

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DİJİTAL HAK YÖNETİMİ DESTEKLİ ÖZYİNELEMELİ İSTEK
YÖNLENDİRME YAKLAŞIMINA SAHİP AĞAÇ-TABANLI YENİ
BİR İÇERİK DAĞITIM AĞI MODELİ

DOKTORA TEZİ

Ahmet ŞANSLI

Bilgisayar ve Bilişim Mühendisliği Anabilim Dalı

HAZİRAN 2025

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DİJİTAL HAK YÖNETİMİ DESTEKLİ ÖZYİNELEMELİ İSTEK
YÖNLENDİRME YAKLAŞIMINA SAHİP AĞAÇ-TABANLI YENİ
BİR İÇERİK DAĞITIM AĞI MODELİ

DOKTORA TEZİ

Ahmet ŞANSLI

Bilgisayar ve Bilişim Mühendisliği Anabilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Tuğrul TAŞCI

HAZİRAN 2025

Ahmet ŞANSLI tarafından hazırlanan “Dijital Hak Yönetimi Destekli Özyinelemeli İstek Yönlendirme Yaklaşımına Sahip Ağaç-tabanlı Yeni Bir İçerik Dağıtım Ağı Modeli” adlı tez çalışması 18.06.2025 tarihinde aşağıdaki jüri tarafından oy birliği ile Sakarya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar ve Bilişim Mühendisliği Anabilim Dalı’nda Doktora tezi olarak kabul edilmiştir.





ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Sakarya Üniversitesi Fen Bilimleri Enstitüsü Lisansüstü Eğitim-Öğretim Yönetmeliğine ve Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesine uygun olarak hazırlamış olduğum “Dijital Hak Yönetimi Destekli Özyinelemeli İstek Yönlendirme Yaklaşımına Sahip Ağaç-tabanlı Yeni Bir İçerik Dağıtım Ağı Modeli” başlıklı tezin bana ait, özgün bir çalışma olduğunu; çalışmamın tüm aşamalarında yukarıda belirtilen yönetmelik ve yönergeye uygun davrandığımı, tezin içerdiği yenilik ve sonuçları başka bir yerden almadığımı, tezde kullandığım eserleri usulüne göre kaynak olarak gösterdiğimi, bu tezi başka bir bilim kuruluna akademik amaç ve unvan almak amacıyla vermediğimi ve 20.04.2016 tarihli Resmi Gazete’de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince Sakarya Üniversitesi’nin abonesi olduğu intihal yazılım programı kullanılarak Enstitü tarafından belirlenmiş ölçütlere uygun rapor alındığını, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun ortaya çıkması halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi beyan ederim.

18.06.2025

Ahmet ŞANSLI







TEŞEKKÜR

Doktora çalışmalarım boyunca engin bilgi ve tecrübelerini benden hiçbir zaman esirgemeyen, her adımda rehberliğini ve desteğini esirgemediğim yanımda olan kıymetli danışmanım Dr. Öğr. Üyesi Tuğrul TAŞCI'ya en içten teşekkürlerimi sunarım. Bilimsel yolculuğumda yalnızca akademik anlamda değil, aynı zamanda insani duruşuyla da bana örnek olmuştur.

Tezin hazırlanmasında desteklerini her zaman hissettiren tüm dostlarıma, özellikle de teşvikleriyle motivasyonumu artıran kıymetli arkadaşım Özkan Canay'a teşekkür ederim.

Bu zorlu süreçte her zaman yanımda olan, anlayışları, sabırları ve fedakarlıklarıyla bana güç veren sevgili eşime ve kıymetli çocuklarıma da sonsuz şükran borçluyum. Varlıkları, bu yolculuğu anlamlı ve değerli kılmıştır.

Ahmet ŞANSLI



İÇİNDEKİLER

Sayfa

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ	v
TEŞEKKÜR	ix
İÇİNDEKİLER	xi
KISALTMALAR	xiii
SİMGELER	xv
TABLO LİSTESİ	xvii
ŞEKİL LİSTESİ	xix
ÖZET	xxi
SUMMARY	xxiii
1. GİRİŞ	1
1.1. Problemin Tanımı ve Gerekçe	5
1.2. Amaç ve Kapsam	8
1.3. Tezin Özgün Katkıları	9
1.4. Tezin Organizasyonu	12
2. TEMEL KAVRAM, SİSTEM VE ALTYAPI BİLEŞENLERİ	15
2.1. İlgili Ağ Altyapısı ve Teknolojileri	16
2.2. Dijital Hak Yönetimi (DRM)	18
2.2.1. DRM türleri	19
2.2.2. DRM mimarisi ve bileşenleri	25
2.3. İçerik Dağıtım Sistemleri	31
2.3.1. İçerik dağıtım sistemi altyapı bileşenleri	38
2.3.1.1. Content placement	43
2.3.1.2. Request routing	46
2.3.1.3. Network infrastructure	47
2.4. Ağ Simülasyon Araçları	49
2.4.1. Popüler ağ simülasyon araçları	50
2.4.2. Kullanım amaçları ve sınırlılıkları	51
2.5. Ağ Gecikmesi ile İlgili Kavramlar	52
3. LİTERATÜR ARAŞTIRMASI VE ÖNCEKİ ÇALIŞMALAR	55
3.1. Dijital Hak Yönetimi (DRM)	56
3.2. İçerik Dağıtım Ağları (CDN)	58
3.3. Simülasyon Araçları	61
4. ÖNERİLEN İÇERİK DAĞITIM AĞI MODELİ VE MİMARİSİ	65
4.1. Önerilen Sistem Mimarisi ve Bileşenleri	67
4.1.1. İçerik ve kullanıcı hakları hazırlık süreci	68
4.1.2. Altyapı kurulum ve dağıtım süreci	68
4.1.3. Ağaç tabanlı sunucu mimarisi	69
4.1.4. Son kullanıcı istek ve yönlendirme süreci	69
4.2. TBCDN: Ağaç Tabanlı İçerik Dağıtım Sistemi	70
4.2.1. Genel CDN topolojisi ve işleyişi	71
4.2.2. TBCDN topolojisi	73

4.2.3. Recursive request routing yaklaşımı	74
4.3. EDU-DRM Sistemi: Dijital Hak Yönetimi Süreci	76
4.3.1. Rol tabanlı erişim ve hak modelleri	81
4.3.2. Modüler mimari: lisans sunucusu, içerik sunucusu, şifreleme.....	87
4.3.3. Güvenlik katmanları ve erişim denetimi	93
4.4. Toplam Uçtan Uca Ağ Gecikmesi.....	94
4.4.1. TBCDN mimarisinde gecikme modellemesi ve karşılaştırmalı analiz	96
5. DENEYSEL ORTAM, BULGULAR VE DEĞERLENDİRME.....	99
5.1. Prototip Sistem Kurulumu ve Test Ortamı	99
5.2. EDU-DRM Gerçekleme Süreci	102
5.2.1. Sağlayıcılar, kullanıcı – içerik dijital hak tanımlamaları	102
5.2.2. Yetkilendirme, lisanslama	104
5.2.3. İçerik dağıtım süreci ile etkileşim	105
5.3. Ağaç Tabanlı İçerik Dağıtım Ağı Gerçekleme Süreci	106
5.3.1. Veri seti	107
5.3.2. Performans ölçütleri ve metodoloji	108
5.3.3. TBNS: tree-based network simulator	111
5.3.3.1. TBNS'in geliştirilme gerekçesi ve kapsamı	111
5.3.3.2. Arayüz özellikleri ve parametre tanımı	112
5.3.3.3. Simülasyon ortamı ve yazılım yığını	114
5.4. Deneysel Çalışma Sonuçları ve Değerlendirme	114
5.4.1. XML – bit tabanlı kullanıcı yetkilendirme karşılaştırmaları.....	115
5.4.2. İçerik dağıtım ağı transfer süresi karşılaştırmaları	116
5.4.2.1. Mini senaryo: 2^3 istek, 3 içerik.....	118
5.4.2.2. Gerçek hayat senaryosu: $\sim 2^{23}$ istek, 5^1 - 5^3 içerik	119
6. SONUÇLAR VE ÖNERİLER.....	121
KAYNAKLAR.....	125
ÖZGEÇMİŞ.....	139

KISALTMALAR

AB	: Avrupa Birliđi
AES	: Advanced Encryption Standart
ASF	: Advanced Systems Format
AXMEDIS	: Automated Cross-Media Content Distribution
BGP	: Border Gateway Protocol
CDN	: Content Delivery Networks
CDNaaS	: Content Delivery Networks as a Service
CDNSim	: Content Delivery Network Simulator
CID	: Content Identifier
CoDaaS	: Content-Delivery-as-a-Service
CORAL	: Content Object Rights and License
CPU	: Central Processing Unit
DASH	: Dynamic Adaptive Streaming over HTTP
DID	: Digital Item Declaration
DLT	: Distributed Ledger Technology
DMAG	: Distributed Multimedia Applications Group
DoS	: Denial of Service
DRM	: Digital Rights Management
EDU-DRM	: Educational Digital Rights Management System
FIFO	: First In First Out
FNCTB	: Fusion Net Cache Test Bed
GEANT	: Gigabit European Academic Network
GUI	: Graphical User Infercace
HLS	: HTTP Live Streaming
ICN	: Information Centric Networking
İDA	: İçerik Dağıtım Ađı
IETF	: Internet Engineering Task Froce
ISP	: Internet Service Provider
LAN	: Local Area Network
LIFO	: Last In First Out

MIPAMS	: Multimedia Information Protection and Management System
MOSES	: MPEG Open Security for Embedded Systems
MPEG	: Moving Picture Experts Group
NFV	: Network Function Virtualization
NS-2	: Network Simulator (Version 2)
NS-3	: Network Simulator (Version 3)
ODRL	: Open Digital Resource Library
OMA	: Open Mobile Alliance
OMNET++	: Objective Modular Network Testbed in C++
OpenSDRM	: Open and Secure Digital Rights Management
OPNET	: Optimized Network Engineering Tools
P2P	: Peer to Peer
QoE	: Quality of Experience
RAM	: Random Access Memory
REL	: Right Expression Language
RLWE	: Ring Learning With Errors
RRR	: Recursive Request Routing
RSA	: Rivest–Shamir–Adleman
RTT	: Round-trip Time
SDCDN	: Software Defined Content Delivery Network
SDN	: Software Defined Network
TBCDN	: Tree-based Content Delivery Network
TBNS	: Tree-based Network Simulator
TCP	: Transmission Control Protocol
TreeDN	: Tree-Based CDN for Live Streaming to Mass Audiences
TTP	: Trusted Third Parties
UAV	: Unmanned Aerial Vehicle
VANET	: Vehicular Ad-hoc Network
VANUG	: Virginia Network User Group
WAN	: Wide Area Network
WMA	: Windows Media Audio
WMRM	: Windows Media Rights Manager
WMV	: Windows Media Video
XML	: Extensible Markup Language

SİMGELER

us : Mikro saniye





TABLO LİSTESİ

Sayfa

Tablo 4.1. EDU-DRM için belirlenmiş erişim türleri.	79
Tablo 4.2. Sistemde tanımlanan roller ve yetkilendirme kodları.	80
Tablo 4.3. İçeriklere bağlı erişim vektörü örneği.	82
Tablo 5.1. Veri seti örneği.....	108





ŞEKİL LİSTESİ

Sayfa

Şekil 1.1. Küresel dijital ekosistem göstergeleri.....	7
Şekil 2.1. Kullanıcı Taleplerinin Zaman İçindeki Değişimi.....	15
Şekil 2.2. Bir DRM sisteminin temel bileşenleri	26
Şekil 4.1. TBCDN Sistem Mimarisi Şeması.....	68
Şekil 4.2. Geleneksel CDN Mimarisi	72
Şekil 4.3. Recursive Request Routing Algoritması	75
Şekil 4.4. EDU-DRM Sisteminin Servis Tabanlı Mimarisi.....	88
Şekil 4.5. Bir kullanıcının içerik talebine ilişkin akış diyagramı.....	91
Şekil 5.1. Bit ve XML tabanlı yetkilendirme yöntemleri test diyagramı.....	101
Şekil 5.2. XML ve Bit bazlı Kimlik Doğrulama ve Yetkilendirme Olayları.....	109
Şekil 5.3. TBNS Simülatör Arayüzü	114
Şekil 5.4. EDU-DRM ile XML tabanlı yetkilendirme karşılaştırmalı sonuçları	116
Şekil 5.5. Ortalama transfer süresi kıyaslaması	117
Şekil 5.6. Ağ Yüğü Analizi ve Karşılaştırması.....	118



DİJİTAL HAK YÖNETİMİ DESTEKLİ, ÖZYİNELEMELİ İSTEK YÖNLENDİRME YAKLAŞIMINA SAHİP AĞAÇ-TABANLI YENİ BİR İÇERİK DAĞITIM AĞI MODELİ

ÖZET

Dijital içerik dağıtım teknolojilerindeki gelişmeler, yüksek bant genişliğini yaygın biçimde erişilebilir kılmıştır. Bugün kullanılan dağıtım yöntemlerin önemli bir kısmı, güvenliği artırırken performans ve ölçeklenebilirlikten ödün vermekte; performansı öne çıkaran yaklaşımlar ise veri güvenliği ve erişim denetimi bakımından yetersiz kalmaktadır. Bu tez, söz konusu açmazı aşmak için güvenlik ve performansı eşzamanlı olarak sağlayan bütünlük bir mimari önermektedir.

Önerilen çözüm bit tabanlı erişim modeliyle çalışan dijital hak yönetimi katmanı olan EDU-DRM ve özyinelemeli istek yönlendirme algoritmasıyla desteklenen ağa tabanlı içerik dağıtım ağı olan TBCDN adlı iki ana bileşenden oluşmaktadır. EDU-DRM, kullanıcı ve içerik haklarını sekiz bitlik erişim vektörleriyle temsil etmekte; bu sayede yetkilendirme kararları daha kısa sürede verilebilmektedir. Geleneksel XML tabanlı yöntemlere kıyasla işlem maliyeti kayda değer biçimde azalmaktadır. Deneysel sonuçlar, EDU-DRM'in yetkilendirme süresini %40'a kadar kısalttığını ve CPU kullanımında belirgin düşüş sağladığını göstermektedir. Böylece, yüksek kullanıcı yoğunluğu altında bile sistemin yanıt verebilirliği korunmaktadır.

TBCDN mimarisi, geleneksel CDN yöntemlerine göre ani gelişen yüksek hacimli istekleri çok daha düşük uçtan uca gecikme değerleri elde etmektedir. Tekrarlayan kullanıcı taleplerinin yalnızca 1–2 düğüm üzerinden karşılanabilmesi, geleneksel CDN'lerde gözlemlenen 3–6 düğümlük yol uzunluklarına kıyasla ciddi bir avantaj yaratmaktadır. Bu yaklaşım, hem ortalama transfer süresini %25–35 oranında azaltmakta hem de toplam ağ trafiğini %40'a kadar düşürmektedir. Özellikle milyonlarca isteğin işlendiği yüksek yoğunluklu senaryolarda bile sistemin istikrarlı performans sergilediği gözlemlenmiştir.

Bütün bu performans değerlendirmeleri, TBNS olarak isimlendirilen özel olarak geliştirilen simülasyon aracı kullanılarak gerçekleştirilmiştir. TBNS, önerilen mimariyi gerçekçi trafik koşullarında test edebilmek için geliştirilmiş parametrik bir simülasyon ortamıdır. Araç, 2^{23} 'e kadar kullanıcı isteğini işleyebilmekte, ani gelişen yüksek hacimli trafik desenlerini modelleyebilmekte ve farklı içerik dağıtım yöntemlerini karşılaştırmaya olanak tanımaktadır. Böylelikle önerilen mimarinin yalnızca teorik olarak değil, deneysel olarak da güçlü bir doğrulanması yapılmıştır.

Sonuçlar bütüncül olarak değerlendirildiğinde, EDU-DRM ve TBCDN bileşenlerinin birlikte çalışması, içerik güvenliğini garanti altına almakta ve ağ performansını optimize etmektedir. Bu yönüyle tez, dijital hak yönetimi ve içerik dağıtım ağlarını bütünlük biçimde ele alan ve deneysel olarak doğrulanmış özgün bir çözüm ortaya koymaktadır.



A NOVEL DRM-ENABLED CONTENT DELIVERY NETWORK MODEL BASED ON TREE STRUCTURE AND RECURSIVE REQUEST ROUTING

SUMMARY

Recent advances in digital content distribution technologies have made high bandwidth widely accessible. While these advances make it technically possible to deliver content to a large number of users simultaneously, two fundamental problems remain to be solved: the protection of personal data and the secure delivery of copyrighted material. Existing infrastructures are insufficient to meet both needs simultaneously, increasing security leads to performance loss, while improving performance leads to security vulnerabilities.

This thesis comprehensively addresses these bottlenecks and proposes a unique solution that combines security and scalability. The work centres on two key components: a bit-level access-based Digital Rights Management architecture called EDU-DRM, and a recursive request-routed tree-based content delivery network called TBCDN. Working together, these two structures ensure that content is only accessible to authorised users, while also providing low latency and balanced network load under heavy concurrent traffic.

Traditional DRM solutions use XML-based schemas to control access to content. However, these methods involve multi-step authentication and complex policy evaluation processes, leading to significant delays during high user traffic. On the other hand, CDN-based distribution approaches are successful in accelerating content access but are insufficient in protecting copyrights and ensuring that content is viewed only by authorised individuals.

Therefore, there is a noticeable lack of a unified solution in the literature that guarantees both security and performance. This thesis addresses precisely this gap; it integrates these two areas by redesigning the DRM and CDN layers as separate but cooperating modules.

The first component of the thesis, EDU-DRM, is built on 8-bit access vectors that compactly represent user and content rights. Each bit represents an independent access privilege: fundamental permissions such as online viewing, controlled downloading, time-limited offline use, printing quotas, note-taking, device binding, internal sharing, and screen capture protection can be defined within this structure.

Thanks to this design, the comparison between the user's vector and the rights vector associated with the content object can be performed in constant time ($O(1)$), thus enabling instant authorisation decisions. Compared to the schema validation and query costs of XML-based methods, EDU-DRM offers a significant efficiency advantage. Experimental findings show that EDU-DRM provides up to a 40% reduction in processing time and a significant decrease in CPU load.

EDU-DRM also adopts a status-based licensing approach. Licences are not time-based but depend on the user's system status. Thus, the relationship between the content and

the user is defined in an irreversible manner; access rights are only updated in cases such as role changes, subscription renewals, or device pairing. This approach goes beyond time-based restrictions and maintains access integrity throughout the content's lifecycle.

The second component of the thesis, TBCDN (Tree-Based Content Delivery Network), is designed to overcome the scalability and load balancing limitations of traditional CDN and cache-proxy methods. In classic CDN logic, the user receives content from the nearest node. However, when there is no direct connection between nodes, the content first goes up to higher levels and is then directed to the side node. This increases the path length, increases latency, and intensifies the load on the network.

TBCDN solves this problem with its recursive request routing (RRR) algorithm. The algorithm can fulfil recurring user requests via only 1–2 nodes, whereas classic CDN structures require passing through 3–6 nodes for the same content. As a result, TBCDN reduces the average transfer time by 25–35 per cent and decreases total network traffic by up to 40 percent. This difference is even more pronounced in high-density scenarios where millions of concurrent requests are processed.

To validate the proposed architecture, TBNS (Tree-Based Network Simulator) was developed as part of the thesis. TBNS can test both EDU-DRM and TBCDN components in a parametric manner; it can also perform fair comparisons with server-client, cache-proxy, and traditional CDN methods.

The key features of TBNS are as follows: Scalability up to 2^{23} (8M) user requests, Ability to model rapidly emerging high-volume traffic patterns, Scenario flexibility based on tree depth, content diversity, and request intensity, Analysis of outputs in CSV format using Pandas/Matplotlib.

Thanks to this tool, theoretical models could be tested under realistic traffic conditions, and the performance gains of the proposed architecture were demonstrated in a concrete manner.

Two levels of experiments were conducted in the study. Mini Scenario (8 requests, 3 contents): In this scenario, supported by visual streams, it was observed that TBCDN delivered content via a much shorter path compared to a classic CDN and reduced the transfer time by nearly half. Realistic Scenario (~8 million requests, 120 pieces of content): In these large-scale experiments, it was found that TBCDN reduced the average transfer time by 25–35% and decreased the total network load by up to 30%. While the server-client model created bottlenecks under high load, the cache-proxy lost its effectiveness as the scale increased. Although the classic CDN was successful in load distribution, it exhibited weaknesses in terms of security and licensing integrity. In contrast, TBCDN provided the lowest latency and the most balanced network load without compromising security.

The main contributions of the thesis to the literature are as follows. EDU-DRM: A bit-level rights management model that can operate in fixed time. TBCDN: A tree-based CDN architecture that provides latency and load optimisation through recursive routing. TBNS: A specialised test infrastructure that realistically simulates high-traffic scenarios.

Among the limitations is that the experiments were conducted with specific hardware configurations and traffic models. Different user behaviours or geographical distributions in the real world may produce different results.

In conclusion, this thesis presents a novel architecture that integrates the DRM and CDN domains. EDU-DRM provides secure, controllable, and low-cost access, while TBCDN ensures low-latency, balanced, and scalable distribution. Experimental findings demonstrate that the system offers significant advantages over existing methods in terms of both security and performance.

In the future, performance could be further enhanced by incorporating artificial intelligence-based adaptive caching algorithms into TBCDN and adding next-generation approaches such as blockchain-based licensing and homomorphic encryption to EDU-DRM. Furthermore, field tests in different geographical regions could be conducted to examine the system's behaviour in large-scale and heterogeneous network environments in greater detail.





1. GİRİŞ

Bilginin dağıtımı, tarih boyunca toplumsal ilerlemenin temel itici güçlerinden biri olmuştur. Antik dönemlerde sözlü anlatımlar ve yazılı belgeler aracılığıyla başlayan bu süreç, matbaanın icadıyla büyük bir ivme kazanmış ve geniş topluluklara bilgi ulaştırılmasını mümkün kılmıştır. Günümüzde ise bilgi, büyük ölçüde sayısal ortamlarda üretilmekte, saklanmakta ve paylaşılmaktadır.

Bilginin dijital formata dönüştürülmesi hem depolama olanakları hem de paylaşım kapasitesi açısından devrimsel bir dönüşüm yaratmıştır. Bu süreçte en kritik rolü ise internet teknolojileri üstlenmiştir. İnternetin küresel ölçekte yaygınlaşması, bilginin sınırlar ötesi dolaşımını kolaylaştırarak hem bireysel hem de kurumsal erişim imkanlarını radikal biçimde dönüştürmüştür.

