; fotoğraflarım; ses; olmadan; telefonumdaki; iznim; kaydı; fotoğraflar; gerekli; bilgilerim; diğer; veya; buna; numaraları; numaram; bildiririm; tarihinde	0,619	308	119	1,70
9	Yasal Haklarımı	haklarımı; kullanacağımı; bildiririm; yasal; verilerimin; durumunda; türlü; kişisel; paylaşılması; işlemleri; halinde; durum; olumsuz; gerekli yasal haklarımı; bir durum; yasal haklarımı kullanacağımı bildiririm; kullanılması durumunda	0,615	152	69	0,98
10	Virüs	virüs; olsun; tane; Allah; razı; sildi; buldu; var; en; programı; tespit; tarama; hepsini virüsü buldu; Allah razı olsun; ellerine sağlık; razı olsun; en iyi güvenlik; helal olsun; tane virüs; ne olsun; tebrik ediyorum; başarılı bir; teşekkür ederim; iyi program; yıldızı hak ediyor; gerçekten güzel; gerçekten güzel bir; hiç düşünmeden; başarılı bir; virüs buldu; eline sağlık; süper ötesi; bence en; en iyi; süper bir; yıldızı hak	0,224	28	27	0,38

Tablo 7, Avast uygulamasına ait kullanıcı yorumlarının tematik olarak 10 boyut altında toplandığını göstermektedir. Birinci boyutta kullanıcıların cihazlarında bulunan görüntüler, telefon numaraları, kimlik bilgileri ve diğer kişisel verilerin paylaşılması veya dışa aktarılmasına yönelik ciddi endişeler taşıdığı anlaşılmaktadır. İkinci boyutta TC kimlik bilgileri, banka verileri, parmak izi, mesajlar ve özel içeriklerin korunmasına yönelik hassasiyet öne çıkmaktadır. Üçüncü boyut rehber, mesajlar, banka bilgileri ve sosyal medya hesaplarına erişim izinlerine karşı kullanıcı direncini yansıtırken, dördüncü boyut uygulamanın temel işlevi olan virüs temizleme, reklam kaldırma ve cihaz performansını iyileştirme konusundaki olumlu değerlendirmeleri içermektedir. Beşinci boyut VPN, proxy ve veri aktarımı gibi ek hizmetlere yönelik algıları yansıtmakta, altıncı boyut ise kullanıcıların veri ihlali durumunda maddi ve manevi tazminat talebinde bulunabileceklerini ifade ettikleri yorumları kapsamaktadır. Yedinci boyutta bazı kullanıcıların verilen izinleri

telefon güvenliği için gerekli gördüğü anlaşılırken, sekizinci boyut kullanıcıların olası sorunlarda yetkili mercilere şikâyette bulunma eğiliminde olduğunu göstermektedir. Dokuzuncu boyutta Türk Ceza Kanunu ve yasal işlem ifadeleri öne çıkmakta, kullanıcıların veri ihlallerini cezai yaptırımlarla ilişkilendirdiği görülmektedir. Son boyut ise uygulamanın telefon performansına katkısı, kullanım kolaylığı ve genel memnuniyet düzeyi gibi olumlu deneyimleri yansıtmaktadır. Bulgular genel olarak değerlendirildiğinde kullanıcı yorumlarının yalnızca uygulamanın virüs temizleme performansına değil, aynı zamanda kişisel veri güvenliği, gizlilik kaygıları, hukuki sorumluluk beklentileri ve genel kullanıcı deneyimine odaklandığı görülmektedir.

