ISSN: 2618-6241
e-ISSN: 2667-5757

HALİÇ ÜNİVERSİTESİ FEN BİLİMLERİ DERGİSİ

HALİÇ UNIVERSITY JOURNAL OF NATURAL AND APPLIED SCIENCES

Cilt: 8 Sayı: 1 Tarih: Mart 2025
Volume: 8 Issue: 1 Date: March 2025

Haliç Üniversitesi Adına Sahibi *Owner on behalf of Haliç University*	**Prof. Dr. Nihat İNANÇ** Haliç Üniversitesi Rektörü
Editörler *Editors*	Prof. Dr. Emine Esra KASAPBAŞI Editör/ Editor-in- Chief Doç. Dr. Alireza SOURİ Editör Yardımcısı/ Associate Arş. Gör. Ceren ÇOLAK Editör Asistanı/ Assistant Arş. Gör. Hilal YILMAZ Türkçe Editörü/ Turkish Editor Arş. Gör. Ömer Faruk ŞAHİN İngilizce Editörü/ English Editor
Sorumlu Yazı İşleri Müdürü *Publishing Manager*	Haliç Üniversitesi
Yönetim Yeri *Head Office*	Haliç Üniversitesi, Güzeltepe Mahallesi, 15 Temmuz Şehitler Caddesi, No: 15 34060 Eyüp/İSTANBUL Tel: 212 924 24 44
Yazışma Adresi *Corresponding Address*	**E-posta:** fbd@halic.edu.tr
İnternet Adresi *Web Address*	http://dergipark.gov.tr/hafebid
Yayın Türü *Publication Type*	Yerel Süreli / *Periodical* Mart ve Eylül Aylarında olmak üzere yılda iki sayı yayımlanır ISSN: 2618-6241
Asitsiz kâğıda basılmaktadır *Printed on acid free paper*	--
Baskı *Printing Press*	
Basım Tarihi *Publication Date*	31.03.2025
Derginin Tarandığı Kaynaklar *Index in*	DergiPark AKADEMİK

Cilt 8 Sayı 1 **Hakem Listesi** *Volume 8 Issue 1* *Reviewer List*	Prof. Dr. Serhat Özekes Doç. Dr. Erdem Yavuz Doç. Dr. Can Eyüpoğlu Doç. Dr. Kazım Yıldız Dr. Öğr. Üyesi Burcu Güleryüz Erkovan Dr. Öğr. Üyesi Deniz Kanca Demirci Dr. Öğr. Üyesi Allison Pınar Eronat

AMAÇ VE KAPSAM

Haliç Üniversitesi Fen Bilimleri Dergisi Eylül 2018 tarihinden itibaren yılda iki kez yayımlanır. Bu dergide temel bilimler, mühendislik ve mimarlık alanlarında araştırmaya dayalı Türkçe veya İngilizce dilinde özgün ve derleme makaleler yayımlanır. Gönderilen makaleler hakemler tarafından incelenerek değerlendirilir ve kabul edilen makaleler derginin web sayfasında online olarak yayımlanır.

Yayın İzni

Bireysel kullanım dışında, Haliç Üniversitesi Fen Bilimleri Dergisi'nde yayınlanan makaleler, şekiller ve tablolar yazılı izin olmaksızın çoğaltılamaz, bir sistemde arşivlenemez ve reklam ya da tanıtım amaçlı materyallerde kullanılamaz. Bilimsel makalelerde, uygun şekilde kaynak gösterilerek alıntılar yapılabilir.

Açık Erişim Politikası

Haliç Üniversitesi Fen Bilimleri Dergisi açık erişim politikasını benimsemiş bir dergidir.

Yazıların Bilimsel ve Hukuki Sorumluğu

Yayınlanan makalelerin bilimsel ve hukuki sorumluluğu yazarlarına aittir. Yazıların içeriğinden ve kaynakların doğruluğundan yazarlar sorumludur. Editör, Yardımcı Editörler, Yayın ve Danışma Kurulu Üyeleri ve Yayımcı dergideki hatalardan veya bilgilerin kullanımından doğacak olan sonuçlardan dolayı sorumluluk kabul etmez.

AIMS AND SCOPE

Haliç University Journal of Natural and Applied Sciences is published twice a year since September 2018. This journal publishes original and compilation articles in Turkish or English based on research in the fields of basic sciences, engineering and architecture. The submit- ted articles will be reviewed and evaluated by the referees and the accepted articles will be published on-line and in print on the web page.

Permission Requests

Apart from individual use, articles, forms and tables published in Haliç University Journal of Natural and Applied Sciences cannot be reproduced without written permission and cannot be archived in a system or used for advertising or promotional materials. Scientific articles can be cited with appropriate references.

Open Access Policy

Haliç University Journal of Natural and Applied Sciences is a journal, which has adopted open access policy.

Scientific and Legal Responsibility of Articles

The scientific and legal responsibility of the published articles belongs to their authors. The authors are responsible for the content of the articles and for the correctness of the sources. The Editor-in-Chief, Associate Editor, Assistant Editors, Members of the Publication and Advisory Board and the Publisher cannot be held responsible for errors or any consequences arising from the use of information contained in this journal.

Değerli Okurlar,

Haliç Üniversitesi Fen Bilimleri Dergisinin sekizinci cildinin ilk sayısını siz değerli okurlarımıza sunmaktan büyük mutluluk duyuyoruz. Dergimizin bu sayısında Bilgi Sistemleri alanında iki araştırma makalesi ve Moleküler Biyoloji ve Genetik alanında bir derleme makale yer almaktadır. Dergimize makale göndererek bilimsel katkı sunan tüm yazarlarımıza, bu makaleleri değerlendirerek yorumlarını bildiren hakemlerimize ve derginin hazırlanmasında emeği geçen tüm çalışma arkadaşlarımıza teşekkürü bir borç biliriz.

Dergimizin bu sayısının siz okurlarımıza yararlı olmasını diler, saygılar sunarız.

Prof. Dr. E. Esra KASAPBAŞI
Editör
Haliç Üniversitesi Fen Bilimleri Dergisi

Dear Readers,

We are pleased to present the first issue of the eighth volume of the Journal of Haliç University Natural and Applied Sciences to you. In this issue, two research articles related to the field of Information Systems and one review article related to the field of Molecular Biology and Genetics are included. We would like to thank all the authors of the articles for their scientific contributions, the reviewers for their valuable comments and our journal team for their help and efforts for preparing this issue for publication. We hope that this issue of our journal will be beneficial to you. Yours sincerely,

Prof. Dr. E. Esra KASAPBAŞI
Editor
Journal of Haliç University Natural and Applied Sciences

İçindekiler / Contents

Araştırma Makaleleri / *Research Articles*

Derleme Makalelesi / *Review Articles*

Haliç Üniversitesi Fen Bilimleri Dergisi 2025, 8/1: 1-39
DOI: 10.46373/hafebid.1602901

ISSN: 2618-6241
e-ISSN: 2667-5757

Kobi ve Orta Ölçekli İşletmelerde Optimum Maliyetle Güvenlik Risklerinin Yönetimi ve Siber Güvenlik Uygulamaları

Burak SARAL[1]*, Mustafa Cem KASAPBAŞI[2]

[1]İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği, İstanbul, Türkiye
Orcid: 0009-0002-0409-1790, (https://orcid.org/0009-0002-0409-1790)
[2]İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği, İstanbul, Türkiye
Orcid: 0000-0001-6444-6659, (https://orcid.org/0000-0001-6444-6659)

Geliş Tarihi: 17.12.2024
Kabul Tarihi: 26.12.2024

***Sorumlu Yazar e mail:** burak@kampist.org

Atıf/Citation: Saral, B., Kasapbaşı, M. C., "Kobi ve Orta Ölçekli İşletmelerde Optimum Maliyetle Güvenlik Risklerinin Yönetimi ve Siber Güvenlik Uygulamaları", Haliç Üniversitesi Fen Bilimleri Dergisi 2025, 8/1: 1-39.

Araştırma Makalesi/ ***Research Article***

Öz

Dijitalleşmenin hızla yaygınlaşması, küçük ve orta ölçekli işletmeler (KOBİ'ler) için yeni fırsatlar yaratırken, aynı zamanda siber güvenlik tehditlerine karşı kırılganlıklarını artırmaktadır. KOBİ'ler, büyük ölçekli işletmelere kıyasla sınırlı bütçeler ve kaynaklarla çalıştıklarından, siber tehditlere karşı etkili koruma sağlamak için maliyet etkin güvenlik stratejilerine ihtiyaç duymaktadır. Bu durum, KOBİ'lerin siber güvenlik yatırımlarını optimize etme ve risk yönetiminde yenilikçi çözümler geliştirme gerekliliğini doğurmaktadır. Bu çalışma, KOBİ'lerin karşılaştığı başlıca siber tehditlere odaklanarak, bu tehditlere karşı etkin ve sürdürülebilir güvenlik stratejilerinin nasıl uygulanabileceğini araştırmaktadır. Özellikle, düşük maliyetli ancak etkili güvenlik çözümleri ve modern siber tehditlerle mücadelede kullanılabilecek yöntemler üzerinde durulmuştur. KOBİ'lere özgün bir bakış açısı sunarak, simülasyon ortamında gerçekleştirilen saldırı analizleriyle güvenlik önlemlerinin etkinliği değerlendirilecek ve elde edilen bulgular üzerinden KOBİ'ler için pratik öneriler sunulacaktır. Makale, KOBİ'lerin kaynaklarını en verimli şekilde kullanarak operasyonel sürekliliklerini nasıl koruyabileceklerine dair rehber niteliğinde bir çalışma sunmayı amaçlamaktadır. Bu bağlamda, atak simülasyonları ve güvenlik katmanlarının performans analizleri, önerilen stratejilerin gerçek dünyadaki uygulanabilirliğini göstermesi açısından önemli bir katkı sağlamaktadır.

Anahtar sözcükler: KOBİ, siber güvenlik, maliyet optimizasyonu, risk yönetimi, siber tehditler

Management Of Security Risks and Cybersecurity Practices With Optimal Costs in Smes and Medium-Sized Enterprises

Abstract

The rapid spread of digitalization creates new opportunities for small and medium-sized enterprises (SMEs) while simultaneously increasing their vulnerability to cybersecurity threats. SMEs, working with limited budgets and resources compared to large-scale enterprises, require cost-effective security strategies to ensure effective protection against cyber threats. This situation necessitates optimizing cybersecurity investments and developing innovative solutions for risk management. This study focuses on the major cybersecurity threats faced by SMEs and explores how effective and sustainable security strategies can be implemented to address these threats. Particular emphasis is placed on low-cost yet effective security solutions and methods to combat modern cyber threats. By offering SMEs a unique perspective, the study evaluates the effectiveness of security measures through attack simulations and provides practical recommendations based on the findings. The article aims to serve as a guide for SMEs on how to maintain operational continuity by utilizing their resources most efficiently. In this context, attack simulations and performance analyses of security layers contribute significantly by demonstrating the real-world applicability of the proposed strategies.

Keywords: SME, cybersecurity, cost optimization, risk management, cyber threats

1. Giriş

Günümüz dünyasında dijitalleşmenin hızla yaygınlaşması, işletmeler için büyük fırsatlar sunduğu gibi, beraberinde ciddi güvenlik risklerini de getirmektedir. Özellikle küçük ve orta ölçekli işletmeler (KOBİ'ler), büyük şirketler kadar geniş bütçelere sahip olmadığından, siber güvenlik yatırımlarını maliyet açısından oldukça etkin bir şekilde planlamak zorundadır [1]. Ancak sınırlı bütçeler ve kaynaklar, bu tarz işletmelerin siber tehditlere karşı savunmasız kalma riskini artırmaktadır. Bu nedenle, KOBİ'lerin siber güvenlik stratejilerini hem maliyet hem de etkinlik açısından optimize etmeleri faaliyetlerinin devamlılığı ve yerel / küresel ekonomiye katkılarının artarak devam edebilmesi için büyük önem taşımaktadır [2].

KOBİ'ler, çoğunlukla dijital altyapılarını güçlendirmeye çalışırken, aynı zamanda veri güvenliğini sağlama, bilgi teknolojileri altyapısını koruma ve siber ataklara karşı önlem alma yükümlülüğü altındadır. Bununla birlikte, bu işletmelerin karşılaştığı siber tehditler büyük ölçüde çeşitlilik göstermekte ve sürekli olarak gelişmektedir. Bu dinamik ortamda, işletmelerin risk yönetimi stratejilerini belirlerken hem mevcut tehditler hem de maliyet faktörlerini dikkate alması gerekmektedir [3]. Siber tehditler arasında fidye yazılımları, kimlik avı saldırıları ve DDoS saldırıları gibi problemler özellikle KOBİ'leri hedef almaktadır. Örneğin, 2023 yılında KOBİ'lerin %73'ünün veri ihlali veya siber saldırı yaşadığını raporlanmıştır [4].

Bu dinamik ortamda, işletmelerin risk yönetimi stratejilerini belirlerken hem mevcut tehditler hem de maliyet faktörlerini dikkate alması gerekmektedir. Bu kapsamda, bulut tabanlı siber güvenlik çözümleri gibi yenilikçi teknolojiler, KOBİ'lerin sınırlı kaynaklarını etkin bir şekilde kullanmasını sağlamaktadır [5]. Bulut bilişim teknolojileri, altyapı maliyetlerini düşürdüğü gibi, daha esnek ve hızlı bir güvenlik yapısı oluşturma imkanı sunmaktadır.

Bu çalışmada, KOBİ'ler ve orta ölçekli işletmeler için optimum maliyetle siber güvenliğin nasıl sağlanabileceği ve güvenlik risklerinin nasıl yönetilebileceği üzerinde durulacaktır. Özellikle, bu işletmelerin kısıtlı kaynaklarını en verimli şekilde kullanarak, siber tehditlere karşı etkin çözümler geliştirmesi için uygulanabilir stratejiler önerilecektir. Ayrıca, başarılı güvenlik uygulamaları ve vaka analizleri ile işletmelerin karşılaştığı gerçek dünyadaki sorunlar ve bunlara yönelik çözümler de detaylandırılacaktır ve istatistiki olarak sunulacaktır.

Bu bağlamda, KOBİ'lerin siber güvenlik yatırımlarını nasıl planlamaları gerektiği, hangi teknolojilerin kullanılabileceği ve bütçe kısıtlamaları altında güvenliği en üst düzeye çıkarmak için atılacak adımlar bu tezin temel sorunsallarını oluşturmaktadır.

2. Yöntem

Küçük ve Orta Ölçekli İşletmelerde (KOBİ'ler) siber güvenlik yönetimi, genellikle sınırlı bütçeler ve kaynaklarla gerçekleştirilmek zorunda olduğu için maliyet etkin çözümler sunan çok katmanlı bir güvenlik modeli önerilecektir. Bu yöntem, siber tehditlere karşı geniş kapsama alanını en düşük maliyetle sağlayacak güvenlik katmanları sunmayı amaçlar. Aşağıdaki adımlar ve süreçler, bu modelin temel yapı taşlarını oluşturmaktadır.

2.1. Simülasyon Ortamı ve Yapılacak Testler

Atak simülasyonu, bir kuruluşun bilgi sistemlerinin güvenliğini değerlendirmek amacıyla gerçekleştirilen kontrollü ve etik siber atak denemeleridir. Bu yöntem, gerçek dünyadaki atak senaryolarını taklit ederek, sistemlerin savunma mekanizmalarının etkinliğini test etmeyi ve olası güvenlik açıklarını belirlemeyi amaçlar. Sızma testleri olarak da bilinen bu uygulamalar, saldırganların kullanabileceği yöntemleri simüle ederek, sistemlerin ne kadar dayanıklı olduğunu ölçer ve gerekli güvenlik iyileştirmelerinin yapılmasına olanak tanır [5].

Bu süreç, olası güvenlik açıklarını ve zayıf noktaları tespit etmenin yanı sıra, mevcut güvenlik çözümlerinin hangi alanlarda daha fazla optimize edilmesi gerektiğini anlamaya da olanak tanır. Yapılacak testlerde, atak simülasyonu sistemi kullanılarak gerçek saldırı senaryoları taklit edilecek ve KOBİ ortamları için fidye yazılımı, kimlik avı, zararlı yazılım ve botnet saldırıları gibi madde 3.2'de açıklanan güvenlik önlemleri ile madde 3.3'te önerilen stratejilerin etkinliği detaylı bir şekilde değerlendirilecektir. Bu yaklaşım, hem mevcut güvenlik katmanlarının performansını ölçmeyi hem de KOBİ'ler için daha güçlü ve verimli bir güvenlik altyapısı oluşturmak adına iyileştirme alanlarını belirlemeyi amaçlamaktadır.

2.2. İşletim Sistemi

Test ortamında bulunan cihazlar Windows 10 22H2 (OS Build 19045.5198) versiyonu ile yapılandırılmış ve tüm güncellemeleri yüklenmiştir.

2.3. Yeni Nesil Güvenlik Duvarı Sistemi

Test ortamında, güvenlik seviyesini en üst düzeye çıkarmak amacıyla Yeni Nesil Güvenlik Duvarı yapılandırılmış ve konumlandırılmıştır [6]. Bu güvenlik duvarı üzerinde SSL Denetimi özelliği etkinleştirilerek şifreli trafik üzerinde derinlemesine analiz yapılması sağlanmıştır. Ayrıca, gelişmiş güvenlik politikalarının uygulanabilmesi için URL Filtresi, DNS Filtresi, Uygulama Kontrolü, IPS ve Antivirüs modülleri aktif hale getirilmiştir.

Bu yapılandırma, test ortamındaki güvenlik açıklarını belirlemek ve saldırılara karşı maksimum koruma sağlamak için tasarlanmıştır. Özellikle SSL trafiğinin çözülmesi, zararlı yazılımların ve diğer siber tehditlerin tespit edilme oranını artırırken, URL ve DNS filtreleme gibi özellikler, kötü niyetli sitelere ve alan adlarına erişimi engellemeyi hedeflemiştir. IPS ve Antivirüs ise, ağ içindeki anormal hareketleri ve kötü amaçlı yazılımları proaktif olarak engelleyerek daha güvenli bir ortam oluşturmayı amaçlamıştır.

Bu kapsamda, Yeni Nesil Güvenlik Duvarı ile yapılan testler, hem gelişmiş koruma seviyelerini değerlendirerek mevcut güvenlik önlemlerinin etkinliğini test etmeyi hem de olası iyileştirme alanlarını belirlemeyi amaçlamaktadır.

2.4. Atak Kategorileri

Madde 2.6'da tanımlanan simülasyon ortamındaki son kullanıcı cihazlarına, Tablo 1'de belirtilen 15 farklı atak kategorisi kapsamında toplam 4.622 farklı siber atak gerçekleştirilmiştir. Bu ataklar,

sistemlerin farklı güvenlik yapılandırmalarına karşı gösterdiği direnci analiz etmek amacıyla, Tablo 2'de yer alan 8 farklı güvenlik statüsü durumuna ayrı ayrı uygulanmıştır. Her bir güvenlik statüsü için tüm atakların tekrarlanması sonucunda, toplamda 36.976 atak eylemi gerçekleştirilerek kapsamlı bir test süreci yürütülmüştür.

Bu testler, modern siber tehditlerin KOBİ'ler üzerindeki etkisini anlamak ve mevcut güvenlik önlemlerinin hangi tehditlere karşı etkili olduğunu belirlemek amacıyla detaylı bir şekilde tasarlanmıştır. Elde edilen veriler, hem mevcut güvenlik çözümlerinin performansını ölçmek hem de KOBİ'ler için daha güçlü ve kapsamlı bir güvenlik stratejisi oluşturmak için temel teşkil etmektedir.

Tablo 1. Atak Kategorileri ve Atak Sayıları

Sıra	**Kategori**	**Atak Sayısı**
1	Arka Kapı	178
2	Bilgi Hırsızlığı	66
3	Botnet	12
4	Casus Yazılım	94
5	Fidye Yazılımı	428
6	Hackleme Aracı	30
7	İndirici İndirme	40
8	Silici	36
9	Solucan	22
10	Truva Atı	180
11	Uç Nokta Atakları	2.842
12	Uzak Kod Çalıştırma	4
13	Yetki Yükseltme	8
14	Yükleyici	58
15	Zararlı Yazılım	624
	Toplam	**4.622**

2.5. Güvenlik Statüleri

Tablo 2. Güvenlik Statüleri ve Toplam Atak Sayıları

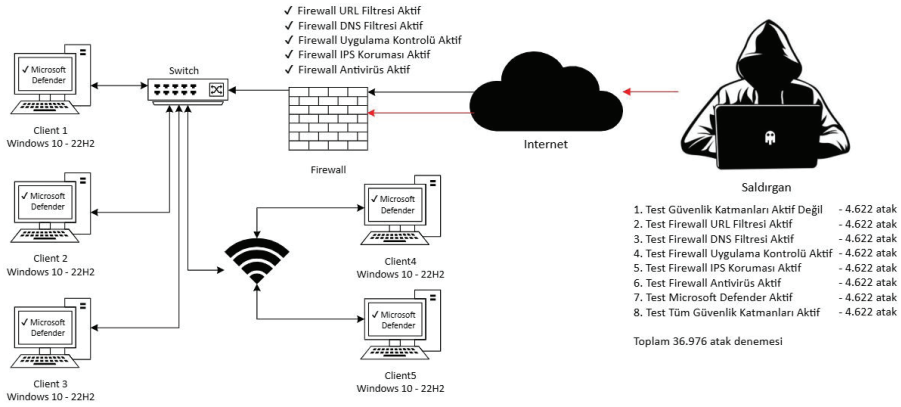
Sıra	Güvenlik Statüsü	Atak Sayısı
1	Güvenlik Katmanları Aktif Değil	4.622
2	Güvenlik Duvarı URL Filtresi Aktif	4.622
3	Güvenlik Duvarı DNS Filtresi Aktif	4.622
4	Güvenlik Duvarı Uygulama Kontrolü Aktif	4.622
5	Güvenlik Duvarı IPS Koruması Aktif	4.622
6	Güvenlik Duvarı Antivirüs Aktif	4.622
7	Microsoft Defender Aktif	4.622
8	Tüm Güvenlik Katmanları Aktif	4.622
	Toplam Yapılan Atak Sayısı	36.976

Simülasyonlar sırasında, Tablo 1'de belirtilen farklı siber saldırı teknikleri, belirlenen sayılarda son kullanıcı cihazlarına uygulanacaktır. Bu süreçte, Tablo 2'de yer alan güvenlik statüleri tek tek devreye alınarak, her bir statünün etkinliği ayrı ayrı değerlendirilecektir. Her güvenlik statüsünün ataklara karşı sağladığı koruma oranları, simülasyon sonuçlarına göre ölçülecek ve analiz edilecektir.

Son aşamada, Tablo 2'de 8. sırada belirtilen tüm güvenlik katmanları bir arada aktif hale getirilerek, bu katmanların birlikte sağladığı toplam koruma oranı ortaya konulacaktır. Simülasyonlar sonucunda, saldırıların engellenme oranları istatistiksel yöntemlerle analiz edilecek ve güvenlik katmanlarının bireysel ve kolektif etkinlikleri üzerine çıkarımlar yapılacaktır. Bu çalışma, güvenlik stratejilerinin optimize edilmesine yönelik önemli veriler sağlayacaktır.

2.6. Simülasyon Ortamı

Yapılacak testlerin temel amacı, önerilen güvenlik katmanlarının gerçek dünyadaki siber saldırı senaryolarında ne kadar etkili olduğunu ölçmek ve KOBİ'ler gibi sınırlı kaynaklara sahip işletmeler için güvenlik çözümlerinin verimliliğini değerlendirmektir.



Şekil 1. Simülasyon Ortamı

Şekil 1 görülebilen simülasyon ortamı, farklı türdeki siber saldırıların kontrollü bir şekilde taklit edilmesini sağlar. Bu süreçte, önerilen güvenlik katmanları birer birer test edilerek her birinin belirli tehditlere karşı etkinliği analiz edilmektedir. Bu testler, zararlı yazılımlar, kimlik avı saldırıları, fidye yazılımları ve diğer yaygın siber tehditlere karşı alınan önlemlerin gerçek koşullarda nasıl performans gösterdiğini anlamaya yönelik önemli veriler sunar.

Simülasyonların sonunda elde edilen bulgular, KOBİ'ler için uygulanabilir güvenlik çözümlerinin etkinliğini somut verilerle ortaya koyar. Ayrıca, bu süreç, güvenlik stratejilerinde mevcut zayıflıkları belirleyerek daha güçlü bir savunma altyapısının oluşturulmasına rehberlik eder. Böylece işletmeler, hem mevcut kaynaklarını daha etkili bir şekilde kullanabilir hem de güvenlik açıklarını en aza indirerek operasyonel ortamlarını daha güvenli hale getirebilirler.

3. Atak Türleri

Simülasyon ortamında gerçekleştirilen 15 farklı siber atak türü, KOBİ'ler ve diğer kurumların karşılaşabileceği en yaygın ve etkili tehditleri kapsamlı bir şekilde yansıtmaktadır. Bu ataklar, modern siber güvenlik sistemlerinin güçlü ve zayıf yönlerini test ederek, kurumların

güvenlik açıklarını anlamalarına ve risk yönetimi stratejilerini geliştirmelerine yardımcı olmaktadır. Aşağıda, bu atak türleri genel hatlarıyla ele alınmıştır: [7]

Arka Kapı (Backdoor): Saldırganların sistemlere yetkisiz erişim sağlamasına olanak tanıyan zararlı yazılımlar, özellikle gizli veri sızıntıları ve kalıcı tehdit oluşturma amacıyla kullanılır.

Bilgi Hırsızlığı (Information Theft): Kullanıcıların hassas verilerini ele geçirmek için tasarlanan bu saldırılar, genellikle finansal ve ticari bilgileri hedef alır.

Botnet: Çeşitli cihazları ele geçirip bir ağ üzerinden koordine edilen bu saldırılar, dağıtık hizmet reddi (DDoS) gibi büyük ölçekli tehditlerde kullanılır.

Casus Yazılım (Spyware): Kullanıcıların sistemlerine sızarak veri toplama ve faaliyetlerini izleme amacı güden yazılımlar, özellikle işletmelerin gizliliğini tehdit eder.

Fidye Yazılımı (Ransomware): Sistemlere sızarak verileri şifreleyen ve erişim karşılığında fidye talep eden saldırılar, KOBİ'ler için büyük mali kayıplara yol açabilir.

Hackleme Araçları: Güvenlik açıklarını keşfetmek veya sistemlere yetkisiz erişim sağlamak için kullanılan araçlar, özellikle sistem yöneticilerinin bilinçsizce kullandığı zafiyetleri hedef alır.

İndirici İndirme (Downloader): Zararlı yazılımları sisteme yüklemek için kullanılan bu araçlar, genellikle diğer saldırıların başlangıç aşamasında devreye girer.

Silici (Wiper): Sistemlerdeki verileri tamamen yok etmeyi amaçlayan bu saldırılar, özellikle kuruluşların operasyonel sürekliliğini tehdit eder.

Solucan (Worm): Ağ bağlantıları üzerinden yayılan ve kendini çoğaltan bu zararlı yazılımlar, kısa sürede geniş bir sisteme yayılabilir.

Truva Atı (Trojan): Meşru bir yazılım gibi görünen ancak zararlı işlemler gerçekleştiren bu yazılımlar, genellikle kullanıcıların dikkatini çekmeden sistemlere yerleşir.

Uç Nokta Atakları (Endpoint Attacks): Cihazların uç noktalarını hedef alarak veri sızıntısı veya sistemi devre dışı bırakmayı amaçlayan saldırılar, özellikle zayıf güvenlik protokollerinden faydalanır.

Uzak Kod Çalıştırma (Remote Code Execution): Saldırganların, hedef sistem üzerinde zararlı kod çalıştırmasını sağlayan bu saldırılar, genellikle sistemin tüm kontrolünü ele geçirme amacı taşır.

Yetki Yükseltme (Privilege Escalation): Sistem içindeki kullanıcı yetkilerini artırmayı hedefleyen bu saldırılar, saldırganlara kritik verilere erişim imkanı sağlar.

Yükleyici (Loader): Zararlı yazılımların sistemlere yüklenmesi için kullanılan bir ara yazılım türüdür ve genellikle diğer saldırıların tamamlayıcı unsuru olarak çalışır.

Zararlı Yazılım (Malware): Genel bir kavram olarak zararlı yazılımlar, sistemlerin işleyişini bozmayı veya veri çalmayı amaçlayan çeşitli yazılım türlerini kapsar.

Bu atak türleri, modern işletmelerin karşı karşıya olduğu siber tehditlerin çeşitliliğini ve karmaşıklığını ortaya koymaktadır. Her bir türün sistemlere olan etkisi, güvenlik açıklarının kapatılmasının ve güçlü bir siber güvenlik altyapısının gerekliliğini vurgulamaktadır.

4. Güvenlik Test Katmanları

Madde 2.6'da belirtilen simülasyon ortamında yer alan cihazlar, belirlenen güvenlik katmanları ve statüler doğrultusunda test edilecektir. Bu testlerin amacı, her bir güvenlik katmanının bağımsız ve bir arada çalıştığında siber tehditlere karşı ne kadar etkili olduğunu ölçmektir. Simülasyon ortamındaki cihazlara aşağıdaki statülerde madde 2.4'de belirtilen ataklar uygulanarak cihazların karşı karşıya kaldığı ataklara karşı gösterdiği direnç ve güvenlik performansı detaylı bir şekilde analiz edilecektir.

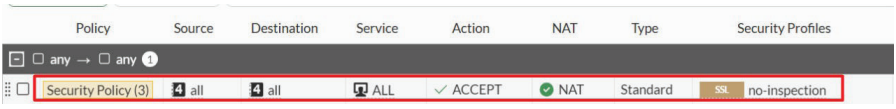
4.1. Güvenlik Katmanları Aktif Değil

Madde 2.2'de belirtilen Windows konfigürasyonunda Microsoft Defender ve Windows güvenlik özelliklerini (gerçek zamanlı koruma, Antivirüs, güvenlik duvarı, bulut tabanlı koruma, kimlik avı koruması, SmartScreen, istenmeyen uygulama engelleme) gibi özellikleri devre dışı bırakmak için, powershell yönetici yetkisi ile çalıştırılarak işletim sistemindeki tüm temel güvenlik katmanları devre dışı bırakılmıştır [8].

Denetim Masası – Internet Özellikleri üzerinden "Internet – Yerel Internet – Güvenilen Siteler

– Yasaklı Siteler" kategorilerindeki tüm güvenlik önlemleri en düşük seviye çekilmiştir.

Madde 2.3'de belirtilen Yeni Nesil Güvenlik Duvarı üzerinde herhangi bir yönden herhangi bir yöne doğru tüm istekleri izin veren ve üzerinde hiçbir güvenlik politikası bulunmayan Şekil 2'de görülen "Security Policy" kuralı yazılmıştır.