Bu dijital dönüşüm, bilginin dağıtımında otomatikleşmiş sistemlerin gelişmesini de beraberinde getirmiştir. Kamu ve özel sektörde yaygınlaşan e-Devlet, e-öğrenme ve e-sağlık gibi “e-” sistemleri; bilginin sistematik, hızlı ve güvenli bir biçimde paydaşlara ulaştırılmasını sağlamaktadır. Mobil cihazların ve taşınabilir teknolojilerin gelişimiyle birlikte, bilgiye her yerden erişim mümkün hale gelmiş; böylece bilgi paylaşımı zamansal ve mekânsal sınırlamalardan büyük ölçüde arınmıştır.

Ancak bu yüksek erişilebilirlik düzeyi, özellikle telif hakkına tabi ya da hassas nitelik taşıyan içeriklerin yetkisiz paylaşımı açısından önemli güvenlik risklerini de beraberinde getirmiştir. Bu bağlamda, dijital hak yönetimi (Digital Rights Management – DRM) sistemleri, sayısal içeriklerin korunması ve yetkisiz erişimin engellenmesi için geliştirilen temel teknolojik çözümler haline gelmiştir.

Sayısallaşma, bir yandan bilgiye erişimi demokratikleştirirken diğer yandan içerik üreticilerinin fikri mülkiyet haklarını tehdit eden bir ortam yaratmaktadır. Bu nedenle, modern bilgi dağıtım altyapılarında hem erişim kolaylığı hem de içerik güvenliği stratejilerinin eşzamanlı olarak ele alınması zorunludur. Dijital materyallerinin yaygınlaşması, bu içeriklerin telif hakkı ile korunması ve yetkisiz kullanımlara karşı güvence altına alınması gereğini doğurmuştur.

DRM sistemleri, dijital içeriklere yetkisiz erişimi önleyen politikaların kriptografik olarak icra edilmesini sağlamaktadır. Bununla birlikte, klasik DRM kurgularının çoğu sabit ve öngörülebilir talep profilleri varsayılarak tasarlanmaktadır. Oysa modern dijital ekosistemlerde talepler, patlamalı eşzamanlılık, zamana bağlanmış erişim kümelenmeleri ve ağır kuyruk uçları üreten dalgalı yükler şeklinde gerçekleşmektedir. Bu dalgalanmaların yeterince kontrol edilemediği durumlarda, uçtan uca gecikmeler artmakta, hizmet kalitesi ve sistem kararlılığı zayıflatılmaktadır.

Dolayısıyla, içerik dağıtım senaryoları için sadece güvenli değil, aynı zamanda esnek, gecikmesiz ve yüksek erişim kapasitesine sahip mimarilere ihtiyaç vardır. Bu bağlamda, merkezi yapılarla çalışan geleneksel dağıtım sistemleri yetersiz kalmakta; bunun yerine dağıtık mimarilere dayalı yeni nesil dijital içerik dağıtım yönetim sistemlerinin geliştirilmesi gerekmektedir.

Bu ihtiyaca cevap verebilecek teknolojilerden biri, içerik dağıtım ağlarıdır (Content Delivery Networks – CDN). CDN mimarileri, içerikleri farklı coğrafi bölgelerdeki sunuculara önbelleğe alarak, kullanıcıların içeriklere en yakın düğümlerden erişmesini sağlar. Bu yöntem, medya akışları ve yazılım güncellemeleri gibi yüksek ölçekli kullanım senaryolarında yaygın biçimde uygulanmakta olup, aynı zamanda kritik erişim performansı gerektiren dinamik içeriklerin yönetiminde de önemli performans iyileştirmeleri sunma potansiyeline sahiptir.

Bununla birlikte, dijital içerik yalnızca video veya statik dokümanlardan ibaret olmayıp; çoğu durumda erişim haklarıyla sınırlandırılmış, kullanıcıya özgü kurgulanmış ve şifrelenmiş öğelerden oluşmaktadır. Bu durum, klasik CDN mimarilerinin ötesine geçilerek, DRM uyumlu ve bağlama özgü olarak özelleştirilmiş güvenlik protokollerinin desteklenmesini zorunlu kılmaktadır. Bu bağlamda, iletim sırasında ve istemci tarafında içerik bütünlüğünün korunabilmesi için şifreleme, erişim kontrolü ve kimlik doğrulama gibi çok katmanlı mekanizmaların eşgüdümlü biçimde çalıştırılması gerekmektedir.

Bu tür sistemler, mikro servis tabanlı mimarilerle modüler hale getirilebilmekte; yük dengeleme, erişim kontrolü, içerik güncelleme ve kimlik doğrulama işlemleri otonom servisler aracılığıyla yürütülebilmektedir. Ayrıca, uç bilişim prensipleri kullanılarak içeriklerin kullanıcılara fiziksel olarak en yakın düğümlerden sunulması

sağlanabilmektedir. Bu sayede uçtan uca gecikmeler azaltılmakta, merkezi sunucular üzerindeki işlem yükü ise hafifletilmektedir.

Sonuç olarak, dijital içeriklerin güvenliğinin korunması ve geniş kitlelere etkin biçimde ulaştırılabilmesi için, klasik DRM çözümlerinin ötesine geçen; dağıtık, güvenli ve esnek niteliklere sahip yeni nesil içerik dağıtım mimarilerinin geliştirilmesi gerekli görülmektedir. Gelecekteki dijital hizmet altyapıları, yüksek erişilebilirlik ve güvenlik gereksinimlerini eşzamanlı olarak karşılayabilen bu tür bütünleşik sistem tasarımları ile şekillenecektir.

Günümüz dijital ekosistemleri, yalnızca içerik üretim ve paylaşım süreçleri açısından değil, aynı zamanda teknolojik altyapılar ve güvenlik stratejileri bakımından da derin bir dönüşüm geçirmektedir. Bu dönüşüm, dijital içeriklerin salt sayısal ortamlara aktarımıyla sınırlı kalmamakta; aynı zamanda bu içeriklere erişim yöntemlerini, kullanıcı yetkilendirme mekanizmalarını ve ağ altyapısına ilişkin mimari yapılanmaları da yeniden tanımlamaktadır. Özellikle geniş ölçekli kullanıcı topluluklarının, çok sayıda dijital kaynağa eşzamanlı ve merkezi platformlar üzerinden erişebilmesi hem sistemlerin esnekliğini artırmakta hem de içeriklerin güncel ve merkezi biçimde yönetilebilmesini mümkün kılmaktadır. Ancak bu kazanımlar, içeriklerin telif haklarına uygun biçimde yalnızca yetkili kullanıcılar tarafından erişilebilir olması ve bu içeriklerin aynı anda yüksek kullanıcı yoğunluklarına gecikmesiz ve sürdürülebilir biçimde sunulabilmesi gibi iki temel teknik gereksinimi de zorunlu kılmaktadır (Medina ve Tnibar-Harrus, 2023; Arrufat ve ark., 2019; Macedo ve ark., 2020; Gebeyew ve ark., 2024).

Birinci gereksinim dijital içeriklerin yalnızca önceden yetkilendirilmiş kullanıcılar tarafından ve tanımlanmış lisans koşulları çerçevesinde erişilebilir olması, temel güvenlik zorunluluklarından biridir. Özellikle telif hakkına tabi dijital varlıkların izinsiz çoğaltımı, yaygın paylaşımı ve dağıtımı; hem içerik üreticilerinin fikri mülkiyet haklarını ihlal etmekte hem de içerik sağlayıcıların sürdürülebilir iş modellerini tehdit etmektedir (Bhatt ve ark., 2009; Chang ve ark., 2010; Burnett ve ark., 2005). Bu bağlamda, içerik güvenliğini sağlayacak teknolojik önlemler, modern dijital ekosistemler için kaçınılmaz bir gereklilik haline gelmektedir (Barakova ve ark., 2024; Özmen ve ark., 2019; Arrufat ve ark., 2021; Heverin ve ark., 2024). Bu gereksinime yanıt olarak geliştirilen DRM sistemleri, erişim haklarını kullanıcı bazında tanımlayarak dijital materyallerin yalnızca yetkilendirilmiş kullanıcılar tarafından ve

sistemce belirlenmiş koşullar altında tüketilmesini sağlamaktadır (Iannella, 2004; Irwin, 2004; Becker ve ark., 2003). Özellikle lisanslı fakat erişime açık dijital varlıkların yönetiminde, bu tür çok katmanlı çözümler hem içerik bütünlüğünün korunması hem de lisanslama süreçlerinin sürdürülebilir biçimde yürütülmesi açısından kritik öneme sahiptir. Bununla birlikte, mevcut DRM sistemlerinin önemli bir bölümü ticari medya platformlarına yönelik sabit kullanım senaryolarına odaklanmakta; dinamik kullanıcı profilleri ve yüksek yoğunluklu talep koşulları karşısında ölçeklenebilir ve esnek çözümler sunmakta sınırlı kalmaktadır (Choi ve ark., 2016; Kubesch ve Wicker, 2015; Han ve Liu, 2024). Bu noktada, güvenliğin yanı sıra performans boyutu da ikinci bir gereksinim olarak ortaya çıkmaktadır.

İkinci gereksinim dijital içeriklerin güvenliğinin sağlanmasının yanı sıra, bu içeriklerin performans açısından erişilebilirliğinin de garanti altına alınması gerekmektedir. Özellikle yüksek yoğunluklu ve eşzamanlı erişim profilleri altında, milyonlarca kullanıcının aynı kaynaklara aynı anda erişim talebinde bulunabildiği senaryolarda bu gereksinim belirginleşmektedir (Ma ve ark., 2017; Jin ve ark., 2014). Bu tür ani ve yoğun talepler karşısında, klasik sunucu–istemci tabanlı sistemler yetersiz kalmakta; ağ tıkanmaları, sistem gecikmeleri ve erişim kesintileri ortaya çıkmaktadır (Gupta ve Garg, 2015). Bu soruna yanıt olarak geliştirilen CDN yapıları, içeriklerin ön belleğe alınarak coğrafi olarak kullanıcılara en yakın noktalardan sunulmasını sağlayan mimariler olarak öne çıkmaktadır (Sahoo ve ark., 2017). CDN mimarileri ağ trafiğini azaltmakta, kullanıcıların bekleme sürelerini kısaltmaktadır. Ancak bu çözümler yoğunlukla statik içerik dağıtımına odaklanmakta ve sabit yoğunluk senaryoları için optimize edilmektedir. Dinamik talep desenlerinin, yüksek kullanıcı sayısının ve içerik tekrar kullanımının yoğun olduğu ortamlarda ise geleneksel CDN çözümleri istenen verimliliği sunmakta sınırlı kalmaktadır (Zhang ve ark., 2022).

Bu tez çalışması, dijital içeriklerin güvenliğini ve erişim performansını eşzamanlı olarak sağlayabilecek bütünlüklü bir sistem mimarisi geliştirmeyi hedeflemektedir. Günümüzdeki dijital hizmet altyapıları, hem içeriklerin telif haklarına uygun biçimde korunmasını hem de bu içeriklerin çok büyük kullanıcı topluluklarına kesintisiz ve ölçeklenebilir biçimde sunulmasını zorunlu kılmaktadır. Mevcut çözümlerin çoğu ya yalnızca güvenliğe ya da yalnızca performansa odaklanmakta; bu durum, bütüncül çözüm üretimini sınırlamaktadır. Tez kapsamında sunulan yaklaşım, söz konusu iki

temel gereksinimi aynı çerçevede birlikte karşılayan ve literatürdeki boşluğu dolduran özgün bir çözüm modeli ortaya koymaktadır.

Tez kapsamında geliştirilen sistem üç ana bileşenden oluşmaktadır: EDU-DRM, TBCDN ve TBNS. EDU-DRM, dijital içeriklerin yalnızca yetkilendirilmiş kullanıcılar tarafından ve tanımlanmış kurallar çerçevesinde erişilebilmesini sağlayan bir dijital hak yönetimi altyapısı olarak tasarlanmaktadır. Bu yapıda erişim hakları, bit tabanlı erişim vektörleri aracılığıyla kodlanmakta ve rollerle ilişkilendirilmektedir. TBCDN ise aynı içeriklerin yüksek ölçekli kullanıcı topluluklarına gecikme yaşanmadan ulaştırılmasını amaçlayan, beş seviyeli hiyerarşik yapıya sahip bir içerik dağıtım ağı olarak konumlanmaktadır. Bu yapı, tekrar eden içerik taleplerini yerel düğümler üzerinden karşılayarak hem ağ yükünü azaltmakta hem de erişim sürelerini kısaltmaktadır. Her iki sistem de modüler olarak bağımsız çalışabilir nitelikte olmakla birlikte, birlikte kullanıldıklarında ortaya çıkan sinerji, güvenlik ve performansın aynı anda talep edildiği ortamlarda kritik önem taşımaktadır.

Bu mimari yalnızca kavramsal bir öneri değil; aynı zamanda özel olarak geliştirilen Tree-Based Network Simulator (TBNS) aracılığıyla uygulanabilirliği test edilmiş bir yapıdır. Simülasyon sonuçları, klasik sunucu–istemci tabanlı sistemlere kıyasla EDU-DRM ve TBCDN bileşenlerinin bütünleşik kullanımının gecikme süresi, eşzamanlı kullanıcı kapasitesi ve ağ trafiği açısından anlamlı kazanımlar sağladığını ortaya koymaktadır. Literatürde yoğunlukla ayrı ayrı ele alınan DRM ve CDN teknolojilerinin bütünleşik bir çerçevede bir araya getirildiği bu çözüm mimarisi hem akademik katkı hem de pratik uygulanabilirlik açısından özgün bir nitelik taşımaktadır.

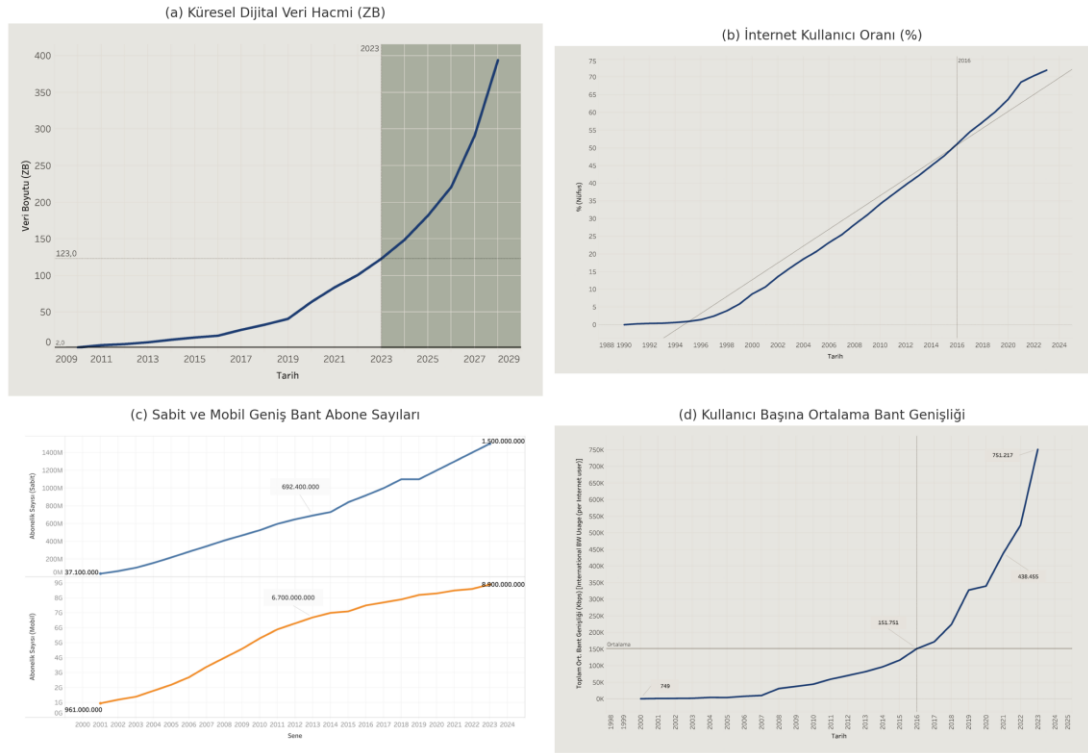
1.1. Problemin Tanımı ve Gerekçe

Son yirmi yılda bilgisayar ve iletişim teknolojilerinde yaşanan hızlı gelişmeler, bilginin üretilme, işlenme ve dağıtım biçimlerini köklü şekilde dönüştürmektedir. Masaüstü sistemlerden mobil cihazlara, giyilebilir teknolojilerden bulut tabanlı servis altyapılarına kadar uzanan yenilikler, bireylerin ve kurumların dijital veriyle etkileşim yöntemlerini yeniden tanımlamaktadır. Bu dönüşümün doğal bir sonucu olarak, dijital içerikler giderek daha fazla çoklu ortam öğeleriyle zenginleştirilmiş formatlarda sunulmakta; bu içeriklerin geniş ölçekli kullanıcı topluluklarına ulaştırılması ise dijital yayıncılık altyapıları üzerinden gerçekleştirilmektedir.

Ancak dijital içeriklerin bu denli yaygın biçimde erişilebilir olması, beraberinde ciddi güvenlik ve hak yönetimi sorunlarını da gündeme getirmektedir. Özellikle telif hakkı ihlalleri, izinsiz çoğaltım ve kişisel verilerin korunması gibi konular, dijital yayıncılığın güvenlik boyutunu ön plana çıkarmaktadır. Dijital içeriklerin güvenli ve kontrollü biçimde sunulması hem hukuki yükümlülükler hem de sürdürülebilir içerik ekosistemlerinin tesisi açısından kritik bir zorunluluk haline gelmektedir. Bu gereklilik, DRM sistemlerinin dağıtım altyapılarına entegrasyonunu zorunlu kılmaktadır. Bununla birlikte, büyük ölçekli kullanıcı tabanlarına hizmet vermesi öngörülen sistemlerde yalnızca hak yönetiminin sağlanması yeterli olmamakta; aynı zamanda performans ve ölçeklenebilirlik gereksinimlerinin de garanti altına alınması gerekmektedir.

Bu noktada, DRM sistemleri ile içerik dağıtım ağları arasındaki yapısal farklılıklar, yeni mimari tasarım yaklaşımlarını zorunlu kılmaktadır. DRM sistemleri, içeriklerin yalnızca yetkilendirilmiş kullanıcılar tarafından erişilebilmesini ve izinsiz çoğaltım veya dağıtım gibi işlemlerin engellenmesini sağlayan güvenlik temelli çözümler sunmaktadır. Buna karşılık CDN yapıları, yüksek kullanıcı yükünü dengelemek ve ağ üzerinden düşük gecikmeli erişimi sağlamak amacıyla geliştirilmiş dağıtım odaklı sistemler olarak konumlanmaktadır. Ancak, bu iki gereksinim çoğu zaman eşzamanlı olarak ortaya çıkmakta ve yalnızca tek taraflı çözümler bütünsel verimlilik sağlayamamaktadır. Özellikle ani, yoğun ve eşzamanlı erişim taleplerinde klasik DRM sistemlerinin performans darboğazlarına sürüklendiği, Amoozegar ve Nezamabadi-pour (2015) tarafından da gösterilmektedir. Dolayısıyla güvenlik ve performans gereksinimlerini birlikte karşılayabilen, bütünleşik nitelikte yeni mimarilere duyulan ihtiyaç giderek artmaktadır.

Bu problemin kapsamını daha açık biçimde ortaya koymak için, dijital içeriklerin üretimi ve tüketimine ilişkin bazı temel istatistiksel göstergeler önem arz etmektedir. Çeşitli çalışmalarda, 2010–2028 yılları arasında küresel dijital veri hacminin katlanarak arttığı ve bu eğilimin 2030 yılına kadar devam edeceği öngörülmektedir. İnternet kullanıcı sayısının toplam nüfusa oranı son yirmi yıl içinde belirgin bir artış göstermekte, sabit ve mobil geniş bant abone sayılarında da kayda değer yükselişler kaydedilmektedir. Ayrıca, kullanıcı başına düşen bant genişliği tüketimi 2000 yılından bu yana sürekli yükselmekte, bu eğilim içerik dağıtım sistemlerinin kapasite ve performans açısından sürekli güncellenmesini zorunlu kılmaktadır.



Şekil 1.1. Küresel dijital ekosistem göstergeleri

Şekil 1.1’de dijital ekosistemlerin dönüşümünü ortaya koyan dört temel gösterge sunulmaktadır. (a) panelinde, küresel dijital veri hacminin 2010 yılında 2 ZB düzeyinden 2023 yılında 123 ZB’ye ulaştığı ve 2030 yılına kadar 400 ZB’nin üzerine çıkmasının beklendiği görülmektedir. (b) panelinde, internet kullanıcı oranının 1990’ların sonunda %1’in altında iken 2023 itibarıyla nüfusun %70’ine yaklaştığı ve bu eğilimin artış yönünde devam ettiği izlenmektedir. (c) panelinde, sabit geniş bant abone sayısının 2000’de 37 milyon iken 2023 yılında 1,5 milyara yükseldiği; mobil geniş bant abone sayısının ise aynı dönemde yaklaşık 961 milyondan 8,9 milyara çıkarak neredeyse tüm dünya nüfusunu kapsayacak düzeye ulaştığı görülmektedir. (d) panelinde ise kullanıcı başına ortalama uluslararası bant genişliği tüketiminin 2000 yılında 749 Kbps seviyesinden 2023 itibarıyla 751 Mbps seviyesine yükselerek üç büyüklük mertebesi artış sergilediği dikkat çekmektedir. Bu göstergeler birlikte değerlendirildiğinde hem veri hacmindeki üstel artış hem de kullanıcı tabanındaki genişleme, içerik dağıtım altyapılarının kapasite ve performans açısından sürekli olarak yenilenmesini zorunlu kılan yapısal bir dönüşümün yaşandığını açık biçimde ortaya koymaktadır.

Bu tür istatistiksel göstergeler ışığında, uluslararası platformlarda tartışılan ve önerilen yeni mimari modeller giderek daha fazla önem kazanmaktadır. Örneğin, Virginia

Network User Group (VA NUG) ve IETF çalışma grubu toplantılarında gündeme getirilen TreeDN ve benzeri yapılar, yüksek ölçekli ve düşük maliyetli içerik dağıtımı için önerilmektedir (Giuliano ve ark., 2025). Avrupa Akademik Ağı GEANT tarafından desteklenen bu tür girişimler, uluslararası alanda birlikte çalışabilirlik ve ölçeklenebilirlik konusunda yeni standartların belirlenmesine yönelik önemli bir katkı sağlamaktadır (IETF/GEANT, 2025).