Tablo 7. Avast- Faktör Analizi

Nu	Faktör Adı	Anahtar Kelimeler	VAR %	Frekans	Vaka	Vaka%
1	Herhangi Bir Görüntü; Veriler	numarası; cihazımdaki; tc; herhangi; kimlik; telefon; numaralar; paylaşılması; kişisel dışa aktarılması paylaşılması; razı değilim ve kabul etmıyorum; paylasılması durumunda asla razı değilim; cihazdakı tüm veriler; kabul etmiyorum; tüm veriler; dışa aktarılması; cıhazımdakı tüm verıler; herhangi bir görüntü; razı değilim; paylaşılması durumundan; razı değilim; kişisel verıler; kişisel verıler; kabul etmıyor; durumuna razı değilim; ındırıp kullanmaya başladım; kullanmaya başladım; dışa aktarılması; cihazımdakı tüm veriler; kullanılması dışa aktarılması paylaşılması durumundan	0,813	3853	1534	4,18
2	Tc Kimlik; Kişisel	kişisel; kimlik; tc; ses; tarihinde; sorumludur; indirdim; antivirüs; video; telefon; banka; numarası; herhangi; no; durumunda; saat; bilgilerim; vermiyorum; bilgilerimin; paylaşılması; izin; fotoğraf; aksi; yasal; iznim; yoktur; resim; bilgileri; kart; belge; kullanılması; mesaj; durumda; dosya; işlem; hukuki; parmak; ait; görüntü; güvenlik; özel; numaram; paylaşılmasına; sorumluluk; korumak; aittir; takdirde; kredi; medya; haklarımı; veriler; sosyal; izi; durumunda	0,534	22358	4633	12,63
3	İznim Yoktur; Rehber	rehber; yoktur; kopyalanmasına; fotoğraflar; paylaşılmasına; iznim; videolar; mesajlar; banka; dosyalar; kişisel; belgeler; ses; şifreler; bilgileri; sosyal; kullanılmasına; bilgiler; şekilde; parmak; medya; kayıtları; hesapları; hiçbir; izi; izin; kimlik; fotoğraf; erişimine; vermiyorum; konum; resimler; no; tc; içindir; şifreleri; izinler; dosya; verdiğim; vs; verilerimin; telefon; telefonumdaki; numarası kopyalanmasına iznim yoktur; erışıme izin; tc kımlık bılgıleri; şahıslara paylaşılmasına; ses kayıtları; rehber banka; erışımıne ızın verdığım; iznim yoktur; paylaşılmasına asla iznim yoktur; banka bilgileri; sosyal medya bilgileri; izin verdiğim; erışıme izin verdiğim; paylaşılmasına ve kopyalanmasına iznim yoktur;	0,584	6359	2769	7,55
4	Virüs	virüs; reklam; virüsü; diye; vardı; yok; sürekli; buldu; hemen; sildim virüsü hemen; vırüsü bulup; virüs yok; reklam geliyordu; reklamlar çıkıyordu; telefona virüs; yok ettı; reklam çıkıyordu; ıyısı yok; durduk yere reklam; artık yok; hemen buldu; şu ana; mükemmel bi; reklam virüsü; sürekli reklam; virüsü yok; reklam çıkıyor; hemen temizledi; gerçekten çok iyi; bilgisayarımda da kullanıyorum; virüsten kurtuldum; şey yok; pişman oldum; durduk yere; reklam çıkıyodu; kasma yok; sıkıntı yaşamadım; tabletimde virüs vardı; antı vırüs uygulaması; olmama rağmen; söze gerek yok; yok oldu; artık reklam; iyi değil; güzel olur; süper süper; gerek yok; beş para etmez; şimdilik güzel; bazı özellıkler; para etmez; uygun fiyatlı; bence en iyi; gönül rahatlığıyla; süreklı reklam çıkıyordu; gerçekten çok güzel; ram takviyesi; aydır kullanıyorum; bı şey; bulup sildi; güzel bir antıvırüs programı; otomatık tarama; güzel bi; arka planda; teşekkür ediyorum; süper bı; türkçe dil; virüs buldu	0,283	226	215	0,59
5	Unlimited proxy; Yetkilendirme	yetkililerine; proxy; unlimited; aittir; verilerin; sorumluluk; durumunda; cihazımdaki; vpn; dışarı; paylaşılması; cihazımdaki; playstore; süper; aktarılması unlımıted proxy; paylasılması dışarı aktarılması durumunda sorumluluk; dışarı aktarılması durumunda sorumluluk; cihazımdakı tüm verilerin paylaşılması; cihazımdakı bu verilerin kullanılması	0,707	1558	501	1,37
6	Manevi	manevi; maddi; tazminat; davası; sosyal; medya; zarar; gelirse; whatsapp; yapılan; türlü; hesaplarım; google; bilgim; paylaşılırsa;	0,584	740	469	1,28

		kart; açacağım; açarım; kredi; açılacaktır; bilginize; zarardan türlü maddı ve manevı; eğer medya; paylaşılırsa her türlü maddı; google hesabı; türlü maddı; maddi ve manevi dava açılacaktır; google hesapları; maddi ve manevi tazminat davası; açarım bilginize; zarar gelirse; zarar görürse; şahsın elıne geçerse; türlü maddı manevı; bilgilerime zarar gelirse; bilgilerime zarar; şahıslarla paylaşılırsa; manevi tazminat davası				
7	İzinler	izinler; içindir; tür; güvenliği; telefonumun; durumlarda; parmak; işlem; indiriyorum; yaşayabileceğim; izi; iznim; gerekli; başlatılacaktır; yoktur; sorundan; sorumludur; kendim; kendimin; mesajlar; sorunda; içindeki; durumlardan; kopyalanmasına; uygulamaları; yasal izinler telefonumun güvenlığı içindir; gerekli durumlarda yasal işlem başlatılacaktır; içindeki bilgilerin güvenliği ıçındır; telefonumun güvenlığı içindir; içindeki bilgilerin; uygulamayı kendimin; gerekli durumlarda yasal işlem; sorumludur gerekli durumlarda yasal ışlem; gereklı durumlarda; uygulamaları sorumludur gerekli; güvenliği içindir; telefonum için indiriyorum; tür durumlarda; gerekli durumlarda yasal işlem yapılacaktır; tüm izinler	0,643	1950	1095	2,99
8	Gerekli Yerlere; Bulunacağım	bulunacağım; yetkili; şikayette; yerlere; durumda; uygulamasına; başladım; kullanmaya; zubat; indirip; durumundan; yetkililerine durumda yetkili yerlerle şikayette bulunacağım; durumda gerekli yerlere; yerlere şikayet; durumda gerekli yerlere şikayet	0,758	658	289	0,79
9	Türk Ceza	ceza; türk; maddesi; gereğince; kanunu; kanununun; başlatırım; işlem; gereği; işlemlere; zararlı; yapılacaktır; yasal türk ceza kanunu maddesi gereğince; uygulanmasını arz ederım; maddesi gereğince hukukı; türk ceza kanununun maddesi gereğince; bilgisayarımdada kullanıyorum; maddesı gereğınce yasal ışlem yapılacaktır; olursa türk ceza; türk ceza kanununun	0,535	504	220	0,60
10	Telefonum	benim; telefon; için; uygulama; değil; en iyi; içinde; çok; bu uygulamayı yapabilirim; in; telefonum; en iyi; türkçe dili; ve ben; teşekkür ederim; ne zaman; çok iyi	0,665	448	163	0,44