Şekil 2. Güvenlik Duvarı Güvenlik Önlemi Yok

Yukarıda belirtilen işlemler yapılarak tüm güvenlik katmanları devre dışı bırakılarak madde 2.4'deki ilgili atak simülasyonları çalıştırılmış ve güvenliksiz ortamın etkinliği ve siber tehditlere karşı direncini ölçmek amacıyla detaylı analizler gerçekleştirilmiştir. Bu analizlerin sonucunda, Madde 4.1'de ayrıntılı olarak sunulan bulgular elde edilmiştir. Bu bulgular güvenlik katmanları aktif değilken başarılı olan atakları ortaya koyarak, analizler için detaylı veriler sunmaktadır.

4.2. Yeni Nesil Güvenlik Duvarında SSL Denetiminin Aktif Hale Getirilmesi

Madde 4.3, 4.4, 4.5, 4.6, 4.7 ve 4.9 daki tüm testlerde SSL Denetimi özelliği aktif hale getirilmiş ve uç nokta cihazlara SSL denetimi için gerekli olan SSL sertifikası yüklenmiştir. Bu sayede Yeni Nesil Güvenlik Duvarının şifreli trafik üzerindeki görünürlüğü artırılmış, tehdit algılama ve önleme süreçlerinde daha etkin bir rol oynaması sağlanmıştır. Şifrelenmiş veri trafiğinin çözülmesi, kötü amaçlı yazılımların, kimlik avı ataklarının ve diğer siber tehditlerin güvenlik katmanları tarafından fark edilmesini kolaylaştırmıştır. Bu yöntem, yalnızca ağ güvenliğini güçlendirmekle kalmamış, aynı zamanda güvenlik duvarının uygulama bazlı ve kullanıcı bazlı politika uygulamalarında daha hassas ve verimli olmasına da olanak tanımıştır [9].

Bu yaklaşım, özellikle modern şifreleme protokollerinin yaygınlaştığı günümüzde, güvenlik tehditlerini önleme açısından kritik bir gereklilik olarak değerlendirilmektedir.

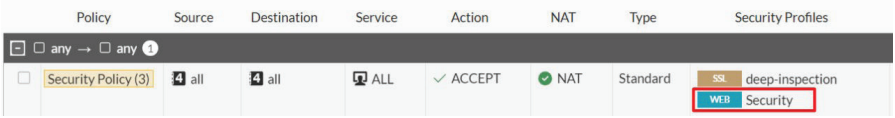
4.3. Yeni Nesil Güvenlik Duvarında URL Filtresinin Aktif Hale Getirilmesi

Güvenlik Duvarı URL filtresi, internet üzerinden belirli web sitelerinin ve URL'lerin erişimini engellemeye yarayan bir güvenlik özelliğidir. Bu özellik, ağda zararlı içeriklere veya istenmeyen sitelere erişimi kısıtlamak amacıyla kullanılır. Güvenlik Duvarı belirli URL'leri veya alan adlarını listeden çıkararak, kullanıcıların bu sitelere erişmelerini engeller. Genellikle kullanım amaçları aşağıdaki gibidir [10].

1. Zararlı Sitelerden Korunma: Kullanıcıların kötü amaçlı yazılım (malware) barındıran veya kimlik avı (phishing) içeren sitelere erişmelerini engeller.
2. Veri Güvenliği: Kurumsal ağlarda, gizli veya hassas bilgilerin dışarıya sızmasını engellemek amacıyla belirli URL'leri engeller.

3. İnternet Kullanımını Kontrol Etme: Özellikle okul veya işyerlerinde, çalışanların veya öğrencilerin zaman kaybettiren veya zararlı içeriklere sahip sitelere girmelerini önler.

Madde 4.1'de belirtilen güvenliksiz ortamın önüne sadece Yeni Nesil Güvenlik Duvarı üzerinde URL filtresi Şekil 3'da görüldüğü şekilde eklenmiştir.



Şekil 3. Sadece Güvenlik Duvarı URL Filtresi Aktif

İlgili politika varsayılan modda aktif hale getirilmiş, engelleme ve izin verme için herhangi bir özelleştirme yapılmamıştır.

Yukarıda belirtilen test ortamında, Güvenlik Duvarı URL Filtresi aktif hale getirilerek atak simülasyonları uygulanmıştır. Bu testler, URL filtresi etkin bir şekilde çalışırken, siber tehditlere karşı etkinliğini ve sağladığı koruma düzeyini değerlendirmek amacıyla gerçekleştirilmiştir. Yapılan analizlerin sonucunda, Madde 6.2'de ayrıntılı olarak sunulan bulgular elde edilmiştir. Bu bulgular, URL filtresinin güçlü ve zayıf yönlerini ortaya koyarak, önerilen stratejilerin etkinliğine ilişkin değerli iç görüler sağlamaktadır.

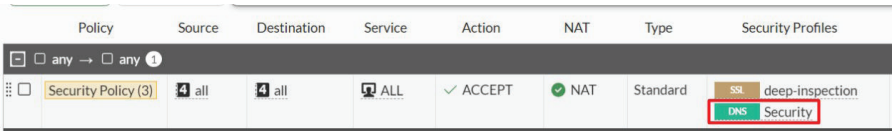
4.4. Yeni Nesil Güvenlik Duvarında DNS Filtresinin Aktif Hale Getirilmesi

Yeni Nesil Güvenlik Duvarı DNS filtresi, ağda yapılan DNS sorgularını kontrol ederek belirli alan adlarına (domain) erişimi engelleyen bir güvenlik özelliğidir. Bu filtre, DNS (Domain Name System) sorgularını, yani bir web sitesine erişim sağlamak için kullanılan IP adreslerini çevirme işlemini denetler. DNS filtresi temel olarak şu işlere yarar [11].

1. Zararlı Siteleri Engelleme: DNS filtresi, kötü amaçlı yazılım içeren veya kimlik avı (phishing) amacı güden sitelere yapılan DNS sorgularını engeller. Bu sayede kullanıcılar bu tür zararlı sitelere erişim sağlayamaz.
2. İstenmeyen İçeriği Engelleme: Çeşitli kategorilerdeki (örneğin, yetişkin içerik, kumar, şiddet) istenmeyen sitelere erişimi engelleyerek, ağ güvenliğini artırır ve kullanıcıların zararlı içeriklere ulaşmalarını önler.
3. Veri Güvenliği: Özel verilerin sızmasını önlemek amacıyla, yalnızca güvenli ve onaylı DNS sunucuları üzerinden yapılan bağlantılara izin verir.

Bu şekilde DNS filtresi, ağda zararlı ve istenmeyen trafiği engelleyerek daha güvenli bir internet deneyimi sağlar.

Madde 4.1'de belirtilen güvenliksiz ortamın önüne sadece Yeni Nesil Güvenlik Duvarı üzerinden DNS filtresi Şekil 4'de görüldüğü şekilde eklenmiştir.



Şekil 4. Sadece Güvenlik Duvarı DNS Filtresi Aktif

İlgili politika varsayılan modda aktif hale getirilmiş, engelleme ve izin verme için herhangi bir özelleştirme yapılmamıştır.

Testler yukarıda belirtilen ortama yapılarak madde 6.3 deki bulgular elde edilmiştir.

4.5. Yeni Nesil Güvenlik Duvarında Uygulama Kontrolünün Aktif Hale Getirilmesi

Yeni Nesil Güvenlik Duvarı Uygulama Kontrolü, bir ağ güvenlik özelliği olarak, ağda çalışan uygulamaların internet bağlantılarını

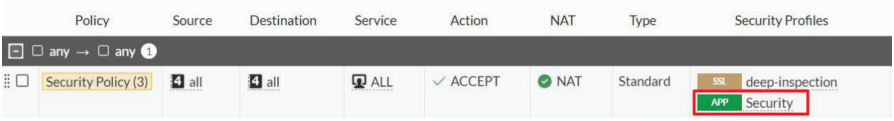
kontrol etmeye ve denetlemeye yarar. Bu özellik, yalnızca onaylı ve güvenli uygulamaların internete bağlanmasına izin verirken, kötü amaçlı veya istenmeyen uygulamaların ağ üzerinden veri gönderip almasını engeller. Uygulama kontrolü, özellikle kurumsal ağlarda veri sızıntılarını ve zararlı yazılım (malware) aktivitelerini önlemek için önemli bir güvenlik katmanı sunar [12].

Temel olarak bu özellik şu amaçlarla kullanılır:

1. Zararlı Uygulamaların Engellenmesi: Güvenlik duvarı, kötü amaçlı yazılımlar veya zararlı uygulamalar tarafından yapılan internet bağlantılarını tespit eder ve engeller.
2. Ağ İzinlerinin Sınırlanması: Yalnızca belirli, izin verilen uygulamaların dışa ve içe bağlantı kurmasını sağlar, böylece yetkisiz yazılımlar ağda çalışamaz.
3. İzinsiz Veri Paylaşımının Önlenmesi: Kullanıcılar veya yazılımlar tarafından yapılan veri paylaşımını izler ve kontrol eder, hassas bilgilerin dışarıya sızmasını engeller.

Bu şekilde, uygulama kontrolü, sadece ağda izin verilen yazılımlar tarafından yapılan trafiğe izin vererek ağın güvenliğini artırır.

Madde 4.1'de belirtilen güvenliksiz ortamın önüne sadece Güvenlik Duvarı üzerinden Uygulama Kontrolü **Şekil 5**'de görüldüğü şekilde eklenmiştir.



Şekil 5. Sadece Güvenlik Duvarı Uygulama Kontrolü Aktif

İlgili politika varsayılan modda aktif hale getirilmiş, engelleme ve izin verme için herhangi bir özelleştirme yapılmamıştır.

Testler yukarıda belirtilen ortama yapılarak madde 6.4 deki bulgular elde edilmiştir.

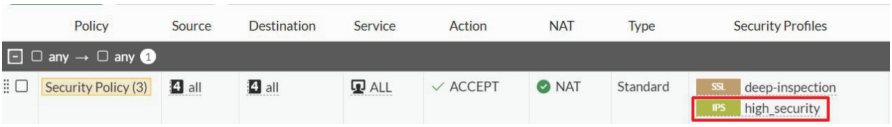
4.6. Yeni Nesil Güvenlik Duvarında IPS Korumasının Aktif Hale Getirilmesi

Yeni Nesil Güvenlik Duvarı IPS (Intrusion Prevention System) koruması, ağ güvenliğini sağlamak için kullanılan bir teknolojidir. Bu özellik, ağda gerçekleşebilecek potansiyel atakları tespit eder ve engeller. IPS, genellikle Güvenlik Duvarı cihazları ile entegre çalışır ve kötü niyetli trafik, exploitler veya atak kalıplarını analiz ederek, saldırganların sisteme zarar vermesini önler [13].

1. Atak Tespiti ve Engelleme: IPS, ağdaki anormal trafiği ve bilinen atak tekniklerini tanıyan bir dizi imzaya sahip olup, bu tür aktiviteleri anında tespit eder ve engeller. Bu, zararlı yazılımların, DDoS ataklarının ve diğer kötü amaçlı faaliyetlerin ağda yayılmasını önler.
2. Gelişmiş Tehdit Öncesi Koruma: IPS, ataklar ağ içine girmeden önce, gelen trafiği analiz ederek, potansiyel tehditleri önler. Bu, sistemlerin korunmasına yardımcı olur ve ağ üzerindeki güvenliği artırır.
3. Gerçek Zamanlı Müdahale: IPS, sadece tehditleri tespit etmekle kalmaz, aynı zamanda bu tehditlere karşı anında müdahale ederek, atakları bloke eder. Bu, ağın kesintisiz bir şekilde çalışmasını sağlar.

Güvenlik Duvarı IPS koruması, ağdaki zararlı etkinlikleri gerçek zamanlı olarak tespit edip engelleyerek, ağ güvenliğini önemli ölçüde artıran bir özelliktir.

Madde 4.1'de belirtilen güvenliksiz ortamın önüne sadece Güvenlik Duvarı üzerinden Uygulama Kontrolü Şekil 6'de görüldüğü şekilde eklenmiştir.



Şekil 6. Sadece Güvenlik Duvarı IPS Koruması Aktif

İlgili politika varsayılan modda aktif hale getirilmiş, engelleme ve izin verme için herhangi bir özelleştirme yapılmamıştır.

Testler yukarıda belirtilen ortama yapılarak madde 6.5'deki bulgular elde edilmiştir.

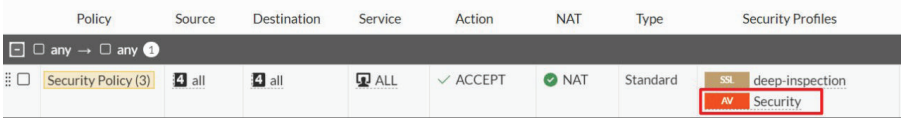
4.7. Yeni Nesil Güvenlik Duvarında Antivirüs Korumasının Aktif Hale Getirilmesi

Yeni Nesil Güvenlik Duvarı Antivirüs koruması, bir ağ güvenlik duvarı üzerinde çalışan ve ağ trafiği içerisindeki kötü amaçlı yazılımları tespit ederek engellemeye yönelik bir özelliktir. Bu, güvenlik duvarının gelen ve giden trafiği analiz etmesini ve potansiyel tehditleri, özellikle virüsleri ve zararlı yazılımları tanımlayıp engellemesini sağlar [14].

1. Kötü Amaçlı Yazılımların Engellenmesi: Antivirüs koruması, ağ üzerinden gelen verileri tarar ve virüsler, solucanlar, truva atları gibi kötü amaçlı yazılımların sistemlere girmesini engeller.
2. Gelişmiş Tehdit Koruması: Bu sistem, daha önce bilinmeyen zararlı yazılımları tespit etmek için davranış tabanlı analiz yöntemleri kullanabilir. Bu sayede, yeni ve bilinmeyen tehditlere karşı da koruma sağlar.
3. Ağ Üzerindeki Taramalar: Güvenlik Duvarı Antivirüs, ağdaki tüm veriyi kontrol ederek, virüslerin yayılmasını engeller. Hem dışardan gelen tehditlere hem de iç ağdaki cihazlar arasındaki tehditlere karşı koruma sunar.

Güvenlik Duvarı Antivirüs koruması, ağ güvenliği sağlamak ve sistemleri kötü amaçlı yazılımlardan korumak için kritik bir bileşendir.

Madde 4.1'de belirtilen güvenliksiz ortamın önüne sadece Güvenlik Duvarı üzerinden Antivirüs özelliği Şekil 7'de görüldüğü şekilde eklenmiştir.



Şekil 7. Sadece Güvenlik Duvarı Antivirüs Koruması Aktif İlgili politika içerisinde herhangi bir özelleştirme yapılmamıştır.

Testler yukarıda belirtilen ortama yapılarak madde 6.6'daki bulgular elde edilmiştir.

4.8. Yalnız Microsoft Defender'ın Aktif Hale Getirilmesi

Microsoft Defender, Windows işletim sistemi üzerinde yerleşik olarak bulunan bir güvenlik yazılımıdır. Bu yazılım, cihazları virüsler, zararlı yazılımlar, kimlik avı atakları ve diğer güvenlik tehditlerine karşı korur. Microsoft Defender, sürekli çalışan bir Antivirüs programı olarak, kullanıcıların internet üzerinde güvenli bir şekilde gezinmesini ve dosyaları güvenle indirmesini sağlar. Ayrıca, cihazda bulunan dosyaları tarar, tehditlere karşı gerçek zamanlı koruma sağlar ve sistemdeki olası zayıf noktaları tespit eder [15].

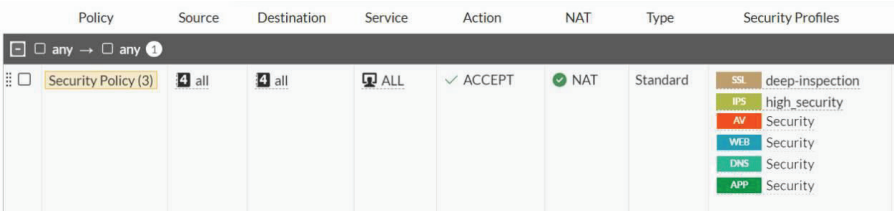
1. Gerçek Zamanlı Koruma: Virüsler, solucanlar, truva atları ve diğer zararlı yazılımlar sisteme girmeden önce tespit edilip engellenir.
2. İnternet Güvenliği: Microsoft Defender, web tarayıcıları üzerinden gelen tehditleri izler ve internet üzerinde güvenli bir gezinme deneyimi sunar.
3. Performans ve Uyumluluk: Microsoft Defender, sistem kaynaklarını optimize ederek cihazın performansını etkilemeden güvenlik sağlar.
4. Kimlik Avı Koruması: Microsoft Defender, kimlik avı atakları ve dolandırıcılık e- postalarını tespit ederek kullanıcıyı uyarır.

Bu özellikler, kullanıcıların cihazlarını tehditlerden korur ve güvenlik sağlar.

Tüm Yeni Nesil Güvenlik Duvarı güvenlik katmanları kapalıyken ve Windows üzerindeki temel tüm güvenlik katmanları aktifken herhangi bir özelleştirme olmadan yapılan testlerde madde 6.7'deki bulgular elde edilmiştir.

4.9. Tüm Güvenlik Katmanlarının Bir Arada Aktif Hale Getirilmesi

Madde 4.3, 4.4, 4.5, 4.6 ve 4.7 deki Yeni Nesil Güvenlik Duvarı üzerindeki tüm güvenlik katmaları varsayılan modda açılmış ve Şekil 8'de görüleceği üzere politikada bir arada uygulanmıştır.



Şekil 8. Tüm Güvenlik Duvarı güvenlik katmanları aktif

Microsoft Defender varsayılan ayarları ile madde 4.8'de belirtildiği gibi aktif hale getirilmiştir.

Bu şekilde hem Yeni Nesil Güvenlik Duvarı özelliklerinin hem de Microsoft Defender'ın birlikte sağladıkları güvenliğin ölçülmesi hedeflenmiştir. Tüm güvenlik katmanları aktifken yapılan simülasyonlarda madde 6.8'deki bulgular elde edilmiştir.

5. Veri

Bu çalışmada kullanılan veri seti, tezdeki analizlerin tekrarlana bilirliğini ve şeffaflığını artırmak amacıyla GitHub platformunda depolanmıştır. Veri setine https://github.com/buroxy/attackdata bağlantısı üzerinden erişilebilir [16].

Veri seti, Excel biçimindedir ve gerekli açıklamaları içeren bir README dosyası ile birlikte paylaşılmıştır. Bu dosya, veri setinin yapısını, değişkenlerin anlamlarını detaylı olarak açıklamaktadır. Çalışmanın tekrar edilebilirliği ve farklı araştırmacılar tarafından kullanılabilirliği için veri seti herkese açık olarak yayınlanmıştır.

6. Bulgular

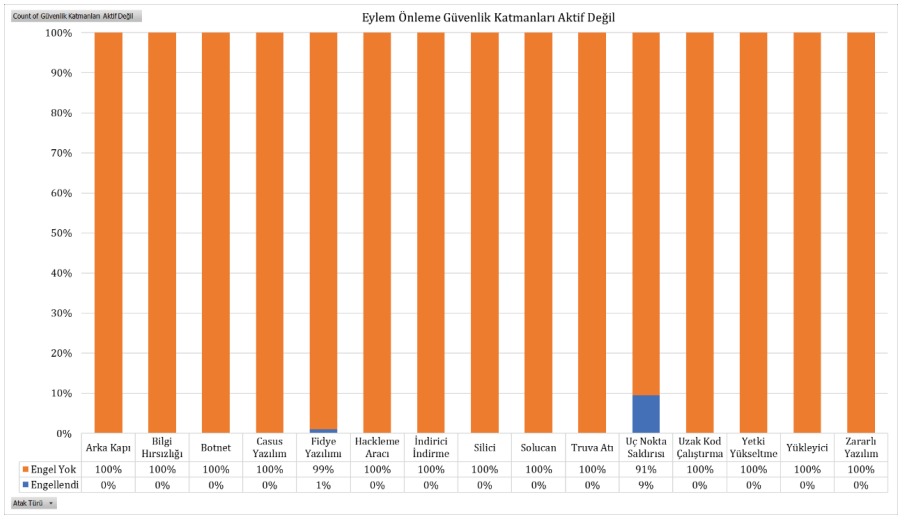
Madde 2.6'de belirtilen test ortamı için madde 0'de bulunan 8 durum statüsü, madde 2.4'deki test atak kategorileri ile ayrı ayrı uygulanarak test edilmiştir.

Yapılan çalışmada tehditlerin gerçekleşmesi için tüm eylemler adım adım uygulanmıştır.

6.1. Hiçbir Güvenlik Katmanı Aktif Değilken

Madde 4.1'de belirtildiği üzere Windows üzerinde varsayılan olarak bulunan Microsoft Defender devre dışı bırakılarak Windows işletim sisteminin çekirdek seviyede güvenliği ölçülmesi amaçlanmıştır.

Şekil 9, Windows işletim sistemi üzerinde hiçbir güvenlik katmanı aktif değilken gerçekleştirilen saldırılara karşı sistemin gösterdiği savunma performansını özetlemektedir. Test ortamında gerçekleştirilen bu saldırılar, işletim sisteminin core (çekirdek) servislerinin belirli saldırı türlerini sınırlı da olsa önleyebildiğini göstermektedir. Ancak genel sonuçlar, güvenlik katmanlarının devre dışı olduğu bir sistemin siber saldırılara karşı büyük ölçüde savunmasız olduğunu ortaya koymaktadır.



Şekil 9. Hiçbir güvenlik katmanı aktif değilken eylem önleme sonucu

Şekil 9'de görüldüğü üzere, fidye yazılımı kategorisindeki saldırıların yalnızca %1'i, uç nokta saldırılarının ise %9'u Windows core servisleri tarafından engellenebilmiştir. Diğer kategorilerde, saldırıların %100'ü başarıyla gerçekleştirilmiştir. Bu sonuç, Windows işletim sistemi üzerinde yerleşik güvenlik önlemlerinin, belirli durumlarda minimal koruma sağlamakla birlikte, kapsamlı bir güvenlik stratejisi olmadan etkisiz kaldığını açıkça göstermektedir.

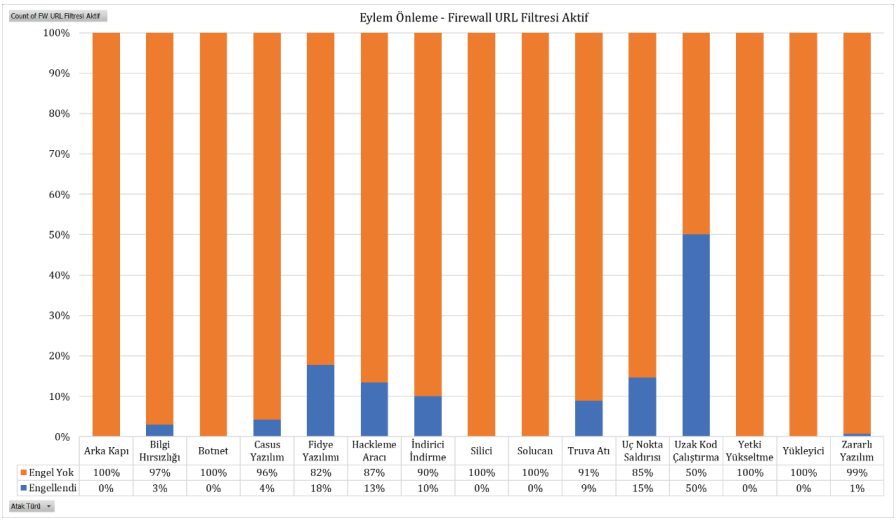
Şekil 17'ya bakıldığında, Windows core servislerinin tüm saldırıların yalnızca %6'sını engellemede başarılı olduğu belirtilmektedir. Bu oran, core servislerin yalnızca kısıtlı bir güvenlik sağlayabildiğini ve modern tehditlere karşı yeterli olmadığını ortaya koymaktadır.

Sonuç olarak, hiçbir ek güvenlik katmanı etkinleştirilmediğinde, Windows işletim sistemi siber saldırılara karşı genel olarak savunmasızdır. Bu durum, işletim sisteminin güvenlik açıklarını kapatmak ve tehditleri etkili bir şekilde engellemek için çok katmanlı bir güvenlik stratejisinin gerekliliğini bir kez daha vurgulamaktadır. Uygulamalı testler, entegre güvenlik katmanlarının etkinleştirilmesinin saldırılara

karşı direnci önemli ölçüde artıracağını ve sistem güvenliğini üst seviyeye taşıyacağını göstermektedir.

6.2. Güvenlik Duvarı URL Filtresi Aktifken

Şekil 10, sadece Güvenlik Duvarı URL filtresinin aktif olduğu madde 4.3'de belirtilen test ortamında, belirli saldırı türlerini engelleme yeteneğini değerlendirmektedir. Test ortamında yapılan analizler, Güvenlik Duvarı URL filtresinin bazı tehdit kategorilerinde kısmi koruma sağladığını ancak genel olarak tek başına yeterli olmadığını göstermektedir.



Şekil 10. Güvenlik Duvarı URL filtresi aktifken eylem önleme sonucu

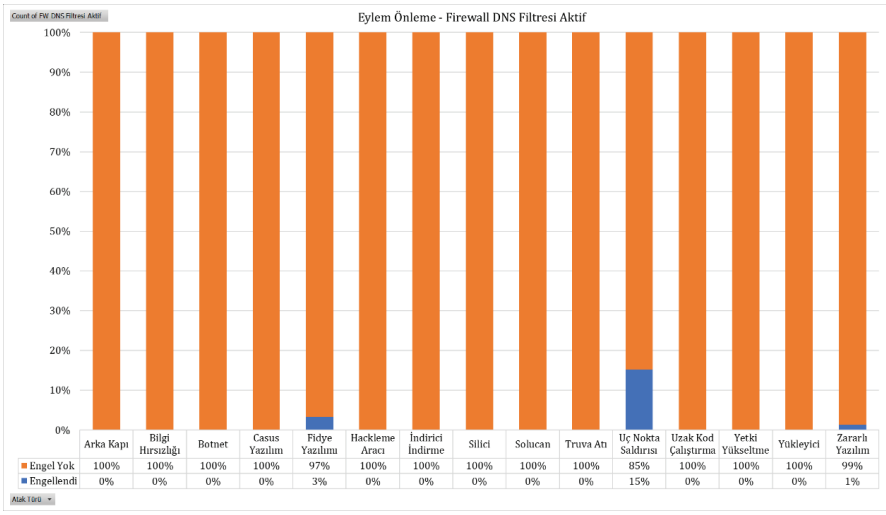
Eylem önleme sonuçlarına göre, Bilgi Hırsızlığı kategorisinin yalnızca %3'ü, Casus Yazılım kategorisinin %4'ü, Fidye Yazılımı kategorisinin %18'i, Hackleme Aracı kategorisinin %87'si, İndirici İndirme kategorisinin %10'u, Truva Atı kategorisinin %9'u, Uç Nokta Atakları kategorisinin %15'i, Uzaktan Kod Çalıştırma kategorisinin %50'si ve Zararlı Yazılım kategorisinin %1'i Güvenlik Duvarı URL

filtresi tarafından engellenmiştir. Bu oranlar, Güvenlik Duvarı URL filtresinin bazı kategorilerde daha başarılı olduğunu, özellikle hackleme araçları (%87) ve uzaktan kod çalıştırma (%50) gibi belirli tehditlerde etkili olduğunu ortaya koymaktadır. Ancak birçok tehdit türü (örneğin, bilgi hırsızlığı ve fidye yazılımı gibi) karşısında etkisinin oldukça sınırlı olduğu görülmektedir. Güvenlik Duvarı URL filtresi, güvenlik stratejisinin bir parçası olarak önemli bir yere sahip olsa da, tek başına uygulanması durumunda cihazlar ciddi ölçüde savunmasız kalmaktadır. Bu durum, çok katmanlı güvenlik çözümlerinin gerekliliğini açıkça ortaya koymaktadır. Şekil 17'da görüldüğü üzere, Güvenlik Duvarı URL filtresi tüm saldırıların yalnızca %11'ini engelleyebilmiştir. Bu oran, Güvenlik Duvarı URL filtresinin yalnızca bir yardımcı güvenlik katmanı olarak değerlendirilmesi gerektiğini ve diğer güvenlik önlemleriyle birleştirildiğinde daha etkili bir savunma sağlayacağını göstermektedir.

Sonuç olarak, Güvenlik Duvarı URL filtresi tek başına belirli tehdit türlerine karşı kısmi bir koruma sağlayabilse de, geniş kapsamlı bir güvenlik stratejisinin bir parçası olarak kullanıldığında daha iyi sonuçlar elde edilebileceği açıktır. Sistem güvenliği açısından, farklı güvenlik katmanlarının entegrasyonu ve uyum içinde çalışması, ağ savunmasını optimize etmek için kritik bir önem taşımaktadır.

6.3. Güvenlik Duvarı DNS Filtresi Aktifken

Güvenlik Duvarı DNS filtresi aktifken uygulanan ataklarda Güvenlik Duvarı DNS filtresinin atakları engelleme konusunda yetkinliği değerlendirilmiştir. Şekil 29, Güvenlik Duvarı DNS filtresinin aktif olduğu madde 4.4'de belirtilen test ortamına doğru gerçekleştirilen saldırılara karşı alınan önleme sonuçlarını özetlemektedir. Test ortamında uygulanan saldırılar, Güvenlik Duvarı DNS filtresinin belirli tehdit kategorilerinde kısmi bir koruma sağladığını, ancak genel olarak tek başına uygulandığında cihazların savunmasız kaldığını göstermektedir.



Şekil 11. Güvenlik Duvarı DNS filtresi aktifken eylem önleme sonucu

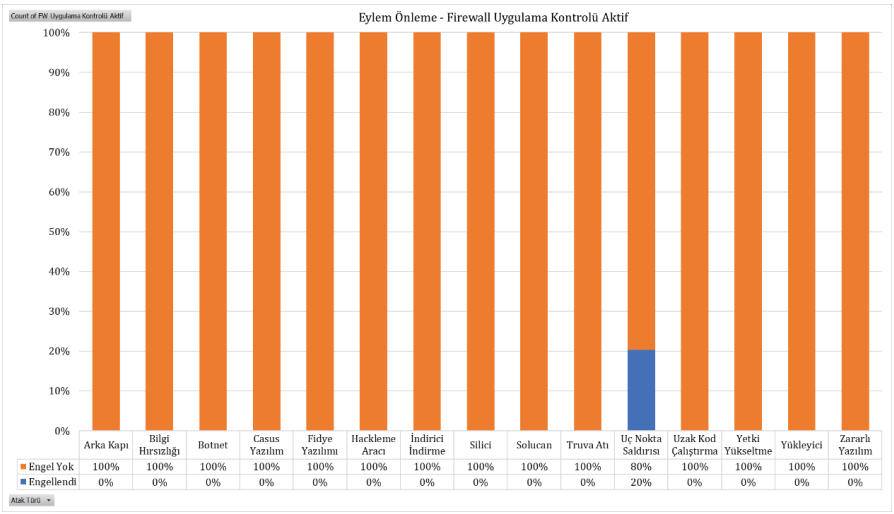
Eylem önleme sonuçlarına göre, Fidye Yazılımı kategorisindeki saldırıların yalnızca %3'ü, Uç Nokta Saldırıları kategorisindeki saldırıların %15'i ve Zararlı Yazılım kategorisindeki saldırıların %1'i Güvenlik Duvarı DNS filtresi tarafından engellenebilmiştir. Diğer tehdit kategorilerinde ise saldırıların tamamının başarılı olduğu dikkat çekmektedir. Bu durum, Güvenlik Duvarı DNS filtresinin güvenlik açısından tek başına yeterli olmadığını ve yalnızca sınırlı bir koruma sağlayabildiğini açıkça ortaya koymaktadır. Şekil 17'ya bakıldığında, Güvenlik Duvarı DNS filtresi tüm saldırıların yalnızca %10'unu engelleyebilmiştir. Bu oran, DNS filtrelemenin bazı durumlarda etkili bir savunma mekanizması olabileceğini ancak daha geniş kapsamlı bir güvenlik politikası içinde kullanılmasının zorunlu olduğunu göstermektedir. DNS filtresi, özellikle fidye yazılımı ve uç nokta saldırıları gibi belirli tehdit türlerinde sınırlı da olsa etkili olurken, diğer tehdit kategorilerinde neredeyse hiçbir koruma sağlayamamaktadır.