Bu çerçevede, içerik dağıtımı ile dijital hak yönetimini aynı mimari altında bütünleştiren, platformdan bağımsız ve yüksek ölçeklenebilirlik özelliklerine sahip bir modelin geliştirilmesi gerekliliği, bu çalışmanın temel motivasyonunu oluşturmaktadır.

1.2. Amaç ve Kapsam

Bu tez çalışması, dijital içeriklerin güvenli, kontrollü ve yüksek performanslı bir biçimde dağıtımını mümkün kılacak, bütünleşik ve modüler bir sistem mimarisi sunmayı hedeflemektedir. Günümüzde çok kullanıcı ortamlarda dijital içeriklerin eşzamanlı ve yoğun talepler doğrultusunda sunulması hem veri güvenliği hem de ağ performansı açısından ciddi mühendislik problemleri doğurmaktadır. Telif hakkı koruması, içerik yetkilendirmesi, kullanıcı erişim kontrolü, gecikme süresi optimizasyonu ve dağıtım kaynaklarının verimli kullanımı gibi çok boyutlu gereksinimler; mevcut içerik dağıtım sistemlerinde parçalı çözümlerle ele alınmakta, ancak bütünsel bir yapı altında birleştirilememektedir. Bu çalışmada önerilen çözüm, dağıtık sistem mimarileri içinde birlikte çalışabilir nitelikte tasarlanmış üç alt bileşen aracılığıyla, söz konusu problemleri aynı çatı altında karşılamayı mümkün kılan bütünsel bir içerik dağıtım altyapısı ortaya koymaktadır.

Sistem tasarımının merkezinde, içerik güvenliği ile dağıtım performansını aynı anda önceleyen ve bu iki önceliği teknik düzeyde uyumlu hale getiren bir mimari model yer almaktadır. Bu model kapsamında geliştirilen **EDU-DRM** bileşeni, içeriklerin yüklenmesi, tanımlanması, şifrelenmesi, meta-veri ile etiketlenmesi ve yalnızca yetkilendirilmiş istemcilerce erişilebilir hale getirilmesini yöneten, uçtan uca bir dijital hak yönetimi sistemidir. Bu yapı, içerik haklarının korunmasını sağlarken, kullanıcı bazında erişim yetkilerinin merkezi biçimde yönetilmesine de olanak tanımaktadır.

İkinci bileşen olan **TBCDN (Tree-Based Content Delivery Network)** ise, içeriklerin geniş çaplı kullanıcı kitlelerine düşük gecikme ile ulaştırılmasını sağlayan, hiyerarşik

ve özyinelemeli yönlendirme algoritmalarıyla yapılandırılmış bir içerik dağıtım ağıdır. Beş seviyeli ağaç tabanlı bu yapı; içeriklerin sistem üzerindeki farklı düğümlerde çoğaltılması, lokal olarak önbellege alınması ve eşzamanlı taleplerin kaynaklara en yakın düğümlerden karşılanması ilkeleriyle çalışmakta; böylece ağ yükünü azaltmakta, erişim süresini minimize etmekte ve sunucu yoğunluklarını dengelemektedir.

Üçüncü bileşen olan **TBNS (Tree-Based Network Simulator)** ise, geliştirilen mimarinin performans kriterleri açısından değerlendirilmesini mümkün kılan özel bir simülasyon altyapısıdır. Bu simülatör sayesinde, önerilen sistem ile geleneksel istemci–sunucu mimarileri karşılaştırmalı olarak test edilmiş; erişim gecikmesi, ağ trafiği, bant genişliği kullanımı ve sistem ölçeklenebilirliği gibi temel göstergeler üzerinden kantitatif analizler gerçekleştirilmiştir.

Simülasyon ortamında yürütülen deneysel çalışmalarda; içerik erişim süresi, ağ yükü ve mimari esneklik gibi ölçütler açısından önerilen sistemin ölçülebilir iyileştirmeler sağladığı ortaya konmuştur. Elde edilen sonuçlar, geliştirilen çözümün salt kuramsal bir öneri olmanın ötesinde, yüksek yoğunluklu içerik dağıtım senaryolarında uygulanabilir bir yapı sunduğunu göstermektedir.

Çalışmanın kapsamı, metin tabanlı dijital içeriklerle sınırlı tutulmuştur. Video, ses veya interaktif medya formatları bu kapsamın dışında bırakılmıştır. Ayrıca sistem, fiziksel donanım ortamlarında değil, simülasyon temelli bir çerçevede test edilmiştir. Bununla birlikte, geliştirilen altyapının hem farklı medya türlerine hem de gerçek sistem entegrasyonlarına genişletilebilecek esneklikte olduğu değerlendirilmektedir.

1.3. Tezin Özgün Katkıları

Bu tez çalışması, dijital içerik güvenliği ve dağıtım performansı gibi genellikle birbirinden bağımsız biçimde ele alınan iki temel teknoloji bileşeni olan DRM ve CDN sistemlerini, ortak bir mimari çatı altında bütünleşik şekilde işletebilen özgün bir sistem tasarımı önermektedir. Geliştirilen model, söz konusu iki teknolojinin yalnızca eşzamanlı kullanılmasını değil, aynı zamanda uygulama alanına özgü darboğazlara karşı uyumlu biçimde optimize edilmesini sağlayan teknik ilkeler ve algoritmik bileşenler içermektedir. Tezin temel katkısı, DRM ve CDN teknolojilerinin bütünleşik olarak tasarlandığı bir mimari aracılığıyla dijital içeriklerin hem güvenliğinin hem de

erişilebilirliğinin sürdürülebilir biçimde aynı anda sağlanabileceğini ortaya koymasındır.

Bu kapsamda geliştirilen çözüm, EDU-DRM ve TBCDN adlı iki temel bileşenden oluşmakta olup, her iki yapı hem bağımsız hem de bütünleşik senaryolarda çalışabilir esnekliktedir. DRM sistemleri içeriklerin yetkisiz erişime karşı korunmasını sağlarken, CDN sistemleri büyük ölçekli kullanıcı taleplerine düşük gecikme ile yanıt verebilmek amacıyla dağıtımı optimize etmektedir. Tez kapsamında önerilen modelde bu iki sistem, teknik düzeyde birbirini tamamlayacak şekilde yeniden yapılandırılmış ve aynı erişim senaryosu içinde hem içerik güvenliğini hem de ağ performansını birlikte sağlayacak biçimde bütünleştirilmiştir.

EDU-DRM bileşeni, klasik DRM sistemlerinden farklı olarak içeriklerin salt şifrlenmesini değil; rol tabanlı erişim kontrolü, meta-veri tanımlama, dijital kimlik doğrulama ve zaman profiline bağlı lisanslama gibi işlevleri de içeren uçtan uca bir hak yönetim altyapısı sunmaktadır. Sistem, içeriklere erişim sürecinde yalnızca kullanıcı kimliği doğrulamasını yeterli görmeyip; içerik türü, kullanım zamanı ve rol uygunluğunu da dikkate alarak çok boyutlu bir yetkilendirme mekanizması işletmektedir. Bu yaklaşım, sabit lisans kodlarına dayalı geleneksel modellerin ötesine geçerek, dinamik ve bağlama duyarlı bir lisans kontrolü sağlamaktadır.

TBCDN bileşeni, beş seviyeli ağaç tabanlı hiyerarşik bir dağıtım mimarisi sunmakta ve içeriklerin yeniden yönlendirme ile önbellekleme süreçlerini özyinelemeli bir algoritma aracılığıyla gerçekleştirmektedir. Bu yapı, merkezi sunucudan aktarılan içeriklerin ağ üzerinde aşağıya doğru çoğaltılmasını ve yerel düğümlerde saklanarak tekrar eden taleplerin bu lokal düğümler üzerinden karşılanmasını sağlamaktadır. Böylece sistem hem veri iletim süresini azaltmakta hem de merkezi sunucu üzerindeki yükü dengeleyerek yüksek trafikli senaryolarda sistemin kararlılığını ve ölçeklenebilirliğini güvence altına almaktadır. Özellikle ani ve yoğun erişim taleplerinde sistemin tepki süresinde istikrar korunmakta, kullanıcı başına düşen gecikme süresi minimize edilmektedir.

Bu iki bileşenin eşzamanlı ve bütünleşik biçimde çalışması, geleneksel sistemlerde karşılaşılan “güvenlik–performans” ikileminin teknik düzeyde aşılmasını mümkün kılmaktadır. EDU-DRM sistemi, her erişim talebinde dijital imza doğrulama, rol uyumu denetimi ve şifre çözme işlemlerini yürütürken; TBCDN, eşzamanlı olarak

içerik yönlendirmesi ve en uygun sunucu seçim süreçlerini gerçekleştirmektedir. Böylece istemcinin erişim süreci hem güvenlik denetiminden geçirilmekte hem de fiziksel olarak en yakın ve en az yük altındaki düğümden içerik aktarımı sağlanmaktadır. Bu etkileşim modeli, içerik sunumunun aynı anda güvenli ve düşük gecikmeli biçimde gerçekleştirilebilmesine olanak tanımaktadır.

Tez kapsamında geliştirilen TBNS aracı, önerilen mimarının performans doğrulamasını gerçekleştirmek amacıyla tasarlanmış özelleştirilmiş bir simülasyon altyapısıdır. TBNS, geleneksel istemci–sunucu modelleri, önbellek vekil sunucu yapılar ve klasik CDN sistemleriyle birlikte kurgulanan senaryolarda, EDU-DRM ve TBCDN sistemlerinin ayrı ve bütünleşik biçimde çalışmasını deneysel olarak karşılaştırmaya olanak tanımaktadır. Araç, 2²³ düzeyine kadar eşzamanlı istek yükünü desteklemekte; patlamalı trafik, tekrarlayan erişim desenleri ve değişken bant genişliği koşullarını simüle edebilmektedir. Bu sayede, önerilen sistemin gecikme süresi, işlem yükü, lisans doğrulama başarımı ve içerik yönlendirme etkinliği gibi ölçütlere ilişkin ayrıntılı performans metrikleri üretilmiştir.

Simülasyon sonuçları, önerilen mimarının geleneksel yöntemlere kıyasla ölçülebilir performans iyileştirmeleri sağladığını ortaya koymaktadır. EDU-DRM bileşeninde, XML tabanlı lisanslama yerine kullanılan bit tabanlı yetkilendirme modeli erişim işlem süresinde yaklaşık %27 oranında zaman kazancı üretmiştir. TBCDN bileşeni ise ağ üzerindeki toplam veri trafiğini yaklaşık %60 oranında azaltmış ve içeriklerin %80'inin lokal sunucular aracılığıyla sağlandığını göstermiştir. Bu bulgular, sistemin hem merkezi sunucu bağımlılığını azalttığını hem de erişim sürelerinde istikrar sağladığını ortaya koymaktadır.

Bir diğer önemli katkı, mimarının dönemsel ve kural tabanlı lisans yönetimini desteklemesidir. EDU-DRM sistemi, kullanıcı yetkilendirmelerini dönemsel takvimlere, kullanıcı rollerine, içerik türlerine ve zaman pencerelerine göre merkezi biçimde tanımlayabilmektedir. Bu mekanizma, dönem başlarında kullanıcı lisanslarının otomatik olarak yeniden dağıtılmasını sağlamakta; böylece sistem yönetimini kolaylaştırmakta ve lisans ihlallerinin ortaya çıkma olasılığını azaltmaktadır.

Önerilen mimari, yalnızca teknik düzeyde değil, yapısal ve operasyonel düzeyde de ölçeklenebilir ve genişletilebilir bir yapıda modellenmiştir. Sistem, video, ses,

etkileşimli nesne ve canlı içerik gibi farklı medya türlerine uygulanabilecek esneklikte olup; kurumsal ağlardan bölgesel içerik dağıtımına ve ulusal ölçekteki sistemlere kadar farklı ölçeklerde bütünleşik biçimde kullanılabilmektedir. EDU-DRM ve TBCDN bileşenlerinin modüler tasarımı, mimarinin çeşitli uygulama senaryolarına uyarlanabilirliğini artırmaktadır.

Bu tez çalışması, sayısal hak yönetimi ve içerik dağıtım ağlarını bağımsız sistemler olmaktan çıkarıp, uygulama ortamına özgü gereksinimleri karşılayan bütünleşik ve senkronize bir mimari çerçevede bir araya getirmiştir. Literatürde çoğunlukla parçalı çözümlerle ele alınan bu iki alan, burada sistematik biçimde bütünleştirilmiş; erişim güvenliği ile sistem performansı ilk kez ortak bir mimari yapı altında teknik olarak dengelenebilir kılınmıştır. Ayrıca geliştirilen simülasyon altyapısı sayesinde bu bütünlüğün kavramsal düzeyin ötesinde, deneysel ve ölçülebilir olarak da doğrulandığı ortaya konulmuştur. Bu mimari, dijital içeriklerin güvenli ve ölçeklenebilir biçimde dağıtılması gereken her ortamda uygulanabilecek esnek, sürdürülebilir ve genişletilebilir bir çözüm olarak önerilmektedir.

1.4. Tezin Organizasyonu

Bu tez çalışması altı ana bölümden oluşmaktadır. Birinci bölümde, dijital içeriklerin güvenli, kontrollü ve yüksek erişilebilirlik düzeyinde sunulmasına yönelik ihtiyaç çerçevesinde; problemin tanımı, araştırmanın amacı, kapsamı ve temel hipotezi ortaya konulmaktadır. Ayrıca, çalışmanın bilimsel ve uygulamalı katkıları açıklanmakta ve tezin genel yapısı hakkında bilgilendirme sunulmaktadır.

İkinci bölümde, önerilen mimarinin dayandığı kavramsal ve teknolojik temeller açıklanmaktadır. Bu kapsamda, dijital hak yönetimi (DRM) sistemlerinin işlevsel bileşenleri, içerik dağıtım ağlarının (CDN) yapısal özellikleri ve yüksek ölçekli dağıtım senaryolarına yanıt veren mimari ilkeler ele alınmakta; ayrıca güvenlik, performans ve erişim kısıtları üzerinden sistemsel gereksinimler gerekçelendirilmektedir.

Üçüncü bölümde, konuya ilişkin mevcut literatür ayrıntılı biçimde incelenmektedir. DRM ve CDN alanlarında yürütülen akademik çalışmalar sınıflandırılmakta, bu teknolojilerin farklı uygulama bağlamlarındaki kullanımları değerlendirilmektedir. Literatürde bu iki alanın çoğunlukla ayrı ayrı ele alınmış olması nedeniyle ortaya çıkan

sınırlılıklar tartışılmakta; çalışmanın özgün yönünün, bu iki katmanı bütüncül bir mimari çerçevede bir araya getirmesi olduğu vurgulanmaktadır.

Dördüncü bölümde, önerilen sistemin iki temel bileşeni olan EDU-DRM ve TBCDN mimarilerinin teknik ayrıntıları sunulmaktadır. Bu kapsamda, sistemlerin iç yapıları, erişim denetim mekanizmaları ve içerik dağıtım stratejileri açıklanmakta; ayrıca mimarilerin değerlendirilmesi amacıyla geliştirilen TBNS aracının tasarımı, modüler kurgusu ve işlevsel özellikleri tanıtılmaktadır.

Beşinci bölümde, EDU-DRM ve TBCDN bileşenlerinin performans değerlendirme sonuçları sunulmakta ve klasik sunucu–istemci mimarileriyle karşılaştırmalı analizler yapılmaktadır. Bu kapsamda, erişim gecikmesi, ağ yükü ve işlem verimliliği gibi ölçütler dikkate alınmakta; testler gerçekçi kullanım senaryoları temelinde yürütülmektedir.

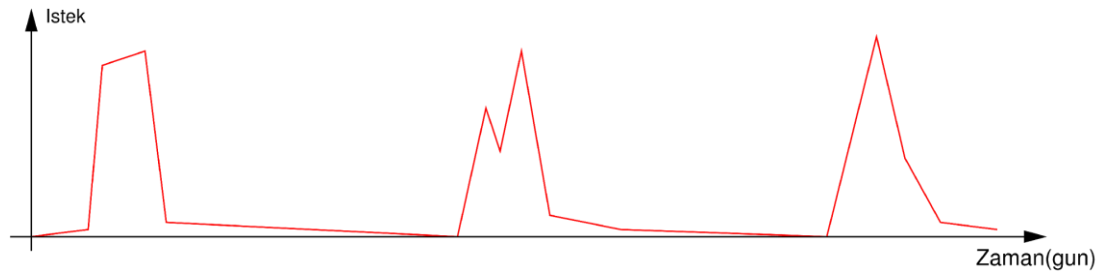
Altıncı bölümde, elde edilen bulguların yorumlanmasına ve önerilen mimarilerin güçlü ve sınırlı yönlerinin değerlendirilmesine yer verilmektedir. Ayrıca, çalışmanın genel sonuçları özetlenmekte, literatüre ve uygulamaya sağladığı katkılar ortaya konulmakta ve gelecekteki araştırmalara yönelik öneriler sunulmaktadır.



2. TEMEL KAVRAM, SİSTEM VE ALTYAPI BİLEŞENLERİ

Bu bölümde, çalışmada geliştirilen EDU-DRM ve TBCDN mimarilerinin dayandığı temel teknolojik bileşenler tanımlanmaktadır. İlk olarak, geleneksel içerik dağıtım ağlarının yapı taşları, performans sınırlılıkları ve yüksek kullanıcı yoğunluğu altında ortaya çıkan darboğaz davranışları incelenmektedir. Ardından, dijital hak yönetimi sistemlerinin işlevsel mimarileri, lisanslama yapıları ve güvenlik gereksinimleri ele alınmaktadır. Bu teknik arka plan, ilerleyen bölümlerde sunulacak mimari çözüm önerilerinin altyapısal gerekçesini oluşturmaktadır.

Dijital dönüşüm girişimleriyle birlikte, geleneksel basılı materyallerin yerini giderek daha etkileşimli ve çok katmanlı dijital içerikler almaktadır. Bu süreç, yalnızca içeriklerin sayısallaştırılmasını değil, aynı zamanda onların erişim, dağıtım ve güvenlik boyutlarının yeniden tasarlanmasını da zorunlu kılmaktadır. Ancak bu dönüşüm beraberinde iki temel teknik gereksinimi gündeme getirmektedir. İlki, içeriklerin yalnızca yetkilendirilmiş kullanıcılar tarafından erişilebilir olmasının sağlanması, içerik bütünlüğünün korunması ve lisans dışı çoğaltımın önlenmesidir. İkincisi ise, milyonlarca kullanıcının eşzamanlı olarak aynı içeriklere erişim talebinde bulunduğu durumlarda, klasik sunucu-istemci mimarilerinin yüksek işlem yükü nedeniyle darboğaza girmesini engelleyebilecek ölçeklenebilir ve verimli dağıtım altyapılarının geliştirilmesidir. Bu bağlamda, yüksek yoğunluklu erişim taleplerini karşılayabilecek, güvenliği ve performansı birlikte optimize eden, dağıtık ve uyarlanabilir mimariler tasarlamak kritik bir araştırma alanı haline gelmiştir.



Şekil 2.1. Kullanıcı Taleplerinin Zaman İçindeki Değişimi

Şekil 2.1, dijital içeriklere erişim sırasında ortaya çıkan tipik talep–zaman desenlerini göstermektedir. Grafik, sistemlerin çoğunlukla düşük yoğunlukta çalışmasına rağmen,

belirli dönemlerde talebin kısa sürede keskin biçimde artarak “patlama” karakteri sergilediğini ortaya koymaktadır. Bu tür ani ve yoğun talepler, klasik sunucu–istemci tabanlı ya da merkeziyetçi DRM sistemlerinde performans darboğazlarına ve gecikmelere yol açmaktadır. Literatürde de vurgulandığı üzere, dijital içerik yönetim sistemlerinin yalnızca ortalama yük altında değil, aynı zamanda bu tür olağandışı yoğunluk senaryolarında da istikrarlı yanıt verebilecek şekilde tasarlanması kritik önem taşımaktadır. Bu bağlamda, otonom çalışabilen, gecikmesiz tepki verebilen ve içerik aktarımını dağıtık bir ağ altyapısı üzerinden optimize edebilen yeni nesil sistem tasarımları temel bir gereklilik haline gelmiştir.

2.1. İlgili Ağ Altyapısı ve Teknolojileri

Önerilen sistem mimarisinin bütüncül işleyişi, dağıtık ağ altyapısına ilişkin bazı temel teknolojik varsayımlar üzerine kuruludur. EDU-DRM, TBCDN ve TBNS bileşenleri, içerik güvenliği, erişim kontrolü, yük dengeleme ve istek yönlendirme gibi işlevleri yerine getirebilmek için çok katmanlı bir iletişim yapısı üzerinde çalışmaktadır. Sistemin omurgasını oluşturan bu yapı, istemcilerden kök sunuculara kadar hiyerarşik biçimde düzenlenmiş, ölçeklenebilir ve çok seviyeli bir topolojiye sahiptir. Her katman, belirli görevleri ve yük dağılımlarını üstlenmekte; içerik taleplerinin doğrulanması, yönlendirilmesi ve karşılanması süreçleri katmanlar arasında koordineli biçimde gerçekleştirilmektedir.

EDU-DRM bileşeni, içeriklerin güvenli biçimde aktarılmasını ve yalnızca yetkilendirilmiş istemciler tarafından erişilebilmesini sağlamak amacıyla istemci–sunucu modeline bütüncül olarak entegre edilmiş bir dijital hak yönetimi çözümüdür. Erişim kontrol katmanında konumlanan bu bileşen, istemci kimlik doğrulamasını takiben içeriklerin şifrelenmiş biçimde sunulmasına olanak tanır. EDU-DRM’in işlevselliğini sürdürebilmesi için, tarayıcı tabanlı istemci yazılımları, HTTPS üzerinden güvenli veri iletimi ve içerik dosyalarının parçalı biçimde sunumunu destekleyen dağıtık sunucu altyapısı temel bileşenler arasında yer almaktadır.

TBCDN, içeriğin ölçeklenebilir, düşük gecikmeli ve yüksek erişilebilirlik düzeyiyle sunulabilmesi için tasarlanmış ağaç tabanlı bir dağıtım mimarisidir. Hiyerarşik bir topolojiye sahip olan bu model, çok katmanlı CDN düğümlerinden oluşmakta; her düğüm hem içerik önbellekleme hem de içerik çoğaltma işlevlerini üstlenerek yukarı katmanlardan gelen yükü azaltmaktadır. Geleneksel CDN mimarilerinde statik içerik

dağıtımını öncelikli iken, TBCDN özellikle tekrar eden ve zamana duyarlı içerik taleplerini yerleştirerek ağ trafiğini minimize etmekte, merkezi sunucu bağımlılığını en aza indirmekte ve istemciye en yakın noktadan hizmet sunarak erişim gecikmesini düşürmektedir. Bu yapı, dinamik talep desenlerine uyum sağlayabilen, özyinelemeli yönlendirme algoritmaları ve optimize edilmiş önbellekleme stratejileri ile desteklenmektedir.