Tablo 8, AVG uygulamasına ait toplam kullanıcı yorumlarının tematik olarak 10 boyut altında toplandığını göstermektedir. Birinci sırada yer alan boyutun, kullanıcıların uygulamayı indirirken ve kullanırken kişisel verilerinin paylaşılması, kopyalanması ve üçüncü şahısların eline geçmesine yönelik endişelerini yansıttığı görülmektedir. İkinci sıradaki boyut, cihazdaki verilerin dışarı aktarılması, paylaşılması ve izinsiz kullanılmasına ilişkin kullanıcı kaygılarını kapsamaktadır. Özellikle kullanıcıların cihazlarında yer alan mesajlar, numaralar, dosyalar ve görüntüler üzerinde kontrol kaybı yaşamaktan çekindikleri görülmektedir. Bu durum, mobil güvenlik uygulamalarında veri aktarımına yönelik şeffaflık beklentisinin yüksek olduğunu göstermektedir. Üçüncü sıradaki boyut, telefon numarası, fotoğraflar, videolar ve şifreler gibi bireysel içeriklerin üçüncü kişilerle paylaşılmasına yönelik açık bir karşı duruşu yansıtmaktadır. Kullanıcıların "iznim yoktur" şeklindeki ifadeleri, kişisel veri güvenliğine yönelik bilinç düzeyinin arttığını göstermektedir. Dördüncü sıradaki boyut, adres bilgileri, kredi kartı verileri ve özel bilgilerin saklanması ya da üçüncü şahıslarla paylaşılması konusundaki endişeleri içermektedir. Beşinci sıradaki boyut, rehber, arama kayıtları, parmak izi, fotoğraflar ve diğer kişisel içeriklere verilen izinlerle ilişkilidir. Altıncı sıradaki boyut, kullanıcıların olası veri ihlalleri veya izinsiz kullanım durumunda suç duyurusunda bulunacaklarını ifade ettikleri yorumlardan oluşmaktadır. Mahkemeler ve hukuki süreçlere yapılan atıflar, kullanıcıların dijital haklar konusunda farkındalık geliştirdiğini göstermektedir. Yedinci sıradaki boyut, uygulamanın temel işlevi olan virüs temizleme, reklam kaldırma ve cihaz performansını iyileştirme deneyimlerini içermektedir. Kullanıcılar uygulamanın zararlı yazılımları hızlı tespit ettiğini, reklam virüslerini kaldırdığını ve cihazlarını rahatlattığını belirtmektedir. Sekizinci sıradaki boyut, kullanıcıların yasal haklarını kullanacaklarını ve gerekli durumlarda sorumlular hakkında işlem başlatacaklarını ifade eden yorumları kapsamaktadır. Dokuzuncu sıradaki boyut, verilen izinlerin telefon güvenliği amacıyla gerekli olduğu yönündeki yorumlardan oluşmaktadır. Onuncu ve son boyut ise, olası sorunlar karşısında gerekli kurumlara şikâyette bulunma eğilimini yansıtmaktadır.