Sonuç olarak, Güvenlik Duvarı DNS filtresi tek başına uygulandığında, cihazlar ciddi ölçüde savunmasızdır. Güvenlik Duvarı DNS filtresi, diğer güvenlik katmanlarıyla birlikte kullanıldığında daha

etkin bir savunma sağlayabilir. Ancak, modern tehditlerin karmaşıklığı ve saldırganların sürekli gelişen teknikleri değerlendirildiğinde, DNS filtrelemenin yalnızca bir yardımcı güvenlik aracı olarak değerlendirilmesi ve diğer katmanlarla entegrasyonunun sağlanması gerektiği açıkça görülmektedir. Bu bağlamda, DNS filtresinin çok katmanlı bir güvenlik çözümünün parçası olarak kullanılmasının sistem güvenliğini artıracağı söylenebilir.

6.4. Güvenlik Duvarı Uygulama Kontrolü Aktifken

Şekil 12, Güvenlik Duvarı Uygulama Kontrolü'nün aktif olduğu madde 4.5'de belirtilen test ortamına doğru gerçekleştirilen saldırılara karşı alınan önleme sonuçlarını göstermektedir. Güvenlik Duvarı Uygulama Kontrolü'nün belirli tehdit türlerine karşı sınırlı bir koruma sağladığını, ancak tek başına genel güvenlik için yetersiz olduğunu ortaya koymaktadır.



Şekil 12. Güvenlik Duvarı uygulama kontrolü aktifken eylem önleme sonucu

Eylem önleme sonuçlarına göre, yalnızca Uç Nokta Saldırıları kategorisindeki saldırıların

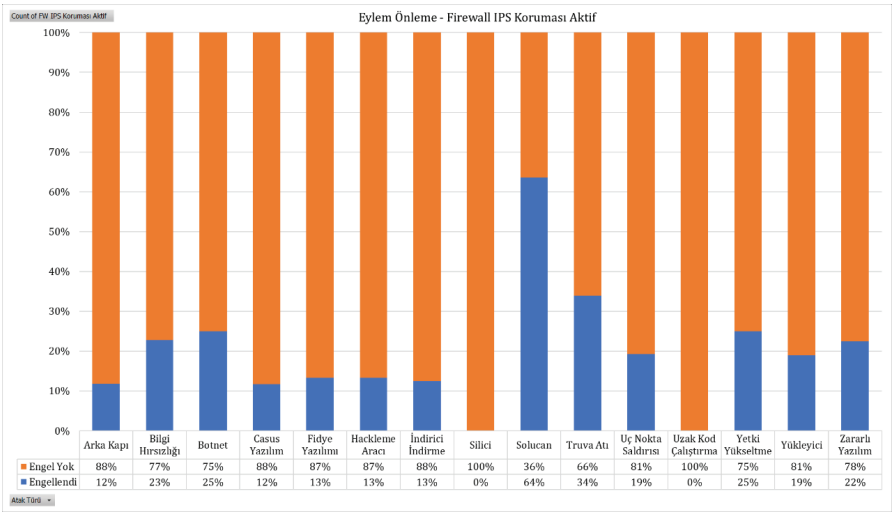
%20'si Güvenlik Duvarı Uygulama Kontrolü tarafından engellenebilmiştir. Diğer tehdit kategorilerinde herhangi bir engelleme sağlanamamıştır. Bu durum, Güvenlik Duvarı Uygulama Kontrolü'nün tek başına siber saldırılara karşı yeterli bir savunma sağlamadığını ve güvenlik katmanlarının birlikte kullanılmasının önemini bir kez daha vurgulamaktadır. Şekil 17'da görüleceği üzere, Güvenlik Duvarı Uygulama Kontrolü tüm saldırıların yalnızca

%13'ünü engellemiştir. Bu oran, Güvenlik Duvarı Uygulama Kontrolü'nün belirli tehditlere karşı etkili bir araç olabileceğini ancak kapsamlı bir güvenlik stratejisi içinde yardımcı bir bileşen olarak değerlendirilmesi gerektiğini göstermektedir. Uygulama kontrolü, özellikle belirli uygulamalardan gelen tehditlere karşı bir bariyer oluşturabilir, ancak saldırganların farklı teknikler kullanarak bu katmanı aşabileceği unutulmamalıdır.

Sonuç olarak, Güvenlik Duvarı Uygulama Kontrolü tek başına uygulanmaya devam ettiğinde cihazlar savunmasız kalmaktadır. Bu durum, siber güvenlikte çok katmanlı yaklaşımların kritik önemini bir kez daha göstermektedir. Uygulama kontrolü, diğer güvenlik katmanları ile entegre edildiğinde daha etkili bir savunma sağlamakta ve modern tehditlere karşı daha güçlü bir koruma oluşturabilmektedir. Bu bağlamda, Güvenlik Duvarı Uygulama Kontrolü'nün, ağ güvenliğinde destekleyici bir katman olarak kullanılması gerektiği açıktır.

6.5. Güvenlik Duvarı IPS Koruması Aktifken

Şekil 13, Güvenlik Duvarı IPS (Saldırı Önleme Sistemi) korumasının aktif olduğu madde 4.6'da belirtilen test ortamına doğru gerçekleştirilen saldırılara karşı alınan önleme sonuçlarını detaylandırmaktadır. Test ortamında yapılan analizler, IPS korumasının belirli tehdit kategorilerinde diğer koruma önlemlerine kıyasla daha tatmin edici bir başarı sağladığını, ancak tek başına tam koruma sağlamadığını göstermektedir.



Şekil 13. Güvenlik Duvarı IPS koruması aktifken eylem önleme sonucu

Eylem önleme sonuçlarına göre: Arka Kapı saldırılarının %12'si, Bilgi Hırsızlığı saldırılarının

%23'ü, Botnet saldırılarının %25'i, Casus Yazılım saldırılarının %12'si, Fidye Yazılımı saldırılarının %13'ü, Hackleme Aracı ve İndirici İndirme kategorilerindeki saldırıların %13'ü, Solucan saldırılarının %64'ü, Truva Atı saldırılarının %34'ü, Uç Nokta Saldırılarının %19'u, Yetki Yükseltme saldırılarının %25'i, Yükleyici saldırılarının %19'u ve Zararlı Yazılım kategorisindeki saldırıların %22'si Güvenlik Duvarı IPS koruması tarafından engellenmiştir.

Bu oranlar, Güvenlik Duvarı IPS korumasının özellikle Solucan (%64) ve Truva Atı (%34) gibi tehdit türlerinde daha etkili olduğunu göstermektedir.

Şekil 17'da görüldüğü üzere Güvenlik Duvarı IPS koruması, tüm saldırıların yalnızca %19'unu engelleyebilmiştir. Bu, IPS'in ağ güvenliği için önemli bir bileşen olduğunu, ancak diğer güvenlik katmanlarıyla birleştirilmesi gerektiğini göstermektedir. IPS, saldırıların sistem üzerinde oluşturabileceği zararları azaltmak için önemli bir savunma hattı oluşturabilir, ancak modern tehditlerin çeşitliliği karşısında tek başına yeterli bir koruma sağlayamamaktadır.

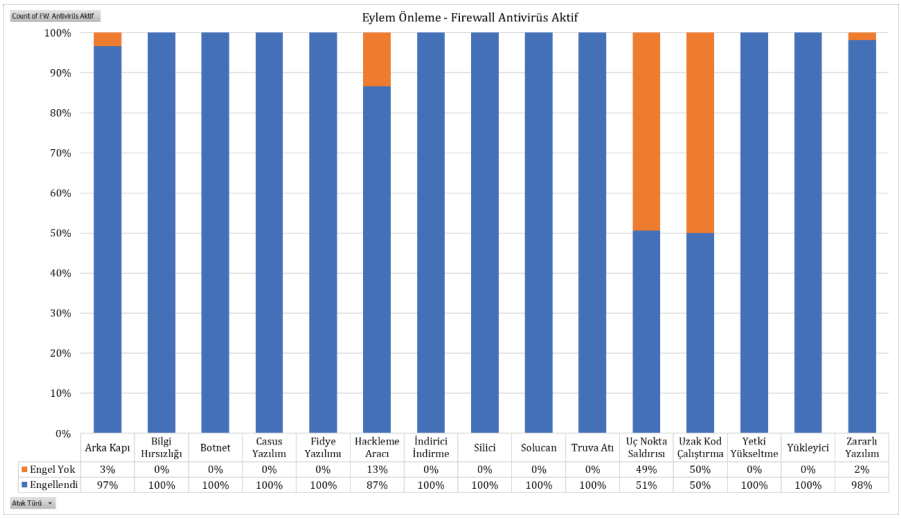
Sonuç olarak, Güvenlik Duvarı IPS koruması diğer güvenlik önlemlerine kıyasla daha tatmin edici sonuçlar sunmakta olsa da çok katmanlı bir güvenlik stratejisi içinde bir destekleyici katman olarak kullanılması gereklidir. IPS'in, Güvenlik Duvarı, DNS Filtreleme ve diğer güvenlik çözümleriyle birlikte entegre bir şekilde kullanılması, daha geniş kapsamlı bir koruma sağlayarak cihazların modern tehditlere karşı dayanıklılığını artıracaktır.

6.6. Güvenlik Duvarı Antivirüs Aktifken

Güvenlik Duvarı Antivirüs korumasının aktif olduğu madde 4.7'de belirtilen test ortamına doğru gerçekleştirilen saldırılara karşı alınan önleme sonuçlarını detaylandırmaktadır. Test ortamında yapılan analizler, Güvenlik Duvarı Antivirüs özelliğinin birçok tehdit kategorisinde etkili koruma sağladığını ancak tüm tehditler için tam koruma sunmadığını ortaya koymaktadır.

Eylem önleme sonuçlarına göre: Arka Kapı kategorisindeki saldırıların %3'ü, Hackleme Aracı kategorisindeki saldırıların %13'ü, Uç Nokta Saldırılarının %51'i, Uzak Kod Çalıştırma kategorisindeki saldırıların %50'si ve Zararlı Yazılım kategorisindeki saldırıların %2'si Güvenlik Duvarı Antivirüs tarafından engellenememiştir.

Buna karşın, diğer tehdit kategorilerinde (örneğin, bilgi hırsızlığı, botnet, casus yazılım ve fidye yazılımı gibi) %100'e yakın bir başarı oranı elde edilmiştir. Bu durum, Güvenlik Duvarı Antivirüs'ün genel koruma kapasitesinin oldukça yüksek olduğunu ancak belirli saldırı türlerinde hala iyileştirmeye ihtiyaç duyulduğunu göstermektedir.



Şekil 14. Güvenlik Duvarı Antivirüs aktifken eylem önleme sonucu

Şekil 17'ya göre, Güvenlik Duvarı Antivirüs koruması tüm saldırıların %69'unu engellemeyi başarmıştır. Bu, Güvenlik Duvarı Antivirüs'ün diğer güvenlik önlemlerine kıyasla daha geniş bir koruma alanı sağladığını ortaya koymaktadır. Ancak, kalan %31'lik saldırı oranı, Güvenlik Duvarı Antivirüs'ün tek başına tam bir güvenlik çözümü sağlayamayacağını göstermektedir.

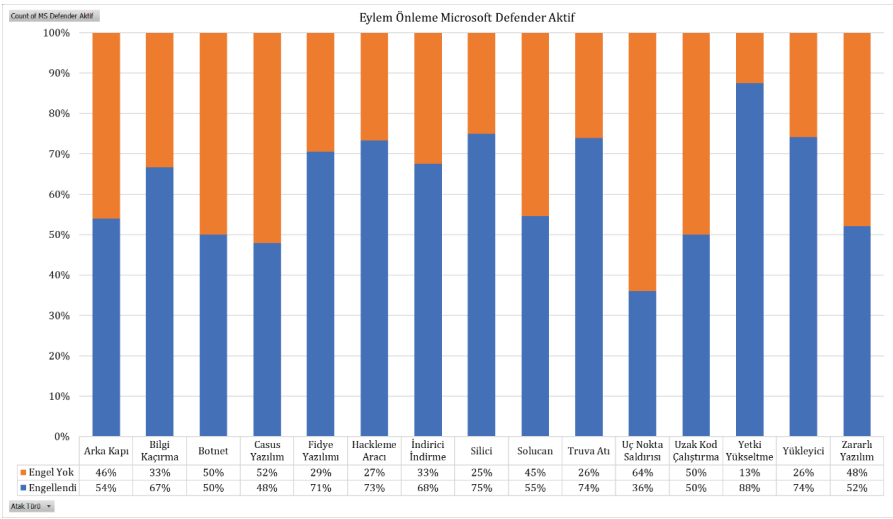
Sonuç olarak, Güvenlik Duvarı Antivirüs, ağ güvenliği stratejisinde güçlü bir bileşen olarak öne çıkmaktadır. Ancak, sistemin tam anlamıyla korunması için diğer güvenlik katmanlarıyla entegre bir şekilde çalışması gerekmektedir. Modern siber tehditlerin çeşitliliği ve karmaşıklığı göz önüne alındığında, Güvenlik Duvarı Antivirüs koruması çok katmanlı bir güvenlik yaklaşımının bir parçası olarak kullanılmalı ve diğer teknolojilerle desteklenmelidir. Bu entegre yaklaşım, cihazların daha güçlü ve kapsamlı bir koruma altında olmasını sağlayacaktır.

6.7. Microsoft Defender Aktifken

Microsoft Defender'ın aktif olduğu madde 4.8'de belirtilen test ortamına doğru gerçekleştirilen saldırılara karşı alınan önleme sonuçlarını detaylı bir şekilde sunmaktadır. Test ortamında yapılan analizler, Microsoft Defender'ın belirli tehdit kategorilerinde güçlü bir koruma sağladığını ancak tüm tehditlere karşı tek başına tam bir güvenlik sunamayacağını açıkça göstermektedir.

Eylem önleme sonuçlarına göre: Arka Kapı kategorisinde %54, Bilgi Kaçırma kategorisinde

%67, Botnet kategorisinde %50, Casus Yazılım kategorisinde %48, Fidye Yazılımı kategorisinde %29, Hackleme Aracı kategorisinde %73,İndirici İndirme kategorisinde %68, Silici kategorisinde %75, Solucan kategorisinde %55, Truva Atı kategorisinde %74, Uç Nokta Saldırıları kategorisinde %36, Uzak Kod Çalıştırma kategorisinde %50, Yetki Yükseltme kategorisinde %88, Yükleyici kategorisinde %74 ve Zararlı Yazılım kategorisinde %52 başarı oranı sağlanmıştır.



Şekil 15. Microsoft Defender aktifken eylem önleme sonucu

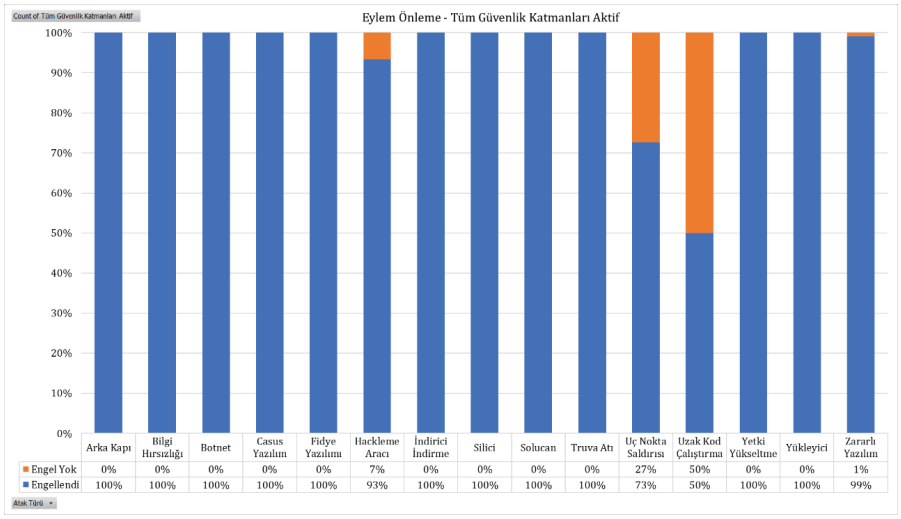
Bu sonuçlar, Microsoft Defender'ın birçok tehdit kategorisinde etkili bir savunma sağladığını, özellikle Yetki Yükseltme %88, Silici %75 ve Truva Atı %74 gibi kategorilerde yüksek engelleme oranlarına ulaştığını göstermektedir. Ancak, Fidye Yazılımı %29 ve Uç Nokta Saldırıları %36 gibi kategorilerde başarı oranlarının nispeten düşük olması, Microsoft Defender'ın tek başına tüm tehditlere karşı tam koruma sağlayamadığını ortaya koymaktadır.

Şekil 17'da görüldüğü üzere Microsoft Defender, tüm saldırıların yalnızca %46'sını engellemede başarılı olmuştur. Bu oran, Defender'ın güvenlik çözümünde önemli bir rol oynadığını ancak diğer güvenlik katmanlarıyla desteklenmediği sürece cihazların tam anlamıyla güvende kalamayacağını göstermektedir.

Microsoft Defender, modern tehditlere karşı güçlü bir savunma mekanizması sunan bir güvenlik aracı olarak öne çıkmaktadır. Ancak, "sıfır güven" yaklaşımı göz önüne alındığında, Defender'ın tek başına kullanılması cihazların güvenliği için yeterli değildir. Bu nedenle, çok katmanlı bir güvenlik stratejisinin bir parçası olarak değerlendirilmesi kritik öneme sahiptir. Microsoft Defender, Güvenlik Duvarı, IPS ve diğer güvenlik çözümleriyle entegre bir şekilde kullanıldığında daha etkili bir koruma sağlamakta ve tehditlerin büyük bir kısmını engelleyebilmektedir. Bu entegre yaklaşım, modern siber tehditlere karşı daha kapsamlı ve dayanıklı bir savunma sağlar.

6.8. Tüm Güvenlik Katmanları Aktifken

Şekil 16, madde 4.3, 4.4, 4.5, 4.6, 4.7 ve 4.8 belirtilen tüm güvenlik katmanlarının bir arada aktif olduğu madde 4.9'de belirtilen test ortamına doğru gerçekleştirilen saldırılara karşı alınan önleme sonuçlarını detaylandırmaktadır. Test ortamında yapılan analizler, çok katmanlı güvenlik mimarisinin, her bir güvenlik katmanının tek başına sağladığı korumadan çok daha yüksek bir başarı oranı elde ettiğini göstermektedir.



Şekil 16. Tüm güvenlik katmanları aktifken eylem önleme sonucu

Eylem önleme sonuçlarına göre, tüm güvenlik katmanları aktifken: Hackleme Aracı kategorisindeki saldırıların yalnızca %7'si, Uç Nokta Saldırıları kategorisindeki saldırıların

%27'si, Uzak Kod Çalıştırma kategorisindeki saldırıların %50'si engellenememiştir.

Buna karşın, diğer tüm tehdit kategorilerinde (örneğin, Arka Kapı, Bilgi Hırsızlığı, Botnet, Fidye Yazılımı ve Solucan gibi) %100'e yakın bir başarı oranı sağlamıştır. Bu sonuçlar, çok katmanlı güvenlik mimarisinin tehditleri önlemede etkili olduğunu ortaya koymaktadır.

Şekil 17'da görüldüğü üzere, tüm güvenlik katmanlarının bir arada kullanıldığı senaryoda, tüm saldırıların %83'ü engellenebilmiştir. Bu oran, tüm katmanların bir arada çalışmasının, tehditlerin büyük bir kısmını etkisiz hale getirdiğini göstermektedir. Ancak, belirli kategorilerde hala engellenemeyen saldırılar bulunması, çok katmanlı güvenlik stratejisinin sürekli izlenmesi, geliştirilmesi ve güncellenmesi gerektiğini vurgulamaktadır.

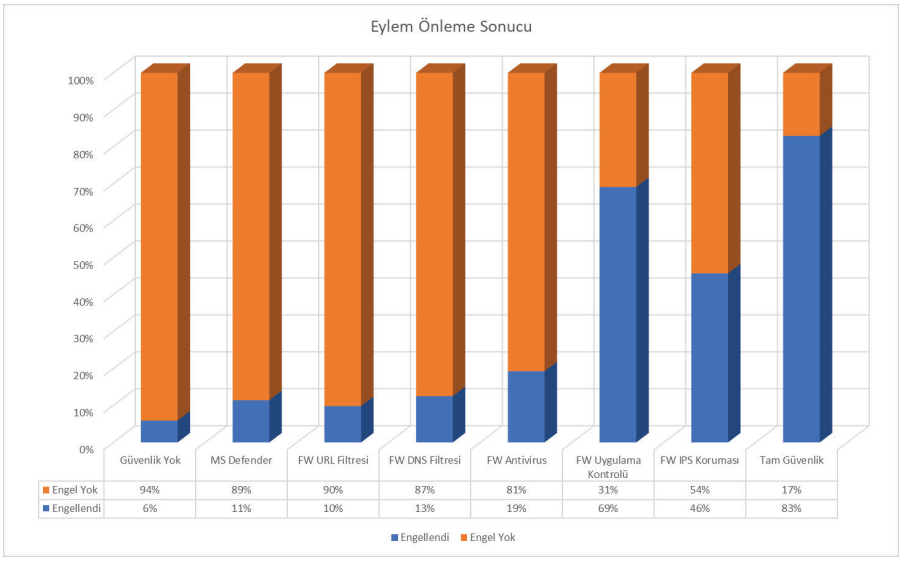
Tüm güvenlik katmanlarının aktif olduğu bir yapı, siber tehditlere karşı güçlü bir savunma mekanizması sağlamaktadır. Katmanlı

güvenlik mimarisi, farklı tehditlere karşı her güvenlik katmanının benzersiz yeteneklerini birleştirerek saldırı yüzeyini azaltır.

Sonuç olarak, tüm güvenlik katmanlarının birlikte kullanıldığı çok katmanlı mimari, modern siber tehditlere karşı kapsamlı ve etkili bir koruma sağlamakta, ancak kalan risklerin de göz önünde bulundurulması gerektiğini açıkça ortaya koymaktadır. Bu bağlamda, entegre güvenlik çözümlerinin proaktif önlemlerle desteklenmesi, cihazların ve ağların daha güvenli hale gelmesini sağlayacaktır.

6.9. Bulguların Karşılaştırılması

Her bir eylemi önlemeye dair sonuç çıktıları Şekil 17'de görüldüğü gibidir.



Şekil 17. Güvenlik Katmanları Eylem Önleme Sonucu Grafiği

Şekil 17'da güvenlik katmanlarının etkinleştirilmesi durumunda alınan sonuçları ve bu katmanların saldırılara karşı sağladığı koruma seviyelerini net bir şekilde ortaya koymaktadır. Grafik, güvenlik

katmanlarının ayrı ayrı kullanıldığında, her birinin belirli ölçüde koruma sağladığını ancak tek başına yeterli olmadığını göstermektedir. Örneğin, DNS filtresi, IPS koruması veya URL filtreleme gibi yöntemler belirli saldırı türlerini önleyebilse de, diğer katmanların eksik olduğu durumlarda sistemin büyük ölçüde savunmasız kaldığı görülmektedir.

Tüm güvenlik katmanlarının bir arada kullanıldığı senaryoda, saldırıların büyük bir çoğunluğunun etkisiz hale getirildiği (saldırıların %83'ü engellenmiş, %17 saldırı başarılı olmuştur) dikkat çekmektedir. Bu durum, katmanlı güvenlik stratejisinin önemini vurgulamaktadır. Her bir güvenlik katmanı, farklı tehdit türlerine karşı koruma sağlarken, birlikte kullanıldıklarında sistemin genel güvenlik seviyesi önemli ölçüde artmaktadır. Ancak, tüm katmanların bir arada kullanılmasına rağmen, hala küçük bir kısmın (saldırıların %17'si) başarılı olduğu göz önünde bulundurulduğunda, güvenlik stratejilerinin sürekli güncellenmesi ve tehditlerin dinamik yapısına uygun hale getirilmesi gerektiği sonucuna varılabilir.

Bu grafik, güvenlik açıklarının sadece tek bir yöntemle değil, farklı tekniklerin bir arada ve uyum içinde kullanılmasıyla minimize edilebileceğini göstermektedir. Ayrıca, herhangi bir güvenlik katmanındaki bir arıza ya da zayıflığın tüm sistemi tehdit edebileceği gerçeği, bütüncül bir güvenlik yaklaşımının önemini bir kez daha ortaya koymaktadır. Bu bağlamda, proaktif güvenlik yönetimi, düzenli izleme ve tehdit analizi gibi süreçlerin, ağ güvenliğini sürdürülebilir kılmak için kritik olduğu vurgulanmalıdır.

7. Sonuç

Yapılan simülasyonların analizlerinden çıkan sonuçlar, her güvenlik katmanının siber tehditleri önleme noktasında birbirinden bağımsız ancak tamamlayıcı bir şekilde fayda sağladığını açıkça ortaya koymaktadır. Bu bağlamda, özellikle KOBİ'ler için güvenlik altyapısının birden fazla katmandan oluşmasının kritik öneme sahip olduğu

anlaşılmaktadır. Katmanlardan herhangi birinde meydana gelebilecek bir aksaklık, atakların başarıya ulaşma olasılığını artırabileceğinden, güvenlik katmanlarının birlikte ve uyum içinde çalışması gerekliliği ön plana çıkmaktadır.

Özellikle, Microsoft Defender ve Güvenlik Duvarı katmanlarının birlikte kullanılması, madde 4.3, 4.4, 4.5, 4.6, 4.7 ve 4.8 belirtilen özelliklerin bir arada etkinleştirilmesi durumunda, KOBİ'lerin karşılaşabileceği tehditlere karşı daha güçlü bir savunma hattı oluşturulabileceği tespit edilmiştir. Bu yaklaşım, farklı güvenlik katmanlarının birbirlerini destekleyerek tehdit yüzeyini en aza indirdiğini göstermektedir.

Bununla birlikte, analizlerin bir diğer çarpıcı bulgusu, güvenlik ürünlerinin yalnızca varsayılan ayarlarla çalıştırılmasının etkili bir koruma sağlamada eksik kaldığıdır. Siber tehditlerin sürekli evrildiği bir ortamda, bu ürünlerin etkili olabilmesi için doğru şekilde yapılandırılması hayati bir öneme sahiptir. Varsayılan ayarlar genellikle genel kullanım senaryolarına göre tasarlandığı için, her işletmenin özel ihtiyaçlarına ve tehdit profiline göre optimize edilmemiş olabilir. Bu durum, güvenlik ekiplerinin ve IT yöneticilerinin konfigürasyon süreçlerine daha fazla önem vermesi gerektiğini ortaya koymaktadır.

Sonuç olarak, KOBİ'lerin kapsamlı bir güvenlik stratejisi oluştururken, çok katmanlı bir yaklaşımı benimsemeleri ve güvenlik ürünlerini doğru yapılandırmaları gerekmektedir. Bu iki temel ilke, modern tehditlere karşı etkili bir savunma sağlamanın anahtarları olarak öne çıkmaktadır.

7.1. Öneriler

Bunların yanında %100 güvenliğe ulaşmak ulaşılması neredeyse imkânsız bir hedeftir. Yukarıda uyguladığımız bu güvenlik katmanlarına temel olarak her KOBİ'nin sahip olması gerekmektedir. Bunun yanı sıra son kullanıcıların bilinçlendirilmesi, güvenlik ürünlerinin temel konfigürasyonlarının engelleyemediği %17'lik atakların hiç ortaya çıkmaması için kritik öneme sahiptir.

Giderek karmaşıklaşan siber tehditlerle karşı karşıya kalırken kısıtlı bütçeler, yetersiz insan kaynağı ve teknik altyapı eksiklikleri gibi faktörler, KOBİ'lerin güvenlik risklerini etkili bir şekilde yönetmesini engelleyebilir. Yapılan araştırmalarda, KOBİ'lerin siber güvenlik önlemlerini uygularken maliyet etkin ve pratik çözümler arayışında olduğu sonucuna ulaşılmıştır. Bu çalışma, optimum maliyetle Windows üzerinde bulunan ücretsiz koruma ve önüne konulacak bir Yeni Nesil Güvenlik Duvarı sayesinde güvenlik risklerini azaltmayı araştırmıştır ve KOBİ'ler için uygulanabilir strateji sunmuştur.

Sonuç olarak, bu en temel model KOBİ'lerin temel güvenlik ihtiyaçlarına uygun, düşük maliyetli ancak etkili bir çözümdür. Özellikle çalışan farkındalığı ve çok faktörlü kimlik doğrulama (MFA) gibi insan faktörüne dayalı önlemler KOBİ'lerin güvenlik stratejilerine ayrıca ekstra fayda sağlayacaktır.

Öneriler:

1. Katmanlı Güvenlik Modelinin Uygulanması: KOBİ'lerin, düşük maliyetli güvenlik önlemlerini aşamalı olarak devreye sokarak bütüncül bir güvenlik altyapısı kurması önerilmektedir. Bu kapsamda Microsoft Defender üzerinde bulunan XDR teknolojileri, hem uç nokta hem de ağ düzeyinde geniş kapsamlı koruma sağlayarak atak riskini azaltır.
2. Personel Eğitimi ve Farkındalık Programları: Çalışanların siber güvenlik konusunda düzenli olarak eğitilmesi, sosyal mühendislik atakları ve veri sızıntılarına karşı etkin bir önlem olacaktır. Özellikle KOBİ'lerde insan hatası büyük bir risk faktörü olduğundan, çalışanların bilinçlendirilmesi öncelikli olmalıdır.
3. Veri Şifreleme ve USB Portlarının Engellenmesi: Özellikle hassas verilerin bulunduğu yerel disklerin şifrelenmesi ve yetkisiz USB cihazlarının engellenmesi, veri sızıntılarına karşı güçlü bir savunma sağlar. Bu tür önlemler, maliyet etkin olmaları açısından KOBİ'ler için uygundur.
4. Yama ve Güncelleme Yönetimi: Sistemlerin güvenliğini artırmak için düzenli yama ve güncelleme politikalarının

uygulanması hayati öneme sahiptir. Otomatik güncelleme süreçlerinin kullanılması, güvenlik açıklarının en aza indirgenmesini sağlayacaktır.