RRR algoritması, istemciden başlayan içerik taleplerinin, en yakın ara düğümde çözümlenememesi durumunda özyinelemeli biçimde üst katmanlara yönlendirilmesine dayalı bir istek akışı mekanizmasıdır. Bu yaklaşım, içerik erişim süresini minimize etmek için en yakın düğümden yanıt üretilmesini hedeflerken, aynı zamanda ağ kaynaklarının dengeli kullanılmasını da sağlar. RRR algoritması, taleplerin kademeli olarak çözülmesini mümkün kılan yapısı sayesinde, sistemin ölçeklenebilirliğini ve kendi kendini optimize etme kapasitesini artırmaktadır.

Geliştirilen mimarinin performans analizini mümkün kılmak amacıyla tasarlanan TBNS, farklı trafik yoğunluklarını, kullanıcı erişim senaryolarını ve ağ koşullarını modelleyebilen özelleştirilmiş bir simülasyon ortamıdır. TBNS, geleneksel istemci–sunucu yapıları, önbellek–vekil sunucular ve klasik CDN mimarileri ile önerilen TBCDN modelini karşılaştırmalı olarak değerlendirme imkanı sunmaktadır. Bu araç, çoklu istemci–sunucu konfigürasyonlarını, içerik erişim loglarını ve ağ gecikmesi parametrelerini işleyebilen senaryo yürütme motorları aracılığıyla, sistemin hem ölçeklenebilirlik hem de gecikme süreleri açısından deneysel doğrulamasını sağlamaktadır.

Bu tez kapsamında geliştirilen mimarinin çalışabilirliği ve ölçeklenebilirliği, modern iletişim ağlarının sunduğu temel altyapı bileşenlerine dayanmaktadır. Dijital içeriklerin farklı coğrafi bölgelerdeki istemcilere güvenli ve düşük gecikmeli biçimde ulaştırılabilmesi için, yerel alan ağları (LAN) ve geniş alan ağlarının (WAN) çok katmanlı yapısının eşgüdümlü olarak kullanılması gereklidir. Kapalı kurumsal ağlar, içerik yönetiminin merkezi denetim altında yürütülmesine olanak sağlarken; internet üzerinden gerçekleştirilen dağıtımlar, ölçeklenebilirlik ve esneklik boyutunu öne çıkarmaktadır.

Ağ altyapısının çekirdeğini sunucular, istemciler, yönlendiriciler, anahtarlar, modemler ve kablosuz erişim noktaları gibi temel donanım bileşenleri

oluşturmaktadır. Sunucular, içeriklerin merkezi veya dağıtık biçimde barındırılmasını sağlarken; istemciler bu içeriklere erişim arabirimini temsil etmektedir. Yönlendirici ve anahtarlar, veri paketlerinin en uygun rotalardan iletilmesini sağlayan ağ cihazlarıdır ve çoklu istemci yükleri altında bant genişliği ve yönlendirme performansı üzerinde doğrudan belirleyici rol oynamaktadır.

Bu altyapı, yalnızca fiziksel donanım bileşenlerine değil, aynı zamanda TCP/IP protokol ailesi, HTTP/HTTPS gibi uygulama katmanı protokolleri ve DNS tabanlı ad çözümleme mekanizmaları gibi yazılımsal bileşenlere de dayanmaktadır. İçerik önbellekleme, erişim kontrolü ve yönlendirme işlevleri, bu katmanların birlikte çalışmasıyla sağlanmakta; böylece güvenli, tutarlı ve kesintisiz bir dağıtım süreci mümkün olmaktadır.

Sonuç olarak, ölçeklenebilir ve yüksek güvenli ağ altyapıları, yalnızca tekil erişim senaryoları için değil, aynı zamanda milyonlarca eşzamanlı istemciyi destekleyen büyük ölçekli sistemler için de zaruri hale gelmiştir. İstemci çeşitliliği, mobil erişim ve dinamik talep desenleri dikkate alındığında hem fiziksel ağ bileşenlerinin hem de bunları yöneten protokollerin tasarımı, önerilen mimarinin başarımı üzerinde kritik bir etkiye sahiptir.

2.2. Dijital Hak Yönetimi (DRM)

Dijital teknolojilerin hızlı gelişimi, bilginin üretim ve paylaşım süreçlerini kolaylaştırırken aynı zamanda içerik güvenliği ve telif haklarının korunması alanında yeni riskleri gündeme getirmiştir. Metin, ses, görüntü ve video gibi dijital içeriklerin izinsiz çoğaltımı, yayılımı ve yeniden dağıtımı, fikri mülkiyet haklarını tehdit eden en yaygın sorunlardan biri olarak ortaya çıkmaktadır. Bu bağlamda geliştirilen DRM sistemleri, dijital içeriklerin yalnızca yetkilendirilmiş kullanıcılar tarafından erişilebilmesini ve önceden tanımlanmış kullanım koşulları çerçevesinde tüketilmesini sağlayan bütüncül bir güvenlik altyapısı sunmaktadır.

DRM sistemleri, bir yandan içerik üreticilerinin telif haklarını korurken diğer yandan son kullanıcıların lisanslı materyallere güvenli, denetlenebilir ve sürdürülebilir şekilde erişebilmesine olanak tanır. Kimlik doğrulama, yetkilendirme, lisanslama ve şifreleme gibi temel güvenlik mekanizmaları aracılığıyla dijital içeriklerin yaşam döngüsü baştan sona kontrol altında tutulur. Ayrıca erişim süreleri, kullanım koşulları ve içeriklerin farklı platformlarda dağıtımına ilişkin kurallar, yazılım tabanlı politikalar

yoluyla uygulanır. Bu yönüyle DRM, yalnızca teknik bir güvenlik çözümü değil; aynı zamanda içerik üretimi, dağıtımı ve tüketimi arasındaki ilişkiyi düzenleyen bir yönetim mekanizması olarak işlev görmektedir.

Günümüzde DRM teknolojileri yalnızca medya endüstrisi ile sınırlı kalmamakta; e-kitaplar, dijital yayıncılık, kurumsal arşivleme, yazılım lisans yönetimi, elektronik sağlık kayıtları ve akademik içerik platformları gibi geniş bir yelpazede kullanılmaktadır. Bu alanların ortak noktası, içeriklerin telif haklarına uygun biçimde korunması ve yetkisiz erişime karşı güvence altına alınmasının yanı sıra, büyük ölçekli kullanıcı gruplarına güvenli ve kesintisiz şekilde sunulma gerekliliğidir. Özellikle dinamik ve yoğun talep senaryolarının gözlemlendiği ortamlarda, DRM çözümlerinin yalnızca içerik güvenliğini sağlaması yeterli olmayıp, aynı zamanda ağ performansı ve erişim ölçeklenebilirliği ile bütünleşik biçimde çalışması zorunlu hale gelmektedir. Bu durum, geleneksel DRM yaklaşımlarının ötesine geçen, dağıtım verimliliğini de gözeten yeni nesil DRM tasarımlarını gerekli kılmaktadır.

DRM sistemlerinin gelişimi, ticari çözümler ile akademik sistemler arasında çeşitli yaklaşım farklarını da beraberinde getirmiştir. Ticari DRM sistemleri çoğunlukla kapalı kaynak kodlu, özel mimariler sunarken; akademik sistemler ise daha çok açık standartlara dayalı ve birlikte çalışabilirlik ilkesiyle tasarlanmaktadır. Bu farklar, yalnızca mimari tercihler düzeyinde değil; aynı zamanda hangi temel bileşenler üzerinden tanımlandığı ve işletildiği noktasında da ortaya çıkmaktadır.

DRM sistemlerinin işlevselliği, yalnızca varlıklarının tanımlanmasıyla değil; bu sistemlerin nasıl yapılandırıldığı, hangi bileşenler aracılığıyla çalıştığı ve kullanıcı etkileşimlerini nasıl yönettiğiyle doğrudan ilişkilidir. Dolayısıyla, DRM mimarisinin temel yapı taşlarını oluşturan şifreleme, lisanslama ve yetkilendirme süreçleri ayrı ayrı ele alınmalı; her bir bileşenin sistem bütünlüğü içindeki rolü açık biçimde tanımlanmalıdır. Aşağıda yer alan alt bölümlerde, bu süreçlerin teknik açıdan nasıl işlediği ve dijital içeriklerin güvenliğini nasıl temin ettiği ayrıntılı biçimde değerlendirilecektir.

2.2.1. DRM türleri

Ticari ve akademik dijital hak yönetimi sistemlerinin büyük çoğunluğu, içeriklerin lisanslanması ve erişim kontrolü gibi temel işlevlere odaklanmaktadır. Ancak bu sistemlerin bazı versiyonları, söz konusu işlevlerin ötesine geçerek içerik güvenliğini

daha ileri düzeyde sağlamak amacıyla çeşitli yapısal ve kriptografik mekanizmalarla genişletilmiştir. Literatürde özellikle kurumsal ortamlarda hassas verilerin korunmasına yönelik geliştirilen Kurumsal Dijital Hak Yönetimi (E-DRM) çözümleri dikkat çekmektedir.

Bu doğrultuda Das, Chang, Chen ve diğer araştırmacılar tarafından önerilen E-DRM modelleri, yalnızca erişim kontrolü değil; aynı zamanda veri bütünlüğü, içerik izlenebilirliği ve sistem denetlenebilirliği gibi güvenliğe ilişkin gelişmiş unsurları da kapsamaktadır (Das vd., 2015; Chang vd., 2013; Chen, 2008; Chang vd., 2010). Bu sistemlerde güvenli veri erişimi, kullanıcı kimlik doğrulama, içerik tüketim geçmişinin izlenmesi ve yetki seviyelerine göre içerik davranışlarının tanımlanması gibi fonksiyonlar ön plandadır. Böylece dijital içerikler yalnızca yetkili kullanıcılar tarafından erişilebilir hale getirilmekte, yetkisiz müdahaleler sistem seviyesinde izlenebilmekte ve içerik üreticisinin hakları teknik olarak korunabilmektedir.

Güvenlik odaklı yaklaşımların bir diğer boyutu, mobil DRM cihazları üzerinden gerçekleşen eşler arası (peer-to-peer – P2P) içerik paylaşım senaryolarına ilişkindir. Bu tür durumlarda ortaya çıkan güvenlik açıklarını önlemek amacıyla çeşitli yöntemler geliştirilmiştir (Li vd., 2010; Ke ve Lin, 2015). Özellikle dijital müzik dosyalarının yasa dışı paylaşımını engellemeye yönelik bazı çalışmalarda, her kullanıcıya özgü dijital parmak izi oluşturulması esasına dayalı yaklaşımlar öne çıkmıştır. RSA algoritması kullanılarak üretilen bu parmak izlerinin içerik dosyalarına gömülmesi sayesinde, dosyaların yetkisiz biçimde dağıtılması halinde kaynağın geriye dönük olarak tespit edilmesi mümkün olmaktadır.

Bu tür ileri düzey güvenlik teknikleri, klasik DRM mimarilerine entegre edildiğinde, içerik haklarının korunmasında daha yüksek düzeyde kontrol ve izleme yetenekleri sağlamaktadır. Dolayısıyla DRM sistemlerinin yalnızca erişim denetimiyle sınırlı kalmayıp; içerik izleme, kimlik doğrulama ve dijital iz bırakma gibi katmanlarla desteklenmesi, dijital içerik güvenliğini daha sağlam bir zemine oturtmaktadır.

Akademik DRM sistemleri literatürde hem halen aktif olarak kullanılan hem de araştırma projeleri kapsamında geliştirilen çok sayıda örnek barındırmaktadır. Bu sistemler genellikle birlikte çalışabilirlik, içerik güvenliği ve açık standartlara dayalı mimari ilkelerini esas alarak tasarlanmış; böylece farklı platform ve uygulamalar arasında uyumlu çalışabilecek esnek çözümler ortaya koymuşlardır.

Literatürde öne çıkan çalışmalardan biri OpenSDRM (Open Secure Digital Rights Management) olup, sistem bileşenleri arasında veri iletim güvenliğini sağlamak amacıyla SSL/TLS protokolünü kullanan, açık kaynaklı bir DRM altyapısı olarak geliştirilmiştir (Serrao, 2004; Delgado vd., 2005). Ayrıca, MPEG-4 standardı üzerinden içerik şifrelemesi sağlayan bu yapı, modüler mimarisi sayesinde birlikte çalışabilirliği desteklemekte ve farklı uygulama alanlarına uyarlanabilir bir çözüm olarak dikkat çekmektedir (Koenen, 2001).

Benzer bir yaklaşım sunan Multimedya Bilgi Koruma ve Yönetim Sistemi (MIPAMS) ise, Avrupa Birliği destekli bir proje olarak Dağıtık Multimedya Uygulamaları Grubu (DMAG) tarafından geliştirilmiştir (Delgado vd., 2011). Bu sistemde içerikler MPEG-21 standardı çerçevesinde yönetilmekte olup, mimari yapı modüler web servisleri üzerine inşa edilmiştir (Karpouzis vd., 2007).

Bir diğer dikkat çekici örnek olan AXMEDIS, Java tabanlı bir altyapı üzerinde geliştirilmiş ve televizyon, bilgisayar ile kiosk gibi farklı cihazlarda kullanılmak üzere tasarlanmıştır (Ng vd., 2005). Açık kaynaklı olmamasına rağmen, çeşitli açık tanımlamalar ve modüller aracılığıyla farklı kullanım senaryolarına esnek uyarlanabilirlik sağlamaktadır.

CORAL (Content Object Rights and License), farklı DRM çözümleri arasında birlikte çalışabilirliği destekleyen bir çerçeve olarak öne çıkmaktadır. Mevcut sistemlere minimal müdahale ile entegre edilebilmesi sayesinde, özellikle içerik alışverişi ve hak yönetiminde platformlar arası geçişi kolaylaştırmayı hedeflemektedir (Kalker vd., 2007).

OpenSDRM (Open Secure Digital Rights Management), Avrupa Birliği'nin 5. Çerçeve Programı (FP5) kapsamında yürütülen MOSES (MPEG Open Security for Embedded Systems) araştırma projesi çerçevesinde geliştirilmiş açık kaynaklı bir DRM altyapısıdır. Sistem, dijital içeriklerin güvenli bir biçimde korunmasını ve telif haklarının ihlal edilmeden erişime sunulmasını sağlamak amacıyla tasarlanmıştır (Serrao, 2004; Delgado vd., 2005). Modüler web servis mimarisi üzerine inşa edilen bu yapı, çok sayıda DRM bileşeninin SSL/TLS protokolleri üzerinden güvenli iletişim kurmasını sağlamaktadır. İçeriklerin kodlanmasında MPEG-4 standardı kullanılmakta olup, bu sayede ses ve görüntü verilerinin sıkıştırılmış ve taşınabilir biçimde korunması mümkün kılınmaktadır. Açık kaynaklı yapısı sayesinde OpenSDRM, farklı

DRM çözümleri arasında birlikte çalışabilirliği artırmakta ve sahip olunan dijital içeriklerin sistemler arası taşınabilirliğine olanak tanımaktadır.

AXMEDIS (Automating Production of Cross Media Content for Multi-channel Distribution) ise, dijital içerik üretimi ve yönetimi alanında Avrupa Birliği'nin 6. Çerçeve Programı (FP6) kapsamında geliştirilen önemli projelerden biridir. Java tabanlı bir mimari üzerine kurulan sistem, dijital içeriklerin üretiminden çok kanallı ortamlarda son kullanıcıya dağıtımına kadar uzanan süreci bütüncül bir biçimde ele almaktadır (Ng vd., 2005). Televizyon, bilgisayar ve kiosk gibi farklı son kullanıcı cihazlarında uygulanabilirliği hedeflenen AXMEDIS, yalnızca bir araştırma altyapısı olmakla kalmayıp, ticarileştirilebilir çözümler üretmeyi de amaçlamaktadır. Genişletilebilir yapısı ve farklı kullanım alanlarına yönelik esnekliği sayesinde, diğer DRM çözümlerine kıyasla daha kapsamlı bir uygulama yelpazesi sunmaktadır.

Bu örnekler, DRM sistemlerinin yalnızca erişim kontrolü ve şifreleme işlevleriyle sınırlı kalmadığını; aynı zamanda birlikte çalışabilirlik, çoklu cihaz desteği, modüler mimari ve ticarileştirilebilirlik gibi boyutlarda da çeşitlenebildiğini göstermektedir.

MIPAMS (Multimedia Information Protection and Management System), multimedya içeriklerinin güvenliğini ve yönetimini hedefleyen, modüler yapıya sahip bir DRM mimarisidir. İçerik üretiminden son kullanıcıya kadar uzanan süreçte, dijital materyallerin telif haklarının korunmasını, yalnızca yetkilendirilmiş kullanıcılar tarafından erişilebilir olmasını ve içerik tüketiminin izlenebilirliğini sağlamayı amaçlamaktadır (Delgado vd., 2011).

Sistemin bileşenleri arasında içerik sunucuları, yetkilendirme servisleri, sertifikasyon otoriteleri ve denetim modülleri yer almakta; bu bileşenler, şifreleme, lisanslama ve erişim kontrolü işlevlerini yerine getirmek üzere standartlara dayalı protokoller üzerinden çalışmaktadır. MIPAMS'in öne çıkan özelliklerinden biri, birlikte çalışabilirlik kapasitesidir: farklı DRM sistemleriyle entegre çalışabilme yeteneği sayesinde, çoklu platformlarda içeriklerin güvenli biçimde dağıtımına olanak tanımaktadır.

Buna ek olarak, sistem kullanıcıların erişim haklarını dinamik biçimde yönetebilmekte ve içerik kullanımına dair ayrıntılı raporlama ve denetim fonksiyonları sunmaktadır. Mobil cihazların sınırlı işlem gücü ve depolama kapasiteleri gözetilerek tasarlanmış olması, MIPAMS'i özellikle mobil ortamlar ve elektronik yayıncılık senaryoları için

uygun kılmaktadır. Kimlik doğrulama ve cihaz güvenliğini destekleyen güvenlik mekanizmalarıyla, mobil kullanıcıların da güvenli içerik erişimini mümkün hale getirmektedir.

CORAL (Content Object Rights and License), dijital hak yönetimi (DRM) sistemlerinde uzun süredir devam eden birlikte çalışabilirlik sorununa çözüm getirmeyi hedefleyen çerçeve bir mimaridir. Farklı DRM altyapılarının genellikle kapalı ve birbirinden bağımsız biçimde tasarlanması, hem içerik sağlayıcıları hem de son kullanıcılar açısından ciddi kısıtlamalara yol açmaktadır. Bu durum, içeriklerin sistemler arası aktarımında, lisansların yeniden tanımlanmasında ve kullanıcıların çoklu platformlar üzerinden kesintisiz erişiminde önemli engeller oluşturmaktadır (Kalker vd., 2007).

CORAL yaklaşımı, mevcut DRM sistemlerine minimal müdahale ile entegre edilebilen bir çözüm önermekte; sistemlerin temel işleyişini değiştirmeden, ortak bir hak ve lisans tanımı etrafında içerik değişimini desteklemektedir. Bu sayede, farklı DRM platformları arasında içerik nesnelerinin ve lisansların karşılıklı tanımlanması, işlenmesi ve paylaşılması mümkün hale gelmektedir.

Özellikle çok paydaşlı içerik dağıtım senaryolarında, CORAL mimarisi operasyonel esnekliği artırmakta; içerik sağlayıcıların yönetim maliyetlerini azaltırken son kullanıcı deneyimini daha akıcı ve kesintisiz hale getirmektedir. Bu yönüyle CORAL, DRM ekosisteminde birlikte çalışabilirliğe dayalı standartların geliştirilmesi açısından önemli bir kilometre taşı olarak değerlendirilmektedir.

Ticari DRM çözümleri, genellikle kapalı kaynaklı ve mülkiyet temelli yapıları nedeniyle mimari detaylarını kamuya açık biçimde paylaşmaktan kaçınmaktadır. Bu yaklaşım, bir yandan içerik sağlayıcıların ticari çıkarlarını ve güvenlik politikalarını korumayı amaçlarken, diğer yandan teknik şeffaflık ve birlikte çalışabilirlik açısından akademik sistemlerle keskin bir karşıtlık oluşturmaktadır. Bununla birlikte, geniş kullanıcı tabanlarına ulaşmaları sayesinde, ticari DRM çözümleri sektörün fiili standartlarını belirlemekte ve dijital içeriklerin korunmasında halen kritik bir rol üstlenmektedir.

Bu çözümlerden biri olan Open Mobile Alliance DRM (OMA-DRM), mobil cihazlar ve taşınabilir platformlarda içerik güvenliğini sağlamak üzere geliştirilmiş uluslararası bir standarttır (Irwin, 2004). OMA-DRM, akademik sistemlerde sıkça kullanılan

MPEG-21 tabanlı Hak İfade Dili (REL) yerine, mobil uygulamalara optimize edilmiş özel bir REL yapısı kullanmakta; böylece lisans tanımlama ve uygulama süreçlerinde cihaz odaklı bir esneklik sunmaktadır.

Benzer şekilde, Microsoft Windows Media Rights Manager (WMRM), ses ve video içeriklerinin sıkıştırılmış formatlar (ASF, WMA, WMV) üzerinden iletimini esas alan ve yalnızca Microsoft tabanlı işletim sistemleri üzerinde çalışan ticari bir çözümdür (Austerberry, 2012; Becker vd., 2003). Bu sistem, içeriklerin yalnızca yetkilendirilmiş cihazlarda oynatılmasını mümkün kılan lisanslama modeli ile dikkat çekmekte; aynı zamanda kendi mülkiyetli medya formatlarını kullanarak içeriklerin izinsiz erişimini ve çoğaltımını teknik düzeyde sınırlandırmaktadır.

Adobe PDF Merchant, özellikle metin tabanlı belgelerin (PDF) korunmasına yönelik olarak geliştirilmiş ticari bir DRM çözümüdür (Michiels vd., 2005). Sistem, kullanıcıların içeriklere yalnızca Acrobat Reader üzerinden erişebilmesini sağlayan bir eklenti aracılığıyla çalışmakta, böylece belge güvenliğini istemci yazılımına bağımlı bir şekilde yürütmektedir. Ancak bu çözüm, Unix tabanlı işletim sistemlerinde desteklenmemesi ve zaman içinde ortaya çıkan güvenlik açıkları nedeniyle sınırlı kalmış; Adobe tarafından 2012 yılında geliştirilen Adobe Digital Experience Protection Technology ile yer değiştirmiştir.