Tablo 8. AVG- Faktör Analizi

Nu	Faktör Adı	Anahtar Kelimeler	VAR %	Frekans	Vaka	Vaka%
1	İznim Yoktur; Ait	ait; ses; iznim; yoktur; tc; video; posta; vb.; şahsıma; belgenin; kimlik; zararlı; fotoğraf; kayıtları; indirdim; parmak; mail; no; uygulamayı; paylaşılmasına; tarihinde; izi; hiçbir; virüslerden; kişisel; bilgileri; bilgi; korumak; şifre; saat; için; yazılımlardan; play; telefonumu; doküman; bilginin; kullanılmasına; belge; avg; şahsıma; store; şifreler; yasal; fotoğraflar; banka; veri; sorumludur; google; dosya; kart; numarası; yazılım; antivirüs; hesap; kaydı; videolar; aksi; dosyalar; türlü; paylaşılması; rehber; kredi; herhangi; korunmak; mesajlar; şifreleri; durumunda; işlem; kullanılması; bilgilerimin; paylaşımına; verilerimin; kesinlikle; kopyalanmasına; başlatılacaktır; bilgilerim; bilgilerin; sorumlu; resim; görüntü; telefon; kartı; izin; beyan; vs.; özel; veriler; halinde; fotoğraf ait hiçbir; saatte telefonumu; şahsıma ait; indirdim şahsıma ait; virüslerden korunmak için indirdim; bilgi ve belgenin; parmak izi vb. veri	0,635	15275	2967	6,67
2	Herhangi Bir Görüntü Aktarılması	aktarılması; görüntü; veriler; dışarı; değilim; mesajlar; kullanılması; paylaşılması; dosya; cihazımdaki; razı; yetkililerine; türlü; durumunda; dışa; numaralar; video; verilerin; cihazımda; no; aittir; ses; sorumluluk; herhangi; vb.; kişisel; ki; avg; play; store; indirip; koruma; kullanmaya; başladım; numara; antivirüs; tc numaralar vb.; paylaşılması durumunda asla razı değilim; herhangi bir görüntü; mesajlar ve numaralar vb.; türlü dosya; cihazımdaki tüm veriler; no herhangi bir görüntü; değilim cihazımdaki; numara vb.; razı değilim cihazımda; dışarı aktarılmasına; cihazımdaki tüm veriler; razı değilim; kullanmaya başladım kişisel veriler; dışarı aktarılması; kişisel veriler; indirip kullanmaya başladım kişisel veriler	0,814	5024	1652	3,71
3	Telefon Numaram Fotoğraflarım	fotoğraflarım; şifrelerim; numaram; videolarım; bilgilerim; cep telefonu; telefon numaram; tc numaram; üçüncü kişilerle; iznim yoktur	0,557	450	197	0,44
4	Adres	adres; saklanmasına; üçüncü; uygulamanın; şahıslarla; özel; kredi; kartları; bilgilerime; yoktur; kopyalanmasına; tc; fotoğraf; iznim; yüklemiş; bulunmaktayım; paylaşılmasına; uygulamasını; kartı; kişisel; paylaşmasına; vb.; hakkında; kullanacağımı; haklarımı; telefon; koruma; tel; bildiririm; tarihinde; bilgileri; numarası; bilgilerimi; banka; saat; saklanmasına ve üçüncü şahıslarla; kopyalanmasına ve saklanmasına; fotoğraf vs.; uygulamanın kişisel ve özel bilgilerimi; saklanmasına üçüncü; üçüncü şahıslarla paylaşılmasına iznim yoktur; uygulamanın kişisel ve özel; uygulamanın kişisel ve özel bilgilerime; şahıslarla paylaşılmasına iznim yoktur; kredi kartları; saklanmasına ve üçüncü; uygulamanın özel; özel bilgilerime; üçüncü şahıslarla; uygulamanın kişisel; özel bilgilerimi; paylaşmasına iznim yoktur; hiçbir şekilde kişisel; adres vb.; fotoğraf vb.; kopyalanmasına; saklanmasına; saklanmasına ve üçüncü	0,658	3220	1576	3,56
5	Parmak İzi Arama	arama; rehber; izinlerin; parmak; dosyalar; içindir; izi; videolar; hepsi; şifreler; kayıtları; verdiğim; kopyalanmasına; kişisel; verilerimin; fotoğraflar; yoktur; ses; güvenliğim; iznim; şifrelerim; kullanılmasına; uygulamasına; sorumluluk; paylaşımına; vb.; hukuki; kullanacağım; aittir; numaram; kayıtlarım; paylaşılmasına; kimlik; kopyalanmasına; banka; numarası; verilerimi; videolarım; fotoğraflarım; kesinlikle; verilerim; tc; vermiyorum; dosyalarım; olup türlü aramalar; arama geçmişim; arama kayıtları vb.; arama kayıtları; arama kayıtlarım; verdiğim izinlerin hepsi güvenliğim içindir; verdiğim izinlerin; içindir tüm kişisel; parmak izim; kopyalanmasına ve paylaşılmasına; tc numarası; yükledim verdiğim izinlerin; verdiğim izinlerin; aksi takdirde her türlü yasal; erişimine kesinlikle iznim yoktur; cep telefonu; ses kayıtları; parmak izi; kesinlikle iznim yoktur aksi; uygulamayı telefonumu ve kişisel verilerimi; avg virüs; güvenliğim içindir; iznim yoktur; kopyalanmasına kesinlikle iznim yoktur; uygulamayı telefonumu ve kişisel; kişisel verilerimin; üçüncü kişilerle; uygulamayı kendi kişisel	0,675	2832	1398	3,14
6	Suç Duyurusunda	duyurusunda; suç; mahkemelerine; hesaplar; olmadan; hakkımı; beyan; hesapları; kaydı; verdiğim; bilgileri; bilgiler; banka; benim;	0,663	786	496	1,12

		türkiye; bilgilerin; izin; hesap; paylaşılması; video; kullanılması; korunmak; fotoğraf; ses; geliştiricilerine beyan ederim; mahkemelerine suç duyurusunda bulunacağımı; mahkemelerine suç duyurusunda; tc mahkemelerine suç duyurusunda; verdiğim tüm izin; verdiğim tüm izin ve bilgilerin; suç duyurusunda; uygulamayı her türlü virüs				
7	Virüs	virüs; reklam; vardı; sürekli; yok; virüsü; çıkıyordu; telefonumda; buldu; sildim virüsü sildi; tek kelime ile mükemmel; güzel olurdu; virüsleri hemen; hemen bulup; şey yok; telefonumda sürekli; güzel olmuş; indirmenizi tavsiye ederim; virüsleri yok ediyor; başarılı tavsiye ederim; durduk yere reklam; bir işe; ana ekranda; reklam virüsü vardı; durduk yere; reklam virüsü; sürekli reklam; iyi bir şey; virüs buldu; yok etti; virüsü yok etti; yok ediyor; gerek yok; ilk defa; fabrika ayarlarına; telefonda virüs vardı; tabletimde virüs; güzel virüsleri; bir virüs; güzel beğendim; güzel indirin; merhaba arkadaşlar; olsa daha iyi; hemen indirin; virüsleri yok; harika bir şey; iyisi yok; virüs yok; sürekli reklam çıkıyordu; bulup sildi; yok oldu; dışında güzel; türkçe dili; kasma yok; sıkıntı yok; güzel ama türkçe; hemen buluyor; kendisi virüs; süper bir uygulama tavsiye ederim	0,329	151	145	0,33
8	Yasal İşlem Haklarımı	haklarımı; yasal; aksi; kullanacağımı; hakkında; bildiririm; play; store; google; avg; antivirüs; uygulaması; play store; sorumluluk; durumda; koruma; aittir; uygulamasına; durumunda; kullanacağım; halde; takdirde aksi durumda google; koruma uygulaması; hakkında yasal haklarımı kullanacağımı; avg antivirüs koruma uygulaması; yasal haklarımı kullanacağımı; hakkında yasal haklarımı kullanacağımı bildiririm; yasal haklarımı; aksi takdirde google play store; play store ve avg antivirüs koruma	0,606	3332	1709	3,84
9	İzinler	izinler; verilen; başıma; indiriyorum; güvenliğim; güvenliği; içindir; telefonumun; gerektiğinde; gelebilecek; gelecek; başlatılacaktır; için; sorumludur; dosya; kendim; kopyalanmasına; uygulamayı; rehber; işlem; kendi; amaçlıdır; güvenlik; verdiğim; google; kişisel; uygulamayı sadece telefonumun; uygulamayı sadece; telefonumun güvenliği için indiriyorum; uygulamayı telefonumun güvenliği için indiriyorum; verilen tüm izinler güvenliğim içindir	0,695	1472	870	1,96
10	Durumunda Gerekli Yerlere Şikayet Edeceğim	yerlere; edeceğim; şikayet; gerekli; durumda gerekli yerlere şikayet edeceğım	0,422	450	197	0,44