Bu öneriler, KOBİ'lerin siber güvenlik altyapılarını güçlendirmek ve siber ataklara karşı dirençlerini artırmak için önemli bir rehber sunmaktadır. Siber güvenlik önlemlerinin aşamalı olarak uygulanması ve sürdürülebilir bir güvenlik politikası izlenmesi, KOBİ'lerin uzun vadeli başarısı için kritik önemdedir.

7.2. Gelecekte Yapılabilecek Çalışmalar

Bu çalışmanın sonuçları, KOBİ'lerin güvenlik altyapılarında çok katmanlı bir yaklaşımın önemini vurgulamış olsa da, gelecekte daha kapsamlı araştırmalara ihtiyaç duyulmaktadır. Özellikle aşağıdaki konuların araştırılması ve geliştirilmesi, güvenlik çözümlerinin etkinliğini artırmak açısından faydalı olacaktır:

Dinamik Tehdit Modelleme: Tehditlerin sürekli değişen doğası göz önüne alındığında, farklı katmanlardaki güvenlik çözümlerinin gerçek zamanlı tehditlere nasıl uyum sağladığını anlamak için dinamik modelleme yöntemleri geliştirilebilir. Bu, KOBİ'lerin karşılaşabileceği özel tehdit türlerini daha iyi tahmin etmeye olanak tanıyabilir [17].

Otomasyon ve Yapay Zeka Kullanımı: Güvenlik ürünlerinin konfigürasyon süreçlerinin daha etkin bir şekilde yapılabilmesi için yapay zeka tabanlı araçlar geliştirilebilir. Bu araçlar, KOBİ'lerin tehdit profillerini analiz ederek optimum güvenlik yapılandırmalarını otomatik olarak önerebilir [18].

Eğitim ve Farkındalık Programları: Güvenlik çözümlerinin teknik bileşenlerinin ötesinde, insan faktörünün etkisini değerlendiren çalışmalar yapılmalıdır. Özellikle KOBİ'lerde çalışanların siber güvenlik farkındalığını artırmak için etkili eğitim yöntemleri araştırılabilir [19].

Ekonomik ve Operasyonel Etki Analizleri: Çok katmanlı güvenlik stratejilerinin KOBİ'lere olan mali ve operasyonel etkileri üzerine detaylı analizler yapılabilir. Bu, KOBİ'lerin sınırlı bütçeleriyle en uygun güvenlik yatırımlarını belirlemesine yardımcı olabilir.

Yukarıda belirtilen gelecek çalışmaların gerçekleştirilmesi, modern tehditlere karşı daha etkin ve sürdürülebilir bir savunma mekanizmasının oluşturulmasına katkı sağlayacaktır.

Teşekkür

Bu araştırma için beni yönlendiren, karşılaştığım zorlukları bilgi ve tecrübesi ile aşmamda yardımcı olan değerli Hocam Dr. Mustafa Cem KASAPBAŞI'na teşekkürlerimi sunarım.

Bu çalışmanın tamamlanmasında desteğini ve yardımlarını gördüğüm Vildan KALKAVAN'a teşekkür ederim.

Referanslar

[1] <https://ekokobi.com/kobiler-icin-dijitallesmenin-maliyet-etki-analizi-ve-yatirim-stratejileri>, (Erişildi : 4.12.2024).

[2] <https://siberulak.com/kalkani-guclendirmek-kobiler-icin-siber-guvenlik-stratejileri>, (Erişildi : 17.12.2024).

[3] <https://kobitek.com/kobileri-siber-riskler-degil-bilgisizlik-tehlikeye-atiyor>, (Erişildi : 5.12.2024).

[4] <https://www.tripwire.com/state-of-security/business-impact-report-small-businesses-and-cyberattacks>, (Erişildi : 7.12.2024).

[5] Kara, Ş., Zengin, A. ve Hızal, S., "Ağ Sistemlerinin Güvenliği İçin Siber Saldırıların Ayrık Olaylı Sistem Tanımlama Tabanlı Modellenmesi ve Simülasyonu," Mühendislik Bilimleri ve Araştırmaları Dergisi, 5(2), (2023), sayfalar 186-202. Doi: 10.46387/bjesr.1268038

[6] Neupane, K., Haddad, R. ve Chen, L., Next Generation Firewall for Network Security: A Survey, 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), (s. 202-209), (2011, Nisan), Paris, IEEE.

[7] Hatipoğlu, C. ve Tunacan, T., Türkiye'de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması, BŞEÜ Fen Bilimleri Dergisi, 8(1), (2021), sayfalar 430-445. Doi: 10.35193/bseufbd.838732

[8] <https://learn.microsoft.com/en-us/powershell/module/defender/set-mppreference>, (Erişildi : 17.12.2024).

[9] Radivilova, T., Kirichenko, L. ve Ageyev, D., Gizli Tehditlerin Tespiti İçin SSL/TLS Trafiğinin Şifre Çözümü, 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), (s. 187-191), (2018, Mayıs), Kiev, IEEE.

[10] Banday, M. T. ve Shah, N. A., A Concise Study of Web Filtering, Sprouts: Working Papers on Information Systems, 10(31), (2010), sayfalar 1-11. Doi: http://sprouts.aisnet.org/10-31

[11] <https://blog.safedns.com/dns-filtering-dns-firewall-any-difference/>, (Erişildi : 6.12.2024).

[12] <https://www.diligent.com/resources/blog/application-controls>, (Erişildi : 6.12.2024).

[13] Abdelkarim, A. A. ve Nasereddin, H. H. O., Intrusion Prevention System, International Journal of Academic Research, 3(1), (2011), sayfalar 432-434.

[14] <https://www.paloaltonetworks.com/cyberpedia/firewall-vs-antivirus>, (Erişildi : 7.12.2024).

[15] Ishihara, Y., Develop of a Sample Classifier Through Multivariate Analysis for Coffee Bitterness Levels Using a Voltammetric Electronic Tongue, HCI International 2022 Posters, Communications in Computer and Information Science, 1583, (s. 3-10), (2022, Haziran), Gothenburg, İsveç. DOI: 10.1007/978-3-031-06394-7_3

[16] <https://github.com/buroxy/attackdata>, (Erişildi : 21.12.2024).

[17] <https://thecyberexpress.com/adaptive-cybersecurity-strategies>, (Erişildi : 20.12.2024).

[18] Kant, D. ve Johannsen, A., Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs), Electronic Imaging 2022, (s. 1-7), (2022, Ocak), Brandenburg, Society for Imaging Science and Technology.

[19] Bada, M. ve Nurse, J. R. C., Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs), Information and Computer Security, 27(3), (2019), sayfalar 393-410. Doi: https://doi.org/10.1108/ICS-07-2018-0080

Haliç Üniversitesi Fen Bilimleri Dergisi 2025, 8/1: 41-79
DOI: 10.46373/hafebid.1610167

ISSN: 2618-6241
e-ISSN: 2667-5757

Post-Kuantum Kriptografi Anahtar Değişim Mekanizması ile Kaotik Akış Şifreleme Algoritması

Vildan KALKAVAN[1]*, Mustafa Cem KASAPBAŞI[2]

[1]İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği, İstanbul, Türkiye
Orcid: 0009-0003-3247-6337, (https://orcid.org/0009-0003-3247-6337)
[2]İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği, İstanbul, Türkiye
Orcid: 0000-0001-6444-6659, (https://orcid.org/0000-0001-6444-6659)

Geliş Tarihi: 30.12.2024
Kabul Tarihi: 28.01.2025

***Sorumlu Yazar e mail:** kalkavanvildan@gmail.com

Atıf/Citation: Kalkavan, V., Kasapbaşı, M. C., "Post-Kuantum Kriptografi Anahtar Değişim Mekanizması ile Kaotik Akış Şifreleme Algoritması", Haliç Üniversitesi Fen Bilimleri Dergisi 2025, 8/1: 41-79.

Araştırma Makalesi/ ***Research Article***

Öz

Bu çalışmada, Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından gerçekleştirilen kuantum sonrası kriptografi standartlaştırılması için açılan gönderimlerde de yer alan ve 3. gönderim turuna da katılan CRYSTALS-Kyber algoritması incelenmiş ve bir uygulama ile post-kuantum kriptografi standartlarına uygunluğunu ve performansını değerlendirilmesi yapılmıştır. [1] Algoritma, Hatalar ile Öğrenme (Learning With Errors - LWE) problemine dayanan matematiksel temeliyle, kuantum bilgisayarların tehditlerine karşı dayanıklılık göstermektedir. Uyarlanabilir Seçimli Açık Metin Saldırısına Karşı Güvenlik (IND-CPA: Adaptive Chosen Plaintext Attack) ve Uyarlanabilir Seçimli Şifreli Metin Saldırısına Karşı Güvenlik (IND-CCA2: Adaptive Chosen Ciphertext Attack) güvenlik seviyelerini başarıyla sağlaması, algoritmanın hem doğruluk hem de güvenlik açısından güçlü bir performans sergilediğini ortaya koymaktadır. Bu çalışmada, algoritmanın performans analizi ve güvenlik değerlendirmesi sürecine kaotik harita uygulaması da entegre edilmiştir. Kaotik harita, başlangıç koşullarına duyarlı ve öngörülemez matematiksel yapısıyla güçlü bir rastgelelik sağlayarak algoritmanın şifreleme süreçlerinde kullanılabilecek bir entropi kaynağı olarak değerlendirilmiştir. Kaotik haritalardan türetilen anahtarlar, CRYSTALS-Kyber algoritmasının şifreleme ve şifre çözme süreçlerinde test edilmiştir. Kyber, farklı güvenlik gereksinimlerine hitap eden üç parametre dizisi (Kyber512, Kyber768, Kyber1024) sunmaktadır. Kyber512 düşük kaynak tüketimi gerektiren IoT cihazları gibi uygulamalarda hızlı ve hafif bir çözüm sunar. Kyber768 dengeli bir güvenlik ve performans seviyesine sahiptir. Kyber1024

yüksek güvenlik gereksinimlerini karşılayan en güçlü seçenek olarak dikkat çeker. Test sonuçları, algoritmanın doğruluğunu ve verimliliğini ortaya koymuştur. Yapılan testlerde, Simetrik Anahtar (ss1) ve Asimetrik Anahtar (ss2) değerleri her testte eşleşmiş ve algoritmanın %100 doğruluğa sahip olduğu gösterilmiştir. Ayrıca, Kyber'in şifreleme ve şifre çözme süreçleri, diğer kafes tabanlı algoritmalara kıyasla dengeli bir performans sergilemiştir. Kyber algoritması, NIST'in post- kuantum kriptografi standartlaştırma sürecinde önemli bir aday olarak öne çıkmıştır. Finansal sistemler, IoT güvenliği ve bulut bilişim gibi uygulama alanlarında geniş bir kullanım potansiyeline sahiptir. Bununla birlikte, algoritmanın büyük anahtar boyutları nedeniyle, depolama ve işlem gücü gereksinimleri açısından daha optimize edilmiş sürümlerinin geliştirilmesi önerilmektedir. Sonuç olarak, CRYSTALS-Kyber algoritması, doğruluk, performans ve kaotik harita gibi yenilikçi yaklaşımlar sayesinde post-kuantum güvenlik ihtiyaçlarını karşılamada güçlü bir adaydır. Ancak, algoritmanın daha geniş çaplı testler, kaotik haritaların daha derinlemesine entegrasyonu ve optimizasyonlarla iyileştirilmesi, gelecekteki siber güvenlik gereksinimlerini karşılama kapasitesini artırabilir.

Anahtar Kelimeler: Akış Şifreleme, NIST, Post-Kuantum Kriptografi, Siber Güvenlik

Chaotic Stream Cipher Algorithm with Post-Quantum Cryptography Key Exchange Mechanism

Abstract

This study evaluates the CRYSTALS-Kyber algorithm, which has been included in the submissions opened by NIST for post-quantum cryptography standardization and participated in the 3rd submission round, along with an application to assess its compliance with post-quantum cryptography standards and its performance. [1] Based on the mathematical foundation of the Learning With Errors (LWE) problem, the algorithm demonstrates resilience against the threats posed by quantum computers. Its ability to successfully achieve IND-CPA and IND- CCA2 security levels highlights the algorithm's strong performance in terms of both accuracy and security. In this study, chaotic map application has also been integrated into the performance analysis and security evaluation process of the algorithm. Chaotic maps, with their mathematical structure sensitive to initial conditions and unpredictability, have been considered as a strong entropy source that can be used in the encryption processes of the algorithm. Keys derived from chaotic maps were tested in the encryption and decryption processes of the CRYSTALS-Kyber algorithm. Kyber offers three parameter sets (Kyber512, Kyber768, Kyber1024) catering to different security requirements. Kyber512 provides a fast and lightweight solution for applications such as IoT devices

with low resource consumption. Kyber768 achieves a balanced level of security and performance. Kyber1024 stands out as the most robust option, addressing high-security requirements. Test results reveal the algorithm's accuracy and efficiency. In the tests conducted, Symmetric Key (ss1) and Decapsulated Symmetric Key (ss2) values matched in every test, proving the algorithm's 100% accuracy. Furthermore, Kyber's encryption and decryption processes demonstrated balanced performance compared to other lattice-based algorithms. The Kyber algorithm has emerged as a significant candidate in NIST's post-quantum cryptography standardization process. It holds broad potential for use in applications such as financial systems, IoT security, and cloud computing. However, due to the algorithm's large key sizes, it is recommended to develop more optimized versions in terms of storage and computational requirements. In conclusion, the CRYSTALS-Kyber algorithm is a strong candidate for addressing post-quantum security needs in terms of accuracy, performance, and innovative approaches such as chaotic maps. However, further extensive testing, deeper integration of chaotic maps, and optimizations are suggested to enhance its capacity to meet future cybersecurity demands.

Keywords: Stream Cipher, NIST, Post-Quantum Cryptography, Cybersecurity

1. Giriş

Günümüzde teknolojinin hızlı gelişmesiyle birlikte, kuantum bilgisayarları gelecekte mevcut kriptografik sistemlerin güvenliğini tehdit eder hale gelmiştir. Şifreleme yapmak için kullanılan yöntemlerin bazılarının kuantum bilgisayarlar tarafından çözülmesi kolay olacaktır [2]. Geleneksel kriptografi algoritmaları, özellikle RSA, Diffie-Hellman ve Eliptik Eğri Kriptografisi (ECC) gibi sistemler, kuantum bilgisayarların kullanabileceği Shor algoritması gibi matematiksel çözümler karşısında savunmasızdır [3]. Bu durumda, post-kuantum kriptografi adı verilen ve kuantum bilgisayarların saldırılarına karşı dayanıklı yeni algoritmaların geliştirilmesini günümüzde gelecek siber saldırıların artmasına karşılık zorunlu hale gelmiştir.

Post-kuantum güvenlik yaklaşımlarında, akış şifreleme (stream cipher) yöntemleri dikkat çekici bir çözüm alanı sunmaktadır. Akış şifreleme algoritmaları, sürekli veri akışını şifreleme kabiliyeti sayesinde, özellikle IoT cihazları, ağ iletişimi ve büyük veri transferlerinde yaygın olarak kullanılmaktadır. Ancak, Shor ve Grover algoritmaları

gibi kuantum algoritmalarının simetrik şifreleme sistemlerine getirdiği potansiyel riskler, post-kuantum bilgisayarların bu algoritmaları çözme kolaylığından dolayı bu sistemlerin anahtar boyutlarının artırılmasını ve güvenlik seviyelerinin gözden geçirilmesini gerektirmektedir [4].

Bu bağlamda, NIST tarafından yürütülen post-kuantum kriptografi standartlaştırma süreci büyük önem taşımaktadır. NIST, kuantum bilgisayarların yaratacağı tehditlere karşı güvenli yeni nesil algoritmaların seçilmesi ve test edilmesi amacıyla çeşitli deneyler ve değerlendirmeler yürütmektedir. Yürüttüğü çalışmalarda 82 algoritma önerisi sunmaktadır [2]. Bu süreçte, kafes tabanlı kriptografi ve simetrik şifreleme gibi alanlar öne çıkmakta, güvenlik performansları detaylı olarak incelenmektedir.

Bu çalışma, CRYSTALS-Kyber algoritmasının performansını ve güvenlik seviyelerini analiz ederek, kuantum sonrası dönemde uygulanabilirliğini değerlendirmeyi amaçlamaktadır. Algoritmanın farklı parametre setlerinde yapılan testlerle doğruluğu, güvenilirliği ve pratik uygulamalardaki potansiyeli ortaya konmuştur. Ayrıca, gelecekteki güvenlik standartlarının belirlenmesinde Kyber'in oynayabileceği rol detaylı bir şekilde incelenmiştir.

2. Literatür Özeti

Shor kuantum bilgisayarların klasik bilgisayarlara kıyasla bazı zorlu problemleri çok daha hızlı çözebileceğini gösterirken bu bağlamda, makale özellikle iki zor problem üzerine odaklanmaktadır.

Tam sayıların çarpanlarına ayrılması (Factoring)**:** RSA gibi şifreleme yöntemleri bu zorlu problem üzerine kurulmaktadır.

Ayrık Logaritmalar: Bir başka zorlu matematiksel problem olan "Ayrık Logaritmalar" problemi de birçok kriptografik sistemin temelini oluşturmaktadır.

Shor, kuantum bilgisayarların bu iki problemi polinomal zamanda çözebileceğini gösteren algoritmalar geliştirmiştir. Kuantum

bilgisayarların klasik bilgisayarlara kıyasla hesaplama yeteneklerindeki farklılıklara değinilirken, kuantum mekaniğinin "süperpozisyon" ve "kuantum dolanıklığı" gibi özellikleri sayesinde, kuantum bilgisayarlar paralel hesaplama gücüne sahip olabilmektedir. Bu durum, klasik bilgisayarlarla çözülmesi zor veya imkânsız olan bazı problemlerin kuantum bilgisayarlarda daha hızlı çözülmesine imkân tanır. Bu da kuantum bilgisayarların gücünü göstermektedir. Shor, kuantum bilgisayarlarda hem tam sayıların çarpanlarına ayrılmasına hem de ayrık algoritmalar problemlerine yönelik polinomal zamanlı algoritmalar geliştirmiştir.

Çarpanlara Ayırma**:** RSA algoritması gibi şifreleme yöntemleri, büyük sayıların çarpanlara ayrılmasının zor olması varsayımına dayanmaktadır. Shor, kuantum bilgisayarların bu sayıları çarpanlarına ayırmak için polinomal zamanda işlem yapabileceğini göstermektedir. Bu da RSA gibi yöntemleri kırılabilir hale getirmektedir.

Ayrık Logaritmalar**:** Shor'un algoritması ayrıca ayrık algoritmalar problemlerini de polinomal zamanda çözebilmektedir. Bu da, Eliptik Eğri Kriptografisi (ECC) gibi sistemlerin güvenliğini tehdit etmektedir.

Ayrıca ilgili makale karmaşıklık teorisine de odaklanmakta ve kuantum bilgisayarların klasik bilgisayarlara göre hız avantajı sunduğunu açıklamaktadır. Bu bağlamda, kuantum hesaplamanın klasik hesaplamadaki karmaşıklık sınıfları olan P, NP gibi sınıflarla ilişkisini tartışmakta ve kuantum karmaşıklık sınıflarının tanımını yapmaktadır.

BQP (Sınırlandırılmış Hata Kuantum Polinomal Zaman)**:** Kuantum bilgisayarların çözebileceği problem sınıfları arasında tanımlanan BQP, klasik bilgisayarlarda çözülemeyen problemleri kuantum bilgisayarların çözebileceğini göstermektedir.

Shor, kuantum bilgisayarların hala teorik bir aşamada olduğunu ve bu algoritmaların pratiğe dökülmesinin zorluklarını tartışmaktadır. Kuantum bilgisayarların inşası, hem fiziksel hem de teknik zorluklar nedeniyle o dönemde gerçekleştirilememiştir. Ancak Shor, bu makale ile kuantum bilgisayar araştırmalarına önemli bir katkı sağlayarak, gelecekte bu tür bilgisayarların yapılabileceği umudunu taşımaktadır.

Shor'un algoritmaları, kuantum bilgisayarların kriptografi üzerindeki potansiyel etkilerini göstermektedir. Bu algoritmaların pratiğe dökülmesi halinde, mevcut şifreleme yöntemlerinin kırılabilir hale geleceği, dolayısıyla post-kuantum kriptografi gibi yeni güvenlik sistemlerinin geliştirilmesi gerektiği vurgulanmaktadır [5].

Kuantum bilgisayarların geleneksel kriptografiye getirdiği tehditleri dikkate almaktadır. Kuantum bilgisayarlar, günümüzde kullanılan şifreleme algoritmalarını (RSA, ECC, DH, DSA vb.) kolayca kırabilir algoritmalar olarak görmektedir. Ancak, kuantum bilgisayarlara karşı dayanıklı post-kuantum kriptografi algoritmaları geliştirilmektedir.

Makale, post-kuantum kriptografi için önerilen şemaların güvenliği, etkinliği ve geçiş süreci ile ilgili birçok zorluğu tartışmaktadır. Post-kuantum kriptografi, geleneksel cihazlarla uyumlu olacak şekilde tasarlanmıştır ve çeşitli matematiksel problemlere dayanmaktadır. Bu makale, post-kuantum şifreleme algoritmalarının akademik ve endüstriyel uygulamalarına genel bir bakış sunmaktadır.

Temel zorluklar arasında hangi şemalara güvenileceği, güvenlik parametrelerinin nasıl belirleneceği ve mevcut sistemlerin nasıl uyumlu hale getirileceği gibi konular yer almaktadır. Makale ayrıca kuantum bilgisayarların etkilerine karşı önlem almak için endüstri, hükümet ve kamuoyunun bilgilendirilmesi gerektiğini vurgulamaktadır [6].

Lov K. Grover'un 1996 yılında yayımladığı makale, kuantum bilgisayarların klasik bilgisayarlara kıyasla belirli problemlerde nasıl avantaj sağladığını gösteren temel çalışmalardan biri olarak görülmektedir. Bu makalede Grover, bir veri tabanında arama işleminin kuantum algoritmalarıyla nasıl hızlandırılabileceğini ele alırken klasik arama algoritmalarına göre polinomal bir hızlanma sağladığını söylemektedir.

Grover'un Algoritması**:** Grover, veritabanındaki n öğe arasında bir öğeyi bulmak için klasik bilgisayarlarda gerekli olan O(n) adım yerine, kuantum bilgisayarlarla bu işlemin O(√n) adımda yapılabileceğini göstermektedir. Bu, veri tabanı aramalarındaki hızlanmanın ciddi bir ölçüde artacağı anlamına gelmektedir.

Kuantum Paralelizmi**:** Kuantum süperpozisyon ve dolanıklık gibi kuantum mekaniği prensipleri sayesinde, kuantum bilgisayar aynı anda birden fazla olasılığı değerlendirebilir ve bu da arama işlemlerini klasik bilgisayarlara kıyasla çok daha verimli hale getirmektedir.

Algoritmanın Önemi**:** Grover'un algoritması, simetrik şifreleme gibi alanlarda şifre kırma süresini de hızlandırabilir, ancak bu tehdit, daha uzun anahtar boyutlarıyla bertaraf edilebilmektedir. Aynı zamanda bu algoritma, kuantum bilgi işleminde birçok pratik uygulamanın temelini oluşturmaktadır.

Grover'un algoritması, veri tabanı araması gibi belirli problemlerde kuantum bilgisayarların klasik bilgisayarlara göre nasıl üstün performans gösterebileceğini etkileyici bir şekilde sergilemektedir [7].

Kuantum bilgisayarlar sayıları çarpanlarına ayırma ve ayrık logaritmaları hesaplama gibi görevler için etkin algoritmalar sunarak bu tür problemlerin klasik bilgisayarlara kıyasla kuantum bilgisayarlarda çok daha hızlı çözülebileceğini göstermektedir. Makale, kuantum Fourier dönüşümünün ve periyodik yapıların belirlenmesinde kuantum bilgisayarların gücüne dayanan algoritmaların kullanımını incelemektedir. Ayrıca, bu yaklaşımların "gizli altgrup problemi" olarak bilinen daha geniş bir gruplama teorisine dayanan problemi nasıl çözdüğünü tartışmaktadır.

Shor'un algoritmalarının, büyük tam sayıların çarpanlarına ayrılması ve ayrık logaritmaların kuantum bilgisayarlar ile polinomal zamanda çözülebileceğini gösterirken, Kuantum Fourier Dönüşümü (QFT) periyodik yapıların belirlenmesi ve ayrık Fourier dönüşümünün kuantum bilgisayarlarla nasıl hızlandırılabileceği üzerine odaklanmaktadır. Gizli Altgrup Probleminde, periyodik yapıları genel bir gruplama teorisi bağlamında incelerken hem klasik hem de kuantum algoritmalar için genel çözümler sunmaktadır. Kuantum bilgisayarların çarpanlara ayırma ve ayrık logaritma hesaplaması gibi problemlerde klasik bilgisayarlara üstünlük sağladığı belirtilmektedir [8].

Makale, Kuantum bilgisayarların klasik şifreleme algoritmalarını tehdit ettiği bir geleceğe hazırlanmak amacıyla post-kuantum

kriptografinin önemini ele almaktadır. Özetle, kuantum bilgisayarların mevcut şifreleme sistemlerini (özellikle RSA ve Eliptik Eğri Kriptografisi - ECC) kırabileceği öngörülmektedir. Bu yüzden bu tehdide karşı dirençli yeni algoritmaların geliştirilmesi gerektiği vurgulanmaktadır.

Shor ve Grover algoritmaları gibi kuantum algoritmalarının, RSA, DSA, ve ECC gibi asimetrik şifreleme yöntemlerini kırabileceği tehdidini belirtilirken özellikle Shor'un algoritması büyük sayıların çarpanlarına ayrılması gibi matematiksel problemlerde kuantum bilgisayarların üstün performans gösterdiğini vurgulamaktadır. Kuantum bilgisayarlara karşı güvenli olduğu düşünülen alternatif kriptografik teknikler tartışılırken, bu teknikler arasında kafes tabanlı, kod tabanlı, hash tabanlı, ve çok değişkenli polinom tabanlı şifreleme algoritmaları yer almaktadır. Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından başlatılan post-kuantum kriptografisi standartlaştırma sürecine değinirken, yeni algoritmaların güvenliği ve performansı test edilmekte ve gelecekte kullanılması planlanan standartlar geliştirilmektedir.

Post-kuantum algoritmaların internet güvenliği, veri transferi ve IoT cihazları gibi alanlarda nasıl uygulanabileceği üzerinde durulmaktadır. Bu çözümlerin hem yüksek güvenlik sağlaması hem de pratik olarak kullanılabilir olması gerektiği belirtilmektedir. Post-kuantum kriptografi, kuantum bilgisayarların klasik şifreleme yöntemlerine yönelik tehditleri bertaraf etmek için geliştirilen alternatif yöntemlere odaklanmaktadır. Bernstein ve ekibi, mevcut şifreleme tekniklerinin zamanla güvenli olmayabileceğini ve yeni kuantum sonrası güvenlik standartlarının belirlenmesi gerektiğini vurgulamaktadır [9].

Kuantum bilgisayarların asimetrik kriptografi sistemleri üzerindeki potansiyel tehditlerini ele alan makale, özellikle Shor'un algoritması kullanılarak RSA (Rivest–Shamir–Adleman) ve ECC (Eliptik Eğri Kriptografisi) gibi yaygın şifreleme algoritmalarının kuantum bilgisayarlar tarafından kırılabileceğini incelemektedir.

Shor'un Algoritması**:** Kuantum bilgisayarlar, Shor'un algoritmasını kullanarak büyük sayıların çarpanlarına ayrılmasını çok hızlı bir şekilde gerçekleştirebilmektedir. Bu, RSA gibi büyük asal sayı faktörizasyonu gerektiren algoritmaları savunmasız hale getirmektedir. Aynı zamanda, ECC'de kullanılan ayrık logaritmalar da kuantum bilgisayarların çözebileceği matematiksel problemler arasında yer almaktadır.

Asimetrik Şifrelemenin Tehlikeye Girmesi**:** RSA ve ECC gibi geleneksel asimetrik şifreleme sistemleri, klasik bilgisayarların zorlukla çözebildiği matematiksel problemler üzerine kurulmuştur. Ancak, kuantum bilgisayarların bu problemlere hızlı çözümler getirebilme kapasitesi, bu sistemlerin güvenliğini tehdit etmektedir. Özellikle finansal işlemler, güvenli iletişim ve dijital imzalar gibi alanlarda kullanılan bu algoritmalar, kuantum dönemiyle birlikte ciddi bir risk altında bulunmaktadır.

Post-Kuantum Kriptografi**:** Makale, bu tehditlere karşı geliştirilen post-kuantum algoritmalarına da değinmektedir. Kafes tabanlı, hash tabanlı ve diğer kuantum dirençli algoritmalar, mevcut sistemlerin yerine geçmesi planlanan yeni yaklaşımlardır. Bu algoritmalar, kuantum bilgisayarların saldırılarına karşı dayanıklı olacak şekilde tasarlanmaktadır. Makale, asimetrik kriptografi sistemlerinin geleceğini ele alırken, kuantum bilgisayarların gelişimine karşı alınması gereken önlemler ve post-kuantum kriptografisinin önemini vurgulamaktadır [10].

Simetrik anahtar şifreleme, hem şifreleme hem de deşifreleme işlemleri için tek bir ortak anahtarın kullanıldığı bir yöntemdir. Makalede, çeşitli simetrik şifreleme algoritmaları (AES, DES, 3DES, Blowfish, RC4 vb.) ele alınmakta ve bu algoritmaların avantajları, dezavantajları ve uygulama alanları karşılaştırmalı olarak sunulmaktadır. Simetrik şifreleme yöntemleri, günümüzdeki veri güvenliği ihtiyaçlarına cevap vermek üzere tasarlanmıştır. Özellikle ağ güvenliği, veri gizliliği ve yetkisiz erişimi engellemek amacıyla kullanılmaktadır. Bu algoritmalar, büyük veri transferlerinde, finansal işlemlerde ve kişisel bilgilerin korunmasında etkin rol oynamaktadır. Makalede

bahsedilen AES ve Blowfish gibi algoritmalar, hız ve güvenlik açısından yüksek performans göstererek geniş çaplı veri şifreleme gereksinimlerini karşılamaktadır. AES, devlet düzeyinde güvenlik sağlarken, Blowfish daha düşük kaynaklı cihazlarda hızlı bir şekilde uygulanabilmektedir. Uygulandığı alanlar:

RC4 gibi algoritmalar, özellikle ağ protokollerinde (örn. SSL/TLS) kullanılır. Bu algoritmalar, sürekli veri akışını güvenli hale getirerek hızlı ve güvenilir şifreleme sağlar.