Ticari alandaki bir diğer örnek, Motorola'nın mobil DRM çözümüdür. Bhatt ve arkadaşları tarafından önerilen bu yapı, Motorola marka akıllı telefonlara özgü güvenlik protokolleri barındırmakta; cihaz düzeyinde kimlik doğrulama ve içerik koruma işlevlerini bütünsel biçimde yönetmektedir (Bhatt vd., 2009). Bu yaklaşım, mobil cihazlara özgü güvenlik risklerini azaltmayı amaçlamakla birlikte, cihaz bağımlı olması nedeniyle ölçeklenebilirlik açısından sınırlı kalmaktadır.

Genel olarak ticari DRM çözümlerinin büyük bölümü, merkezi içerik sunucusu modeline dayanmaktadır. Amazon, Google, Apple ve Microsoft gibi büyük teknoloji şirketlerinin geliştirdiği kapalı ekosistemlerde, içerikler çoğunlukla merkezi sunucular üzerinden istemcilere iletilmektedir. Bu yapı, kullanım kolaylığı ve güvenlik açısından belirli avantajlar sunsa da yüksek kullanıcı yoğunluğunun yaşandığı ortamlarda performans darboğazlarına ve erişim gecikmelerine neden olabilmektedir.

Bu tez çalışmasında ise, söz konusu merkezi yaklaşımların doğurduğu kısıtları aşmak amacıyla yeni bir mimari model önerilmektedir. Geliştirilen çözüm, içerik

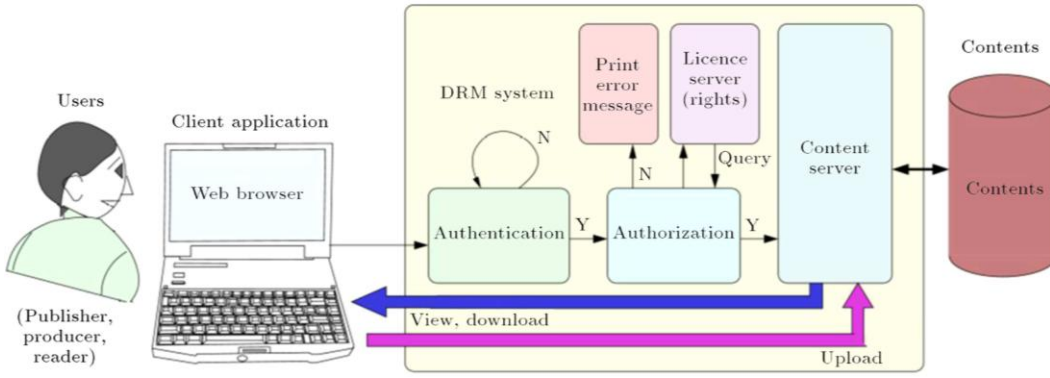
sunucularını dağıttık ve ağaç tabanlı bir yapıya dönüştürmekte; böylece içeriklerin erişim talepleri özyinelemeli yönlendirme algoritmaları aracılığıyla en yakın düğümden karşılanabilmektedir. Bu model, kullanıcı sayısının artması durumunda dahi erişim sürelerinin uzamasını engellemekte, sistemin ölçeklenebilirliğini ve sürdürülebilirliğini önemli ölçüde artırmaktadır.

2.2.2. DRM mimarisi ve bileşenleri

DRM sistemlerinin temel mimarisi, büyük ölçüde istemci–sunucu modeli üzerine kurgulanmaktadır. Bu yaklaşımda dijital içerikler, merkezi bir sunucu üzerinden istemcilere iletilmekte; içerik taleplerinin homojen dağıldığı ve içerik boyutlarının görece küçük olduğu senaryolarda yüksek verimlilik sağlamaktadır. Ancak kullanıcı sayısındaki hızlı artış, içerik hacimlerinin büyümesi ve zaman duyarlılığı yüksek veri türlerinin yaygınlaşması, bu mimarinin performans açısından darboğazlarla karşılaşmasına yol açmaktadır.

Özellikle telif hakkına tabi, yüksek hacimli ve gerçek zamanlı erişim gerektiren dijital içeriklerin korunmasında, geleneksel istemci–sunucu mimarisinin sınırlılıkları daha belirgin hale gelmektedir. Bu nedenle modern DRM sistemleri, yalnızca telif haklarını korumakla kalmayıp, aynı zamanda bu içeriklerin kullanıcıya güvenli, ölçeklenebilir ve gecikmesiz biçimde ulaştırılmasını hedeflemektedir. Bu gereksinim, DRM mimarilerinin hem içerik güvenliği hem de sistem performansı boyutunda yeniden değerlendirilmesini zorunlu kılmaktadır.

Bu yeniden yapılandırma süreci, üç temel işlev etrafında şekillenmektedir: şifreleme, lisanslama ve yetkilendirme. Şifreleme, içeriklerin yalnızca güvenli kanallar üzerinden iletilmesini güvence altına alırken; lisanslama, kullanıcıların hangi koşullar altında erişim sağlayabileceğini tanımlar; yetkilendirme ise tanımlanan bu koşulların istemci düzeyinde uygulanmasını sağlar. Bu üç katman, DRM mimarisinin hem içerik güvenliği hem de erişim kontrolünü sağlayan çekirdek yapısını oluşturmaktadır.



Şekil 2.2. Bir DRM sisteminin temel bileşenleri

DRM sistemlerinin mimarisi, işlevsel bileşenlerin bütünleşik biçimde çalışmasına dayanır. Bu bileşenler arasındaki etkileşim, istemci–sunucu temelli bir yapı üzerinde kurgulanmış olup; kimlik doğrulama, yetkilendirme ve içerik erişimi süreçlerini kapsar. **Şekil 2.2**, tipik bir DRM sisteminde bu süreçleri yöneten ana bileşenleri ve aralarındaki veri akışlarını göstermektedir.

Kullanıcılar (örneğin yayıncı, üretici veya okuyucu rollerinde), istemci uygulaması üzerinden sisteme erişim sağlar; çoğunlukla web tarayıcısı veya benzeri bir istemci yazılımı bu amaçla kullanılmaktadır. Kullanıcıdan gelen her erişim talebi ilk olarak kimlik doğrulama (authentication) bileşenine yönlendirilir. Doğrulama başarısız olduğunda süreç sonlandırılır ve sistem hata mesajı üretir. Başarılı doğrulama sonrası talep, yetkilendirme (authorization) modülüne aktarılır. Bu aşamada sistem, kullanıcının ilgili içerik için erişim haklarını, lisans sunucusu üzerinden yürütülen bir sorgu ile değerlendirir.

Yetkilendirme olumlu sonuçlandığında kullanıcı, içerik sunucusuna (content server) yönlendirilir. Buradan içerikler yalnızca “görüntüleme” veya “indirme” amacıyla tüketilebilmekte; yayıncı veya üretici rolündeki kullanıcılar için ayrıca “yükleme” (upload) işlemi de mümkün olmaktadır. Bu iş akışı sayesinde içeriklere erişim, yalnızca yetkili kullanıcılarla sınırlandırılmakta ve sistemde tanımlanmış koşullar çerçevesinde gerçekleşmektedir.

Bu yapı, DRM sisteminin yalnızca erişim denetimini değil, aynı zamanda lisansların merkezi yönetimini ve içeriklerin güvenli dağıtımını nasıl bütünleştirdiğini göstermektedir. Böylece, dijital içeriklerin yaşam döngüsü boyunca hem fikrî mülkiyet hakları hem de erişim güvenliği garanti altına alınmaktadır.

Önerilen sistem mimarisinde şifreleme katmanı, dijital içeriklerin hem iletim hem de depolama süreçlerinde yetkisiz erişime karşı korunmasını sağlayan en kritik güvenlik bileşenidir. Bu katman, yalnızca veri gizliliğini sağlamakla sınırlı kalmamakta; aynı zamanda erişim kontrol mekanizmaları ile bütünleşik çalışarak, içeriklerin yalnızca yetkilendirilmiş istemciler tarafından kullanılabilmesini garanti altına almaktadır. Tez kapsamında geliştirilen EDU-DRM modülü, şifreleme sürecini mimarinin merkezine yerleştirerek içerik güvenliğini sistem düzeyinde sürdürülebilir kılmaktadır.

Sistemde benimsenen şifreleme yaklaşımı, hibrit kriptografi modeli üzerine kurgulanmıştır. Bu modelde, içerik verileri öncelikle Advanced Encryption Standard (AES) gibi simetrik algoritmalarla şifrelenmektedir. AES'in yüksek işlem hızı, düşük gecikme süresi ve büyük veri kümeleri üzerinde sunduğu verimlilik, yüksek hacimli içeriklerde kritik avantaj sağlamaktadır. Her içerik, kendisine özgü bir oturum anahtarı (session key) ile şifrelenmekte; bu anahtar içerik türüne, oturuma ya da kullanıcı rolüne göre dinamik olarak üretilebilmektedir.

Simetrik şifrelemenin sağladığı performans, güvenli anahtar iletimiyle tamamlanmaktadır. Bu amaçla, üretilen her AES oturum anahtarı, istemcinin yalnızca kendi özel anahtarıyla çözebileceği biçimde RSA gibi asimetrik algoritmalar ile tekrar şifrelenmektedir. İstemciye, yalnızca kendi özel anahtarına özgü şekilde şifrelenmiş oturum anahtarı gönderilir. Kullanıcı bu anahtarı çözdüğünde, AES üzerinden içeriği açabilmesini sağlayan gerçek oturum anahtarına ulaşır. Böylece sistem, yüksek hızlı veri şifreleme (AES) ve güvenli anahtar dağıtımı (RSA) işlevlerini bir araya getiren dengeli bir yapı sunar.

Bu mimari hem performans hem de güvenlik açısından çift katmanlı bir koruma mekanizması sağlamaktadır: büyük hacimli verilerin hızlı şifrelenmesi ve yalnızca lisans sunucusu tarafından yetkilendirilmiş istemcilerin çözebileceği anahtarların güvenli biçimde dağıtılması. Böylelikle, önerilen çözüm klasik DRM modellerinin ötesine geçerek, içerik güvenliğini sistem düzeyinde bütünsel ve ölçeklenebilir bir biçimde ele almaktadır.

Lisans sunucusu, sistemde yetkili rol bilgisi, zaman aralığı ve kapsam sınırlamaları ile dijital lisansları üretmekte; her istemciye özel açık anahtar üzerinden yalnızca belirli içeriğe erişim izni verecek şekilde AES anahtarlarını şifrelemektedir. Bu tasarım, kullanıcı lisanslarının dinamik olarak yönetilmesini ve içerik erişiminin koşula bağlı

biçimde denetlenmesini mümkün kılar. Gelecek çalışmalar için ise, homomorfik şifreleme gibi ileri düzey kriptografik yöntemlerin, içeriklerin şifreli biçimde işlenmesini gerektiren senaryolarda sistemle bütünleştirilmesi potansiyel bir araştırma alanı olarak değerlendirilebilir.

Önerilen hibrit şifreleme yapısı, içeriklerin yalnızca yetkili istemcilere sunulmasını ve sistem dışı sızıntıların engellenmesini sağlayan bütüncül bir güvenlik katmanı sunmaktadır. Şifreleme katmanı, EDU-DRM'in diğer bileşenleri olan yetkilendirme, rol tanımı ve zaman profili kontrolü ile çalışarak, içerik güvenliğini uçtan uca kapsayan sağlam bir altyapı oluşturmaktadır. Ayrıca hibrit modelin benimsenmesi, sistemin hem yüksek veri hacimli içerikleri desteklemesine hem de lisans güvenliğini dinamik olarak korumasına olanak tanımaktadır.

DRM sistemlerinde lisanslama, dijital içeriklere erişim hakkının tanımlandığı ve bu erişimin hangi koşullar altında, ne tür işlemlerle gerçekleştirilebileceğinin belirlendiği kritik bir süreçtir. Bu mekanizma, yalnızca bir erişim izni vermekle sınırlı değildir; erişimin kapsamını, süresini, kullanılabilecek cihaz sayısını, içerik kullanım türünü (görüntüleme, indirme, yazdırma vb.) ve hatta erişim bağlamına ilişkin koşulları da tanımlayan çok katmanlı bir politika yönetim aracı işlevi görür. Dolayısıyla lisanslama, dijital içeriklerin yaşam döngüsünü denetleyen en merkezi kontrol düzeneği olarak kabul edilmektedir.

Bu süreçte merkezi rol üstlenen bileşen, lisans sunucusudur. Lisans sunucusu, dijital içeriklere ilişkin hakların ve bu hakları kullanabilecek kullanıcıların bilgilerini yöneten otorite konumundadır. Bir kullanıcı içerik talebinde bulunduğu anda, lisans sunucusu devreye girerek ilgili içeriğe ait lisans kurallarını doğrular, koşulları değerlendirir ve istemciye erişim izninin verilip verilmeyeceğine karar verir. Bu süreç, istemci uygulamasına gönderilen lisans paketleri aracılığıyla işler ve erişim haklarının bağlamsal olarak uygulanabilirliğini güvence altına alır.

Lisans sunucusunun bu işlevleri gerçekleştirmesinde kritik rol oynayan unsur, Hak İfade Dilleri (Rights Expression Languages, REL) olmaktadır. REL, dijital içeriklere ilişkin hakların biçimsel olarak tanımlanmasını, bu hakların farklı sistemler arasında birlikte çalışabilir biçimde iletilmesini ve makine tarafından işlenebilir kurallara dönüştürülmesini sağlayan standartlaştırılmış bir ifade dilidir. Yaygın kullanılan örneklerden biri, W3C ODRL Topluluğu tarafından geliştirilen Open Digital Rights

Language (ODRL)'dir (Iannella, 2004). Bir diğerk önemli örnek ise MPEG-21 kapsamında geliştirilen REL standardıdır (ISO, 2004). XML tabanlı olan bu diller, lisanslama sürecine platform bağımsızlık, esneklik ve birlikte çalışabilirlik kazandırmaktadır.

Tez kapsamında geliştirilen EDU-DRM mimarisinde ise, klasik XML tabanlı REL modellerinin yüksek işlem yükü yaratan sınırlılıklarını aşmak amacıyla, hakların bit tabanlı erişim vektörleriyle temsil edildiğı özgün bir yaklaşım benimsenmiştir. Bu yöntem, ayrıntıları ilerleyen bölümlerde açıklanacağı üzere, lisanslama sürecinin daha hafif, hızlı ve ölçeklenebilir biçimde uygulanmasını mümkün kılmaktadır. Bununla birlikte, lisanslama mekanizmasının tek başına yeterli olmadığı; şifreleme ve yetkilendirme katmanlarıyla birlikte çalıştığında bütüncül bir güvenlik modeli oluşturulmaktadır.

Lisanslama süreci, DRM mimarisinde şifreleme ve yetkilendirme bileşenleriyle doğrudan bütünleşmektedir. Şifrelenmiş içerikler yalnızca geçerli bir lisans aracılığıyla çözülebilirken, yetkilendirme katmanı bu lisansın hangi kullanıcıya, hangi koşullar altında uygulanacağını belirlemektedir. Böylece lisans, salt bir erişim izni olmaktan çıkarak, sistemin içerik yaşam döngüsünü yöneten dinamik bir kontrol mekanizmasına dönüşmektedir.

Yetkilendirme, içerik erişiminin yalnızca tanımlı kullanıcı rollerine sahip istemciler tarafından gerçekleştirilmesini sağlayan kritik bir güvenlik katmanıdır. Bu süreç, kullanıcıların kimlik bilgileri, sistemdeki rolleri, oturum durumları ve lisans koşulları temelinde işletilmektedir. Kullanıcının içeriğı görüntüleyip görüntüleyemeyeceğı, indirip indiremeyeceğı veya üzerinde işlem yapıp yapamayacağı gibi kararlar, bu aşamada alınır. Yetkilendirme kontrolleri hem istemci tarafında (örneğin DRM eklentili belge görüntüleyici) hem de sunucu tarafında (lisans sunucusu veya erişim kontrol modülü) uygulanabilmektedir.

DRM sistemlerinde kullanıcılar çoğunlukla üç temel rol altında tanımlanmaktadır: Üretici, içerikleri oluşturan ve sisteme yükleyen aktördür; içerik haklarını tanımlama ve yükleme yetkisine sahiptir. Yayıncı, erişim politikalarını ve lisans sunucusunda yer alan hakları yöneten ara aktördür; kullanıcıların erişim düzeylerini düzenler. Okuyucu ise içeriğı tüketen son kullanıcıdır ve yetkileri lisans koşullarına göre sınırlandırılmaktadır. Bazı okuyucular yalnızca içerik meta-verilerine erişebilirken,

bazıları görüntüleme, indirme veya yazdırma gibi daha geniş işlemler gerçekleştirilebilmektedir.

Yetkilendirme mekanizması, bu rollerin tanımlanması ve denetlenmesinde kimlik doğrulama katmanı ile bütünleşik çalışmaktadır. Kullanıcı sisteme giriş yaptığı anda kimliği doğrulanır, rolü belirlenir ve ardından lisans koşullarıyla eşleştirilerek ilgili erişim izinleri uygulanır. Böylece, sistem genelinde içerik güvenliği hem teknik şifreleme hem de kural tabanlı yetki yönetimi aracılığıyla sürdürülebilir hâle gelmektedir.

Bazı gelişmiş DRM sistemlerinde yetkilendirme, yalnızca kullanıcı kimliği veya rolüne değil; aynı zamanda zaman aralığı, cihaz türü, coğrafi konum veya oturum bağlamı gibi koşullara dayalı durum-bazlı erişim politikaları ile desteklenmektedir. Bu yaklaşım, çok kullanıcı ve çok cihazlı ortamlarda içerik güvenliğinin kapsamını genişleterek daha ayrıntılı bir kontrol mekanizması sunmaktadır.

Modern DRM eğilimleri, yalnızca içerik sunucusu–lisans sunucusu–istemci üçlüsünden oluşan temel yapıya bağlı kalmamakta; işlevlerin ayrıştırıldığı, modüler ve servis tabanlı mimarilere yönelmektedir. Bu modüler yapı, sistemlerin yönetilebilirliğini artırmakta, özelleştirilebilir ve genişletilebilir çözümler geliştirilmesine olanak tanımakta ve birlikte çalışabilirliği (interoperability) uluslararası standartlarla (ör. MPEG-21, ODRL) uyumlu hale getirmektedir. Özellikle kimlik doğrulama, lisans yönetimi ve erişim kontrolü gibi güvenlik kritik işlevlerin bağımsız servisler olarak tasarlanması, farklı güvenlik politikalarının esnek biçimde uygulanmasına imkân tanımaktadır.

Bu bağlamda Avrupa Birliği destekli MIPAMS sistemi, modüler DRM mimarisine örnek teşkil etmektedir (Delgado vd., 2011). Kimlik doğrulama, yetkilendirme, içerik sunumu ve lisans yönetimi gibi işlevleri ayrı modüller aracılığıyla yürüten MIPAMS, standart protokollerle birlikte çalışabilirlik sağlayarak sistemin farklı platformlara ve kullanım senaryolarına entegrasyonunu mümkün kılmaktadır.

Bu tez çalışmasında DRM yaklaşımı, yalnızca klasik erişim denetiminden ibaret bir güvenlik katmanı olarak değil; aynı zamanda yüksek hacimli ve eşzamanlı içerik erişimlerinde performans kriterlerini doğrudan etkileyen bir mimari bileşen olarak yeniden kurgulanmıştır. Geliştirilen EDU-DRM modeli, XML tabanlı geleneksel yapılara göre daha düşük gecikme süresi sağlayan, bit-tabanlı bir yetkilendirme

vektörü kullanarak işlem yükünü minimize etmektedir. Bu çözüm, yalnızca içeriklerin lisanslı ve güvenli sunumunu garanti etmekle kalmamakta, aynı zamanda sistemin ölçeklenebilirlik ve gecikme performansını da iyileştirmektedir.

2.3. İçerik Dağıtım Sistemleri

İçerik dağıtım sistemleri, dijital verilerin kullanıcıya hızlı, güvenilir ve kontrollü biçimde ulaştırılmasını sağlayan temel altyapı çözümleridir. Bu sistemler; kullanıcı sayısı, içerik türü, erişim yoğunluğu ve ağ koşulları gibi parametrelere bağlı olarak farklı mimari biçimlerde tasarlanabilmektedir. Eğitim, medya, eğlence, IoT ve kurumsal uygulamalar gibi geniş yelpazede kullanılan bu çözümler, merkezi yapılardan dağıtık ve hibrit modellere kadar çeşitlenmektedir. Geleneksel sunucu–istemci yaklaşımlarından, modern CDN, P2P ve yazılım tanımlı ağ (SDN) tabanlı yapılara uzanan bu evrim, performans, güvenlik ve ölçeklenebilirlik bakımından farklı avantajlar ve sınırlılıklar doğurmaktadır.

İçerik dağıtım sistemleri yalnızca veri iletimini hızlandıran teknik çözümler değil; aynı zamanda içerik güvenliği, erişim kontrolü, yük dengeleme ve sistem ölçeklenebilirliği açısından da kritik rol üstlenen bütüncül mimari bileşenlerdir. Aşağıdaki alt bölümlerde, içerik dağıtım sistemleri türleri teknik mimari ve işlevsel açıdan karşılaştırmalı olarak ele alınacak, ardından önerilen ağaç tabanlı yaklaşımın bu genel çerçevedeki konumu açıklanacaktır.

İstemci–sunucu modeli, internetin erken dönemlerinden bu yana en temel içerik iletim mimarilerinden biri olarak kullanılmaktadır (Wolman vd., 2000). Bu yapıda tüm içerik merkezi bir sunucuda tutulur ve kullanıcı istekleri doğrudan bu sunucuya yönlendirilerek karşılanır. Mimari basitliği ve uygulanabilirliği nedeniyle uzun yıllar boyunca varsayılan çözüm olmuştur; özellikle düşük yoğunluklu trafik koşullarında yeterli performans sunabilmesi bu yaygınlığın temel nedenidir (Gupta ve Garg, 2015).