5. Sonuç ve Tartışma

Bu çalışmada, McAfee, Avast ve AVG güvenlik uygulamalarına ilişkin kullanıcı yorumları metin madenciliği yöntemiyle incelenmiş, sık kullanılan kelime grupları, yıldız derecelendirmeleri ve yıllar içerisindeki tematik değişim analiz edilmiştir. Elde edilen bulgular, kullanıcı deneyimlerinin zamanla farklılaştığını ve belirli konulara ilişkin ilgi düzeyinin uygulama bazında farklı eğilimler gösterdiğini ortaya koymuştur.

Pozitif kullanıcı deneyimlerinin ortak göstergesi olarak her üç uygulamada “tavsiye ederim”, “güzel bir”, “iyi bir” ve “harika bir” gibi olumlu yargı içeren kalıpların yüksek frekanslarla yer aldığı görülmektedir. Bu ifadelerin öne çıkması, kullanıcıların memnuniyetlerini başkalarına aktarma motivasyonlarını yansıtmaktadır. Bu durum, Davis (1989) tarafından geliştirilen Teknoloji Kabul Modeli kapsamında değerlendirildiğinde, algılanan faydanın kullanıcı tutumlarını olumlu yönde etkilediğini göstermektedir. Bununla birlikte, AVG ve Avast uygulamalarında veri gizliliğine dair endişeleri ifade eden yorumlar da dikkat çekicidir. AVG kullanıcılarının sıkça kullandığı "iznim yoktur" ve "kişisel" temalı ifadeler, uygulamanın veri erişim izinleri konusundaki kullanıcı duyarlılıklarını yansıtmaktadır. Avast yorumlarında da "tc kimlik" ve "iznim yoktur" gibi ifadelere yer verilmesi, kullanıcıların kişisel veri güvenliği konusunda hassasiyet taşıdığını göstermektedir. Bu bulgu, Venkatesh ve diğ. (2003) tarafından geliştirilen Birleştirilmiş Teknoloji Kabul ve Kullanım Teorisi bağlamında değerlendirildiğinde, güven ve algılanan riskin kullanıcı kabulünü etkileyen kritik faktörler olduğunu göstermektedir. McAfee kullanıcı yorumlarında ise veri gizliliğine yönelik eleştirel vurgu daha az görülmektedir. Bu durum, McAfee'nin kullanıcılar nezdinde daha istikrarlı ve alışıldık bir hizmet deneyimi sunduğu şeklinde yorumlanabilir. Yapılan araştırmalarda pozitif yıldız derecelendirmelerin kullanıcılar üzerinde olumlu etkisinin olduğunu doğrulamaktadır (Aktaş vd., 2021; Aslan & Akbıyık, 2017; Cakar & Akbiyik, 2018).

Yıldız derecelendirmeler incelendiğinde yıldız derecelerin azaldıkça yorum dilinin olumlu ifadelerden teknik eleştirilere ve memnuniyetsizlik bildirimlerine doğru kaydığı görülmektedir. Bu dönüşüm, kullanıcıların uygulamalara yönelik algılarının sadece genel memnuniyet düzeyiyle değil, aynı zamanda uygulamanın sunduğu hizmetlerin kalitesi ve güvenliğine ilişkin beklentileriyle de şekillendiğini göstermektedir. Özellikle kullanıcıların düşük puanlı yorumlarında dile getirdikleri teknik sorunlar ve veri gizliliği endişeleri, uygulamaların kullanıcı odaklı geliştirilmesi sürecinde dikkate alınması gereken öncelikli alanlara işaret etmektedir. Öte yandan, yüksek puanlı yorumlarda sıkça tekrar eden olumlu ifadeler, kullanıcı deneyiminin hangi yönlerinin güçlü bulunduğunu belirleme açısından anlamlı ipuçları sağlamaktadır. Bailey vd., 2019; Chen vd., 2021; Hassan vd., 2018; Outay vd., 2021; Savarimuthu vd., 2021; Srisopha vd., 2020 bulguları bu araştırmayı destekler niteliktedir.

2020–2025 yılları arasında McAfee, Avast ve AVG uygulamalarına ilişkin kullanıcı yorumları incelendiğinde üç uygulama için de gözlemlenen ortak eğilim, erken dönemlerde duygusal ve genel değerlendirmelerin ön planda olması, ilerleyen yıllarda ise teknik ve işlevsel geri bildirimlerin artmasıdır. Teknoloji Kabul Modeli açısından bu durum, başlangıçta algılanan kullanım kolaylığının baskın olduğu; zamanla ise algılanan faydanın ve performans beklentisinin ön plana çıktığı şeklinde yorumlanabilir. Benzer şekilde Birleştirilmiş Teknoloji Kabul ve Kullanım Teorisi çerçevesinde, deneyim arttıkça bireysel değerlendirme kriterlerinin daha belirleyici hale geldiği söylenebilir. Tüm uygulamalar açısından ortak olan bir diğer bulgu da "VPN" temasının yükselişidir. Bu durum, kullanıcıların siber güvenlik farkındalığının arttığını ve antivirüs programlarından yalnızca temel koruma değil, bütünleşik güvenlik çözümleri beklediklerini ortaya koymaktadır. "Güncelleme" ve "abonelik" temalarının da zaman içinde daha fazla dile getirilmesi, kullanıcıların lisans politikaları, yazılım sürekliliği ve deneyim sürekliliği gibi operasyonel konularda daha hassas hale geldiğini göstermektedir.