Finans ve Bankacılık Sistemleri**:** AES ve 3DES, finansal sistemlerde sıkça kullanılır. Bu sistemlerde veri güvenliği kritik olduğundan, güçlü şifreleme algoritmalarına ihtiyaç vardır.

Kişisel Verilerin Korunması**:** Simetrik şifreleme algoritmaları, kişisel verilerin güvenliğinin sağlanmasında da büyük rol oynar. Şirket içi gizli bilgiler, kullanıcı verileri ve diğer hassas bilgiler bu algoritmalarla korunur.

Güvenlik karşılaştırmaları yapıldığında, AES, özellikle güçlü güvenlik gerektiren ortamlarda yaygın olarak kullanılmaktadır. Hem 128-bit hem de 256-bit anahtar boyutları ile çeşitli güvenlik seviyeleri sağlamaktadır. Blowfish**,** daha esnek anahtar boyutlarına sahip olması nedeniyle, hem küçük ölçekli cihazlarda hem de yüksek hızlı veri şifreleme uygulamalarında yaygın olarak tercih edilmektedir. DES ve 3DES**,** artık modern güvenlik gereksinimlerini karşılayamamakla birlikte, daha önce kullanılan algoritmalar arasında yer almaktadır. 3DES, DES algoritmasını üç defa uygulayarak güvenliği artırmaya çalışsa da, işlem gücü gereksinimleri açısından verimsizdir ve yerini AES gibi daha güvenli algoritmalara bırakmıştır [11].

Çalışma, Simetrik şifreleme yöntemlerinin mevcut durumunu ele alarak bu algoritmaların güvenlik özelliklerini, karşılaştıkları zorlukları ve kuantum bilgisayarların oluşturduğu tehditlere karşı gelecekte nasıl korunabileceklerini tartışmaktadır.

Makale, DES, Uluslararası Veri Şifreleme Algoritması (IDEA: International Data Encryption Algorithm), RC5 ve AES gibi yaygın kullanılan simetrik şifreleme algoritmalarını incelemektedir. DES, eski

bir algoritma olduğu için modern güvenlik ihtiyaçlarını karşılayamamaktadır. Uluslararası Veri Şifreleme Algoritması (IDEA: International Data Encryption Algorithm) algoritması diferansiyel ve lineer saldırılara dayanıklı olmasına rağmen çarpışma ve anahtar-zamanlama saldırılarına karşı savunmasızdır. RC5, esnek anahtar uzunlukları ve verimliliğiyle dikkat çekerken, AES ise modern güvenlik standartlarında en güçlü algoritmalardan biri olarak öne çıkmaktadır. AES, 128, 192 ve 256 bitlik anahtar boyutları ve sabit blok boyutları ile yüksek düzeyde güvenlik sağlar. AES'in bayt dönüşümü, satır kaydırma, sütun karıştırma ve anahtar ekleme gibi yapısal işlemleri, şifreleme sürecinin güçlü ve güvenilir olmasını sağlayarak geniş bir kullanım alanı oluşturmaktadır.

Makale ayrıca kuantum bilgisayarların simetrik şifreleme üzerindeki etkilerini incelemektedir. Kuantum bilgisayarların Grover algoritması sayesinde anahtar arama sürelerini karekök hızında azaltabileceği belirtilmektedir. Bu durum, simetrik algoritmalar için bir tehdit oluştursa da, anahtar boyutlarının artırılmasıyla bu tehdit minimize edilebilmektedir. Örneğin, AES-128 yerine AES-256 kullanımı, kuantum saldırılarına karşı daha dirençli bir çözüm sunmaktadır.

Kuantum bilgisayarların oluşturduğu bu tehditler karşısında post-kuantum kriptografi çözümleri önerilmektedir. Yeni nesil kuantum dirençli teknikler, simetrik şifreleme algoritmalarının güvenliğini güçlendirmekte önemli bir rol oynayacaktır. Makale, post- kuantum araştırmalarının, simetrik şifreleme yöntemlerinin gelecekteki güvenlik altyapılarını nasıl destekleyeceğine dair önemli bilgiler sunmaktadır.

Sonuç olarak, bu makale, simetrik şifreleme algoritmalarının mevcut güvenlik durumunu analiz ederek, kuantum bilgisayarların oluşturduğu tehditlere karşı alınması gereken önlemleri vurgulamaktadır. AES gibi güçlü algoritmaların önemi bir kez daha öne çıkarken, anahtar boyutlarının artırılması ve kuantum sonrası kriptografi çözümlerinin geliştirilmesi, güvenliğin sürdürülebilirliği açısından kritik bir adım olarak ele alınmaktadır. Bu çalışma, simetrik şifreleme alanında çalışan araştırmacılar ve uygulayıcılar için değerli bir referans kaynağıdır [12].

Kafes tabanlı kriptografinin hem teorik hem de uygulamalı yönlerini basit ve anlaşılır bir şekilde açıklamayı hedeflemektedir. Yazarlar, özellikle Chris Peikert'in 2013'te verdiği Bonn derslerinden esinlenerek bu konuyu detaylandırmıştır. Notlar, hem temel kavramları hem de bu kavramların kriptografik uygulamalardaki yerini kapsamaktadır.

Kafes, çok boyutlu uzaylarda düzenli noktalar kümesi olarak tanımlanmaktadır. Kafes tabanlı kriptografi, kuantum bilgisayarlar karşısında dirençli olduğu bilinen Shortest Vector Problem (SVP) ve Hatalar ile Öğrenme (Learning With Errors - LWE) gibi matematiksel problemlere dayanmaktadır. Bu problemler, hem teorik olarak sağlam bir güvenlik temeli sunar hem de kuantum algoritmalarının bu yapıları çözmekte yetersiz kalması nedeniyle post-kuantum dönemde büyük bir avantaj sağlamaktadır.

Halka Tabanlı Hatalar ile Öğrenme (Ring-LWE) ve Kriptografik Uygulamaları çalışmanın ikinci bölümünde, Lyubashevsky, Peikert ve Regev'in "A Toolkit for Ring-LWE" adlı makalesine dayanmaktadır. Halka Tabanlı Hatalar ile Öğrenme (Ring-LWE), kafes tabanlı algoritmaların verimliliğini artırmak için kullanılan önemli bir optimizasyondur. Bu bölümde, halka yapıları ve bu yapılar üzerinden geliştirilen algoritmalar detaylandırılmıştır. Özellikle NTRUEncrypt gibi şifreleme sistemleri ve Dilithium gibi dijital imza algoritmalarının temelinde Halka Tabanlı Hatalar ile Öğrenme (Ring-LWE)'nin kullanıldığı vurgulanmıştır.

Çoklu Doğrusal Haritalar ve Güvenlik Analizleri ders notlarının üçüncü kısmı, Hu ve Jia'nın GGH haritası ile ilgili kriptografik analizlerini ve çoklu doğrusal haritaların kullanımını incelemektedir. Çoklu doğrusal haritalar, homomorfik şifreleme ve diğer ileri düzey kriptografik uygulamalar için kritik bir bileşendir [13].

3. Stream Cipher (Akış Şifreleme Algoritması)

Akış şifreleme (stream cipher), veriyi bit veya byte düzeyinde, sürekli bir akış halinde şifreleyen simetrik şifreleme yöntemidir. Bu

yöntem, özellikle donanım uygulamalarında ve gerçek zamanlı veri iletiminde yaygın olarak kullanılmaktadır. Akış şifreleme algoritmaları, genellikle yüksek hız ve düşük gecikme avantajları sunmaktadır.

3.1 Akış Şifreleme Çalışma Prensibi

Akış şifreleme algoritmalarının temel çalışma prensibi, bir anahtar ve genellikle bir başlatma vektörü (IV) kullanarak bir anahtar akışı (keystream) üretmektir. Bu anahtar akışı, açık metinle (plaintext) bit düzeyinde XOR işlemine tabi tutularak şifreli metin (ciphertext) elde edilir. Deşifreleme işlemi ise aynı anahtar akışıyla şifreli metnin tekrar XOR işlemine tabi tutulmasıyla gerçekleştirilir. Akış şifreleme, veriyi bireysel bitler veya baytlar düzeyinde şifreleyen bir sistemdir. Şifreleme sırasında şu adımlar izlenir:

Anahtar Akışı Üretimi: Anahtar akışı üreteci, bir başlangıç anahtarı ve bir başlangıç vektörü (IV) kullanarak uzun bir anahtar dizisi (key stream) oluşturur. Bu diziler, rastgele bir akış gibi görünür, ancak tamamen deterministiktir [14].

XOR İşlemi: Anahtar akışı, şifrelenecek veriyle (plaintext) bit düzeyinde XOR işlemine tabi tutulur. XOR işlemi şu şekilde çalışır:

- Eğer bitler aynıysa (0 ve 0 veya 1 ve 1), sonuç 0 olur.
- Eğer bitler farklıysa (0 ve 1 veya 1 ve 0), sonuç 1 olur. [14]

Şifreli Veri: XOR işleminin çıktısı, şifrelenmiş veri (ciphertext) olarak elde edilir. Aynı anahtar akışı, ciphertext ile XOR yapıldığında orijinal veriyi (plaintext) geri verir.

Akış şifreleme algoritmaları, donanım uygulamalarında ve gerçek zamanlı veri iletiminde yaygın olarak kullanılmaktadır. Özellikle düşük donanım maliyeti ve yüksek hız gerektiren uygulamalarda tercih edilmektedir. Ancak, akış şifreleme algoritmalarının güvenliği, kullanılan anahtar akışının rastgeleliği ve gizliliği ile doğrudan ilişkilidir. Bu nedenle, anahtar yönetimi ve başlatma vektörlerinin doğru kullanımı kritik öneme sahiptir.

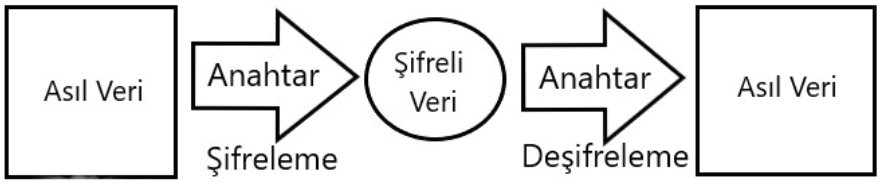
Akış şifreleme algoritmalarının güvenliği, üretilen anahtar akışının rastgeleliği ve tahmin edilemezliği ile doğrudan ilişkilidir. Eğer anahtar akışı yeterince rastgele değilse veya tekrar ediyorsa, saldırganlar şifreli metni çözebilmektedir. Bu nedenle, güvenli bir akış şifreleme sistemi için güçlü bir anahtar yönetimi ve uygun başlatma vektörü (IV) kullanımı gerektirmektedir. Akış şifreleme algoritmalarının avantajları arasında yüksek hız, düşük gecikme ve donanım uygulamalarına uygunluk bulunmaktadır. Ancak, anahtar ve IV yönetimi zorlukları, potansiyel güvenlik açıkları ve senkronizasyon gereksinimleri gibi dezavantajları da vardır [15].

Akış şifreleme algoritmaları, donanım maliyeti açısından düşük ve hız açısından yüksek uygulamalar tercih edildiği görülmektedir. Örnek olarak kablosuz iletişim, akıllı kartlarda ve gerçek zamanlı veri şifrelemelerde farklı uygulamalarda kullanılır. Simetrik şifreleme için Akış Şifreleme algoritmaları önemli bir yere sahip ve belirli uygulama alanlarında avantajları olduğu düşünülür. Ancak, güvenli bir kullanım için dikkatli bir anahtar yönetimi ve algoritma seçimi önemlidir.

3.1.1 Akış Şifreleme Türleri

3.1.1.1 Simetrik Şifreleme

Gönderilen bir metnin şifrelemek ve şifreyi çözmek için kullanılan tek anahtar olan bir şifreleme türüdür. Burada şifreyi çözmek için kullanılan bir anahtar varken sistem daha basit ve hızlıdır ancak buradaki dezavantaj iki tarafında anahtara doğru ve düzgün şekilde ulaşabilmesidir. Anahtara ulaşılsa bile tam metine ulaşılabilmesi kesin değildir [16]. Sezar, DES, 3DES, Blowfish gibi algoritmalar da örnek olarak verilebilir.

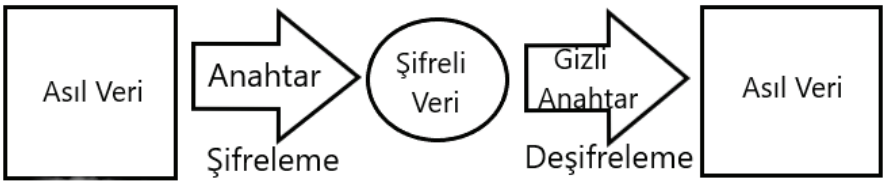


Şekil 1. Simetrik Şifreleme.

Simetrik Şifreleme avantajları olarak sadece anahtara sahip kişi şifreyi çözebileceği için metnin çözülmesi mümkün değildir. Veri kayıplarından etkilenmediği düşünülmektedir.

3.1.1.2 Asimetrik Şifreleme

Simetrik şifrelemede tek anahtar varken burada şifreleme için açık anahtar kullanılır. Deşifreleme işlemi için gizli ayrı bir anahtar kullanılmaktadır. Buradaki ayrıntı anahtarın simetrik olmamasıdır. Açık anahtar saldırgan eline geçse bile gizli anahtarı bilmediği için her hangi bir işe yaramamaktadır. RSA şifreleme algoritması da buna örnek olarak verilebilir. Şifrelemede açık anahtar alıcıya koruma yapılmadan iletildiğinde çözecek kişi açık anahtardan gizli anahtarı üreterek deşifreleme yapar. Açık anahtarın da tehlikeli kişilerin eline geçmesi bir şey ifade etmemektedir [17].



Şekil 2. Asimetrik Şifreleme.

3.1.2 Avantajları ve Dezavantajları

Akış şifreleme algoritmaları hız ve sürekli veri akışları daha iyi olduğu için ve düşük kaynak tüketimi açısından donanıma sahip IoT cihazları gibi uygulamalarda da kullanımı idealdir. Esneklik gerektiren gerçek zamanlı olması gereken uygulamalarda da güvenli mesajlaşma gibi uygunluğu avantajlarından biridir.

Şifreleme ve deşifrelemede aynı anahtar akışını senkronize bir şekilde kullanmayı gerektirmektedir. Aksi takdirde veriler erişilemez olur. Anahtarların güvenliği kritik öneme sahiptir ve güvenli olmayan anahtar yönetimi sistem için ciddi riskler oluşturabilmektedir. RC4 gibi eski algoritmalar, içerdiği zayıflıklar nedeniyle modern saldırılara karşı savunmasız hale gelmektedir. Bunlar da dezavantajları arasında değerlendirilebilmektedir.

3.1.3 Post-Kuantum Dönem ve Akış Şifreleme

Kuantum bilgisayarların gelişmesiyle birlikte akış şifreleme algoritmalarının güvenliği yeniden ele alındığında kuantum bilgisayarların Shor Algoritması ile asimetrik şifrelemeyi kırma yeteneği, Grover Algoritması ile simetrik şifrelemede anahtar arama sürelerini hızlandırma potansiyeli, akış şifreleme algoritmalarının da güvenlik seviyelerinin artırılmasını gerektirmiştir.

ChaCha20 gibi modern akış şifreleme algoritmalarının kuantum sonrası dönemde kullanılabilirliği araştırılmaktadır. Ayrıca, daha uzun anahtar boyutlarının kullanımı (örneğin, 256 bit ve üzeri) bu tür tehditlere karşı etkili bir savunma sunmaktadır.

AES-256, 256 bitlik anahtar uzunluğuyla yüksek güvenlik sağlamasıyla öne çıkar ve hassas verilerin korunmasında tercih edilen bir yöntemdir. Hem donanım hem de yazılım uygulamaları için hızlı ve etkili bir çözüm sunan bu algoritma, disk şifreleme ve güvenli iletişim gibi çeşitli alanlarda yaygın olarak kullanılmaktadır [18].

4. Kafes Tabanlı Algoritma

Kafes tabanlı algoritmalar, günümüzün klasik kriptografik sistemlerinin kuantum bilgisayarlar tarafından tehdit edilmesi durumuna karşı geliştirilen en etkili post-kuantum kriptografi yöntemlerinden biridir. Bu algoritmalar, matematiksel olarak çok boyutlu kafes adı verilen yapılara dayanmakta ve özellikle güçlü güvenlik özellikleriyle

dikkat çekmektedir. Klasik ve kuantum bilgisayarların çözmesi matematiksel olarak son derece zor olan belirli problemleri temel almaktadır. Bu nedenle, kuantum bilgisayarlar gibi güçlü teknolojilerin bile bu algoritmaları kırması pratikte mümkün değildir [2].

Tablo 1. Bilinen bazı kuantum işlemcileri.

İsim	Geliştirici	Kübit Sayısı	Geliştirme Yılı
IBM Osprey	IBM (Amerika Birleşik Devletleri)	433	2022 (Kasım)
Borealis	Xanadu (Kanada)	216	2022 (Haziran)
IBM Eagle	IBM (Amerika Birleşik Devletleri)	127	2021
Jiuzhang	Çin Bilim ve Teknoloji Üniversitesi (ÇHC)	76	2020
Sycamore	Google (Amerika Birleşik Devletleri)	53	2019
Tangle Lake	Intel (Amerika Birleşik Devletleri)	49	2018
Advantage	D-Wave (Kanada)	5640	2020

Kafes tabanlı algoritma çok boyutlu bir uzayda düzenli bir şekilde dağıtılmış noktalar kümesi olarak tanımlanmaktadır. Matematiksel olarak, kafes bir temel vektör kümesiyle oluşturulan tüm tamsayı kombinasyonlarıyla ifade edilmektedir [19]. Örneğin, iki boyutlu bir kafes, bir düzlemde düzenli bir şekilde yerleştirilmiş sonsuz sayıda nokta olarak düşünülebilir. Daha yüksek boyutlarda, bu yapı karmaşık matematiksel özelliklere sahip olur ve güvenlik açısından avantaj sağlamaktadır. Bu tanım, kafes kavramının matematiksel ve kriptografik bağlamdaki genel kabul görmüş tanımına dayanmaktadır. Kafes tanımı, lineer cebir ve matematiksel analizde kullanılan temel bir kavramdır.

Kafes, bir temel vektör kümesiyle (örneğin, $b_1, b_2, ..., b_n$) oluşturulan ve bu vektörlerin tüm tamsayı kombinasyonlarını içeren nokta kümesi olarak ifade edilir:

$$L = \{\sum_{i=1}^{n}(z_i b_i \mid \in \mathbb{Z})\}$$

Bu matematiksel model, kriptografi uygulamalarında kafes tabanlı problemler için temel oluşturmaktadır [19].

Kafes tabanlı algoritmalar, özellikle şu iki zor matematiksel probleme dayanır: Shortest Vector Problem (SVP): Bir kafesteki en kısa vektörün bulunması.

Closest Vector Problem (CVP): Rastgele bir noktaya en yakın kafes noktasının belirlenmesi [13].

Bu problemlerin, hem klasik hem de kuantum bilgisayarların çözmesi açısından hesaplama olarak oldukça zor olduğu kabul edilmektedir.

Kafes tabanlı algoritmalar, homomorfik şifreleme gibi yenilikçi uygulamalara olanak tanımaktadır. Bu teknik, verilerin şifreli haldeyken işlem görmesine imkan verir ve bulut bilişim gibi alanlarda büyük avantajlar sağlamaktadır. Ancak anahtar boyutu olarakta klasik sistemlere kıyasla daha büyük anahtar boyutlarına sahip olması depolama ve işlem gücü gereksinimlerini artırabilmektedir.

Güvenlik yönünden dikkat çeken kafes tabanlı problemler, hem klasik hem de kuantum bilgisayarlarla çözülmesi zor matematiksel yapılara dayanırken uygulama alanları da dijital imzalar, anahtar değişimi ve şifreleme gibi kritik kriptografik işlevlerde kullanılmaktadır. Bu tür algoritmalar, NIST'in post-kuantum kriptografi standartlaştırma sürecinde öne çıkan adaylar arasında yer almaktadır. Dayanıklılık açısından şifreleme algoritmasını belirlemek için yürütülen çalışmalarda CRYSTALS-KYBER ve CRYSTALS-Dilithium gibi algoritmaları standart olarak kabul etmişlerdir. Dijital imza, anahtar oluşturma gibi işlemler için tasarlanmışlardır [20].

"Klasik bilgisayarlardaki bitlerin aksine kuantum bilgisayarlardaki kübitler, sadece "0" ve "1" durumunda değil bu durumların bir süperpozisyonunda da bulunabilmektedir. Kübitler üzerinde yapılan

işlemler her iki durumu da aynı anda etkilemektedir. Kuantum bilgisayarları n tane kübit varsa, kuantum mekaniği ilkeleriyle uyumlu, 2^n farklı durumun süperpozisyonunda bulunabilmektedir. Dolayısıyla n tane kübite sahip bir kuantum bilgisayarı, tek bir seferde 2^n tane işlemi paralel olarak gerçekleştirebilmektedir. Kuantum bilgisayarların klasik bilgisayarlara kıyasla güçlü olmasını sağlayan bu özelliktir." [2]

5. Yöntem

Literatür taramasında, öncelikli olarak Shor, Grover algoritmalarının değerlendirmelerine ve akış şifreleme algoritmalarının güvenliği, kriptografi yöntemlerinin kuantum bilgisayarların tehditlerine karşı güvenliğe nasıl bir çözüm sunduğunu ve NIST'in post-kuantum kriptografi standartlaştırma sürecinde bu algoritmaların önemi ele alındı. Bu bölümde, çalışmamızın uygulama aşamasında izlenen yöntemsel çerçeve açıklanacaktır.

Bu çalışmada, NIST'in standartlaştırma sürecinde önerilen Kyber ve Dilithium gibi öne çıkan, yayımlanan kafes tabanlı algoritmalardan Kyber'in yayımlanan açık kaynak kodları çeşitli testler ve analizler gerçekleştirilmiştir. Temel amaç, bu algoritmanın performans, güvenlik ve uygulama uygunluğu açısından değerlendirilmesi ve kuantum sonrası dönemde kullanılabilirliğinin ortaya konmasıdır.

5.1 Test Ortamının Kurulması

Performans ve güvenlik analizleri için deney ortamı oluşturulacaktır. Bu ortamda:

Testler, belirli işlemci ve bellek kapasitelerine sahip bir sistemde gerçekleştirilecektir. Algoritmaların NIST tarafından sağlanan CRYSTALS-Kyber kodlarının farklı parametre setlerinde (Kyber512, Kyber768, Kyber1024) performansını ve doğruluğunu, algoritmanın şifreleme, şifre çözme ve ortak anahtar üretim süreçlerinin doğruluğunu

değerlendirmek için test vektörleri kullanarak doğruluğu ispatlanacaktır [21].

Test ortamında kullanılan araç ve teknolojiler:

- Dil ve Kütüphaneler:
  - o Programlama dili: JavaScript
  - o Kriptografik kütüphaneler: SHA3, SHAKE (Node.js için).
  - o Rastgele sayı üretimi: WebCrypto API.
- Sistem Özellikleri:
  - o Windows 10
  - o Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz 2.59 GHz
- Test Verileri:
  - o PQCkemKAT_1632.rsp, PQCkemKAT_2400.rsp gibi dosyalar (NIST tarafından sağlanan test vektörleri) [22].
- Araçlar:
  - o Node.js dosya okuma modülü (fs), algoritma uygulamaları ve doğrulama işlemleri.

5.2 Algoritma ve Akış

5.2.1 Crystals-Kyber Algoritması

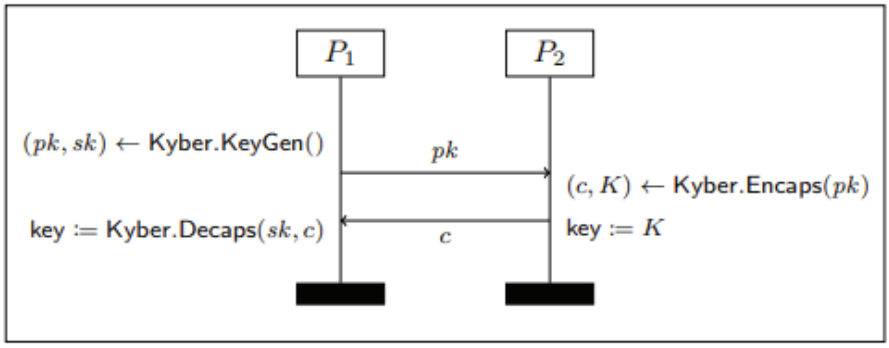
Kyber parametre setlerinde, her parametre dizisi belirli bir anahtar uzunluğu ve performans gereksinimine sahiptir. Kyber'in esnekliği ve güvenlik avantajlarıyla birlikte, Halka Tabanlı Hatalar ile Öğrenme (Ring-LWE) tabanlı şemalara benzer verimlilik sunduğunu göstermektedir. Bu özellikleriyle Kyber, post-kuantum kriptografi standartları arasında öne çıkmaktadır [21].

- **Kyber512:** Hafif güvenlik düzeyi.
- **Kyber768:** Orta güvenlik düzeyi.
- **Kyber1024:** Yüksek güvenlik düzeyi.

Anahtar Üretimi (KeyGen): Algoritmanın KeyGen işlevi ile şifreleme ve şifre çözme için kullanılan anahtar çifti üretilir.

- Kyber algoritmasıyla uyumlu bir genel anahtar (pk) ve özel anahtar (sk) oluşturur.

• Özel anahtar, genel anahtarın bir hash değeri (h(pk)) ve rastgele değerlerden (rnd) oluşan birleştirilmiş bir yapıya sahiptir.



Şekil 3. Kyber.KE – Kyber anahtar kapsülleme mekanizmasını (KeyGen, Encaps, Decaps) kullanan bir anahtar değişim protokolü [21].

Şifreleme (Encrypt): Rastgele bir mesaj alınır, bu mesaj şifreleme işlevi kullanılarak şifrelenir.

• Bir genel anahtar (pk) ile bir mesajı şifreler ve bu işlem sonucunda bir şifreli metin (c) ve simetrik bir anahtar (ss) oluşturur.
• SHA3 ve SHAKE gibi kriptografik hash algoritmaları kullanılarak güvenlik sağlanır.

Şifre Çözme (Decrypt): Şifrelenen mesaj, Decrypt işlevi ile çözülür ve paylaşılan anahtar (shared secret) doğrulanır.

• Bir şifreli metni (c) ve özel anahtarı (sk) kullanarak simetrik anahtarı (ss) geri elde eder.
• Şifreleme sırasında kullanılan adımlar tersine uygulanarak güvenli bir şekilde çözümleme yapılır.

IND-CPA ve IND-CCA2 dönüşümünde kod, IND-CPA güvenlik seviyesinde bir anahtar çifti oluşturur ve ardından "FO dönüşümü" kullanarak IND-CCA2 güvenliği sağlamaktadır. Matris ve polinom işlemlerinde A matrisi oluşturma, polinomu baytlara çevirme, Modüler Sayı Dönüşümü, sadeleştirme gibi işlemler polinomlar üzerinde matematiksel işlemleri gerçekleştirmektedir. Kriptografik hash

kullanımında SHA3-256, SHA3-512 ve SHAKE-256, çeşitli veri yapılarını hashleyerek güvenliği artırır [23].

5.2.2 Testlerin Detayları ve Çıktıları

Kyber'in vermiş olduğu test verilerinden yola çıkıp algoritma akışını inceleyelim.

5.2.2.1 Test Verilerinin Okunması

NIST tarafından sağlanan test dosyaları (PQCkemKAT_*) kullanılarak testler yapılmıştır. Örnek:

Plaintext

ct: Ciphertext

ss: Shared Secret sk: Private Key

5.2.2.2 Kod Örneği

Javascript

let fs = require('fs');

let textByLine = fs.readFileSync('./node_modules/crystals- kyber/PQCkemKAT_1632.rsp').toString().split("\n");

Her test vektörü, algoritmanın şifreleme ve deşifreleme işlevleriyle doğrulandı.

5.2.3 Test Sonuçları

5.2.3.1 Doğruluk Kontrolü

Şifreleme ile üretilen paylaşılan gizli şifreleme anahtarı (SS1) ve deşifreleme ile üretilen paylaşılan gizli deşifreleme anahtar (SS2) karşılaştırılmıştır. Doğruluk için SS1 ve SS2'nin eşit olması beklenmektedir.

Çıktı:
plaintext
Test run [0] success Test run [1] success
...
Test run [99] success

5.2.3.2 Başarısız Test Durumları

Eğer SS1 ve SS2 farklıysa, test çıktısı hata olarak işaretlenir. Örnek:
plaintext
Test run [10] failed

5.2.4 Performans ve Doğruluk Analizi

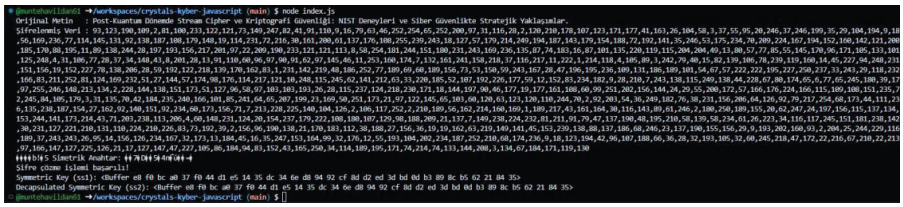
Testlerden elde edilen bulgular, doğruluk ve performans açısından analiz edilerek karşılaştırmalı bir şekilde incelenmiştir.

5.2.4.1 Doğruluk

Elde edilen datalarda Kyber512, Kyber768 ve Kyber1024 de ayrı ayrı yapılan testlerde SS1 ve SS2 değerlerinin hepsi için eşit olduğu görülmüştür. SS1 ve SS2'nin eşit olmaları algoritmanın doğruluğunu kanıtlamaktadır.

5.2.4.1.1 Kyber512 Testi

Symmetric Key (ss1): <Buffer e8 f0 bc a0 37 f0 44 d1 e5 14 35 dc 34 6e d8 94 92 cf 8d d2 ed 3d bd 0d b3 89 8c b5 62 21 84 35>
Decapsulated Symmetric Key (ss2): <Buffer e8 f0 bc a0 37 f0 44 d1 e5 14 35 dc 34 6e d8 94 92 cf 8d d2 ed 3d bd 0d b3 89 8c b5 62 21 84 35>

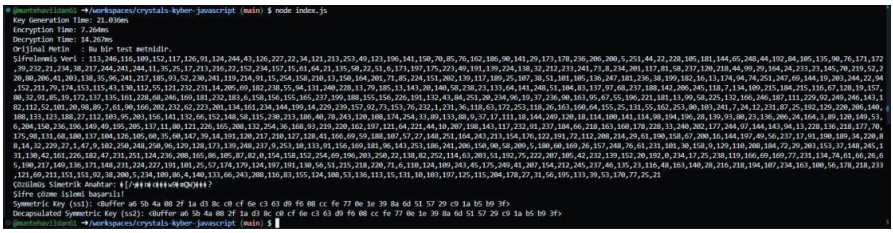


Şekil 4. Kyber512 Test Çıktısı.