Bununla birlikte, kullanıcı sayısının hızla artması ve içerik hacimlerinin büyümesi, bu modelin ölçeklenebilirlik sınırlarını açığa çıkarmıştır. Tek bir merkezi sunucuya bağımlılık, yoğun trafik altında işlemci (CPU), bellek (RAM) ve ağ arabirimi gibi kaynaklarda ciddi darboğazlar oluşturmakta; yanıt sürelerini yükseltmekte ve servis sürekliliğini tehdit etmektedir. Özmen ve arkadaşlarının (2019) 10.000 eşzamanlı kullanıcı talebi altında yaptığı testler, bu modelin belirgin performans sınırlılıkları sergilediğini ve paket kayıplarının ortaya çıktığını göstermiştir. Benzer şekilde, Zhang,

Rao ve Towsley (1998), istemci ile sunucu arasındaki fiziksel mesafe arttıkça gecikme sürelerinin dramatik biçimde yükseldiğini rapor etmektedir.

Büyük ölçekli servis sağlayıcılar, bu sınırlılıkları aşmak amacıyla merkezi yapıdan dağıtık çözümlere yönelmiştir. Nam ve diğerleri (2014), YouTube'un farklı coğrafi bölgelerde konumlandırılmış yüzlerce önbellek sunucusu aracılığıyla içerik erişimini optimize ettiğini belirtmektedir. Ancak Famaey ve çalışma arkadaşları (2013), merkezi yükün dağıtılmasıyla performans artışı elde edilse de içeriklerin çok noktada çoğaltılmasının veri tutarlılığı ve güncelleme maliyetlerini gündeme getirdiğini vurgulamaktadır.

Bu noktada öngörücü önbellekleme algoritmaları, istemci–sunucu modelinin kısmen optimize edilmesini sağlayan bir yaklaşım olarak öne çıkmaktadır. Famaey, Wauters ve Turck (2011), geçmiş kullanıcı davranışlarına dayalı talep tahminine dayanan bu tür mekanizmaların, sıkça erişilen içeriklerin daha erişilebilir konumlarda tutulmasını sağlayarak hem gecikmeyi azalttığını hem de sunucu yükünü dengelediğini göstermektedir.

İstemci–sunucu modelinin sınırlılıklarını aşmak amacıyla, istemciler ile merkezi sunucu arasına yerleştirilen ara sunucular (proxy-cache) geliştirilmiştir (Wang ve Padmanabhan, 2000). Bu yaklaşımda, sık erişilen içerikler ara katmanda saklanarak tekrar eden taleplerin doğrudan proxy üzerinden karşılanması hedeflenir. Elkhameesy ve Mohamed (2013), bu yöntemin orijin sunucu üzerindeki yükü önemli ölçüde azalttığını ve gecikmeleri optimize ettiğini göstermiştir. Ancak istemci–sunucu tabanlı sistemler, ölçeklenebilirlik ve coğrafi dağılımı etkin biçimde yönetme açısından yetersiz kalmakta; bu nedenle içerik dağıtım ağları (CDN) gibi daha gelişmiş çözümlerin geliştirilmesi kaçınılmaz hâle gelmektedir.

Önbellek–proxy yöntemi, istemci–sunucu mimarisinin sınırlamalarını hafifletmek üzere tasarlanmış, performans odaklı bir stratejidir (Zhang, Rao ve Towsley, 1998). Bu modelde, merkezi sunucudan bağımsız ara düğümler üzerinde sık kullanılan içeriklerin kopyaları tutulur; böylece sonraki istekler doğrudan önbellekten karşılanır. Bu yöntem hem ağ üzerindeki yükü azaltmakta hem de merkezi sunucu üzerindeki işlem baskısını hafifletmektedir (Wang ve Padmanabhan, 2000). Özellikle yüksek trafikli senaryolarda, bu ara katman mimarisi gecikmeleri düşürerek sistemin genel yanıt verebilirliğini artırır.

Önbellekleme performansını daha da iyileştirmek amacıyla, kullanıcı davranışlarının analizine dayalı öngörücü algoritmalar geliştirilmiştir. Famaey, Wauters ve Turck (2011), geçmiş istek örüntülerine dayanarak içeriklerin popülerlik temelli önceliklendirilmesinin önbellek verimliliğini artırdığını göstermektedir. Bu tür dinamik mekanizmalar, özellikle ani popülerlik kazanan içerikler veya canlı yayınlar gibi gerçek zamanlı senaryolarda sistemin hızla uyum sağlamasını mümkün kılmakta ve içerik sunum sürekliliğini güvence altına almaktadır.

Bununla birlikte, önbellek yapılarının uygulanmasında zorluklar da bulunmaktadır. Özellikle içeriğin sık güncellendiği ortamlarda, önbellekteki verinin geçerliliği ve bütünlüğü önemli bir sorun alanı oluşturmaktadır. Shi ve çalışma arkadaşları (2011), bu sorunu çözmek için medya nesnelerinin tam içerik yerine segmentlere bölünerek önbelleğe alınmasını öneren segment tabanlı yaklaşımlar geliştirmiştir. Bu yöntem, güncelleme sürelerini azaltırken depolama kaynaklarının daha etkin kullanılmasını sağlar.

İstemci–sunucu ve önbellek–sunucu mimarileri performans, ölçeklenebilirlik ve gecikme açısından farklı avantajlar sunmaktadır. Gupta ve Garg (2015), bu iki yaklaşımın içerik dağıtım ağları içerisinde senaryoya bağlı olarak birlikte veya ayrı ayrı kullanılabileceğini vurgulamaktadır. Canlı yayınlar veya viral içerikler gibi düşük gecikmeli erişim gerektiren uygulamalarda önbellek tabanlı çözümler öne çıkarken; zaman duyarlılığı daha düşük içeriklerde istemci–sunucu mimarisi hâlen geçerli bir çözüm olarak kullanılmaktadır.

Mobil cihazların yaygınlaşmasıyla birlikte, içerik dağıtım stratejilerinde yeni optimizasyon gereksinimleri ortaya çıkmıştır. Kovvali ve Boyle (2014), mobil ağlara entegre edilen performans artırıcı önbellek sunucuların kullanıcılara daha yakın veri erişimi sağladığını ve sistemin toplam verimliliğini yükselttiğini göstermektedir. Bu bulgu, içerik dağıtım mimarilerinin yalnızca sunucu–istemci ilişkisi ile sınırlı kalmayıp, ağın tüm bileşenlerini kapsayan esnek ve dağıtık bir yapıda tasarlanması gerektiğini ortaya koymaktadır.

Önbellek–sunucu yaklaşımı; veri trafiğini yerel düzeyde çözümleyerek merkezi yükü azaltmakta, yanıt sürelerini optimize etmekte ve ani trafik dalgalanmalarına karşı ağın dayanıklılığını artırmaktadır. Bu özellikleriyle sistem, geleceğin içerik dağıtım mimarilerine ölçeklenebilirlik ve esneklik gibi kritik avantajlar sunmaktadır.

Peer-to-Peer (P2P) mimarisi, merkezi bir sunucuya bağımlı olmaksızın, ağ üzerindeki istemcilerin hem içerik tüketicisi hem de sağlayıcısı olarak işlev gördüğü dağıtık bir iletişim modelidir. Bu yaklaşımda her istemci (peer), diğer düğümlerden veri alabilir ya da onlara veri sağlayabilir. Doğal ölçeklenebilirlik kapasitesi ve hata toleransını artıran yapısı, P2P'yi geleneksel istemci-sunucu mimarilerine kıyasla önemli ölçüde avantajlı kılmaktadır (Kumar ve Professor, 2023; Fortino ve Mastroianni, 2009). Ayrıca cihazdan cihaza doğrudan veri aktarımını esas alan Device-to-Device (D2D) stratejileri, yüksek kullanıcı yoğunluğu altında P2P ağlarının etkinliğini daha da artırmaktadır (Xu ve ark., 2019).

Bununla birlikte, P2P mimarisi özellikle erişim denetiminin kritik olduğu senaryolarda ciddi güvenlik ve bütünlük sorunları doğurabilmektedir. DRM korumalı içeriklerin düzensiz replikasyonu, lisans ihlalleri ve veri suistimalleri için zemin hazırlamaktadır. Bu nedenle, önerilen TB-CDN modeli; P2P'nin sunduğu dağıtık erişim esnekliğini, merkezi kontrol mekanizmaları ve güvenli replikasyon ilkeleriyle bütünleştirerek daha denetimli bir çözüm sunmaktadır. Literatürde BitTorrent gibi P2P sistemlerinde katkı bazlı kaynak tahsisi ve teşvik mekanizmaları önerilmiştir (Carbunaru ve ark., 2011); ancak bu sistemler çoğunlukla açık veri ortamlarına odaklanmakta ve kontrollü senaryolar için sınırlı kalmaktadır. Eğitim ya da kurumsal ortamlarda, kullanıcı kimlik doğrulaması ve içerik şifreleme katmanları bu nedenle kritik rol üstlenmektedir.

Son dönemde geliştirilen Wi-Fi tabanlı mobil P2P protokolleri (Tuono ve ark., 2019) ve blockchain tabanlı içerik paylaşım modelleri (Pasupuleti, 2025), bu mimarinin farklı alanlara entegrasyonu için umut verici örnekler sunmaktadır. Öte yandan, kullanıcı davranışlarının sistem verimliliği üzerindeki olumsuz etkileri yoğun biçimde incelenmiştir (Hosanagar ve ark., 2010). Gelecekte, yapay zekâ destekli talep tahmin sistemleri (Chakraborty ve ark., 2022) ile ölçeklenebilir içerik bulutlama çözümlerinin, P2P tabanlı içerik dağıtım mimarilerini daha dengeli, güvenli ve sürdürülebilir hâle getirmesi beklenmektedir.

Yazılım Tanımlı İçerik Dağıtım Ağları (SDCDN – Software Defined Content Delivery Networks), geleneksel içerik dağıtım mimarilerine kıyasla merkezi kontrol, dinamik kaynak tahsisi ve ağ görünürlüğü sağlayarak içerik sunumunda önemli bir dönüşüm sunmaktadır (Yang vd., 2023). SDN yaklaşımının sağladığı kontrol ve veri düzlemlerinin ayrıştırılması, SDCDN mimarilerinin içerik taleplerine ve ağ koşullarına gerçek zamanlı uyarlanabilirlik göstermesine olanak tanımaktadır. Bu

bağlamda tez kapsamında geliştirilen TBCDN altyapısı, SD CDN paradigmasının temel ilkeleriyle yapısal uyum göstermekte; özellikle RRR algoritması aracılığıyla SDN'in sunduğu esnek yönlendirme davranışlarını işlevsel düzeyde karşılamaktadır.

TBCDN bileşeni, içeriklerin beş seviyeli hiyerarşik bir yapı üzerinden dağıtılmasını sağlayarak ölçeklenebilirliği garanti altına almaktadır. Literatürde SD CDN mimarilerinde öne çıkan yeniden yapılandırılabilirlik özelliği, TBCDN içinde RRR algoritmasının özyinelemeli yönlendirme kapasitesiyle desteklenmektedir. Bu algoritma, içerik taleplerinin merkezi sunucuya ulaşmadan en yakın önbellek düğümünde çözülmesini sağlayarak hem yanıt süresini minimize etmekte hem de ağ üzerindeki yükü dengeli biçimde dağıtmaktadır. Böylece SDN'in uçtan uca akış kontrol vizyonu, TBCDN'de yerel karar mekanizmaları üzerinden işlevsel karşılık bulmaktadır.

Zhang vd. (2015) tarafından önerilen Kaleidoscope gibi SD CDN mimarileri, içerik dağıtımı için sanal ağ segmentasyonu ve dinamik bulut kaynağı tahsisini bir araya getirirken; TBCDN yapısı, fiziksel sunucularla birlikte rol-tabanlı sanal düğümler üzerinden erişim tanımını yaparak hem güvenliği hem de performansı artırmaktadır. RRR algoritmasının merkezi kontrol gerektirmeksizin özyinelemeli biçimde içerik yönlendirmesi, SDN tabanlı yerel politika şemalarına alternatif bir çözüm ortaya koymaktadır. Benzer biçimde, Boros vd. (2019) tarafından geliştirilen TCP oturumu el değiştirme mekanizması, SDN'in CDN ortamlarında kesintisiz hizmet potansiyelini ortaya koyarken; bu tezde önerilen mimari, kesintisizliği içerik düzeyinde sağlamaktadır. EDU-DRM bileşeninin dinamik lisanslama yapısı sayesinde, erişim talepleri sistem içinde yeniden doğrulanmakta ve yalnızca yetkilendirilmiş oturumlara içerik sağlanmaktadır. Böylece hem güvenlik gereksinimleri korunmakta hem de yönlendirme sürekliliği garanti altına alınmaktadır.

SD CDN'lerin en güçlü katkılarından biri, ağ yüküne göre dinamik kaynak tahsisi yapabilmeleridir. Bu kapsamda geliştirilen TBNS, TBCDN'in farklı trafik profillerindeki davranışını ölçmek üzere kurgulanmış özel bir simülasyon ortamıdır. Bhardwaj vd. (2025) tarafından önerilen biçimsel doğrulama ve simülasyon tabanlı test metodolojilerine benzer biçimde TBNS, erişim gecikmesi, önbellek isabet oranı ve sistem esnekliği gibi metrikler üzerinden analiz gerçekleştirmekte; klasik CDN sistemlerine kıyasla daha düşük gecikme ve daha yüksek eşzamanlı kullanıcı kapasitesi sağlandığını göstermektedir.

Bu tez kapsamında geliştirilen mimari yapı, SDCDN literatüründe tanımlanan yapısal özelliklerle hem kavramsal hem de işlevsel düzeyde uyumludur. TBCDN'in hiyerarşik yapısı ve RRR algoritması, SDN'in merkezi kontrolcüye dayalı yaklaşımına alternatif olarak özyinelemeli bir karar mekanizması sunarken; EDU-DRM bileşeni, dinamik ve rol-tabanlı lisanslama modeliyle SDCDN güvenlik gereksinimlerine karşılık vermektedir. Bu bütünlük içinde önerilen çözüm, medya, IoT ve yüksek ölçekli veri dağıtımını gerektiren tüm ortamlara uygulanabilecek özgün bir model ortaya koymaktadır.

CDN ise dijital içeriklerin kullanıcıya coğrafi olarak en yakın sunuculardan ulaştırılmasını sağlayan geleneksel dağıtık sunucu mimarisidir. Önbellekleme, yük dengeleme ve coğrafi replikasyon gibi stratejilerle gecikmeyi azaltmayı ve erişim performansını artırmayı hedefler. Eğitim, medya ve IoT gibi birçok alanda yaygın kullanılan CDN yapıları, istemci sayısındaki artışa rağmen servis kalitesini sürdürülebilir kılmakta; bu yönüyle TBCDN gibi özelleştirilmiş çözümler için temel altyapıyı oluşturmaktadır.

Geleneksel CDN mimarileri, sabit konumlandırılmış önbellek sunucuları aracılığıyla içerik dağıtan, kural tabanlı yönlendirme ve statik replikasyon tekniklerine dayalı yapılardır. İstemciler, en yakın kenar sunucusuna DNS veya HTTP yönlendirmesi ile ulaşır ve içerik talepleri ilgili düğüm tarafından karşılanır. Ancak bu model, ağ üzerindeki anlık yük değişimlerine ve içerik taleplerinin dinamik doğasına karşı sınırlı adaptasyon yeteneğine sahiptir. Tez kapsamında önerilen TBCDN yaklaşımı, bu sınırlılıkları gidermek üzere daha esnek ve öz yinelemeli yönlendirme temelli bir alternatif geliştirmiştir.

Hibrit CDN yapıları, geleneksel CDN mimarilerini P2P veya bulut tabanlı çözümlerle entegre ederek kaynak kullanımında esneklik sağlar. Bu mimarilerde içerikler, yalnızca statik ön bellek sunucular üzerinde değil, istemciler veya bulut kaynakları aracılığıyla da dağıtılabilir. Ağ koşullarına göre içerik yönlendirmesi dinamik biçimde optimize edilir. Ancak çeşitliliğin artması, yönetim sürecini karmaşıktırmakta ve güvenlik risklerini artırabilmektedir. TBCDN modeli, hibrit yapılara kıyasla daha katı hiyerarşik yapısıyla kontrol ve denetim avantajı sunar.

Blockchain tabanlı CDN mimarileri, içerik replikasyonu ve erişim kayıtlarını dağıtık defter teknolojisi (DLT) ile şeffaf biçimde yönetir. Merkezi kontrol noktalarının

zayıflıklarını ortadan kaldırırken, içerik sahipliği, lisanslama ve erişim logları gibi kritik verilerin manipülasyona karşı korunmasını sağlar. Ancak yüksek işlem maliyetleri ve gecikme sorunları, özellikle gerçek zamanlı içerik dağıtımı için performans sınırlamaları doğurur. TBCDN mimarisi, blockchain kadar maliyetli olmayan ama merkezi denetim gücünü koruyan DRM tabanlı bir güvenlik modeliyle bu ihtiyaca karşılık vermektedir.

Bulut tabanlı CDN yapıları, fiziksel kenar sunucular yerine bulut sağlayıcılarının yönettiği sanal kaynakları kullanır. Bu yaklaşım, içeriklerin coğrafi olarak çoklu veri merkezlerinde yedeklenmesine ve ani trafik artışlarında kaynakların dinamik biçimde ölçeklendirilmesine olanak tanır. Ancak bulut tabanlı CDN'ler, yerel önbellekleme kadar düşük gecikme sağlayamayabilir. TB-CDN modeli, bulut esnekliği yerine yerel önbellek optimizasyonunu önceliklendirmekte ve düşük gecikme hedefini merkeze almaktadır.

Mobil CDN mimarileri, mobil kullanıcılar için içerik erişimini optimize etmeyi hedefler. İçerikler, baz istasyonları, mobil ağ geçitleri ve uç cihazlar üzerinde önbelleğe alınarak erişim süreleri azaltılır. Özellikle yoğun trafiğe sahip kentsel alanlarda taleplerin baz istasyonuna en yakın ön bellek düğümünden karşılanması mümkündür. TBCDN, doğrudan mobil ortamlar için tasarlanmamış olsa da ağ katmanlarını uç cihazlara yakınlaştırması yönüyle Mobile CDN ile benzerlik göstermektedir.

Ağaç tabanlı içerik dağıtım ağları, yüksek eşzamanlılık gerektiren uygulamalarda verimlilik, ölçeklenebilirlik ve kaynak optimizasyonu açısından güçlü bir mimari yaklaşım sunar. Hiyerarşik düğüm yapısı sayesinde içerikler, çok noktaya yayın (multicast) desteğiyle minimum bant genişliği kullanılarak çok sayıda kullanıcıya ulaştırılabilir. Bu yapı, gecikmeyi azaltırken yük dengelemesi ve kullanıcı deneyiminin iyileştirilmesine de katkı sağlar. Ayrıca, düğüm hatalarında alternatif yolların hızla devreye alınabilmesi hizmet sürekliliğini güçlendirir. Ancak performans; ağ topolojisi, tıkanıklık noktaları ve yük dengesizliklerinden doğrudan etkilenir. Bu nedenle, yapay zekâ destekli uyarlamalı algoritmalar, dinamik izleme mekanizmaları ve gerektiğinde P2P entegrasyonu gibi hibrit çözümler, gelecekteki ağaç tabanlı CDN modelleri için kritik geliştirme alanlarıdır. Tez kapsamında bu mimari yapının ayrıntılı analizi ve literatür örnekleri Bölüm 4.2'de sunulmaktadır.

2.3.1. İçerik dağıtım sistemi altyapı bileşenleri

İçerik Dağıtım Ağları modern internet mimarisinin temel bileşenlerinden biri haline gelmiş ve geniş ölçekli dijital içeriklerin hızlı, güvenli ve verimli biçimde son kullanıcıya ulaştırılmasını mümkün kılmıştır. Bu yapılar yalnızca içerik erişimini kolaylaştırmakla kalmayıp; performans optimizasyonu, güvenlik, kullanıcı deneyimi ve teknolojik evrim boyutlarında çok yönlü araştırma alanlarını da beraberinde getirmektedir.

CDN'lerin kullanıcı deneyimini artırmadaki rolü literatürde sıkça vurgulanmaktadır. Krishnan ve Sitaraman (2013), yüksek kaliteli video akışlarında düşük başlangıç gecikmesi ve kesintisiz oynatımın kullanıcı memnuniyetini doğrudan belirleyen faktörler olduğunu, bu gereksinimlerin ise uç sunucular üzerinden sağlanan içerik önbellekleme mekanizmalarıyla karşılandığını göstermiştir. Benzer şekilde, Karaata, Almutairi ve Alsubaihi (2022) çalışmasında, CDN altyapısının erişim gecikmelerini azaltarak içerik sunum hızını artırdığını; özellikle artan video tüketimi çağında izleyici bağlılığını sürdürmenin bu mekanizmalarla mümkün olduğunu ortaya koymuştur. Maillé, Simon ve Tuffin (2015) de kullanıcı memnuniyetinin CDN performansı ile doğrudan ilişkili olduğunu vurgulamaktadır.

CDN başarımını etkileyen bir diğer kritik unsur ise akış protokolleridir. Özellikle DASH (Dynamic Adaptive Streaming over HTTP) ve HLS (HTTP Live Streaming) protokolleri üzerine yapılan karşılaştırmalı çalışmalar, her iki protokolün ölçeklenebilirlik, kullanıcı deneyimi ve CDN uyumluluğu açısından farklı güçlü ve zayıf yönler sergilediğini ortaya koymaktadır (Fan ve ark., 2018; Khan, 2023). DASH, adaptif bitrate (ABR) yönetiminde esnek çözümler sunarken, HLS'in daha geniş cihaz ve platform uyumluluğu öne çıkmaktadır. Bu nedenle, içerik dağıtımında tercih edilen protokol yalnızca teknik kısıtlar değil, aynı zamanda kullanıcı profili ve hizmet sağlayıcının önceliklerine göre şekillenmektedir.

Bu bulgular, içerik dağıtım sistemlerinin operasyonel başarısının yalnızca altyapı ölçeklenebilirliğine değil, aynı zamanda kullanılan akış protokollerinin sistemle olan teknik uyumuna da doğrudan bağlı olduğunu göstermektedir.

CDN altyapıları açısından güvenlik, performans kadar kritik bir odak noktasıdır. Doğaları gereği DoS (Denial of Service) gibi saldırılara açık olan bu yapılar, ayrıca yönlendirme tutarsızlıkları veya önbellek manipülasyonu gibi zafiyetler nedeniyle kötüye kullanım risklerini de barındırmaktadır (Zheng, 2024; Guo ve ark., 2020).