Sonuç olarak, elde edilen bulgular kullanıcı yorumlarının yalnızca memnuniyet düzeyini değil, aynı zamanda kullanıcıların teknolojiye yönelik algılarını, beklentilerini ve davranışsal niyetlerini yansıttığını ortaya koymaktadır. Teknloji Kabul Modeli ve Birleştirilmiş Teknoloji Kabul ve Kullanım Teorisi çerçevesinde değerlendirildiğinde, kullanıcı deneyiminin duygusal tatminden işlevsel değerlendirmeye doğru evrildiği; güven, performans beklentisi ve algılanan faydanın teknoloji kabulünde belirleyici rol oynadığı görülmektedir.

Teorik ve Uygulamaya Yönelik Katkılar

Bu çalışmanın teorik katkısı, mobil güvenlik uygulamalarına ilişkin kullanıcı deneyimlerini çevrim içi kullanıcı yorumları üzerinden incelemesidir. Bu yönüyle çalışma, siber güvenlik davranışları, mahremiyet endişesi, teknoloji kabulü ve dijital güven literatürüne alternatif bir veri kaynağı sunmaktadır. Ayrıca kullanıcıların mobil antivirüs uygulamalarını değerlendirirken yalnızca virüs temizleme performansına odaklanmadıkları; veri paylaşımı, izin yönetimi, hukuki sorumluluk, güven duygusu ve genel kullanım deneyimi gibi çok katmanlı kriterleri dikkate aldıkları ortaya konulmuştur. Böylece çalışma, mobil siber güvenlik araçlarının kullanıcı perspektifinden nasıl algılandığını açıklayarak mevcut teorik çerçevelerin genişletilmesine katkı sağlamaktadır.

Uygulamaya yönelik katkı bakımından ise çalışma bulguları, McAfee, Avast ve AVG gibi uygulama geliştiricilerine kullanıcı beklentilerini doğrudan yansıtan stratejik bilgiler sunmaktadır. Özellikle kullanıcıların veri gizliliği konusundaki hassasiyetleri dikkate alınarak daha anlaşılır gizlilik politikaları hazırlanması, izin taleplerinin sadeleştirilmesi, teknik sorunların azaltılması ve müşteri destek süreçlerinin güçlendirilmesi gerektiği anlaşılmaktadır. Bunun yanında çalışma, siber güvenlik farkındalığı programları yürüten kurumlar ve düzenleyici otoriteler açısından kullanıcıların mobil güvenlik uygulamalarına yönelik güven düzeylerini ve temel kaygı alanlarını belirlemede yararlı bir karar destek kaynağı niteliği taşımaktadır.

Uygulamaya Yönelik Öneriler

Yorumlarda sık geçen "arayüz" ve "güncelleme" gibi kelimeler, kullanıcıların tasarımsal değişikliklere duyarlı olduğunu göstermektedir. Geliştiricilere, arayüz değişikliklerini kademeli olarak uygulaması ve kullanıcıya adaptasyon süreci sağlaması önerilmektedir. AVG ve Avast kullanıcılarının sıkça dile getirdiği veri gizliliği endişeleri, uygulama içi bilgilendirmelerin güçlendirilmesi gerektiğini ortaya koymaktadır.

Kullanıcılara, hangi verilerin nasıl işlendiğine dair açık, anlaşılır ve düzenli güncellenen bilgilendirmeler sunulmalıdır.

McAfee'de düşük yıldızlı yorumlarda sıkça geçen "para" ve "VPN" gibi kavramlar, kullanıcıların lisans ücretleri ve ek hizmet maliyetleri konusunda hassas olduklarını göstermektedir. Bu nedenle, ücretlendirme politikalarının daha şeffaf ve öngörülebilir hale getirilmesi önerilmektedir. Kullanıcıların sadece temel koruma değil, bütünleşik güvenlik çözümleri (VPN, kimlik koruma, parola yönetimi vb.) talep ettikleri görülmektedir. Geliştiricilere, bu tür entegre hizmetler sunarken performans kaybı ve kullanım kolaylığını da gözetmeleri önerilmektedir.

Sınırlılıklar ve Gelecek Araştırmalara Öneriler

Her çalışmada olduğu gibi bu araştırmanın da bazı sınırlılıkları bulunmaktadır. İlk olarak, çalışma kapsamında kullanılan veriler yalnızca Google Play Store ortamında paylaşılan kullanıcı yorumlarından elde edilmiştir. Bu nedenle Apple App Store, Amazon Appstore veya Huawei App Store gibi farklı platformlarda yer alan kullanıcı deneyimleri ve değerlendirmeleri araştırma kapsamı dışında kalmıştır. İkinci olarak, analiz yalnızca McAfee, Avast ve AVG olmak üzere üç mobil güvenlik uygulaması ile sınırlandırılmıştır. Bu durum, bulguların tüm mobil güvenlik uygulamalarına genellenmesini sınırlayabilir. Üçüncü olarak, kullanıcı yorumları anonim ve gönüllü içeriklerden oluştuğu için yaş, cinsiyet, bölge, eğitim düzeyi veya teknik yeterlilik gibi demografik değişkenlere ilişkin değerlendirme yapılamamıştır. Ayrıca yorumların öznel nitelikte olması, aşırı olumlu veya aşırı olumsuz deneyimlerin daha görünür olmasına neden olabilmektedir.