Symmetric Key (ss1): <Buffer a6 5b 4a 08 2f 1a d3 8c c0 cf 6e c3 63 d9 f6 08 cc fe 77 0e 1e 39 8a 6d 51 57 29 c9 1a b5 b9 3f>

Decapsulated Symmetric Key (ss2): <Buffer a6 5b 4a 08 2f 1a d3 8c c0 cf 6e c3 63 d9 f6 08 cc fe 77 0e 1e 39 8a 6d 51 57 29 c9 1a b5 b9 3f>

Key Generation Time: 21.036ms Encryption Time: 7.264ms Decryption Time: 14.267ms



Şekil 5. Kyber512 Test Çıktısı.

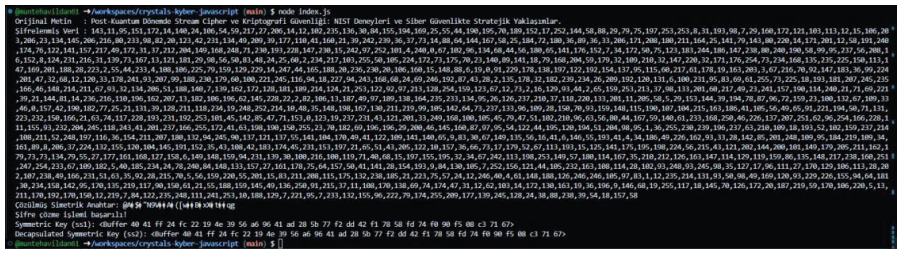
5.2.4.1.2 Kyber768 Testi

Symmetric Key (ss1): <Buffer 40 41 ff 24 fc 22 19 4e 39 56 a6 96 41 ad 28 5b 77 f2 dd 42 f1

78 58 fd 74 f0 90 f5 08 c3 71 67>

Decapsulated Symmetric Key (ss2): <Buffer 40 41 ff 24 fc 22 19 4e 39 56 a6 96 41 ad 28 5b

77 f2 dd 42 f1 78 58 fd 74 f0 90 f5 08 c3 71 67>

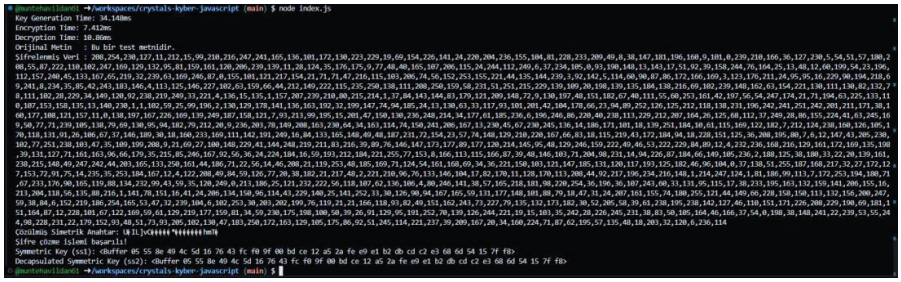


Şekil 6. Kyber768 Test Çıktısı.

Symmetric Key (ss1): <Buffer 05 55 8e 49 4c 5d 16 76 43 fc f0 9f 00 bd ce 12 a5 2a fe e9 e1 b2 db cd c2 e3 68 6d 54 15 7f f8>

Decapsulated Symmetric Key (ss2): <Buffer 05 55 8e 49 4c 5d 16 76 43 fc f0 9f 00 bd ce 12 a5 2a fe e9 e1 b2 db cd c2 e3 68 6d 54 15 7f f8>

Key Generation Time: 34.148ms Encryption Time: 7.412ms Decryption Time: 10.86ms



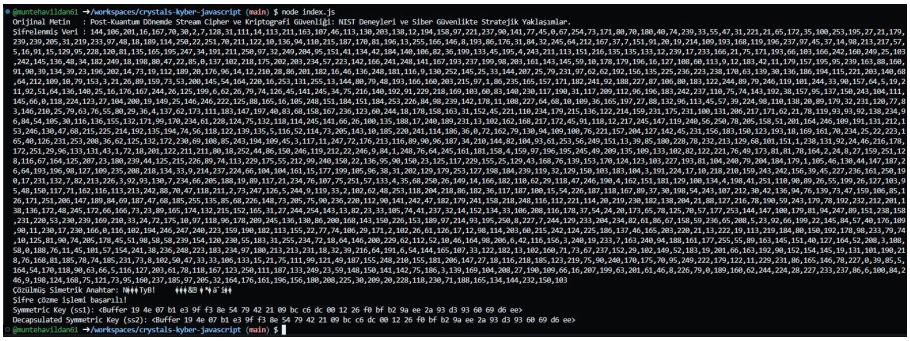
Şekil 7. Kyber768 Test Çıktısı.

5.2.4.1.3 Kyber1024 Testi

Symmetric Key (ss1): <Buffer 19 4e 07 b1 e3 9f f3 8e 54 79 42 21 09 bc c6 dc 00 12 26 f0 bf

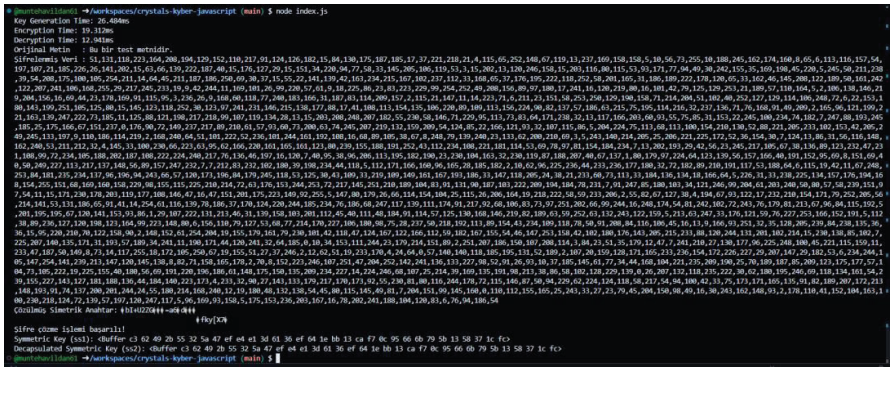
b2 9a ee 2a 93 d3 93 60 69 d6 ee>

Decapsulated Symmetric Key (ss2): <Buffer 19 4e 07 b1 e3 9f f3 8e 54 79 42 21 09 bc c6 dc
00 12 26 f0 bf b2 9a ee 2a 93 d3 93 60 69 d6 ee>



Şekil 8. Kyber1024 Test Çıktısı.

Symmetric Key (ss1): <Buffer c3 62 49 2b 55 32 5a 47 ef e4 e1 3d 61 36 ef 64 1e bb 13 ca f7
0c 95 66 6b 79 5b 13 58 37 1c fc>
Decapsulated Symmetric Key (ss2): <Buffer c3 62 49 2b 55 32 5a 47 ef e4 e1 3d 61 36 ef 64
1e bb 13 ca f7 0c 95 66 6b 79 5b 13 58 37 1c fc> Key Generation Time: 26.484ms
Encryption Time: 19.312ms Decryption Time: 12.941ms



Şekil 9. Kyber1024 Test Çıktısı.

5.2.4.2 Karşılaştırma

Anahtar boyu olarak farklılık gösterse de Kyber512, Kyber768 ve Kyber1024 için doğrulukları, anahtarların denk olduğu görülerek kanıtlanmıştır. Deney ortamında yapılan testler, CRYSTALS-Kyber algoritmasının doğruluğunu yüksek güvenle ortaya koymaktadır. Kyber, doğruluk ve performans açısından genelde en dengeli seçimdir. Bunun yanı sıra, testlerde elde edilen şifreleme süreleri (Encryption Time) ve şifre çözme süreleri (Decryption Time) parametre setleri arasında farklılık göstermiştir. Kyber512 ve Kyber768 için şifre çözme süreleri, şifreleme sürelerinden daha uzun bulunurken, Kyber1024 testinde durum tersine dönmüş ve şifreleme süresi daha fazla olmuştur. Bu farklılık, özellikle Kyber1024'teki daha büyük anahtar boyutunun şifreleme işlemlerinde ek matematiksel işlem yükü gerektirmesinden kaynaklanabilir. Kyber512 ve Kyber768, düşük kaynak tüketimi gerektiren uygulamalarda uygun bir çözüm sunarken, Kyber1024 yüksek güvenlik gerektiren senaryolarda daha uygun bir seçenek olarak öne çıkmaktadır. Bu bulgular, algoritmanın farklı güvenlik ve performans gereksinimlerini karşılayacak şekilde esneklik sunduğunu göstermektedir.

6. Araştırma Bulguları ve Tartışma

Bu bölümde, CRYSTALS-Kyber algoritması üzerinde yapılan testlerden elde edilen bulgular özetlenmekte ve tartışılmaktadır. Bulgular, algoritmanın doğruluğu, performansı ve post- kuantum güvenlik gereksinimlerini ne ölçüde karşılayabildiği üzerinde yoğunlaşmaktadır.

6.1 Doğruluk ve Güvenlik

CRYSTALS-Kyber algoritması, NIST tarafından sağlanan test vektörleriyle gerçekleştirilen doğrulama testlerinde %100 başarı göstermiştir. Test sonuçlarına göre Symmetric Key (ss1) ve Decapsulated Symmetric Key (ss2) değerleri, her bir parametre dizisi (Kyber512, Kyber768 ve Kyber1024) için birebir eşleşmiştir.

Bu sonuç, algoritmanın hem şifreleme hem de şifre çözme işlemlerini güvenilir bir şekilde gerçekleştirdiğini ve hatasız bir çalışma prensibine sahip olduğunu kanıtlamaktadır.

6.2 Performans Analizi

Şifreleme ve şifre çözme süreleri bakımından Kyber512, daha hafif bir güvenlik seviyesine sahip olduğu için en hızlı işlem süresini sunmuştur. Kyber768 ve Kyber1024 ise güvenlik seviyesine bağlı olarak daha fazla işlem gücü gerektirmiştir.

Anahtar boyutları bakımından Kyber512, 512-bit anahtar uzunluğuyla düşük kaynak tüketimi gerektiren uygulamalar için uygundur. Kyber1024 ise daha yüksek güvenlik gerektiren sistemlerde kullanılabilmektedir. Anahtar boyutları, depolama ve iletişim maliyetini arttırsa da güvenlik açısından kabul edilebilir düzeydedir.

6.3 Kyber Parametre Setleri Karşılaştırması

Tablo 2. Kyber parametre setlerinin karşılaştırması.

Parametre Dizisi	Güvenlik Seviyesi	Avantajlar	Dezavantajlar	Uygulama Alanı
Kyber512	Düşük güvenlik	Hafifliği ve hızlı işlem süresi, düşük güç tüketimi gereksinimlerini karşılar	Yüksek güvenlik gereksinimleri için uygun değildir	IoT cihazları, düşük güç tüketimi gerektiren uygulamalar
Kyber768	Orta düzey güvenlik	Güvenlik ve performans arasında iyi bir denge sağlar	Orta düzey güvenlik, kritik uygulamalar için yeterli olmayabilir	Genel güvenlik gereksinimleri, performans-fayda dengesi
Kyber1024	Yüksek güvenlik	En yüksek güvenlik seviyesi, kritik uygulamalar için ideal	Daha yüksek işlem süresi ve bellek kullanımı maliyeti	Finansal sistemler, kritik veri transferi uygulamaları

6.4 Kuantum Sonrası Güvenlik

CRYSTALS-Kyber algoritmasının kuantum sonrası güvenlik açısından etkinliği analiz edilmiştir. Algoritmanın matematiksel temeli, Hatalar ile Öğrenme (Learning With Errors - LWE) problemine dayanır ve bu problem hem klasik hem de kuantum bilgisayarlarla çözülmesi zor bir problem olarak kabul edilmektedir.

Kyber parametre setleri, kuantum bilgisayarların saldırılarına karşı dayanıklı olacak şekilde tasarlanmıştır. Özellikle, IND-CCA2 güvenlik seviyesi, algoritmanın kuantum sonrası güvenlik gereksinimlerini karşıladığını göstermektedir [24].

6.5 Crystals-Kyber ve Alternatif Algoritmalar

Kyber algoritmasının diğer post-kuantum kriptografi algoritmalarıyla karşılaştırıldığında, aşağıdaki avantajlara sahip olduğu gözlemlenmiştir: Kyber, performans açısından dengeli bir çözüm sunar. Özellikle Kyber512, hafif ve hızlı uygulamalar için ideal bir seçenektir. Kyber768 ve Kyber1024, yüksek güvenlik gereksinimlerini karşılarken performans-fayda dengesini korumaktadır. Farklı parametre setleri, çeşitli uygulama senaryolarına uyarlanabilmektedir.

6.6 Dezavantajlar ve İyileştirme Önerileri

Kafes tabanlı algoritmaların anahtar boyutları, klasik kriptografik sistemlere göre daha büyüktür. Bu durum, özellikle sınırlı depolama ve bant genişliği gerektiren uygulamalar için zorluk oluşturabilmektedir.

Daha yüksek güvenlik seviyelerine sahip parametre setleri (ör. Kyber1024), işlem süresi açısından daha fazla maliyet getirmektedir. Bu nedenle, belirli senaryolar için daha optimize edilmiş sürümler geliştirilmelidir.

6.7 Tartışma

CRYSTALS-Kyber algoritması, doğruluk ve güvenlik açısından yüksek bir performans sergilemiştir. Algoritmanın farklı parametre setlerinin, farklı güvenlik ve performans gereksinimlerine uygun olduğu görülmüştür. Özellikle, Kyber512'nin düşük işlem gücü gerektiren IoT cihazları gibi uygulamalarda uygun olduğu, Kyber1024'ün ise daha kritik güvenlik gereksinimlerini karşıladığı anlaşılmıştır.

Sonuç olarak, CRYSTALS-Kyber algoritmasının post-kuantum güvenlik ihtiyaçlarını karşılamada güçlü bir aday olduğu ve NIST'in standartlaştırma sürecinde haklı bir şekilde öne çıktığı kanıtlanmıştır. Ancak, daha geniş çaplı testler ve optimizasyon çalışmaları, algoritmanın uygulama alanlarını daha da genişletebilir ve performansını artırabilmektedir. Bu, özellikle kuantum sonrası dönemin güvenlik gereksinimlerine yanıt vermek açısından önemli bir adım olacaktır.

7. Kaotik Sistem: Lojistik Harita Akış Şifreleme

Kaotik harita (chaotic map), matematikte ve fiziksel sistemlerde kaos teorisi kapsamında incelenen bir kavramdır. Genellikle, başlangıç koşullarına çok duyarlı olan dinamik sistemleri tanımlamak için kullanılmaktadır. Kaotik haritalar, belirli bir başlangıç durumundan hareketle zamanla karmaşık ve öngörülemez davranışlar sergileyen sistemlerin matematiksel modelleridir. Kaos, sistemlerin uzun vadeli davranışlarının, başlangıç koşullarındaki çok küçük değişikliklere son derece hassas olduğu bir durumdur. Bu tür sistemler, belirli kurallara göre işler, ancak sonuçları öngörmek genellikle zordur. Kaotik haritalar bu tür sistemleri matematiksel olarak modellemek için kullanılır ve genellikle belirli kurallar ve denklem formülleri ile tanımlanmaktadır. Bu haritalar, deterministik olmasına rağmen, yani her bir girdiye karşılık bir çıkış olmasına rağmen, sonuçları kaotik ve öngörülemez olabilmektedir [25].

Deterministik Doğa: Kaotik sistemler tamamen deterministiktir; yani başlangıç koşulları sabit tutulursa sonuçlar tekrar edilebilmektedir.

Başlangıç Koşullarına Hassasiyet: Başlangıç değerlerindeki küçük bir değişiklik, tamamen farklı sonuçlara yol açabilmektedir (kelebek etkisi).

Periodiklik ve Karmaşıklık: Bazı kaotik haritalar belirli periyotlarda tekrar eden davranışlar gösterebilirken, bazıları tamamen karmaşık ve tekrar etmeyen yapıya sahiptir.

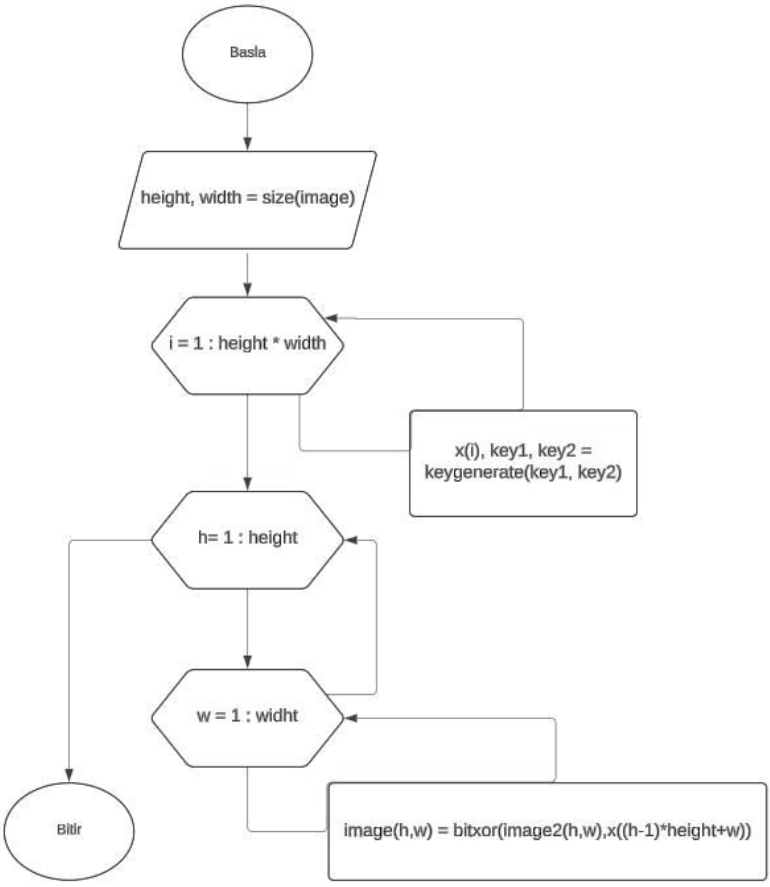
Bölünmüş Alan: Kaotik sistemlerde hareket, belirli bir faz uzayı içinde karmaşık yollar oluşturur ve zamanla tüm olası durumları kapsar.

7.1 Lojistik Harita (Logistic Map)

En yaygın kaotik haritalardan biridir. Bir popülasyon büyümesini modellemek için kullanılmaktadır. Denklem :

$$x_1 = x_0 * \lambda (1 - x_0) \quad (1)$$

Burada λ büyüme oranını temsil eder. x_0, bir sonraki adımın değerini belirlemek için kullanılan mevcut durumdur. λ belirli bir eşik değeri aştığında sistem kaotik davranış gösterir [26].



Şekil 10. Kaotik Şifre Oluşturma Akış Diyagramı [27].

Kaotik haritalar, şifreleme algoritmalarında rastgelelik ve karmaşıklık sağlamak için sıklıkla kullanılır:

Anahtar Üretimi: Kaotik haritalar, öngörülemeyen rastgele anahtarlar üretmek için kullanılır. Veri Şifreleme: Kaotik haritalar, veri bitlerini karıştırmak ve şifrelemek için uygulanabilir.

Görüntü Şifreleme: Görüntülerin piksellerini karıştırmak için kaotik sistemler kullanılabilir [28].

7.2 Anahtarda Lojistik Harita Uygulaması

CRYSTALS-Kyber algoritmasının testlerinden elde edilen Şekil 4 'te yer alan ss1 ve ss2 anahtarını baz alarak şifreleme uygulanacaktır.

Symmetric Key (ss1): <Buffer e8 f0 bc a0 37 f0 44 d1 e5 14 35 dc 34 6e d8 94 92 cf 8d d2 ed 3d bd 0d b3 89 8c b5 62 21 84 35> de bulunan rakamları bir araya getirerek ilk 15 tanesi ile kaotik hesaplamadaki x0 değeri elde edilip, sonraki 15 tane rakam ile de λ değeri elde edilecektir.

$$x0 = 0{,}800370441514353 \quad (2)$$

$$\lambda = 3{,}998949282303898 \quad (3)$$

Şimdi (2) ve (3) değerleri (1) numaralı formülüne uyarlanması:

$$x_1 = 0{,}800370441514353 * 3{,}998949282303898\ (1 - 0{,}800370441514353)$$

$$x_1 = 0.6385665061208377 \quad (4)$$

(4) değeri elde edilir. Bu elde edilen x değerlerini kullanarak anahtar oluşturulur.

$$Key_0 = (x_0 * 10\ \hat{}15) mod 256 \quad (5)$$

(5) denkleminde bulunan bütün x değerleri işleme alınır.

$$Key_0 = (0{,}800370441514353 * 10\hat{}15) mod 256$$

$$Key_0 = (800370441514353) mod 256$$

$$Key_0 = 113 \quad (6)$$

(6) de Key_0 değeri elde edilir. Sonrasında metin belirlenir ve işleme alınıp şifreli metin elde edilir.

"ISTANBUL TICARET UNIVERSITESI" metninin bütün harflerinin binary değerleri bulunur. Elde edilen bütün Key değerlerine binary değerleri ile XOR işlemi uygulanır.

"I" harfinin binary değeri = 01001001 (7)

113'in binary değeri = 01110001 (8)

(7) ve (8) binary değerleri XOR'lanır.

01110001 ⊕ 01001001 = 00111000 değeri elde edilir.

00111000_2 = 56 = 8 (9)

Artık (9) işleminin sonucunda "I" harfinin binary değerine karşılık gelen değer bulundu.

Şifreleme işlemi tamamlanmış oldu. Aynı şekilde bütün işlemler Key değerlerinin hepsine sırasıyla metnin bütün harflerine uyarlanıp şifreleme işlemi gerçekleştirilir.

Şifrelenmiş metin : "8FÿZªMÇ ¼¥á d¿öÖfBÛê r²ÄYnÎƒÿ" şeklinde elde edilir.

Şifreleme işleminden sonra metnin doğru çıktığını teyit etmek için deşifreleme işlemi yapılır. İlk etapta elde edilen şifrelenmiş metnin ilk harfinin ASCII değeri alınır.

"8" ASCII değeri = 56 (10)

(2) ve (3)' de bulunan değerler işleme alınıp Key0 değeri bulunur.

$$Key_0 = (0{,}800370441514353 * 10\text{^}15) mod 256 \quad (11)$$

$$Key_0 = 113 \quad (12)$$

(12) sonucu elde edilir.

(10) ve (12)'de elde edilen değerlerin binary karşılıkları bulunur.

56 = 00111000 ve 113 = 01110001 değerlerine XOR işlemi uygulanır.

00111000 ⊕ 01110001 = 01001001 (13) sonucuna ulaşılmış olunur.

01001001 binarynin ASCII karşılığı 73 çıkar ve 73 ASCII'nin karşılığı da "I" harfine yani metnin ilk harfine denktir. Böylelikle deşifreleme işleminin doğru bir şekilde çalıştığı görülmüştür. Sırasıyla bütün işlemler uygulandığında "ISTANBUL TICARET UNIVERSITESI" metnine ulaşılmış olunur.

8. Sonuç ve Öneriler

Bu çalışmada, NIST'in post-kuantum kriptografi standartlaştırma sürecinde öne çıkan bir kafes tabanlı algoritma olarak ele alınmış ve kapsamlı bir şekilde incelenmiştir. Yapılan testler ve analizler sonucunda, Kyber algoritmasının güvenlik ve doğruluk açısından yüksek performans sergilediği görülmüştür. Simetrik anahtar doğruluğu testlerinde %100 eşleşme sağlanarak algoritmanın güvenilirliği kanıtlanmıştır.

Algoritmanın matematiksel temeli olan Hatalar ile Öğrenme (Learning With Errors - LWE) problemi, kuantum bilgisayarların çözmesi zor bir yapı olarak öne çıkmaktadır. Algoritmanın IND-CPA ve IND-CCA2 güvenlik seviyelerini başarıyla sağlaması, post-kuantum güvenlik standartlarına uygunluğunu kanıtlamaktadır.

Performans açısından değerlendirmek istersek Kyber parametre setlerinin (Kyber512, Kyber768, Kyber1024) farklı güvenlik ve performans gereksinimlerine uyum sağladığı görülmüştür. Kyber512**,** düşük kaynak tüketimi gerektiren uygulamalarda uygun bir seçenek sunarken, Kyber1024 en yüksek güvenlik seviyesini gerektiren senaryolarda güvenilir bir çözüm sunmaktadır. Şifreleme ve deşifreleme süreleri açısından Kyber algoritmasının, diğer kafes tabanlı algoritmalara kıyasla dengeli bir performans gösterdiği anlaşılmıştır.

Kyber algoritması, post-kuantum güvenlikte önemli bir rol oynamakta olup, kuantum sonrası dönemde güvenlik ihtiyaçlarını karşılayacak potansiyele sahiptir. NIST'in standartlaştırma sürecindeki diğer algoritmalarla birlikte, dijital imza, anahtar değişimi ve veri şifreleme gibi kritik uygulamalarda geniş bir kullanım alanı bulabileceği öngörülmektedir.

Kyber algoritmasının anahtar boyutları, klasik sistemlere göre oldukça büyük olduğundan, özellikle düşük depolama kapasitesine sahip cihazlar için daha optimize sürümler geliştirilmelidir. Hafif versiyonların oluşturulması, IoT cihazları gibi düşük işlem gücüne sahip sistemlerde kullanım potansiyelini artıracaktır.

Kyber algoritmasının, finansal sistemler, bulut bilişim ve IoT güvenliği gibi farklı alanlardaki uygulanabilirliği daha geniş çaplı testlerle değerlendirilmelidir. Özellikle veri transfer hızının kritik olduğu uygulamalarda, Kyber algoritmasının performansı artırılabilir.

Algoritmanın farklı güvenlik senaryolarında (ör. saldırı simülasyonları) uzun vadeli testlerle değerlendirilmesi gerekmektedir. Kuantum bilgisayarların daha ileri seviyelere ulaşması durumunda algoritmanın güvenlik seviyesini koruyup koruyamayacağına dair simülasyonlar yapılmalıdır.

Standartların uygulanması NIST tarafından belirlenen post-kuantum güvenlik standartlarının farklı sektörlerde uygulanabilirliğini artırmak için eğitim ve farkındalık çalışmaları yapılmalıdır. Özellikle kritik altyapıların ve kamu kuruluşlarının, post-kuantum güvenlik standartlarına uyum sağlaması için teşvik edilmesi gerekmektedir.

Gelecekteki yapılacak çalışmalarda da Kyber algoritması üzerinde yapılacak yeni çalışmalar, hem matematiksel yapısının daha verimli hale getirilmesine hem de performans-fayda dengesinin daha iyi optimize edilmesine odaklanmalıdır. Diğer kafes tabanlı algoritmalarla yapılan karşılaştırmalı çalışmalar, post-kuantum güvenlik ekosistemini zenginleştirebilir.

Kyber algoritmasının test sonuçları, bu algoritmanın post-kuantum dönemin güvenlik ihtiyaçlarını karşılamada güçlü bir aday olduğunu göstermektedir. Gerek performans gerekse güvenlik açısından elde edilen bulgular, bu algoritmanın gelecekteki standartlar ve uygulamalar için kritik bir bileşen olabileceğini işaret etmektedir. Ancak, algoritmanın belirli alanlarda optimize edilmesi ve geniş çaplı uygulamalarda test edilmesi, potansiyelini tam anlamıyla ortaya koymak açısından önemlidir.

Bu çalışmada yapılan kaotik map uygulaması, CRYSTALS-Kyber algoritmasının performansını ve güvenlik seviyesini artırmada önemli bir role sahiptir. Kaotik map'lerden türetilen anahtarlar, algoritmanın şifreleme ve şifre çözme süreçlerinde başarıyla uygulanmış ve kaotik map'lerden türetilen anahtarlar, algoritmanın rastgelelik ve karmaşıklık gereksinimlerini karşılamış, şifreleme sürecinde güçlü bir güvenlik sağlamıştır. Logistic map formülüne dayalı anahtar üretim yöntemi, algoritmanın farklı güvenlik seviyelerinde test edilmesine olanak tanımış ve hem Symmetric Key (ss1**)** hem de Decapsulated Symmetric Key (ss2) değerleriyle başarılı bir şekilde entegre edilmiştir. Test sonuçlarında, kaotik harita uygulaması sayesinde elde edilen anahtarların, CRYSTALS-Kyber algoritmasının doğruluk ve performansında başarılı sonuçlar alındığı görülmüştür.

Bu bağlamda, kaotik map'in güvenlik ve performans üzerindeki etkisi, algoritmanın gelecekteki uygulama potansiyelini artıran önemli bir yenilik olarak değerlendirilebilir.

Teşekkür

Bu araştırma için beni yönlendiren, karşılaştığım zorlukları bilgi ve tecrübesi ile aşmamda yardımcı olan değerli Hocam Doç. Dr. Mustafa Cem KASAPBAŞI'na teşekkürlerimi sunarım.

Bu çalışmanın tamamlanmasında desteğini ve yardımlarını gördüğüm Burak SARAL'a teşekkür ederim.

Referanslar

[1] Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G. ve Stehlé, D., CRYSTALS-Kyber Algorithm Specifications And Supporting Documentation, 2017.

[2] Ocak, D. M., Kuantum Bilgisayarlar Çağında Kriptografi, 2020.

[3] Bavdekar, R. ve Jozsa, E., Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research, 2022.

[4] Çelik, S. Kuantum Kriptolojisi ve Siber Güvenlik, 14(1), 2021.

[5] Shor, P. W. Algorithms for Quantum Computation, 35th Annual Symposium on Foundations of Computer Science (FOCS), 1994.

[6] Niederhagen, R. Practical Post-Quantum, Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT), 2024.

[7] Grover, L. K. A Fast Quantum Mechanical Algorithm for Database Search, Proceedings of the Twenty- Eighth Annual ACM Symposium on Theory of Computing (STOC), ACM, 1996.

[8] Jozsa, R., Quantum Factoring, Discrete Logarithms, and the Hidden Subgroup Problem, 2001.

[9] Bernstein, D. J., Post-Quantum Cryptography, 2017.

[10] Abiade, O., The Impact of Quantum Computing on RSA and ECC Algorithms, EasyChair, 2024.

[11] Chandra, S., Bhattacharyya, S., Paira, S. ve Alam, S. S., A Study and Analysis on Symmetric Cryptography, IEEE, 2017.

[12] Hasija, T., Ramkumar, K., Singh, B., Kaur, A., Mittal, S. K., Jhanda, K. ve Kaiserslautern, S., Symmetric Key Cryptography: Review, Algorithmic Insights, and Applications, Chitkara University Research and Innovation Network (CURIN), 2023.

[13] Chi, D. P., Choi, J. W., Kim, J. S. ve Kim, T., Lattice-Based Cryptography for Beginners, IACR Cryptology ePrint Archive, 2015.

[14] Fischer, S., Analysis of Lightweight Stream Ciphers, 2008.