Giura ve Reyes (2011), farklı CDN mimarilerinde güvenlik mekanizmalarının uygulanma maliyetlerini karşılaştırmalı olarak incelemiş ve performans–güvenlik dengesinin, ölçeklenebilir hizmetlerin sürdürülebilirliği için kritik olduğunu vurgulamıştır.

CDN teknolojilerinin evrimi, yalnızca güvenlik çözümlerinin değil, aynı zamanda mimari çeşitliliğin ve işlevsel esnekliğin de gelişmesini beraberinde getirmiştir. Fog Computing ile CDN entegrasyonu (Alghamdi, Mahfoudh ve Barnawi, 2019), özellikle gerçek zamanlı içerik sunumunda düşük gecikme ihtiyacını karşılamaya yönelik güçlü bir yaklaşım olarak öne çıkmaktadır. Bunun yanı sıra, CDN-as-a-Service (CDNaaS) yapıları, sanallaştırılmış CDN örneklerinin talebe bağlı olarak dinamik biçimde oluşturulmasına olanak tanımakta; içerik sağlayıcılara kaynak esnekliği ve ölçeklenebilirlik avantajları sunmaktadır (Frangoudis, Yala ve Ksentini, 2017).

Ölçeklenebilirliği artırmak ve değişen kullanıcı taleplerine hızlı yanıt verebilmek için çoklu CDN iş birlikleri günümüzde öne çıkan bir diğer eğilimdir. Rodrigues ve arkadaşları (2014), yerleştirilmiş CDN’ler arasında kurulan bu tür iş birliklerinin hem toplam operasyon maliyetlerini düşürdüğünü hem de kullanıcı deneyimini anlamlı ölçüde iyileştirdiğini rapor etmiştir. Benzer şekilde, Balachandran ve ark. (2013), farklı CDN’ler arasında kaynak paylaşımı ve önbellekleme stratejilerinin senkronizasyonunun, bölgesel erişim desenleri ve zamanlama varyasyonları analiz edilerek optimize edilebileceğini göstermektedir.

Bununla birlikte, kullanıcı tarafından oluşturulan içeriklerin (User-Generated Content – UGC) hacmindeki hızlı artış, geleneksel CDN mimarilerine önemli bir baskı oluşturmuştur. Jin, Wen ve Zhang (2014), bu artan yükün üstesinden gelebilmek için Content-Delivery-as-a-Service (CoDaaS) modelini önermiş; bulut tabanlı bu yaklaşımın içerik yönlendirmeyi kolaylaştırırken aynı zamanda ölçeklenebilirlik sağladığını göstermiştir. Bu model, klasik CDN yapılarının UGC yoğun ortamlara uyum sağlamasında kritik bir dönüm noktası olarak değerlendirilmektedir.

Ağ uçlarında gerçekleştirilen içerik önbellekleme stratejileri, özellikle mobil kullanıcılar için gecikmeleri minimize ederek video akışı gibi yüksek bant genişliği gerektiren uygulamalarda QoE’yi ciddi biçimde artırmaktadır. Monsao ve arkadaşları (2022), içeriklerin kullanıcılara daha yakın noktalarda konumlandırılmasının erişim sürelerini belirgin şekilde azalttığını ortaya koymuştur. Bu bulgular, Ma ve

arkadaşlarının (2017) mobil video akış senaryolarındaki bant genişliği kısıtları ve ağ istikrarsızlıkları üzerine yaptığı çalışmalarla da örtüşmektedir.

CDN sistemlerinin geleceği, yeni nesil ağ teknolojileriyle olan entegrasyon süreçleri tarafından şekillendirilmektedir. Özellikle Information-Centric Networking (ICN) paradigmasının CDN yapılarıyla bütünleştirilmesi, içerik erişimini hızlandırmak ve ağ kaynaklarını daha verimli kullanmak için umut verici bir yaklaşım olarak görülmektedir (Yan ve ark., 2019). Bu tür birleşik yapılar, 5G ve ötesi iletişim altyapılarının gereksinim duyduğu ağ dilimleme (network slicing) gibi ileri tekniklerle de uyumlu çözümler sunmayı hedeflemektedir.

Güncel literatür, CDN sistemlerinin yalnızca içerik dağıtımını hızlandırmakla kalmadığını; aynı zamanda güvenlik, performans, iş birliği ve teknoloji entegrasyonu gibi çok boyutlu gereksinimlere çözüm üreten bir ekosisteme dönüştüğünü ortaya koymaktadır. Bu bağlamda, CDN günümüz internet altyapısında kritik bir rol üstlenmekte ve gelecekteki araştırmaların bu yapının esneklik, ölçeklenebilirlik ve güvenlik boyutlarını derinleştirilmesi hem akademi hem de sektör için stratejik avantajlar yaratacaktır.

CDN içinde sunucu yerleşimi, sistemin genel performansı, verimliliği ve kullanıcı deneyimi üzerinde belirleyici bir faktör olarak öne çıkmaktadır. Hem geleneksel hem de modern ağ mimarilerinde, içerik erişiminin gecikmesiz, güvenilir ve yüksek verimlilikle sağlanabilmesi için sunucuların doğru konumlandırılması kritik bir tasarım parametresidir. Bu bağlamda literatür, sunucu yerleşiminin yalnızca içerik dağıtımını değil, aynı zamanda istek yönlendirme, yük dengeleme ve ağ maliyetlerini doğrudan etkilediğini ortaya koymaktadır.

Chen ve Li (2022), etkili sunucu yerleşiminin hizmet kalitesi (QoS) hedefleri doğrultusunda stratejik bir karar mekanizması olduğunu vurgulamaktadır. Doğru konumlandırma, gecikmeyi azaltmakta, bant genişliği maliyetlerini düşürmekte ve ağ üzerindeki yükü dengeleyerek kullanıcıya daha yüksek kalitede hizmet sunulmasını sağlamaktadır.

Bununla birlikte, büyük ölçekli çevrimiçi hizmetlerde kullanıcı talebinin zaman ve coğrafyaya bağlı olarak değişkenlik göstermesi, yerleşim problemini oldukça karmaşık bir hale getirmektedir. Kuo ve Lin (2016), geleneksel yöntemlerin genellikle statik yerleşim modellerine dayandığını ve bu nedenle dinamik içerik tüketim

desenlerine yeterince cevap veremediğini belirtmektedir. Bu durum, gerçek zamanlı talep dalgalanmalarına uyum sağlayabilecek esnek ve uyarlanabilir stratejilere olan ihtiyacı artırmaktadır.

Bu doğrultuda literatürde farklı algoritmik yaklaşımlar geliştirilmiştir. Örneğin, Liu ve çalışma arkadaşları (2019), bulut tabanlı CDN'lerde (CCDN) sunucu yerleşimini optimize etmek amacıyla Q-learning algoritmasını önermiştir. Çalışma, öğrenme temelli modellerin içerik yerleşimini dinamik biçimde optimize ederek hem kaynak kullanımını verimli hale getirdiğini hem de hizmet düzeylerini korurken maliyetleri azalttığını göstermektedir.

Öte yandan, sunucu yerleşimi ile içerik önbelleklemenin birlikte ele alındığı bütüncül yaklaşımlar literatürde dikkat çekmektedir. Xu ve çalışma arkadaşları (2018), içerik çoğaltımı, önbellekleme ve yük dağıtımını süreçlerini entegre biçimde yöneten bir mimari önererek, sistemde karşılanamayan istek oranını önemli ölçüde azalttıklarını ve performans darboğazlarını önlediklerini raporlamıştır. Bu tür bütünleşik yapılar, özellikle yoğun kullanıcı trafiği altında CDN altyapısının sürdürülebilirliğini artıran kritik çözümler arasında değerlendirilmektedir.

Önbellekleme stratejileri, sunucu yerleşiminin etkinliğini doğrudan belirleyen unsurlardan biridir. Li ve Simon (2013), birçok CDN sisteminde kullanıcı taleplerine göre dinamik güncellenebilen içerik önbellekleme stratejilerinin benimsendiğini vurgulamaktadır. Bu tür esnek mekanizmalar, yüksek önbellek isabet oranlarının korunması ve dolayısıyla sistem performansının artırılması açısından kritik öneme sahiptir. Özellikle içerik popülaritesinin hızla değiştiği senaryolarda, dinamik önbellek yönetimi kullanıcı deneyimini (QoE) doğrudan iyileştirmektedir.

Bunun yanında, kodlanmış önbellekleme (coded caching), sunucu yerleşim stratejilerini güçlendiren yenilikçi bir yaklaşım olarak öne çıkmaktadır. Yang ve Gündüz (2018), dosyaların kodlanmış parçalar halinde çoklu sunuculara dağıtılması yoluyla iletim sürecinin optimize edilebildiğini ve toplam bant genişliği tüketiminin azaltılabildiğini göstermektedir. Bu yöntem yalnızca içerik dağıtım verimliliğini artırmakla kalmayıp, aynı zamanda multicast fırsatları oluşturarak CDN performansını ileri düzeye taşımayı amaçlamaktadır.

Buna karşın, sunucu yerleşimi alanındaki ilerlemelere rağmen çözülmesi gereken zorluklar varlığını sürdürmektedir. Özellikle içeriğin sık güncellendiği sistemlerde,

önbellek tutarlılığı ve veri bütünlüğünün korunması halen kritik bir problem alanıdır. Dharmapal (2023), kullanıcıların her zaman en güncel içerik sürümlerine erişebilmesini sağlarken, dağıtık sunucular arasında önbellek uyumunu sürdürmenin karmaşık algoritmalar gerektirdiğini vurgulamaktadır.

Sunucu yerleşiminin etkinliğini belirleyen bir diğer faktör ise kullanıcıların coğrafi dağılımıdır. Ghorbel, Kobayashi ve Yang (2016), sunucu yerleşim stratejilerinin başarısının yalnızca sunucu konumlarıyla değil, aynı zamanda kullanıcıların fiziksel konumları ve ağ koşullarıyla yakından ilişkili olduğunu göstermektedir. Bu nedenle modern CDN çözümleri, yalnızca sunucu yerleşimini değil, aynı zamanda ağ topolojisi ve kullanıcı demografilerini de dikkate alan daha kapsamlı optimizasyon stratejilerine ihtiyaç duymaktadır.

Gelecekteki sunucu yerleşimi stratejilerinin, makine öğrenimi ve yapay zeka teknikleriyle desteklenmesi öngörülmektedir. Sahoo ve çalışma arkadaşları (2017), kullanıcı davranışlarını analiz eden öngörücü algoritmaların, sunucu konumlarının talep modellerine göre dinamik biçimde ayarlanmasını mümkün kıldığını ortaya koymuştur. Bu yaklaşım, CDN altyapılarının daha esnek, öngörülebilir ve talebe duyarlı hale gelmesine katkı sunmaktadır.

Bunun yanında, merkezi olmayan sunucu yerleşimi modelleri de giderek artan bir araştırma ilgisine sahiptir. Maddah-Ali ve Niesen (2015), bu tür dağıtık yaklaşımların daha dengeli bellek kullanımı ve daha hızlı erişim sağlayarak, büyük ölçekli içerik dağıtım sistemlerinde dayanıklılık ve esneklik avantajı sunduğunu belirtmektedir. Bu mimariler, özellikle dinamik trafik senaryolarında CDN altyapısının daha verimli kullanılmasına olanak tanımakta ve gelecekteki içerik dağıtım tasarımlarının yönünü belirlemektedir.

TBCDN modeli, hiyerarşik ağaç tabanlı yapısıyla hem önbellek tutarlılığı sorunlarını azaltmayı hem de coğrafi dağılımın doğurduğu gecikmeleri minimize etmeyi hedeflemektedir. Özyinelemeli istek yönlendirme algoritmasına bağlı olarak içerik talepleri en yakın seviyedeki önbellek düğümünde çözülmekte, böylece hem yük dengesi korunmakta hem de yüksek eşzamanlı erişim senaryolarında sürdürülebilir performans elde edilmektedir. Bununla birlikte ağ trafik yükünü önemli ölçüden azaltmakta ve transfer süresini kısaltmaktadır. Bu yönüyle TBCDN literatürdeki zorluklara karşı özgün ve uygulanabilir bir çözüm modeli ortaya koymaktadır.

2.3.1.1. Content placement

CDN sistemlerinde içerik yerleşimi, sistem performansı, verimlilik ve kullanıcı deneyimi üzerinde doğrudan belirleyici bir bileşendir. Literatürde bu konu hem geleneksel hem de modern ağ mimarilerinde içerik dağıtımını optimize etmeye yönelik farklı stratejiler ve bu stratejilerin altında yatan bilimsel yaklaşımlar üzerinden tartışılmaktadır.

İçerik yerleşimi, kullanıcıya en düşük gecikmeyle ve en yüksek güvenilirlikle içerik sunabilmek amacıyla, verilerin CDN sunucuları arasında stratejik olarak dağıtılmasını ifade eder. Makhkamov (2023), internet servis sağlayıcıları (ISP) açısından trafik yükünü azaltmak ve CDN performansını artırmak için etkin içerik yerleşim algoritmalarının kritik rol oynadığını vurgulamaktadır. Bu algoritmalar, farklı coğrafi bölgelerdeki kullanıcı taleplerine hızlı yanıt verebilmek için içeriklerin hangi düğümlerde önbelleğe alınacağını belirler.

Yerleşim yalnızca operasyonel bir optimizasyon konusu değil; aynı zamanda CDN mimarisini stratejik düzeyde şekillendiren bir tasarım kararıdır. Dieye ve arkadaşları (2018), CDN altyapılarının içerik çoğaltma prensibine dayalı olarak işlediğini ve uç sunucular aracılığıyla içeriklerin son kullanıcıya daha hızlı ulaştırılmasının, kullanıcı deneyimi (QoE) açısından kritik olduğunu belirtmektedir.

Bu çerçevede, içerik yerleşimini optimize etmeye yönelik çok sayıda yöntem geliştirilmiştir. Örneğin Ahvar ve arkadaşları (2018), kullanıcı taleplerini öngörerek içeriklerin ağı farklı noktalarına önceden dağıtılmasına dayalı proaktif bir Sanal Ağ Fonksiyonu (VNF) yerleşim yaklaşımı önermektedir. Bu yaklaşım hem gecikmeyi azaltmakta hem de popüler içeriklerin uç noktalarda konumlandırılmasıyla genel sistem verimliliğini artırmaktadır.

Makine öğrenmesi tekniklerinin içerik yerleşimi süreçlerine entegrasyonu da literatürde öne çıkan önemli eğilimlerden biridir. Lei ve arkadaşları (2017), önbellekleme destekli heterojen ağlarda içerik yerleşimini optimize etmek amacıyla derin öğrenme tabanlı bir yöntem geliştirmiştir. Bu yöntem, kullanıcı davranışlarını ve içerik popülerliğini analiz ederek sistemin yerleşim politikalarını dinamik biçimde ayarlamasına olanak tanımaktadır. Böylece, yüksek talep gören içerikler kullanıcılara daha yakın önbelleklerde saklanmakta ve erişim gecikmeleri kayda değer ölçüde azaltılmaktadır.

Enerji verimliliği de içerik yerleşiminde dikkate alınması gereken kritik bir faktördür. Mandal ve arkadaşları (2011), dağıtık depolama sistemlerinde enerji tüketimini azaltmayı hedefleyen sürdürülebilir içerik yerleşim stratejilerinin önemini vurgulamaktadır. CDN altyapılarının ölçeği büyüdükçe, çok sayıda sunucunun bakım ve işletme maliyetleri de artmaktadır. Bu nedenle içerik yerleşimini optimize etmek, yalnızca performans değil aynı zamanda sürdürülebilirlik perspektifinden de stratejik bir değer taşımaktadır.

Maliyet etkeni de içerik yerleşim stratejilerinde belirleyici bir unsurdur. Dharmapal (2023), bulut tabanlı CDN mimarileri için hizmet kalitesini korurken aynı zamanda işletim maliyetlerini en aza indirmeyi hedefleyen kopya sunucu yerleşim modeli önermektedir. Bu model, sunucu kaynakları, işletim giderleri ve kullanıcı taleplerini birlikte değerlendirerek içeriklerin ekonomik açıdan en verimli şekilde dağıtılmasını sağlamaktadır.

Buna karşın, içerik yerleşim stratejilerinde sağlanan tüm ilerlemelere rağmen halen çözülmesi gereken zorluklar mevcuttur. Özellikle içeriğin sık güncellendiği ortamlarda, önbellek tutarlılığı ve veri bütünlüğü kritik sorunlar olarak öne çıkmaktadır. Zhang ve arkadaşları (T. Zhang vd., 2022), içerik yerleşiminin yönetimi sırasında kullanıcıların daima en güncel sürüme erişmesini sağlamanın oldukça karmaşık bir görev olduğunu belirtmektedir. Bu durum, dağıtık sunucular arasında güçlü bir önbellek senkronizasyonu ve güncelleme algoritmaları ihtiyacını gündeme getirmektedir.

Bununla birlikte, kullanıcıların coğrafi olarak geniş bir alana dağılmış olması içerik yerleşimi açısından başka zorluklar doğurmaktadır. Tuncer ve arkadaşları (2013), farklı bölgelerdeki içerik yerleşim faaliyetlerinin, İnternet Servis Sağlayıcı (ISP) ağları üzerinde baskı yarattığını belirtmektedir. Özellikle kullanıcı taleplerinin belirli coğrafyalarda yoğunlaşması, merkezi kontrol mekanizmalarının verimsizliklere yol açabileceğini göstermektedir. Bu nedenle içerik yerleşim stratejileri, yalnızca içerik kopyalarının konumlandırılmasını değil; aynı zamanda ağ topolojisi, kullanıcı coğrafyası ve talep dinamiklerini birlikte değerlendiren bütüncül bir yaklaşımla ele alınmalıdır.

Geleceğe dönük araştırmalar, yapay zekâ ve blok zincir gibi ileri teknolojilerin entegrasyonu ile içerik yerleşiminin başarısını artırmayı hedeflemektedir. Öngörücü

analizler sayesinde kullanıcı davranışları önceden tahmin edilerek içeriklerin hangi düğümlerde saklanması gerektiği dinamik olarak belirlenebilir (Li ve Simon, 2013). Herbaut ve arkadaşları (2016) ise merkezi yönetim sistemlerinin sınırlamalarını azaltmak amacıyla karar alma süreçlerinin dağıtık düğümlere aktarılmasını önermekte; bu tür merkeziyetsiz modellerin özellikle büyük ölçekli ağlarda daha yüksek dayanıklılık ve esneklik sunduğunu vurgulamaktadır.

Sonuç olarak, içerik yerleşimi CDN performansı, kaynak kullanımı ve kullanıcı memnuniyeti üzerinde kritik bir rol oynamaktadır. Literatür, proaktif yaklaşımlardan makine öğrenimi tabanlı çözümlere ve maliyet odaklı modellere kadar geniş bir yelpazeye işaret etmektedir. Ancak önbellek tutarlılığı, coğrafi dağılım ve kullanıcı taleplerindeki dalgalanmalar, bu stratejilerin uygulanabilirliğini sınırlayan temel zorluklar olmaya devam etmektedir. Gelecek çalışmalarda bu sorunların, merkezi olmayan mimariler ve yapay zekâ destekli uyarlamalı algoritmalarla ele alınması beklenmektedir.

Önbellekleme, CDN performansını doğrudan etkileyen temel mekanizmalardan biridir. İçeriklerin ağ üzerindeki farklı düğümlerde önceden saklanması, kullanıcılara daha düşük gecikmeyle erişim imkânı sunarak hem erişim sürelerini kısaltır hem de orijin sunucular üzerindeki yükü azaltır. Adhikari ve arkadaşları (2012), YouTube gibi büyük ölçekli platformların, trafik hacmi ve coğrafi kullanıcı dağılımını dikkate alarak karmaşık önbellekleme stratejileri uyguladığını belirtmektedir. Etkili bir önbellekleme yapısı, özellikle yoğun talep dönemlerinde sistemin güvenilirliğini artırmaktadır.

Makine öğrenimi gibi ileri tekniklerin önbellekleme süreçlerine entegrasyonu, içerik dağıtımını daha da optimize edebilmektedir. Kullanıcı davranışlarını ve içerik popülerliğini tahmin eden öngörücü algoritmalar, sık talep edilen içeriklerin uç sunucularda önceden saklanmasını sağlayarak kullanıcı deneyimini (QoE) anlamlı ölçüde iyileştirmektedir (Tuncer vd., 2013).

Artan trafik ve kullanıcı sayısı ise güvenlik sorunlarını da gündeme getirmektedir. Chen (2015), içerik tesliminde paralel TCP bağlantıları ve WAN hızlandırma gibi teknolojilerin güvenliği güçlendirdiğini vurgulamaktadır. Ayrıca Named Data Networking (NDN) gibi alternatif mimariler, içeriğin doğrudan ağ içinde önbelleğe alınmasına imkân tanıyarak merkezi yapılara olan bağımlılığı azaltmakta ve daha esnek güvenlik çözümleri sunmaktadır.

CDN altyapısının geleceđi, Information-Centric Networking (ICN) gibi yeni nesil paradigmalardan etkilenmektedir. ICN, ieriklerin IP adreslerine deđil, dođrudan ierik isimlerine gre ynlendirilmesini sađlayarak nbellekleme verimliliđini artırmayı ve ađ ykn dengelemeyi hedeflemektedir (Zhang, 2015). Bununla birlikte, geleneksel CDN'lerin P2P sistemlerle entegre edilmesiyle oluřan hibrit yapılar da giderek nem kazanmaktadır. Ghareeb ve arkadaşları (2013), istemci-sunucu modeli ile P2P yaklařımının birleřiminin leklenebilirliđi ve ierik eriřilebilirliđini artırabileceđini gstermektedir.

Sonuç olarak, nbellekleme stratejileri CDN'lerin performans, gvenlik ve leklenebilirlik gereksinimlerini karřılamada kritik rol oynamaktadır. NFV, bulut biliřim, ICN ve P2P gibi teknolojilerle desteklenen nbellekleme czmleri, sistem kaynaklarının daha verimli kullanılmasını sađlamaktadır. Ancak gvenlik aıkları, ierik gncelliđi ve kullanıcı taleplerinin deđiřkenliđi gibi sorunlar, CDN altyapılarında srekli yenilik ve adaptasyon ihtiyaını gndemde tutmaktadır.

2.3.1.2. Request routing

CDN'lerde istek ynlendirme, kullanıcı taleplerinin en uygun sunucuya iletilmesini sađlayan temel mekanizmalardan biridir. Bu sre, yalnızca performans optimizasyonu deđil, aynı zamanda yk dengeleme, ekonomik kaynak tahsisi ve srdrlebilirlik gibi ck boyutlu faktrleri kapsayan karmařık bir yapıdadır.