Gelecek araştırmalara farklı dijital platformlardan elde edilecek veriler kullanılarak platformlar arası karşılaştırmalı analizlerin gerçekleştirilmesi önerilmektedir. Bunun yanında marka, iş modeli veya uygulama özelliklerine göre kullanıcı algılarındaki farklılıkların incelenmesi önerilmektedir. Ayrıca kullanıcı profillerine erişim sağlayan veri setleri aracılığıyla yaş grubu, coğrafi bölge ve teknik bilgi düzeyi gibi demografik değişkenlerin kullanıcı yorumlarına etkisinin araştırılması önerilmektedir. Geleneksel metin madenciliği yöntemlerine ek olarak derin öğrenme tabanlı doğal dil işleme modelleri, duygu analizi ve büyük dil modelleri kullanılarak kullanıcı deneyimlerinin daha derinlemesine analiz edilmesi önerilmektedir. Son olarak, zaman serisi analizleriyle kullanıcı algısının uygulama güncellemeleri, veri ihlalleri veya önemli siber güvenlik olayları sonrasında nasıl değiştiğinin ortaya konulması önerilmektedir.

Kaynaklar

Akbıyık, A. (2019). *Sosyal Bilimlerde Metin Madenciliği Wordstat Uygulamaları*. Sakarya Yayıncılık.

Baz Aktaş, N., Aktaş, B., & Akbıyık, A. (2021). Koronavirüs'ün (covid-19) Türkiye'de e-ticaret müşteri memnuniyetine etkisi: trendyol örneği. *Journal of Information Systems and Management Research*, 3(1), 39

Al-ghaith, W. (2016). Extending protection motivation theory to understand security determinants of anti-virus software usage on mobiles devices. *International Journal of Computers*, *10*, 125–138.

Alhejji, S., Albesher, A., Wahsheh, H., & Albarrak, A. (2022). Evaluating and comparing the usability of mobile banking applications in saudi arabia. In *Information* 13(12). https://doi.org/10.3390/info13120559

Alismail, M. A., & Albesher, A. S. (2023). Evaluating developer responses to app reviews: the case of mobile banking apps in saudi arabia and the united states. *Sustainability*, *15*(8). https://doi.org/10.3390/su15086701

Aslan, T., & Adem Akbıyık. (2017). Mobil trafik uygulamaları üzerine tüketici yorumlarının içerik analizi: İbb cep trafik uygulama örneği. *4. Uluslararası Yönetim Bilişim Sistemleri Konferansı .*

Bailey, K., Nagappan, M., & Dig, D. (2019). Examining user-developer feedback loops in the iOS app store. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2019-Janua*, 7411–7420. https://doi.org/10.24251/hicss.2019.892

BalaGanesh, D., Chakrabarti, A., & Midhunchakkaravarthy, D. (2018). Smart devices threats, vulnerabilities and malware detection approaches: a survey. *European Journal of Engineering Research and Science*, *3*(2), 7. https://doi.org/10.24018/ejers.2018.3.2.302

Cakar, E., & Akbıyık, A. (2018). Focus ıssue in consumer reviews on fmcg: ıs the product evaluated or the sales service. *Ajit-e Online Academic Journal of Information Technology*, *9*(33), 147–158. https://doi.org/10.5824/1309-1581.2018.3.009.x

Chen, C., Zhang, K. Z. K., Gong, X., Zhao, S. J., Lee, M. K. O., & Liang, L. (2017). Understanding compulsive smartphone use: An empirical test of a flow-based model. *International Journal of Information Management*, *37*(5), 438–454. https://doi.org/10.1016/j.ijinfomgt.2017.04.009

Chen, Q., Chen, C., Hassan, S., Xing, Z., Xia, X., & Hassan, A. E. (2021). How should ı ımprove the uı of my app? a study of user reviews of popular apps in the google play. *ACM Trans. Softw. Eng. Methodol.*, *30*(3). https://doi.org/10.1145/3447808

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. *2009 42nd Hawaii International Conference on System Sciences*, 1–10. https://doi.org/10.1109/HICSS.2009.74

Christinne M. T. P. Subagyo Yunitha R. Sumarandak , M. E. L. S. (2021). Comparative study of antivirus adoption rates on smartphone-based operating systems. *International Journal of Information Technology and Education*, *1*(1 SE-Articles), 108–115. https://ijite.jredu.id/index.php/ijite/article/view/20

Clarke, N., Symes, J., Saevanee, H., & Furnell, S. (2016). Awareness of mobile device security. *International Journal of Mobile Computing and Multimedia Communications*, *7*, 15–31. https://doi.org/10.4018/IJMCMC.2016010102

Davis, F. (1986). Doktora Tezi. A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results. Sloan School of Management, Massachusetts Institute of Technology.

Feldman, R., & Sanger, J. (2007). *The Text Mining Handbook Advanced Approaches in Analyzing Unstructured Data*. Cambridge University Press.