[15] Garipcan, A. M., Erdem, E. ve Tuncer, T., Donanım Tabanlı Trivium Akış Şifreleme Algoritmasının FPGA Ortamında Gerçekleştirilmesi, 29(2), 2017.

[16] Aghayev, M., Kriptoloji ve Veri Şifreleme Teknikleri Üzerine, Yök Açık Bilim/ Ege Üniversitesi, 2017.

[17] Yerlikaya, T., Yeni Şifreleme Algoritmalarının Analizi, Trakya Üniversitesi / Fen Bilimleri Enstitüsü, 2006.

[18] «Veri Şifreleme: Nasıl çalışır, neden ihtiyacınız var?», (Erişildi: 12 2024).

[19] Eduard, S., Post-Quantum Cryptography: Lattice-based Encryption, 2016.

[20] «https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards», (Erişildi: 12 2024).

[21] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G. ve Stehlé, D., CRYSTALS – Kyber: A CCA-secure module-lattice-based KEM, 2017.

[22] «https://pq-crystals.org/kyber/software.shtml», (Erişildi: 12 2024).

[23] Zeng, P., Chen, S. ve Choo, K.-K. R., An IND-CCA2 Secure Post-Quantum Encryption Scheme and a Secure Cloud Storage Use Case, 9(32), 2019.

[24] Bernstein, D. J., Chuengsatiansup, C., Lange, T. ve v. Vredendaal, C., NTRU Prime: Reducing Attack Surface at Low Cost, 2017.

[25] Çıraklı, Y. D. D. Ü., Dalkılıç, A. G. S. ve Hacıhasanoğlu, D. D. T., Kaos Teorisi, Karmaşık Teorisi, Karmaşık Uyarlamalı Sistemler: Sağlık Hizmetleri Açısından Bir Derleme, International Journal of Academic Value Studies, pp. 330-343, 2017.

[26] Aydın, Y. ve Özkaynak, F., Kaotik Sistemler Tabanlı Kriptografik Tasarımlar İçin Bir Analiz Aracı, Turkish Journal of Science and Technology, 18(2), pp. 387-395, 2023.

[27] Seval, G. ve Kasapbaşı, M. C., Görüntüler İçin Kaotik Şifreleme Sistemi ve Performans Analizi, Avrupa Bilim ve Teknoloji Dergisi, no. 44, pp. 13-20, 2022.

[28] Tuna, M. ve Fidan, C. B., A Study on the Importance of Chaotic Oscillators Based on FPGA for True Random Number Generating (TRNG) and Chaotic Systems, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, pp. 473-491, 2018.

Haliç Üniversitesi Fen Bilimleri Dergisi 2025, 8/1: 81-101
DOI: 10.46373/hafebid.1652048

ISSN: 2618-6241
e-ISSN: 2667-5757

Nanoparticle-Based Drug Delivery Systems and Targeting Strategies in Breast Cancer Therapy

Ceren ÇOLAK[1,2*]

[1]Department of Molecular Biology and Genetics Department, Haliç University, İstanbul, Türkiye
Orcid: 0009-0000-7097-8141, (https://orcid.org/0009-0000-7097-8141)
[2]Department of Biotechnology, Yeditepe University, İstanbul, Türkiye

Geliş Tarihi: 03.03.2025
Kabul Tarihi: 22.04.2025

***Sorumlu Yazar e mail:** cerencolak@halic.edu.tr

Atıf/Citation: Çolak, C., "Nanoparticle-Based Drug Delivery Systems and Targeting Strategies in Breast Cancer Therapy", Haliç Üniversitesi Fen Bilimleri Dergisi 2025, 8/1: 81-101.

Derleme Makalesi / *Review Article*

Abstract

Breast cancer continues to be a major contributor to cancer-related mortality globally, highlighting the critical importance of developing more efficient and safer therapy strategies. Nanoparticle-based drug delivery systems offer a promising approach by enhancing drug accumulation in tumor tissues while minimizing systemic toxicity. This article explores the unique properties and advantages of various nanoparticles, including liposomal, polymer-, metal-, carbon- and mesoporous silica nanoparticles, in breast cancer therapy. Additionally, it delves into three key targeting mechanisms: passive targeting via the enhanced permeability and retention (EPR) effect, active targeting using ligands and antibodies, and stimuli-responsive drug delivery systems. Integrating nanotechnology into breast cancer therapy paves the way for more precise, efficient, and personalized therapy options, offering new hope for improved patient outcomes.

Keywords: Breast Cancer, Drug Delivery Systems, Nanoparticle

Meme Kanseri Tedavisinde Nanopartikül Tabanlı İlaç Taşıma Sistemleri ve Hedefleme Stratejileri

Özet

Meme kanseri, dünya genelinde kansere bağlı ölümlerde önemli bir rol oynamaya devam etmekte olup, daha etkili ve daha güvenli tedavi stratejileri geliştirmenin kritik önemini vurgulamaktadır. Nanopartikül bazlı ilaç dağıtım sistemleri, sistemik toksisiteyi en aza indirirken tümör dokularında ilaç birikimini artırarak umut verici bir yaklaşım sunmaktadır. Bu makale, meme kanseri tedavisinde lipozomal, polimer, metal, karbon ve mezogözenekli silika nanopartiküller de dahil olmak üzere çeşitli nanopartiküllerin benzersiz özelliklerini ve avantajlarını araştırmaktadır. Ayrıca, üç temel hedefleme mekanizması üzerinde durulmaktadır: gelişmiş geçirgenlik ve tutma (EPR) etkisi yoluyla pasif hedefleme, ligandlar ve antikorlar kullanılarak aktif hedefleme ve uyarıcıya duyarlı ilaç dağıtım sistemleri. Nanoteknolojinin meme kanseri tedavisine entegre edilmesi, daha hassas, verimli ve kişiselleştirilmiş tedavi seçeneklerinin önünü açarak hasta sonuçlarının iyileştirilmesi için yeni umutlar sunmaktadır.

Anahtar Sözcükler: Meme Kanseri, İlaç Dağıtım Sistemleri, Nanopartikül

1. Introduction

Cancer, a complicated and severe group of diseases defined by uncontrolled cell proliferation and tissue invasion, presents a serious threat to global healthcare systems [1]. Breast cancer is one of the most common and investigated cancers, with numerous subtypes depending on molecular features [2]. The mortality rate for women diagnosed with breast cancer was around 30% in 2022. Breast cancer continues to pose a significant challenge to worldwide health, even with advancements in early diagnosis and therapeutic approaches [3]. Genetic predisposition, late-stage diagnosis, and inadequate access to healthcare remain significant challenges [4].

Breast cancer is complex, and knowing its heterogeneity is critical to develop targeted therapy methods [5]. Recent research has shed light on the molecular complexities and identifying multiple subtypes with varied clinical features and treatment outcomes [6]. The

identification of molecular markers such as human epidermal growth factor receptor 2 (HER2) and hormone receptor statuses has transformed treatment methods, allowing for targeted therapy approaches such as Herceptin in HER2-positive breast cancer [7]. Despite advancements, late-stage diagnosis still poses a significant problem. Early detection has been improved through screening programs and the development of enhanced imaging techniques. Genetic propensity, as indicated by the BRCA1 and BRCA2 mutations, is very important in assessing and preventing breast cancer [8].

Depending on the type and stage of the tumor, current treatment techniques include surgery, radiation therapy, hormone therapy and chemotherapy [9]. While these treatments have made significant progress in improving the lives of patients, they have some negative aspects. Chemotherapy and radiation therapy typically cause serious adverse effects such as exhaustion and nausea, whilst surgical therapies can include complications following surgery and organ damage [10]. Furthermore, traditional treatments may have limited effect, especially in metastatic cancer types, and may unintentionally promote resistance to drugs. In addition, high financial costs can have a significant influence on patients' financial stability and well-being [11].

Traditional medications play an important role in the treatment of cancer, collaborating with new targeted therapies and immunotherapies to achieve better results. Adjuvant radiation treatment, for example, has significantly boosted survival rates while lowering the risk of recurrence [12]. Immunotherapy has become known as an efficient strategy for breast cancer in recent years. Clinical trials are being conducted for examining immune checkpoint inhibitors, which utilize the immune system to fight cancer cells. Some examples of these inhibitors are programmed cell death protein 1 (PD-1) and programmed cell death ligand 1 (PD-L1) [13]. With the help of genetics and biomarker studies, personalized medicine optimizes therapeutic outcomes by creating treatment plans that are tailored to each patient's particular cancer tendency [14].

Targeted drug delivery systems are critical in cancer therapy since they improve the effectiveness of drugs by accurately delivering drugs to tumor areas, raising drug concentration in the intended area while decreasing off-target effects [15]. Additionally, these methods make it easier to get across biological barriers like the blood–brain barrier, which makes it possible to transport drugs to areas that would otherwise be inaccessible. Furthermore, targeted drug delivery systems provide personalized treatment approaches, improving therapeutic outcomes and minimizing side effects [16]. Moreover, targeted drug delivery systems have attracted lots of interest in the treatment of breast cancer.

2. Nanoparticles as Targeted Drug Delivery Systems

Nanoparticles are particles which are 1-100 nm in size with an exterior layer of diverse organic or inorganic coatings. Many studies have been carried out to take advantage of nanoparticles in drug delivery systems for breast cancer therapy. However, they have not yet been commonly employed in clinical treatments. Nanoparticles have gained popularity as nanocarriers because of their properties such as water dispersibility, biodegradability and biocompatibility. The bioavailability of many chemotherapeutic treatments is increased when nanoparticles are used to treat cancer because they increase the solubility and half-life of the drugs [17]. Additionally, nanoparticles may promote accumulation of drugs in cancer tissues by EPR effect [18].

Finally, using target ligands to target particular cancer locations, nanoparticle-based drug delivery systems can decrease adverse effects and increase therapy efficacy [19]. Several types of nanoparticles have been used in targeted drug delivery systems for breast cancer. Figure 1 presents a schematic overview of five widely utilized nanoparticle types in drug delivery. Several features of liposomal, polymer-, metal-, carbon-, and mesoporous silica nanoparticles will be explained below.

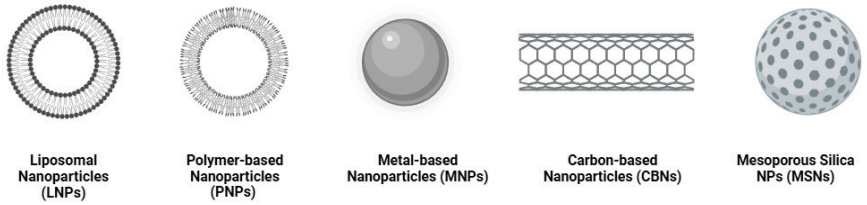


Figure 1. Schematic Illustration of Common Nanoparticle Types in Drug Delivery Systems

This figure presents a schematic overview of widely utilized nanoparticle types in drug delivery: (A) Liposomal Nanoparticles (LNPs), (B) Polymer-based Nanoparticles (PNPs), (C) Metal-based Nanoparticles (MNPs), (D) Carbon-based Nanoparticles (CBNs), (E) Mesoporous Silica Nanoparticles (MSNs).

2.1. Liposomal Nanoparticles (LNPs)

LNPs are spherical vesicles formed by integrating one or more phospholipid bilayers and their size may exceed hundreds of nanometers. These nanoparticles have a hydrophilic inner core that is covered by a hydrophobic lipid bilayer. Due to its distinct form, the phospholipid bilayer is typically used to encapsulate hydrophobic drugs for delivery. LNPs are additionally used for hydrophilic drugs through encapsulation in the inner core. Because of non-target dispersion, encapsulation of drugs significantly lowers the toxicity of drugs. In addition, it is possible to encapsulate amphiphilic drugs, including doxorubicin (Dox), inside of the inner core of LNP. This has been demonstrated to specifically lower Dox's cardiocytotoxicity when compared to its unencapsulated form [20].

LNPs accumulate in cancer tissue via integrating the bilayer across the membrane of cells. Studies have shown that surface modification of liposomal nanoparticles with PEG results in longer half-lives and increased targeting success [21]. PEGylated LNPs demonstrated

successful passive targeting in studies. Also, LNPs have been employed to encapsulate multiple drugs in order to deliver drug combinations that have synergistic effects. Vincristine and quercetin were encapsulated together in a PEGylated liposome by Wong and Chiu to treat breast cancer that is unresponsive to trastuzumab and hormones. According to this study, co-encapsulation promoted more synergism, extended circulation of drugs in plasma with regulated release for JIMT-1 cells in vivo. Furthermore, compared to the two separate drugs, liposomal encapsulation is the most successful method for inhibiting the proliferation of JIMT-1 cells [22].

Doxil®/Caelyx®, Myocet®, Lipodox®, and Lipusu® are the four liposomal drugs that have been licensed for use as breast cancer therapy and have undergone clinical testing. The first chemotherapeutic nanosystem to be used in clinical settings, Doxil® is a PEGylated nano-liposomal drug delivery system loaded with DOX for metastatic breast cancer. The liposomal formulation and its PEGylation are regarded as innovative since they increase the chemotherapeutic agent's circulation time while lowering the blood's level of free DOX without compromising its anticancer action [23].

2.2. Polymer-based Nanoparticles (PNPs)

PNPs are colloidal particles with a size around 100-400 nm. They are typically created via attaching a copolymer onto a different polymer matrix. Natural polymers such as cellulose and chitosan can be employed in this application [60]. However, synthetic polymers can also be utilized to create PNP that fulfill particular chemical and biological purposes, which makes them extremely desirable for use in biomedical fields [24]. PNPs are chemically synthesized using standard techniques such as nanoprecipitation, salting-out, and emulsification [25]. Chemically synthesized PNPs may be engineered to have the necessary charge, lipophilicity, and biocompatibility for transporting the given drug into its target [26].

Delivering the anti-cancer drug to the target region, it can be encapsulated in a PNPs, loaded onto the surface of the PNPs through surface adsorption, as well as chemically conjugated [27]. Most PNPs are efficient carriers for drugs that are less hydrophilic due to their permeability and high solubility, which enables them to maintain stability with a prolonged, gradual release of the drug. Furthermore, PNPs have shown low toxicity and great drug loadability, particularly when capped with a PEG-phospholipid copolymer [28]. Several chemotherapeutic drugs, including Doxorubicin, trastuzumab, and cisplatin, have been explored for PNP and drug conjugation. Several PNPs, such as polyhydroxyalkanoates, PLGA, and cyclodextrin-derived PNPs, were investigated as nanocarriers in cancer therapy [26].

2.3. Metal-based Nanoparticles (MNPs)

MNPs, commonly referred to as inorganic nanoparticles, have been intensively investigated for medicinal and imaging features. Their typical composition consists of an organic-coated shell and a core that determines electrical, magnetic, and optical properties. Gold nanoparticles (AuNPs), superparamagnetic iron oxide nanoparticles (SPIONs), and quantum dots (QDs) are three common varieties utilized in breast cancer treatment [29].

AuNPs have been produced by modifying their size, shape, and surface functionalities for a range of uses [30]. Most popular method for synthesizing AuNPs is to reduce Au3+ in aqueous medium with citrate. These nanoparticles were frequently employed as drug delivery systems due to its special properties and notably low toxicity [31]. For the nanoparticles to target particular receptors or biomarkers, organic surface coating is essential. Because of these surface coatings, thiolates and disulfides are frequently utilized primarily because of their propensity to adhere to the surface of Au. Covalent or non-covalent bonds can then be used to attach drugs or other therapeutic substances to the surface of AuNPs [32]. By targeting EGFR/

VEGFR-2, enhances angiogenesis and cell proliferation, plays an essential role in metastasis of breast cancer, a study demonstrated a significant suppression of breast cancer. Based on this research, AuNPs containing quercetin may suppress the epithelial-mesenchymal transition, and that is a factor of MCF-7 and MDA-MB-231 breast cancer cell lines [33]. Because of their distinctive properties, particularly their controlled functionalization and ease of imaging using microscopic methods like transmission electron microscopy (TEM), AuNPs were commonly used in drug delivery. Despite the low cytotoxicity, AuNPs may have a significant disadvantage in terms of biodegradability in a biological system [29].

SPIONs are ranging in size from 1-100 nm. They contain a magnetic inner core made from magnetite (Fe_3O_4) or maghemite (γ-Fe_2O_3). One of the best inner core materials for SPIONs is thought to be maghemite. since it has the lowest risk of toxicity of Fe(III) in the body, as opposed to Fe(II) released by magnetite [34]. One major drawback of using them directly in therapeutic and biological applications is that they may produce biofouling and aggregation in blood plasma [35]. Thus, a hydrophilic coating, like polymers, is applied to the magnetic core to stabilize it and allow for targeted delivery of molecules to particular areas. Polysaccharides, PEG, dextran, and alginate are among the most extensively utilized biopolymers for stabilization [36]. Du et al. utilized ultrasmall iron oxide nanoparticles (IONPs) modified with a breast cancer brain metastasis-targeting peptide (BRBP1), enhancing imaging contrast and tumor specificity [37]. Similarly, Zheng et al. developed self-illuminating nanoprobes targeting neutrophil infiltration, achieving 98% sensitivity and 96% specificity in detecting lung metastases. These approaches highlight the potential of nanoparticle-based imaging for early metastasis detection, supporting more precise, personalized breast cancer treatment [38].

QDs are semiconductor nanocrystals with diameters ranging from 2-10 nm. They are generally made up of a metal inner core that emits a narrow range of visible to infrared (IR) light based on size. Depending

on its intended use, the shell could be made of semiconductor layers or doped metals. When QDs are conjugated with surface modifying ligands and peptides, they can be utilized for cancer investigations with targets [39]. QDs made it possible to image cells in vivo much more than most other NPs because of their good adjustable optical characteristics, high brightness, resistance to photobleaching and large surface-to-volume ratio. Nonetheless, one disadvantage of QDs is their extreme hydrophobicity. They need to have polymers or multilayer ligand shells applied to their surface in order to reach an ideal level of water solubility [40]. The main disadvantage of these nanoparticles is that their inner core is often composed of heavy metals, which may be hazardous to the body in the long term due to accumulation in organs like the liver. Furthermore, QDs' exceptional stability reduces their biodegradability and, consequently, their biocompatibility. As a result, recent research has concentrated on non-metal nanoparticles as an alternative to traditional metal-based QDs [29].

Nanoparticle-based platforms also show promise in detecting circulating tumor cells (CTCs), offering insights into metastasis and cancer progression [41]. Since CTCs are key indicators of metastatic disease, their early detection is crucial for timely, personalized treatments. Wang M et al. developed a fluorescent technique using peptide-functionalized magnetic nanoparticles to quantify HER2 on CTCs, providing both prognostic data and potential guidance for therapy decisions [42].

2.4. Carbon-based Nanoparticles (CBNs)

CBNs, such as fullerene, graphene, carbon nanotubes (CNTs), and carbon dots (CDs), are attractive tools for treating breast cancer because of their distinct biological, physicochemical, optical features [43]. CBNs were designed to replace hazardous, heavy-metal-containing QDs and other metal nanoparticles with a nonmetallic system. CBNs have various advantages, including high specific surface area,

biocompatibility, small size, variable surface functional groups, low toxicity, and distinct optical and thermal properties. Thus, CBNs might be considered a better and prospective drug delivery system to be used in cancer therapy than metal-based nanoparticles [44].

CNTs are fullerene allotropes with a cylindrical shape and long, hollow structures having a wall made of graphene sheet coiled at an angle. CNTs are divided into single-walled and multi-walled types according to whether they have one or more graphene sheets. CNTs are still being developed, and they show many remarkable qualities, including electrical, optical, and thermal conductivity. Furthermore, CNTs have emerged as a multipurpose tool for the use of nanomedicine, especially in cancer targeting [45]. Since biological systems are extremely transparent in near-infrared (NIR) light, CNTs can be used as an efficient optical absorber because of their tunable surface and special thermal properties [46]. Drug loading into CNTs may be difficult because they are pre-formed supramolecular nanotubes. Direct loading to the surface and filament loading are the two drug loading patterns of CNTs. They can be filled with drugs using a simple capillarity-induced filling method. However, the loadable amount of drugs might be 5% (w/w) [47].

CDs a novel family member of carbon-based nanoparticles. When they first discovered, the majority of the research focused on photoluminescence (PL) employing different synthetic methods, starting materials, and surface changes [48]. Surface doping boosted fluorescence quantum yield (QY) as a PL measurement by up to 93.3% [49]. Hsu et al. demonstrated that green tea-derived CDs inhibited cancer cell growth. Three cancer cell lines were used: MCF-7, MDA-MB-231, and HeLa. While the concentration of CDs increased, the viability of cells decreased. According to their respective cell viability percentages of 20, 18, and 68%, MCF-7, MDA-MB-231, and HeLa cells showed a significant inhibitory effect on breast cancer cell lines when using CDs [50].

2.5. Mesoporous Silica Nanoparticles (MSNs)

MSNs received a lot of interest as a different inorganic nanoparticle in targeted drug delivery and imaging because of their distinctive characteristics, such as pore volume, large surface area, and the ability to vary pore size beside providing a surface that can be easily modifiable [51]. The unique porous surface of MSNs allows for a high and controlled drug loading capacity. They can also carry medications without releasing them prematurely before they reach their target site, making them an excellent carrier for molecules that degrade easily, such as proteins and DNA. In order to selectively target breast cancer cells, a study reported an anti-HER2/neu monoclonal antibody based on nanoparticles and employing green fluorescent MSNs as drug carriers [52]. In another study, researchers created an MSNs drug delivery system to deliver siRNA for reducing Dox resistance in multi drug resistance breast cancer cells in mice [53].

3. Targeting Strategies For Breast Cancer Therapy

The treatment of breast cancer has been mostly transformed by targeted drug delivery systems, which have the potential to improve therapeutic effect while lowering systemic toxicity. This may be developed to circumvent drug resistance processes, which commonly hinder therapeutic outcomes [54]. Targeted drug delivery has a high promise for overcoming resistance to drugs by improving delivery of drugs to cancer cells that are resistant or using combination treatments that focusing several pathways [55]. Figure 2. shows an illustration of drug delivery strategies. This part goes into several targeting strategies for improving the delivery of drugs, particularly for breast cancer, focusing on developments and their clinical consequences.

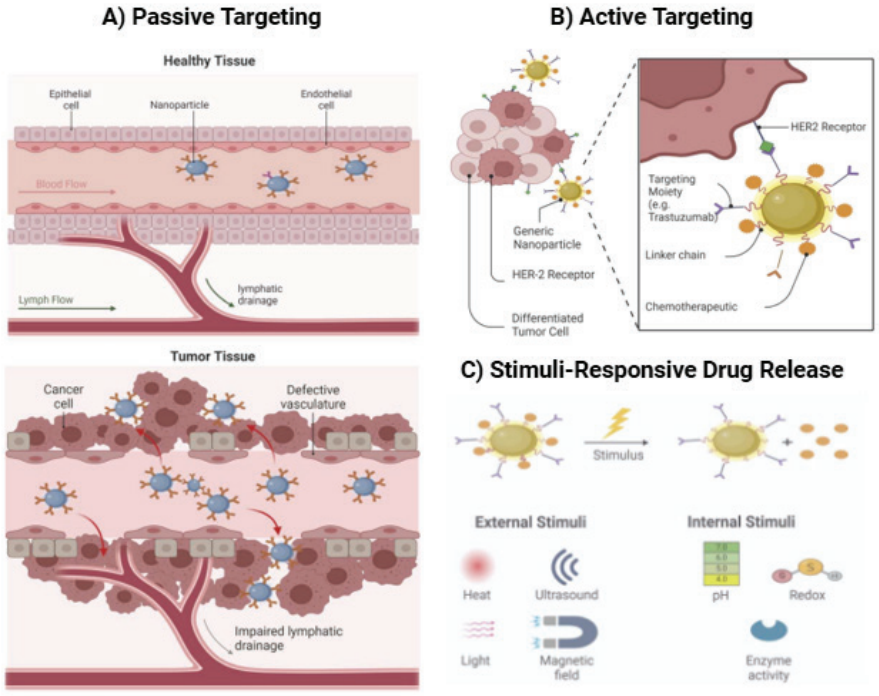


Figure 2. Schematic Illustration of Drug Delivery Strategies

This figure illustrates three major strategies employed in targeted drug delivery systems: (A) Passive Targeting, (B) Active Targeting, (C) Stimuli-Responsive Drug Release.

3.1. Passive Targeting

In breast cancer treatment, passive targeting is based on a basic phenomenon called the increased permeability and retention (EPR) effect. This impact is achieved using unique properties of the tumor microenvironment [56]. Some solid tumors have abnormal blood vessels which provide nutrition to the tumor. Due to their irregular form and leakiness, nanoparticles can passively infiltrate the tumor tissue [57]. These nanoparticles tend to gather within the tumor because of

poor lymphatic drainage. In cancer, the lymphatic system, which is in charge of removing waste and fluid from tissues, is frequently weakened, which makes nanoparticles more likely to remain in the tumor microenvironment [58].

Optimizing the design of drug carriers and nanoparticles to maximize the EPR effect has been the focus of recent studies. Particle size, drug release profiles, and surface charge are precisely set for optimizing drug delivery while minimizing off-target effects. Researchers intend to enhance breast cancer therapy selectivity and efficacy by leveraging the EPR effect [59].

3.2. Active Targeting

Active targeting techniques employ a more accurate method by actively guiding drug delivery systems to their target cancer cells using particular molecules, like ligands, antibodies or peptides. Targeting moieties are chosen for their high affinity in binding to overexpressed receptors on cancer cell surfaces [60]. When these targeting ligands are coupled with drug carriers like nanoparticles, liposomes, or exosomes, It is possible to precisely target drug delivery to the tumor area. By using this technique, the negative effects of therapeutic drugs are greatly reduced in off-target effects and healthy tissues can be protected [61].

Creating antibody-drug conjugates (ADCs) to specifically treat breast cancer represents a significant advancement in this field. ADCs are monoclonal antibodies that target receptors on the surface of cancer cells and deliver powerful cytotoxic cargoes. This enables a very specific and powerful treatment strategy. The drug is directly delivered to the cancer cell by the antibody, thus promoting apoptosis in cancer cell while preserving healthy cells [62].

3.3. Stimuli-Responsive Drug Delivery Systems

One of the most innovative approaches to breast cancer therapy is the use of stimuli-responsive drug delivery systems. These systems release therapeutic drugs based on certain parameters in the tumor microenvironment. These variables may include pH, temperature or enzyme activity variations that are particular to cancer cells. Drug delivery systems that are stimulus-responsive are designed to react to these signals, guaranteeing release of the drugs inside the tumor while preserving healthy tissue. As an example, the acidic environment of breast cancer may be used as an initiator for the release of drugs [63]. The acidic environment in the tumor tissue causes nanoparticles or carriers to release the therapeutic payload as they enter, lowering negative effects in surrounding tissues and enhancing drug exposure to cancer cells [64].

This strategy has various benefits, such as decreased systemic toxicity and enhanced drug absorption at the target location. It has enormous potential to improve the therapeutic effect in breast cancer treatment.

4. Conclusions

Nanoparticle-based drug delivery systems have become a game-changer in the treatment of breast cancer since they provide better drug solubility, more precise tumor targeting, and less systemic toxicity. By utilizing their distinct physicochemical characteristics, these nanocarriers which include liposomal, polymer-based, carbon-based, mesoporous silica nanoparticles offer flexible platforms for effective drug delivery. When compared to traditional medicines, they have the potential to greatly improve treatment outcomes by improving drug accumulation at tumor locations and overcoming biological obstacles.

In order to maximize the therapeutic effects of nanoparticles, targeting strategies are essential. Because of abnormal vasculature and

impaired lymphatic drainage, passive targeting, which is primarily enabled by the increased EPR effect, enables nanoparticles to accumulate in tumor tissues. Active targeting improves selectivity and reduces off-target effects by enabling precise binding to overexpressed receptors on cancer cells using ligands, antibodies, and peptides. Additionally, stimuli-responsive systems, triggered by tumor-specific microenvironmental factors such as pH, temperature, or enzyme activity, provide controlled and localized drug release, further minimizing adverse effects on healthy tissues. Despite these encouraging developments, a number of obstacles need to be overcome in order to facilitate the clinical translation of nanoparticle-based treatments. Long-term toxicity, immunogenicity, large-scale manufacturing, stability, and regulatory approval are still major obstacles. Furthermore, because breast cancer subtypes are diverse, personalized nanomedicine strategies that are suited to each patient's unique profile must be developed. The combination of therapeutic and diagnostic properties in multifunctional nanoparticles offers enormous promise for real-time tracking of disease development and treatment efficacy.

Future studies should concentrate on enhancing targeted delivery efficiency, optimizing nanoparticle formulations for improved biocompatibility, and ensuring safety through thorough preclinical and clinical testing. The development of next-generation nanocarriers will be further accelerated by the convergence of nanotechnology with areas including biomarker-driven precision medicine and genomics. With continued advancements and interdisciplinary collaboration, nanoparticle-based targeted drug delivery systems possess the power to change the treatment of breast cancer, paving the way for more effective and personalized therapeutic approaches.

References

[1] F. Bray, J. Ferlay, I. Soerjomataram, R. L. Siegel, L. A. Torre, and A. Jemal, "Global cancer statistics 2018: GLOBOCAN estimates of incidence and mortality worldwide for 36 cancers in 185 countries," *CA Cancer J Clin*, vol. 68, no. 6, pp. 394–424, Nov. 2018, doi: 10.3322/CAAC.21492.

[2] R. L. Siegel, K. D. Miller, H. E. Fuchs, and A. Jemal, "Cancer Statistics, 2021," *CA Cancer J Clin*, vol. 71, no. 1, pp. 7–33, Jan. 2021, doi: 10.3322/CAAC.21654.

[3] C. E. DeSantis *et al.*, "Breast cancer statistics, 2019," *CA Cancer J Clin*, vol. 69, no. 6, pp. 438–451, Nov. 2019, doi: 10.3322/CAAC.21583.

[4] L. A. Torre, F. Islami, R. L. Siegel, E. M. Ward, and A. Jemal, "Global Cancer in Women: Burden and Trends," *Cancer Epidemiol Biomarkers Prev*, vol. 26, no. 4, pp. 444–457, Apr. 2017, doi: 10.1158/1055-9965.EPI-16-0858.

[5] B. D. Lehmann *et al.*, "Identification of human triple-negative breast cancer subtypes and preclinical models for selection of targeted therapies," *J Clin Invest*, vol. 121, no. 7, pp. 2750–2767, Jul. 2011, doi: 10.1172/JCI45014.

[6] T. Sørlie *et al.*, "Gene expression patterns of breast carcinomas distinguish tumor subclasses with clinical implications," *Proc Natl Acad Sci U S A*, vol. 98, no. 19, pp. 10869–10874, Sep. 2001, doi: 10.1073/PNAS.191367098.

[7] D. J. Slamon *et al.*, "Use of chemotherapy plus a monoclonal antibody against HER2 for metastatic breast cancer that overexpresses HER2," *N Engl J Med*, vol. 344, no. 11, pp. 783–792, Mar. 2001, doi: 10.1056/NEJM200103153441101.