Hassan, S., Tantithamthavorn, C., Bezemer, C.-P., & Hassan, A. E. (2018). Studying the dialogue between users and developers of free apps in the google play store. *Empirical Software Engineering*, *23*. https://doi.org/10.1007/s10664-017-9538-9

Hong, W. C. H., Chi, C. Y., Liu, J., Zhang, Y. F., Lei, V. N. L., & Xu, X. S. (2022). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. In *Education and Information Technologies* 28(1). Springer US. https://doi.org/10.1007/s10639-022-11121-5

Jin, S., Baek, H., Lee, U., & Kim, H. (2025). I was told to ınstall the antivirus app, but ı'm not sure ı need ıt: understanding smartphone antivirus software adoption and user perceptions. *Conference on Human Factors in Computing Systems - Proceedings* . https://doi.org/10.1145/3706598.3713452

Karayel, T. (2025). AI threats in cyber security: Empowering employee awareness and training for cyber security culture. In A. Almomani & M. Alauthman (Eds.), *Examining Cybersecurity Risks Produced by Generative AI* (pp. 553-572). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0832-6.ch023

Karayel, T., & Saygılı, M. (2025). Understanding smartphone security behavior through the core constructs of protection motivation theory: A comparative study of iOS and android users. *Computers and Security*, *158*(August). https://doi.org/10.1016/j.cose.2025.104652

Kaspersky. (2024). *IT Threat Evolution in Q1 2024. Mobile Statistics.* https://securelist.com/it-threat-evolution-q1-2024-mobile-statistics/112750/

Koyuncu, M., & Pusatli, T. (2019). Security awareness level of smartphone users: an exploratory case study. *Mobile Information Systems*, *2019*. https://doi.org/10.1155/2019/2786913

Lane, R., & Torri, S. A. (2024). Comparing ios and android anti-virus protection: a survey. *proceedings of the 2024 9th International Conference on Mobile and Secure Services, MOBISECSERV 2024*, *CFP24RAC-A*, 1–5. https://doi.org/10.1109/MobiSecServ63327.2024.10759904

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445–454. https://doi.org/10.1080/01449290600879344

Li, M., & Zhao, L. (2025). Understanding fashion omnichannel experience through mobile application customer reviews. *Journal of Global Fashion Marketing*, *16*(1), 90–108. https://doi.org/10.1080/20932685.2024.2417304

Malleswari, D. N., Dhavalya, A., Sai, V. D., & Srikanth, K. (2018). A detailed study on risk assessment of mobile app permissions. *Proceedings of the 3rd International Conference on Innovative Research in Science and Technology (ICIRST)*, Vol. 2, pp. 69-73.

McIlroy, S., Ali, N., Khalid, H., & E. Hassan, A. (2016). Analyzing and automatically labelling the types of user issues that are raised in mobile app reviews. *Empirical Software Engineering*, *21*(3), 1067–1106. https://doi.org/10.1007/s10664-015-9375-7

McIlroy, S., Shang, W., Ali, N., & Hassan, A. E. (2017). Is ıt worth responding to reviews? studying the top free apps in google play. *IEEE Software*, *34*(3), 64–71. https://doi.org/10.1109/MS.2015.149

Mudambi, S., & Schuff, D. (2010). What makes a helpful online review? a study of customer reviews on amazon.com. *MIS Quarterly*, *34*, 185–200. https://doi.org/10.2307/20721420

Outay, F., Malik, H., & Dampier, D. (2021). What do developers reply to? An empirical study of the top Unmanned Aerial Vehicles (UAVs) apps. *Proceedings of the International Conference on Software Engineering and Knowledge Engineering, SEKE*, *2021-July*, 261–264. https://doi.org/10.18293/seke2021-159

Pereira, G. L., Brito, L. S., & Lima, S. M. L. de. (2025). Antivirus applied to Google Chrome's extension malware. *Computers & Security*, *156*, 104465. https://doi.org/https://doi.org/10.1016/j.cose.2025.104465

Savarimuthu, B. T. R., Licorish, S. A., Devananda, M., Greenheld, G., Dignum, V., & Dignum, F. (2021). *Developers' responses to app review feedback – a study of communication norms in app development bt - coordination, organizations, ınstitutions, norms, and ethics for governance of multi-agent systems xıı* (A. Aler Tubella, S. Cranefield, C. Frantz, F. Meneguzzi, & W. Vasconcelos (eds.); pp. 57–75). Springer International Publishing.

Srisopha, K., Link, D., Swami, D., & Boehm, B. (2020). Learning features that predict developer responses for ios app store reviews. *Proceedings of the 14th ACM / IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*. https://doi.org/10.1145/3382494.3410686

Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). A risk assessment method for smartphones marianthi. *Ifip Aict*, *376*, 443–456. http://www.motorola.com/mdirect/manuals/V3i_9504A48O.pdf

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The Privacy ımplications of cyber security systems: a technological survey. *ACM Comput. Surv.*, *51*(2). https://doi.org/10.1145/3172869

Venkatesh, Viswanath & Morris, Michael & Davis, Gordon & Davis, Fred. (2003). User Acceptance of Information Technology: Toward A Unified View1. MIS Quarterly. 27. 425-478. 10.2307/30036540.

Vu, P. M., Nguyen, T. T., & Nguyen, T. T. (2019). Why do app reviews get responded: A preliminary study of the relationship between reviews and responses in mobile apps. *Proceedings of the 2019 ACM Southeast Conference*, 237–240. https://doi.org/10.1145/3299815.3314473

Zhou, G., Gou, M., Gan, Y., & Schwarzer, R. (2020). Risk awareness, self-efficacy, and social support predict secure smartphone usage. *Frontiers in Psychology*, *11*(June), 1–8. https://doi.org/10.3389/fpsyg.2020.01066