[8] N. Mavaddat *et al.*, "Polygenic Risk Scores for Prediction of Breast Cancer and Breast Cancer Subtypes," *Am J Hum Genet*, vol. 104, no. 1, pp. 21–34, Jan. 2019, doi: 10.1016/J.AJHG.2018.11.002.

[9] F. Cardoso *et al.*, "Early breast cancer: ESMO Clinical Practice Guidelines for diagnosis, treatment and follow-up†," *Ann Oncol*, vol. 30, no. 8, pp. 1194–1220, Aug. 2019, doi: 10.1093/ANNONC/MDZ173.

[10] M. Stehr, K. Deilmann, R. J. Haas, and H. G. Dietz, "Surgical complications in the treatment of Wilms' tumor," *Eur J Pediatr Surg*, vol. 15, no. 6, pp. 414–419, Dec. 2005, doi: 10.1055/S-2005-872915.

[11] R. Chaudhari, V. Patel, and A. Kumar, "Cutting-edge approaches for targeted drug delivery in breast cancer: beyond conventional therapies," 2024, doi: 10.1039/d4na00086b.

[12] S. Darby *et al.*, "Effect of radiotherapy after breast-conserving surgery on 10-year recurrence and 15-year breast cancer death: meta-analysis of individual patient data for 10,801 women in 17 randomised trials," *Lancet*, vol. 378, no. 9804, pp. 1707–1716, Nov. 2011, doi: 10.1016/S0140-6736(11)61629-2.

[13] L. A. Emens, "Breast Cancer Immunotherapy: Facts and Hopes," *Clin Cancer Res*, vol. 24, no. 3, pp. 511–520, Feb. 2018, doi: 10.1158/1078-0432.CCR-16-3001.

[14] A. Prat, B. Adamo, M. C. U. Cheang, C. K. Anders, L. A. Carey, and C. M. Perou, "Molecular characterization of basal-like and non-basal-like triple-negative breast cancer," *Oncologist*, vol. 18, no. 2, pp. 123–133, Feb. 2013, doi: 10.1634/THEONCOLOGIST.2012-0397.

[15] M. T. Manzari, Y. Shamay, H. Kiguchi, N. Rosen, M. Scaltriti, and D. A. Heller, "Targeted drug delivery strategies for precision medicines," *Nat Rev Mater*, vol. 6, no. 4, pp. 351–370, Apr. 2021, doi: 10.1038/S41578-020-00269-6.

[16] D. Rosenblum, N. Joshi, W. Tao, J. M. Karp, and D. Peer, "Progress and challenges towards targeted delivery of cancer therapeutics," *Nat Commun*, vol. 9, no. 1, Dec. 2018, doi: 10.1038/S41467-018-03705-Y.

[17] D. Peer, J. M. Karp, S. Hong, O. C. Farokhzad, R. Margalit, and R. Langer, "Nanocarriers as an emerging platform for cancer therapy," *Nat Nanotechnol*, vol. 2, no. 12, pp. 751–760, Dec. 2007, doi: 10.1038/NNANO.2007.387.

[18] J. Fang, H. Nakamura, and H. Maeda, "The EPR effect: Unique features of tumor blood vessels for drug delivery, factors involved, and limitations and augmentation of the effect," *Adv Drug Deliv Rev*, vol. 63, no. 3, pp. 136–151, Mar. 2011, doi: 10.1016/J.ADDR.2010.04.009.

[19] V. Torchilin, "Tumor delivery of macromolecular drugs based on the EPR effect," *Adv Drug Deliv Rev*, vol. 63, no. 3, pp. 131–135, Mar. 2011, doi: 10.1016/J.ADDR.2010.03.011.

[20] N. L. Boman, P. R. Cullis, L. D. Mayer, M. B. Bally, and M. S. Webb, "Liposomal Vincristine: The Central Role of Drug Retention in Defining Therapeutically Optimized Anticancer Formulations," *Long Circulating Liposomes: Old Drugs, New Therapeutics*, pp. 29–49, 1998, doi: 10.1007/978-3-662-22115-0_3.

[21] T. Yang *et al.*, "Enhanced solubility and stability of PEGylated liposomal paclitaxel: in vitro and in vivo evaluation," *Int J Pharm*, vol. 338, no. 1–2, pp. 317–326, Jun. 2007, doi: 10.1016/J.IJPHARM.2007.02.011.

[22] M. Y. Wong and G. N. C. Chiu, "Liposome formulation of co-encapsulated vincristine and quercetin enhanced antitumor activity in a trastuzumab-insensitive breast tumor xenograft model," *Nanomedicine*, vol. 7, no. 6, pp. 834–840, Dec. 2011, doi: 10.1016/J.NANO.2011.02.001.

[23] J. Nel *et al.*, "Functionalized liposomes for targeted breast cancer drug delivery," *Bioact Mater*, vol. 24, pp. 401–437, Jun. 2023, doi: 10.1016/J.BIOACTMAT.2022.12.027.

[24] A. Kumari, S. K. Yadav, and S. C. Yadav, "Biodegradable polymeric nanoparticles based drug delivery systems," *Colloids Surf B Biointerfaces*, vol. 75, no. 1, pp. 1–18, Jan. 2010, doi: 10.1016/J.COLSURFB.2009.09.001.

[25] J. P. Rao and K. E. Geckeler, "Polymer nanoparticles: Preparation techniques and size-control parameters," *Progress in Polymer Science (Oxford)*, vol. 36, no. 7, pp. 887–913, 2011, doi: 10.1016/j.progpolymsci.2011.01.001.

[26] F. Masood, "Polymeric nanoparticles for targeted drug delivery system for cancer therapy," *Mater Sci Eng C Mater Biol Appl*, vol. 60, pp. 569–578, Mar. 2016, doi: 10.1016/J.MSEC.2015.11.067.

[27] K. S. Soppimath, T. M. Aminabhavi, A. R. Kulkarni, and W. E. Rudzinski, "Biodegradable polymeric nanoparticles as drug delivery devices," *Journal of Controlled Release*, vol. 70, no. 1–2, pp. 1–20, Jan. 2001, doi: 10.1016/S0168-3659(00)00339-4.

[28] H. Jin *et al.*, "EGFR-targeting PLGA-PEG nanoparticles as a curcumin delivery system for breast cancer therapy," *Nanoscale*, vol. 9, no. 42, pp. 16365–16374, Nov. 2017, doi: 10.1039/C7NR06898K.

[29] P. Y. Liyanage *et al.*, "Nanoparticle-mediated targeted drug delivery for breast cancer treatment," *Biochim Biophys Acta Rev Cancer*, vol. 1871, no. 2, pp. 419–433, Apr. 2019, doi: 10.1016/J.BBCAN.2019.04.006.

[30] Y. C. Yeh, B. Creran, and V. M. Rotello, "Gold nanoparticles: preparation, properties, and applications in bionanotechnology," *Nanoscale*, vol. 4, no. 6, pp. 1871–1880, Mar. 2012, doi: 10.1039/C1NR11188D.

[31] L. Dykman and N. Khlebtsov, "Gold nanoparticles in biomedical applications: recent advances and perspectives," *Chem Soc Rev*, vol. 41, no. 6, pp. 2256–2282, Feb. 2012, doi: 10.1039/C1CS15166E.

[32] M. Prabaharan, J. J. Grailer, S. Pilla, D. A. Steeber, and S. Gong, "Gold nanoparticles with a monolayer of doxorubicin-conjugated amphiphilic block copolymer for tumor-targeted drug delivery," *Biomaterials*, vol. 30, no. 30, pp. 6065–6075, Oct. 2009, doi: 10.1016/J.BIOMATERIALS.2009.07.048.

[33] S. Balakrishnan *et al.*, "Gold nanoparticle-conjugated quercetin inhibits epithelial-mesenchymal transition, angiogenesis and invasiveness via EGFR/VEGFR-2-mediated pathway in breast cancer," *Cell Prolif*, vol. 49, no. 6, pp. 678–697, Dec. 2016, doi: 10.1111/CPR.12296.

[34] F. M. Kievit and M. Zhang, "Surface engineering of iron oxide nanoparticles for targeted cancer therapy," *Acc Chem Res*, vol. 44, no. 10, p. 853, Oct. 2011, doi: 10.1021/AR2000277.

[35] W. J. Rogers and P. Basu, "Factors regulating macrophage endocytosis of nanoparticles: implications for targeted magnetic resonance plaque imaging," *Atherosclerosis*, vol. 178, no. 1, pp. 67–73, Jan. 2005, doi: 10.1016/J.ATHEROSCLEROSIS.2004.08.017.

[36] Y.-X. Wang, S. Xuan, M. Port, and J.-M. Idee, "Recent advances in superparamagnetic iron oxide nanoparticles for cellular imaging and targeted therapy research," *Curr Pharm Des*, vol. 19, no. 37, pp. 6575–6593, Sep. 2013, doi: 10.2174/1381612811319370003.

[37] J. Du *et al.*, "Targeted NIRF/MR dual-mode imaging of breast cancer brain metastasis using BRBP1-functionalized ultra-small iron oxide nanoparticles," *Mater Sci Eng C Mater Biol Appl*, vol. 116, Nov. 2020, doi: 10.1016/J.MSEC.2020.111188.

[38] H. Zheng *et al.*, "Early diagnosis of breast cancer lung metastasis by nanoprobe-based luminescence imaging of the pre-metastatic niche," *J Nanobiotechnology*, vol. 20, no. 1, Dec. 2022, doi: 10.1186/S12951-022-01346-4.

[39] B. A. Kairdolf, A. M. Smith, T. H. Stokes, M. D. Wang, A. N. Young, and S. Nie, "Semiconductor quantum dots for bioimaging and biodiagnostic applications," *Annu Rev Anal Chem (Palo Alto Calif)*, vol. 6, no. 1, pp. 143–162, Jun. 2013, doi: 10.1146/ANNUREV-ANCHEM-060908-155136.

[40] R. Bilan, I. Nabiev, and A. Sukhanova, "Quantum Dot-Based Nanotools for Bioimaging, Diagnostics, and Drug Delivery," *Chembiochem*, vol. 17, no. 22, pp. 2103–2114, Nov. 2016, doi: 10.1002/CBIC.201600357.

[41] K. Barzaman *et al.*, "Breast cancer: Biology, biomarkers, and treatments," *Int Immunopharmacol*, vol. 84, Jul. 2020, doi: 10.1016/J.INTIMP.2020.106535.

[42] M. Wang *et al.*, "HER2 status of CTCs by peptide-functionalized nanoparticles as the diagnostic biomarker of breast cancer and predicting the efficacy of anti-HER2 treatment," *Front Bioeng Biotechnol*, vol. 10, Sep. 2022, doi: 10.3389/FBIOE.2022.1015295.

[43] S. Augustine, J. Singh, M. Srivastava, M. Sharma, A. Das, and B. D. Malhotra, "Recent advances in carbon based nanosystems for cancer theranostics," *Biomater Sci*, vol. 5, no. 5, pp. 901–952, May 2017, doi: 10.1039/C7BM00008A.

[44] Q. L. Yan, M. Gozin, F. Q. Zhao, A. Cohen, and S. P. Pang, "Highly energetic compositions based on functionalized carbon nanomaterials," *Nanoscale*, vol. 8, no. 9, pp. 4799–4851, Mar. 2016, doi: 10.1039/C5NR07855E.

[45] C. Cha, S. R. Shin, N. Annabi, M. R. Dokmeci, and A. Khademhosseini, "Carbon-based nanomaterials: multifunctional materials for biomedical engineering," *ACS Nano*, vol. 7, no. 4, pp. 2891–2897, Apr. 2013, doi: 10.1021/NN401196A.

[46] M. Hoseini-Ghahfarokhi and R. Fayazi, "Carbon Nanotubes as Near Infrared Radiation (NIR) Molecules for Cancer treatment," *Iranian Journal of Medical Physics*, vol. 15, no. Special Issue-12th. Iranian Congress of Medical Physics, pp. 264–264, Dec. 2018, doi: 10.22038/IJMP.2018.12908.

[47] S. Hampel *et al.*, "Carbon nanotubes filled with a chemotherapeutic agent: a nanocarrier mediates inhibition of tumor cell growth," *Nanomedicine (Lond)*, vol. 3, no. 2, pp. 175–182, Apr. 2008, doi: 10.2217/17435889.3.2.175.

[48] Y. P. Sun *et al.*, "Quantum-sized carbon dots for bright and colorful photoluminescence," *J Am Chem Soc*, vol. 128, no. 24, pp. 7756–7757, Jun. 2006, doi: 10.1021/JA062677D.

[49] C. Zheng, X. An, and J. Gong, "Novel pH sensitive N-doped carbon dots with both long fluorescence lifetime and high quantum yield," *RSC Adv*, vol. 5, no. 41, pp. 32319–32322, 2015, doi: 10.1039/C5RA01986A.

[50] P. C. Hsu, P. C. Chen, C. M. Ou, H. Y. Chang, and H. T. Chang, "Extremely high inhibition activity of photoluminescent carbon nanodots toward cancer cells," *J Mater Chem B*, vol. 1, no. 13, pp. 1774–1781, Apr. 2013, doi: 10.1039/C3TB00545C.

[51] C. Bharti, N. Gulati, U. Nagaich, and A. Pal, "Mesoporous silica nanoparticles in target drug delivery system: A review," *Int J Pharm Investig*, vol. 5, no. 3, p. 124, 2015, doi: 10.4103/2230-973X.160844.

[52] C. P. Tsai, C. Y. Chen, Y. Hung, F. H. Chang, and C. Y. Mou, "Monoclonal antibody-functionalized mesoporous silica nanoparticles (MSN) for selective targeting breast cancer cells," *J Mater Chem*, vol. 19, no. 32, pp. 5737–5743, Aug. 2009, doi: 10.1039/B905158A.

[53] H. Meng *et al.*, "Codelivery of an optimal drug/siRNA combination using mesoporous silica nanoparticles to overcome drug resistance in breast cancer in vitro and in vivo," *ACS Nano*, vol. 7, no. 2, pp. 994–1005, Feb. 2013, doi: 10.1021/NN3044066.

[54] X. Wang, H. Zhang, and X. Chen, "Drug resistance and combating drug resistance in cancer," *Cancer Drug Resist*, vol. 2, no. 2, pp. 141–160, 2019, doi: 10.20517/CDR.2019.10.

[55] C. Holohan, S. Van Schaeybroeck, D. B. Longley, and P. G. Johnston, "Cancer drug resistance: an evolving paradigm," *Nat Rev Cancer*, vol. 13, no. 10, pp. 714–726, Oct. 2013, doi: 10.1038/NRC3599.

[56] D. Kalyane, N. Raval, R. Maheshwari, V. Tambe, K. Kalia, and R. K. Tekade, "Employment of enhanced permeability and retention effect (EPR): Nanoparticle-based precision tools for targeting of therapeutic and diagnostic agent in cancer," *Mater Sci Eng C Mater Biol Appl*, vol. 98, pp. 1252–1276, May 2019, doi: 10.1016/J.MSEC.2019.01.066.

[57] F. Danhier, O. Feron, and V. Préat, "To exploit the tumor microenvironment: Passive and active tumor targeting of nanocarriers for anti-cancer drug delivery," *J Control Release*, vol. 148, no. 2, pp. 135–146, Dec. 2010, doi: 10.1016/J.JCONREL.2010.08.027.

[58] M. Overchuk and G. Zheng, "Overcoming obstacles in the tumor microenvironment: Recent advancements in nanoparticle delivery for cancer theranostics," *Biomaterials*, vol. 156, pp. 217–237, Feb. 2018, doi: 10.1016/J.BIOMATERIALS.2017.10.024.

[59] H. Maeda, J. Wu, T. Sawa, Y. Matsumura, and K. Hori, "Tumor vascular permeability and the EPR effect in macromolecular therapeutics: a review," *J Control Release*, vol. 65, no. 1–2, pp. 271–284, Mar. 2000, doi: 10.1016/S0168-3659(99)00248-5.

[60] M. Srinivasarao and P. S. Low, "Ligand-Targeted Drug Delivery," *Chem Rev*, vol. 117, no. 19, pp. 12133–12164, Oct. 2017, doi: 10.1021/ACS.CHEMREV.7B00013.

[61] R. Chaudhari, P. Patel, N. Meghani, S. Nasra, and A. Kumar, "Fabrication of methotrexate-loaded gold nanoconjugates and its enhanced anticancer activity in breast cancer," *3 Biotech*, vol. 11, no. 4, Apr. 2021, doi: 10.1007/S13205-021-02718-7.

[62] S. Verma *et al.*, "Trastuzumab Emtansine for HER2-Positive Advanced Breast Cancer," *New England Journal of Medicine*, vol. 367, no. 19, pp. 1783–1791, Nov. 2012, doi: 10.1056/NEJMOA1209124.

[63] R. Wang, Z. Huang, Y. Xiao, T. Huang, and J. Ming, "Photothermal therapy of copper incorporated nanomaterials for biomedicine," *Biomater Res*, vol. 27, no. 1, Dec. 2023, doi: 10.1186/S40824-023-00461-Z.

[64] V. P. Torchilin, "Multifunctional, stimuli-sensitive nanoparticulate systems for drug delivery," *Nat Rev Drug Discov*, vol. 13, no. 11, pp. 813–827, Oct. 2014, doi: 10.1038/NRD4333.

YAYIN KOŞULLARI

1. Gönderilecek makalelerde alanında bir boşluğu dolduracak özgün bir araştırma sonuçlarını içermesi şartı aranır.
2. Yayın Kurulu, dergiye gönderilen makaleleri öncelikle yayın ilkeleri, dergi kapsamı, bilimsel içerik ve şekil açısından inceler. Ön incelemeden geçen makaleler değerlendirilmek üzere en az 2 hakeme gönderilir. Eserin dergiye kabul edilebilmesi için iki hakemden de olumlu değerlendirme alması gerekir. Gerekli görülmesi durumunda üçüncü hakemden de değerlendirme sürecine katkı sağlaması istenebilir. Son karar editöre aittir.
3. Yayınlanmak üzere gönderilen makalelerin daha önceden yayımlanmamış olduğu ve intihal içermediği iThenticate programı aracılığıyla teyit edilir. Benzerlik raporu dergi editörleri tarafından kontrol edildikten sonra referanslar hariç benzerlik oranı % 20 ve altında çıkan makaleler değerlendirilmek üzere hakemlere gönderilir. Sonucu referanslar hariç % 20 üzerinde çıkan makaleler için yazardan düzeltme talep edilir. Gerekli düzeltmelerin 30 gün içerisinde yapılmaması durumunda makale reddedilir.
4. Makale yazarlarından değerlendirme ve yayın işlemleri için herhangi bir ücret talep edilmez.
5. Makalelerin tüm sorumluluğu ilgili yazarlara aittir. Makaleler uluslararası kabul görmüş bilimsel etik kurallarına uygun olarak hazırlanmalıdır. Gerekli olması halinde Etik kurul Raporu'nun bir kopyası eklenmelidir.
6. Dergide yayınlanan yazılar ayrıca elektronik ortamda (http://dergipark.gov.tr/hafebid/) yayımlanır.
7. Bireysel kullanım dışında, Haliç Üniversitesi Fen Bilimleri Dergisi'nde yayınlanan makaleler, şekiller ve tablolar yazılı izin olmaksızın çoğaltılamaz, bir sistemde arşivlenemez veya reklam ya da tanıtım amaçlı materyallerde kullanılamaz. Bilimsel makalelerde, uygun şekilde kaynak gösterilerek alıntılar yapılabilir.

Haliç Üniversitesi Fen Bilimleri Dergisi 2025, 8/1: 105-110
DOI:

YAZIM KLAVUZU

Çalışmanın Türkçe İsmi Her Kelimenin İlk Harfi Büyük (Bağlaçlar Hariç) ve "Times New Roman" Fontunda 14 Punto Olacak Şekilde

Birinci YAZAR[1*], İkinci YAZAR[2], Üçüncü YAZAR[1]

[1]Üniversite, Fakülte ve/veya Bölüm, Şehir, Ülke
ORCID ID: orcid.org/ 0000-0000-0000-0000
ORCID ID: orcid.org/ 0000-0000-0000-0000

[2]Üniversite, Fakülte ve/veya Bölüm, Şehir, Ülke
ORCID ID: orcid.org/ 0000-0000-0000-0000

Geliş Tarihi: XX.XX.20XX
***Sorumlu Yazar e mail:** xxx@xxx.xxx **Kabul Tarihi:** XX.XX.20XX
Atıf/Citation: Yazar, B., Yazar, İ., Yazar, Ü. "Çalışmanın Türkçe İsmi Her Kelimenin İlk Harfi Büyük (Bağlaçlar Hariç) ve "Times New Roman" Fontunda 14 Punto Olacak Şekilde", Haliç Üniversitesi Fen Bilimleri Dergisi 2025, 8/1: 105-110
Araştırma/ Derleme Makalesi / *Research/ Review Article*

Özet

Bu Microsoft Word belgesi Haliç Üniversitesi Fen Bilimleri Enstitüsü Müdürlüğü tarafından yayınlanan Fen Bilimleri Dergisi'ne gönderilecek olan makaleler için örnek olması amacıyla hazırlanmıştır. Dergimizde yayınlanmak üzere gönderilen makalelerin bu şablona göre düzenlenmeleri gerekmektedir. Özet kısmında çalışmanın yenilikleri ve temel bulguları vurgulanmalıdır. Türkçe ve İngilizce özet kısımları Times New Roman yazı tipi ile yazılmalı ve 10 punto büyüklüğü seçilmelidir. Yazım metni iki tarafa yaslanmalıdır. Özet bölümünün yazımında tek satır aralığı seçilmelidir. Makale özetinin 100 ila 200 kelime arasında olmasına dikkat edilmelidir. Türkçe ve İngilizce özetlerin 1 (bir) sayfayı geçmemesi gerekmektedir. Makalenin İngilizce olarak sunulmak istenmesi durumunda başlık, özet ve anahtar kelimelerin önce İngilizcelerinin sonra Türkçelerinin verilmesi gerekmektedir. Anahtar kelime sayısı en az 3 en fazla 6 olmalıdır.

Anahtar Kelimeler: Anahtar kelime 1, Anahtar kelime 2, Anahtar kelime 3.

Çalışmanın İngilizce İsmi Her Kelimenin İlk Harfi Büyük (Bağlaçlar Hariç) ve "Times New Roman" Fontunda 14Punto Olacak Şekilde

Abstract

Bu Microsoft Word belgesi Haliç Üniversitesi Fen Bilimleri Enstitüsü Müdürlüğü tarafından yayınlanan Fen Bilimleri Dergisi'ne gönderilecek olan makaleler için örnek olması amacıyla hazırlanmıştır. Dergimizde yayınlanmak üzere gönderilen makalelerin bu şablona göre düzenlenmeleri gerekmektedir. Özet kısmında çalışmanın yenilikleri ve temel bulguları vurgulanmalıdır. Türkçe ve İngilizce özet kısımları Times New Roman yazı tipi ile yazılmalı ve 10 punto büyüklüğü seçilmelidir. Yazım metni iki tarafa yaslanmalıdır. Abstract bölümünün yazımında tek satır aralığı seçilmelidir. Makale özetinin 100 ila 200 kelime arasında olmasına dikkat edilmelidir. Türkçe ve İngilizce özetlerin 1 (bir) sayfayı geçmemesi gerekmektedir. Makalenin İngilizce olarak sunulmak istenmesi durumunda başlık, özet ve anahtar kelimelerin önce İngilizcelerinin sonra Türkçelerinin verilmesi gerekmektedir. Anahtar kelime sayısı en az 3 en fazla 6 olmalıdır.

Keywords: Keywords 1 , Keywords 2 , Keywords 3.

1. Giriş

Ana metin, A4 kağıt boyutuna 2 cm kenar boşlukları ile 12 punto yazı büyüklüğünde Times New Roman yazı tipi ile 1 satır aralığı ve her iki yana yaslı şekilde yazılmalıdır. Ana bölüm başlıkları numaralandırılmalı, kelimelerin ilk harfleri büyük olmalı ve **koyu (bold)** karakterde yazılmalıdır. Ana bölüm başlığından sonra 1,5 satır aralıklı boşluk bırakılarak metne geçilmelidir. Başlıkla üst metin arasında da bir satır boşluk bırakılmalıdır. Paragraflar arasında boşluk bırakılmamalıdır. Çalışmanın İngilizce olarak sunulmak istenmesi durumunda bölüm başlığı "**Introduction**" olarak verilmelidir.

Bu bölümde çalışmayla ilgili yeterli literatür bilgisi verilmeli ve çalışmanın gerekçesi belirtildikten sonra amacı vurgulanmalıdır. Ancak konu ile ilgisi olmayan ve gereğinden fazla literatür bilgisi vermekten kaçınılmalıdır.

2. Materyal ve Metot

Bu bölümde, uygulanan yöntemler ve teknikler anlaşılır bir şekilde verilmeli ve metin "Times New Roman" yazı tipinde 12 punto büyüklüğünde ve tek satır aralıkla yazılmalıdır. Metinle ilgili olarak Giriş bölümünde yapılan açıklamalar bu bölüm için de geçerlidir. Başlıkta bağlaç haricindeki tüm kelimelerde ilk harf büyük yazılmalıdır.

Çalışmanın İngilizce olarak sunulmak istenmesi durumunda bölüm başlığı "**Material and Method**" olarak verilmelidir. Bölüm içerisinde alt bölüm başlıkları açılması mümkündür.

2.1. Materyal ve metot alt başlığı

Materyal ve metot bölümünde alt başlık altında bilgi verilmek istenmesi durumunda alt başlık "Times New Roman" yazı tipi, 12 punto ve kalın olarak yazılmalıdır. Alt başlığın ilk kelimesinin ilk harfi büyük, geri kalan kısmı ise küçük harflerle yazılmalıdır.

2.2. Şekiller, Tablolar ve Denklemler

Şekiller grafik, diyagram, fotoğraf, resim ve harita şeklinde olabilir. Şekil yazısı şeklin alt kısmına yazılmalıdır. Hem şekil hem de şekil yazısı sayfaya ortalanmalıdır. Şekil yazıları okunaklı olmalıdır. Şekil ile üst metin arasında 1 satır boşluk bırakılmalıdır. Şekil yazısı ile alt metin arasında da 1 satır boşluk bırakılmalıdır. Şekil yazısı 11 punto olarak yazılmalı ve aşağıdaki örnekte (Şekil 1) olduğu gibi verilmelidir. Metin içerisinde şekillere atıfta bulunulmalıdır.

Şekil 1. Örnek Resim

Tablolar açık çerçeveli tercih edilebilir. Tablo yazısı tablonun üst kısmına yazılmalıdır. Hem tablo hem de tablo yazısı sayfanın soluna

hizalanmalıdır. Tablo yazısı ile üst metin arasında 1 satır boşluk bırakılmalıdır. Tablo ile alt metin arasında 1 satır boşluk bırakılmalıdır. Tablo yazıları tercihen 11 punto ile yazılmalı ve tek satır aralığı seçilmelidir. Metin içerisinde tablolara atıfta bulunulmalıdır.

Tablo 1. Tablo Başlığı

Sütun Başlığı	Sütun Başlığı	Sütun Başlığı
Bilgi satırı	Bilgi satırı	Bilgi satırı
Bilgi satırı	Bilgi satırı	Bilgi satırı
Bilgi satırı	Bilgi satırı	Bilgi satırı
Bilgi satırı	Bilgi satırı	Bilgi satırı

Denklemler sırasıyla 1'den başlanarak numaralandırılmalıdır. Denklem sola yaslanarak yazılmalı ve denklem numarası sağ kenara yerleştirilmelidir. Denklem ile metin arasında üstten ve alttan birer satır boşluk bırakılmalıdır. Denklemler resim formatında olmamalıdır. Word denklem düzenleyicisi tercih edilebilir.

$$E=mc^2 \tag{1}$$

3. Bulgular

Bu bölümde çalışma sonucunda elde edilen bulgular çalışma sırasına göre sunulmalıdır. Çalışmanın İngilizce olarak sunulmak istenmesi durumunda bölüm başlığı "**Results**" olarak verilmelidir.

4. Tartışma

Bu bölümde, yapılan çalışmadan elde edilen bulgular bilimsel ilkelerin ışığı altında önceki verilerle karşılaştırılarak irdelenmelidir. İstenilmesi halinde, elde edilen bulgular ve bunların irdelenmesi **Bulgular ve Tartışma** başlığı altında da verilebilir.

5. Sonuçlar

Bu bölümde çalışmadan elde edilen özgün sonuçlar bir sıra dâhilinde sunulmalıdır. Çalışmanın İngilizce olarak sunulmak istenmesi durumunda bölüm başlığı "**Conclusions"** olarak verilmelidir.

Teşekkür

Bu bölümde, çalışmada yardım ya da destekleri bulunan kişi veya kişilere ya da kurum yetkililerine teşekkür edilebilir. Çalışmanın İngilizce olarak sunulmak istenmesi durumunda bu bölümün başlığı "**Acknowledgment**" olarak verilmelidir.

Kaynaklar

Çalışmada yararlanılan kaynaklar kullanım sırasına göre numaralandırılarak verilmelidir. Ancak Özet bölümünde kaynak gösterilmez. Kaynak numaraları köşeli parantez içerisinde gösterilmelidir. Kaynakların tamamı çalışmanın son sayfasındaki "Kaynaklar" başlığı altında, makale içerisindeki kullanım sırasına göre aşağıdaki örneklere uygun biçimde verilmelidir. Kaynaklar "Times New Roman" fontunda 10 punto olarak yazılmalıdır. Kaynak numaraları otomatik numaralandırma ile eklenmelidir ve her referans arasında 6 punto boşluk olmalıdır. Çalışmanın İngilizce olarak sunulmak istenmesi durumunda bölüm başlığı "**References**" olarak verilmelidir.

Periyodik yayınlar:

[1] Soyadı, A., Soyadı, B. B., ve Soyadı, C.,. Yayınlanan makalenin adı, Makalenin yayınlandığı dergi adı, Cilt ve sayı numarası 7(1), (yıl) sayfa numarası aralığı 1-12. Doi:

Kitaplar:

[2] Soyadı, A. A., Kitap adı, Yayınevi, Kitabın basıldığı yer, (yıl).

Sempozyum, Kongre, Bildiri:

[3] Soyadı, A., Soyadı, B. B., ve Soyadı, C., Yayınlanan bildirinin adı, Bildirinin yayınlandığı sempozyum kongre, toplantı ya da konferans adı (s. 1-12), (yıl, Ay), Şehir, Varsa üniversite veya kuruluş.

Tez:

[4] Soyadı, A. A., Yüksek Lisans veya Doktora tezinin adı, Tezin türü, Üniversite, Enstitü, (yıl).

Web sitesi:

[5] http://www.halic.edu.tr, (Erişim tarihi:).

Prof. Dr. Emine Esra KASAPBAŞI
Editör

Doç. Dr. Alireza SOURİ
Editör Yardımcısı

e-posta: fbd@halic.edu.tr http://dergipark.gov.tr/hafebid Haliç Üniversitesi Fen Bilimleri Dergisi
Haliç Üniversitesi, Güzeltepe Mahallesi, 15 Temmuz Şehitler Caddesi, No 15 34060 – İSTANBUL Tel: 212 924 24 44