Anycast tabanlı ynlendirme teknikleri, CDN uygulamalarında ne cıkkan eđilimlerden biridir. Cicalese ve arkadaşları (2015), Anycast'ın BGP yakınlıđına gre paketleri topolojik olarak en yakın sunucuya ynlendirdiđini; bu sayede ađ yk dengelemesini kolaylařtırarak ani trafik artıřları veya sistem arızaları gibi durumlarda performans srekliiliđini sađladıđını ortaya koymaktadır.

Ynlendirme stratejilerinin optimizasyonu yalnızca teknik faktrlerle sınırlı deđildir. Ekonomik ve katılımcı modeller de giderek nem kazanmaktadır. Garmehi ve arkadaşları (2015), P2P destekli ierik dađıtımında kullanıcı katkılarını en st dzeye cıkırırken kaynak kullanımında adalet ve verimliliđi gzeten mekanizmaların gerekliliđini vurgulamaktadır. Bu yaklařım, istek ynlendirmenin kullanıcı katılımı, ierik eriřilebilirliđi ve kaynak ynetimi ile dođrudan bađlantılı olduđunu gstermektedir.

Poese ve arkadaşları (2010), yönlendirme algoritmalarının sürekli izlenmesi ve güncellenmesi gerektiğini savunmakta; küçük ölçekli değişikliklerin bile genel ağ dinamikleri ve kullanıcı memnuniyeti üzerinde büyük etki yaratabileceğini belirtmektedir. Bu yinelemeli optimizasyon yaklaşımı, CDN'lerin hızla değişen kullanıcı davranışlarına uyum sağlaması açısından kritik öneme sahiptir.

Yeni nesil ağ paradigmaları da istek yönlendirme süreçlerini dönüştürmektedir. Information-Centric Networking (ICN) yapılarında içeriklerin IP adreslerine değil, doğrudan içerik isimlerine göre yönlendirilmesi, kullanıcı deneyimi ve sistem performansı açısından önemli bir paradigma değişimini temsil etmektedir. Detti ve arkadaşları (2012), bu modelin doğrudan içerik odaklı yönlendirme sayesinde erişim verimliliğini artırabileceğini ortaya koymaktadır.

Yönlendirmenin etkileri yalnızca teknik verimlilikle sınırlı kalmayıp, CDN-ISP iş birliklerini de kapsamaktadır. Khare ve Zhang (2011), CDN ve İnternet Servis Sağlayıcıları arasında simbiyotik yönlendirme politikalarının, altyapı yükünü dengeleyerek hem hizmet kalitesini hem de genel ağ performansını artırabileceğini vurgulamaktadır.

Gelişmiş yönlendirme algoritmaları enerji verimliliği ve çevresel sürdürülebilirlik boyutuyla da ele alınmaktadır. Goudarzi ve Mousavinejad (2019), akıllı şebeke (smart grid) teknolojileriyle entegre edilen yönlendirme algoritmalarının enerji tüketimini optimize ederek operasyonel maliyetleri düşürebileceğini ve “yeşil” CDN stratejilerine katkı sağlayabileceğini göstermektedir.

CDN'lerde etkili istek yönlendirme; ağ yakınlığı, yük dengeleme, ekonomik teşvik mekanizmaları, servis sağlayıcı iş birlikleri ve sürdürülebilirlik faktörlerinin bütüncül yönetimini gerektiren çok katmanlı bir süreçtir. Bu alandaki gelişmeler, CDN'lerin yüksek kaliteli içerik taleplerine verimli ve dayanıklı biçimde yanıt vermesini sağlayarak, kullanıcı deneyiminin üst düzeye çıkarılmasında kritik rol oynamaktadır.

2.3.1.3. Network infrastructure

Ağ altyapısı, dijital içeriklerin son kullanıcılara hızlı, güvenilir ve ölçeklenebilir biçimde ulaştırılmasını sağlayan temel bir bileşen olarak öne çıkmaktadır. Bu literatür incelemesi, CDN mimarisinin yapı taşlarını, işlevsel bileşenlerini ve gelişen teknolojik eğilimlerini ele alarak, altyapının performans, güvenilirlik ve esneklik üzerindeki kritik rolünü ortaya koymaktadır.

CDN mimarilerinde temel yaklaşım, içeriklerin son kullanıcıya en yakın konumdan sunulabilmesi için sunucuların farklı coğrafi bölgelere stratejik olarak dağıtılmasıdır. Bu dağıtık yapı, erişim gecikmesini azaltmakta ve kullanıcı deneyimini iyileştirmektedir. Tuncer ve arkadaşları (2013), CDN sağlayıcılarının farklı içerik üreticilerinden gelen verileri saklayan çok sayıda yedek sunucuyu ISP uç noktalarına entegre ederek veri akışını optimize ettiğini ve bant genişliği tüketimini azalttığını ortaya koymuştur.

Geleneksel CDN altyapısı üç temel katmandan oluşmaktadır: orijin sunucular, uç sunucular ve merkezi yönetim katmanı. Orijin sunucular içeriğin ana kaynağını barındırırken; uç sunucular, sıkça erişilen içeriklerin kopyalarını önbellekleyerek son kullanıcıya daha düşük gecikmeyle ulaşım sağlar. Yönetim katmanı ise içerik replikasyonu, istek yönlendirme ve yük dengeleme gibi süreçleri koordine eder. Bu çok katmanlı yapı, sistemin sürdürülebilirliğini artırırken aynı zamanda içerik sunum performansını da optimize etmektedir (Tuncer ve ark., 2013).

Son yıllarda Ağ Fonksiyonlarının Sanallaştırılması (Network Function Virtualization – NFV), CDN altyapılarının esnekliğini ve ölçeklenebilirliğini artıran dönüştürücü bir teknoloji olarak öne çıkmıştır. Mangili, Martignon ve Capone (2014), NFV’nin ağ işlevlerinin fiziksel donanımlardan bağımsız, yazılım tabanlı sanal sunucular üzerinde çalışmasına imkân tanıyarak kaynak kullanımını verimli hale getirdiğini belirtmektedir. NFV destekli CDN altyapıları, özellikle video akış hizmetleri ve sosyal medya platformları gibi yüksek bant genişliği gerektiren uygulamalarda artan yükü daha etkin biçimde yönetebilmektedir.

Ek olarak, CDN işlevlerinin bulut bilişim altyapılarına entegre edilmesi, modern ağ mimarilerinde önemli bir eğilim haline gelmiştir. Grégoire ve Hamel (2014), CDN yeteneklerinin bulut tabanlı hizmetlerle birleştirilmesinin, içerik sağlayıcıların kendi donanımlarına yatırım yapmadan geniş ölçekli içerik sunumu gerçekleştirmelerine olanak tanıdığını vurgulamaktadır. Bulut altyapılarının sunduğu dinamik kaynak ölçekleme kabiliyeti, CDN’nin trafik yoğunluğuna bağlı olarak kaynakları otomatik artırıp azaltabilmesine imkân tanımakta; böylece hem hizmet kalitesi yükselmekte hem de operasyonel maliyetler düşmektedir.

CDN altyapısının evrimi, geleneksel fiziksel sunucu tabanlı yapılardan sanallaştırılmış ve bulut destekli mimarilere doğru kaymakta; bu dönüşüm performans, güvenlik ve

esneklik açısından yeni fırsatlar yaratmaktadır. NFV ve bulut entegrasyonu gibi teknolojik gelişmeler, CDN'leri yalnızca içerik teslim altyapısı değil, aynı zamanda ağ optimizasyonunun stratejik bir bileşeni haline getirmektedir.

2.4. Ağ Simülasyon Araçları

Büyük ölçekli ve yüksek dinamikli bilgisayar ağlarının tasarımı ve performans analizi, yalnızca kuramsal modelleme ile sınırlandırılmaz; gerçekçi senaryolar altında sistem davranışlarının gözlemlenmesi ve yeni mimarilerin test edilmesi için uygulamaya dönük yöntemlere ihtiyaç duyulmaktadır. Ancak bu tür sistemlerin doğrudan fiziksel donanım ortamlarında incelenmesi, yüksek maliyet, karmaşık kurulum gereksinimleri, zaman kısıtları ve sınırlı ölçeklenebilirlik gibi önemli zorluklar içermektedir. Bu nedenle, ağ simülasyon araçları hem akademik hem de endüstriyel araştırmalarda kritik bir metodolojik alternatif olarak konumlanmaktadır.

Ağ simülatörleri, farklı ağ topolojilerinin, iletişim protokollerinin, trafik yükü senaryolarının ve kaynak tüketim modellerinin sanal ortamda modellenmesine olanak tanır. Böylece araştırmacılar, sistem parametrelerini kontrollü bir biçimde değiştirerek performans üzerindeki etkilerini analiz edebilir; önerilen yeni mimarilerin mevcut çözümlerle karşılaştırmalı değerlendirmelerini gerçekleştirebilir. Bunun yanı sıra, simülasyon ortamları deneylerin tekrar edilebilirliğini güvence altına alarak bilimsel çalışmaların metodolojik güvenilirliğini artırmaktadır.

Literatürde, NS-2/NS-3, OMNeT++, OPNET, Mininet gibi açık kaynaklı veya ticari simülatörlerin yaygın olarak kullanıldığı görülmektedir. Bu araçlar, farklı düzeylerde işlevsellik, ölçeklenebilirlik ve gerçekçilik sunmakta; araştırmacılara çeşitli senaryoları modelleme ve analiz etme imkânı sağlamaktadır. Bununla birlikte, klasik simülatörlerin çoğu, özellikle yüksek düğüm sayısı, patlamalı trafik karakteristiği ve içerik odaklı veri akışları gibi modern ağ gereksinimlerini tam anlamıyla karşılamakta sınırlı kalmaktadır. Bu durum, özellikle CDN, SDN ve IoT tabanlı büyük ölçekli altyapılar gibi alanlarda daha özelleşmiş çözümlere olan ihtiyacı artırmaktadır.

Bu tez çalışmasında, mevcut simülatörlerin söz konusu eksiklikleri ayrıntılı biçimde tartışılmakta; özellikle içerik dağıtım sistemlerinin test edilmesi için geliştirilen TBNS aracının motivasyonu ortaya konulmaktadır. TBNS, klasik paket tabanlı simülasyon yaklaşımlarından farklı olarak içerik merkezli veri akışlarını, çok katmanlı topolojileri ve ağaç tabanlı yönlendirme algoritmalarını bir arada değerlendirme imkânı

sunmaktadır. Böylece yalnızca ağ düzeyi performans değil, aynı zamanda erişim gecikmesi, önbellek isabet oranı ve ölçeklenebilirlik gibi içerik odaklı göstergeler de sistematik olarak ölçümlenebilmektedir.

2.4.1. Popüler ağ simülasyon araçları

Ağ simülatörleri, bilgisayar ağlarının işleyişini sanal ortamda modelleyerek farklı senaryoların test edilmesini mümkün kılan araçlardır. Bu sayede, fiziksel donanım yatırımlarına gerek kalmadan yeni protokoller denenebilir, ölçeklenebilirlik sorunları incelenebilir ve sistem performansı güvenilir biçimde değerlendirilebilir. Literatürde hem açık kaynaklı hem de ticari simülasyon araçlarının yaygın biçimde kullanıldığı görülmektedir.

NS-2, ağ simülasyonlarında öncü araçlardan biridir (McCanne, 1997). Ayrık olay (discrete-event) tabanlı yapısıyla kablolu ve kablosuz ağ protokollerini desteklemekte; geniş model kütüphanesi sayesinde araştırmalarda uzun yıllar boyunca yaygın kullanılmıştır. Ancak eski mimarisi ve sınırlı esnekliği nedeniyle günümüzde kısmen yerini daha gelişmiş platformlara bırakmıştır.

NS-3, NS-2'nin devamı niteliğinde geliştirilmiş olup modern bir yazılım mimarisi üzerine inşa edilmiştir (Henderson vd., 2008). C++ ve Python desteği ile genişletilebilirlik ve kullanıcı dostu betikleme imkânı sunmakta; kablosuz ağlar, IP tabanlı protokoller ve yeni nesil mimariler için kapsamlı modüller sağlamaktadır. Bu yönüyle, günümüzde akademik çalışmalarda en yaygın kullanılan açık kaynak simülatörlerden biridir.

OMNeT++, modüler ve bileşen tabanlı yapısıyla öne çıkan, esnek bir simülasyon platformudur (Varga ve Hornig, 2008). Kablosuz sensör ağları, mobil ağlar ve internet protokollerini üzerine yapılan çalışmalarda yaygın tercih edilmekte; görselleştirme ve hata ayıklama araçları sayesinde kullanıcı deneyimini zenginleştirmektedir. OMNeT++, topluluk desteği ve geniş eklenti ekosistemi ile araştırma projelerinde güçlü bir konuma sahiptir.

OPNET Modeler, ticari bir yazılım olup hem akademik hem de endüstriyel uygulamalarda yaygın biçimde kullanılmaktadır (Mittal, 2012). Geniş kapsamlı modelleme yetenekleri, gerçekçi trafik senaryoları oluşturma imkanı ve kapsamlı analiz araçları ile öne çıkmaktadır. Bununla birlikte, lisans maliyeti ve kapalı kaynak yapısı, araştırma topluluğu için kısıtlayıcı unsurlar olarak değerlendirilmektedir.

NetSim, endüstriyel ölçekli senaryolar için tercih edilen bir diğer ticari simülatördür (Veith, Kobza ve Koelling, 1999). Özellikle telekomünikasyon altyapılarının test edilmesinde kullanılmakta; ancak yine lisans maliyeti ve kapalı kaynak yapısı nedeniyle akademik projelerde sınırlı bir yaygınlığa sahiptir.

Bunların yanında, belirli ihtiyaçlara odaklanmış daha özelleşmiş simülatörler de geliştirilmiştir. CDNSim, yüksek ölçekli içerik dağıtım ağlarının (CDN) modellenmesi amacıyla tasarlanmıştır (Stamos vd., 2010). FNCTB (Fusion Net Cache Test Bed) ise, ani kullanıcı taleplerinin ve yüksek trafikli önbellekleme senaryolarının modellenmesinde öne çıkmaktadır (Wen vd., 2020). Bu tür özelleşmiş araçlar, klasik simülatörlerin sınırlı kaldığı içerik odaklı senaryolar için önemli bir katkı sağlamaktadır.

NS-3 ve OMNeT++ gibi açık kaynaklı simülatörler araştırma topluluğu tarafından esneklikleri ve geniş topluluk desteği nedeniyle yoğun biçimde tercih edilmektedir. OPNET ve NetSim gibi ticari platformlar ise kapsamlı modelleme olanakları sunmalarına rağmen, lisans kısıtları nedeniyle sınırlı kullanılmaktadır. CDN ve içerik odaklı senaryolara dönük CDNSim ve FNCTB gibi özel çözümler ise, klasik simülatörlerin yetersiz kaldığı durumlarda önemli bir boşluğu doldurmaktadır.

2.4.2. Kullanım amaçları ve sınırlılıkları

Ağ simülasyon araçları, farklı senaryolarda protokol ve mimari performanslarını analiz etmede araştırmacılara önemli avantajlar sunmaktadır. Ancak, bu araçların sağladığı faydalara rağmen, özellikle büyük ölçekli sistemlerin modellenmesi söz konusu olduğunda yapısal sınırlılıklar belirgin biçimde ortaya çıkmaktadır. Bu sınırlamaların başında, doğruluk ile ölçeklenebilirlik arasındaki denge gelmektedir. Ağ topolojisi büyüdükçe ve düğüm sayısı arttıkça, işlemci gücü ve bellek gereksinimleri üstel biçimde yükselmekte; bu durum milyonlarca istemciyi kapsayan ağların gerçekçi şekilde modellenmesini zorlaştırmaktadır. Ayrıca, gerçek ağların soyutlanarak temsil edilmesi, kaçınılmaz biçimde modelleme basitleştirmeleri içerdiğinden, elde edilen sonuçların doğruluğunu ve genellenebilirliğini sınırlayabilmektedir (Weingartner, vom Lehn ve Wehrle, 2009; Liu, 2008; Musa ve Awan, 2022; La vd., 2021).

Mevcut araçlar genellikle kablosuz ve sensör ağlarına yönelik tasarlandıkları için, içerik dağıtım ağları gibi yüksek eşzamanlılık ve patlamalı trafik gerektiren yapıları

simüle etmekte zorlanmaktadır. Örneğin, OMNeT++ ile gerçekleştirilen en büyük senaryolarda 3025 düğüm (Zarrad ve Alsmadi, 2017), NS-2 ile ise en fazla 5000 kullanıcı isteği modellenebilmiştir (Kabir vd., 2014). Günümüz uygulamaları milyonlarca eşzamanlı kullanıcıya hitap ettiğinden, bu değerler pratik gereksinimlerin oldukça gerisinde kalmaktadır.

Ayrıca, yaygın kullanılan simülatörlerin (OMNeT++, NS-2, NS-3, OPNET) büyük çoğunluğu, düşük düğüm sayısına optimize edilmiş yapılardır. Bu araçlar, CDN altyapılarında görülen yüksek trafik dalgalanmalarını ve yoğun eşzamanlı talepleri gerçekçi biçimde yansıtmakta yetersiz kalmakta; işlemci ve bellek sınırlamaları nedeniyle ölçeklenebilirlik problemleri ve performans düşüşleri ortaya çıkmaktadır.

Bu sınırlamalar, yeni nesil simülasyon çözümleri için güçlü bir motivasyon oluşturmaktadır. Bu bağlamda geliştirilen TBNS, 2²³'e kadar eşzamanlı kullanıcı isteğini destekleyen, patlamalı trafik desenlerini modelleyebilen ve parametrik senaryolar üzerinden geleneksel çözümlerle karşılaştırma yapmaya imkan tanıyan özgün bir simülasyon platformudur. TBNS, ağ topolojisini hiyerarşik bir yapıda kurgulayarak özyinelemeli istek yönlendirmeyi desteklemekte; böylece hem büyük ölçekli CDN'lerin davranışlarını gerçekçi biçimde modellemekte hem de tez kapsamında önerilen TBCDN mimarisiyle bütünleşik analiz sağlamaktadır. TBNS'in mimarisi, işlevsel bileşenleri ve uygulama senaryoları, ilgili 5.3.3. bölümde ayrıntılı biçimde sunulmaktadır.

2.5. Ağ Gecikmesi ile İlgili Kavramlar

Toplam uçtan uca gecikme, bir veri paketinin kaynak düğümden hedef düğüme iletilmesi sırasında maruz kaldığı gecikmeleri ifade eder. Bir iletişim yolundaki toplam gecikme, her ara düğümde meydana gelen iletim gecikmesi $T_{transfer}$, yayılım gecikmesi $T_{propagation}$, işlem gecikmesi $T_{processing}$ ve kuyruklama gecikmesi $T_{queuing}$ olmak üzere dört temel bileşenden oluşur. Her biri, verinin ağ boyunca geçtiği düğümler veya bağlantılar üzerinde farklı seviyelerde zaman kaybına neden olur.

İletim gecikmesi, bir paketin tüm bitlerinin iletim ortamına aktarılması için geçen süredir ve doğrudan paket boyutuna ve bağlantının bant genişliğine bağlıdır. Bant genişliğindeki daralmalar ya da paket boyutundaki artış, bu süreyi doğrudan artırarak toplam gecikmeyi olumsuz etkileyebilir. Bu bileşen, yüksek bant genişliği-gecikme

çarpanına sahip senaryolarda kritik önem taşır (Krishnamoorthy et al., 2020; Zhang et al., 2010).

Yayılım gecikmesi, sinyalin fiziksel ortam üzerinden bir düğümden diğerine ulaşması için gereken süredir. Bu gecikme, düğümler arası mesafeye ve kullanılan iletim ortamının (örneğin fiber, bakır, kablosuz) yayılma hızına bağlıdır. Fiziksel mesafenin artması ve ortamın özellikleri, bu tür gecikmede önemli değişkenlikler yaratabilir (Li et al., 2019; Boriboon & Pongpadpinit, 2016).

İşlem gecikmesi, ağ cihazlarının (yönlendiriciler, anahtarlar) gelen paketleri analiz etmesi, hata kontrolü yapması ve yönlendirme kararlarını alması sırasında oluşur. Bu süre, cihazın işlem gücüne ve yönlendirme algoritmalarının karmaşıklığına bağlı olarak değişir. Yüksek trafik yükü altında ya da karmaşık yönlendirme senaryolarında işlem gecikmesi artarak ağ darboğazlarına yol açabilir (Shen et al., 2023).

Kuyruklama gecikmesi, bir paketin iletim öncesinde ağ cihazı üzerinde sırada beklemesidir. Bu durum, özellikle çok sayıda paketin aynı anda yönlendirilmek istendiği senaryolarda belirgindir. FIFO, LIFO veya daha gelişmiş zamanlama algoritmalarına göre kuyrukta kalma süresi değişebilir. Uygun kuyruk yönetimi stratejileri, bu tür gecikmeleri azaltarak toplam performansa doğrudan katkı sağlar. Ancak yoğun ağ trafiği durumlarında kuyruklar dolabilir, bu da hem gecikmenin dramatik bir şekilde artmasına hem de paket kayıplarına yol açabilir (Sugirtham, 2021; Gettys & Nichols, 2011).



3. LİTERATÜR ARAŞTIRMASI VE ÖNCEKİ ÇALIŞMALAR

Dijital içerik yönetimi alanındaki çalışmalar, büyük ölçüde içerik güvenliği, erişim kontrolü ve dağıtım performansı gibi teknik başlıklar etrafında yoğunlaşmaktadır. Ancak bu başlıklar çoğu zaman birbirinden bağımsız incelenmekte; içeriklerin güvenli erişim ile ölçeklenebilir dağıtım gereksinimlerini birlikte ele alan bütüncül yaklaşımlar oldukça sınırlı kalmaktadır. Özellikle yüksek hacimli veri trafiği ve eşzamanlı kullanıcı erişimi gerektiren alanlarda (örneğin medya, eğlence, IoT ve kurumsal bilgi yönetimi) bu iki teknik ihtiyacın aynı mimari çerçevede karşılanması kritik öneme sahiptir.

Bu eksikliğin temelinde birkaç yapısal neden bulunmaktadır. İlk olarak, DRM ve CDN sistemleri tarihsel olarak farklı mühendislik yönelimleriyle gelişmiştir. DRM teknolojileri; lisanslama, hak tanımı, medya koruması ve kullanıcı kimlik doğrulama gibi güvenlik odaklı gereksinimlerden doğarken; CDN yapıları web içeriklerinin ve medya akışlarının hızlı, istikrarlı ve verimli sunumu amacıyla geliştirilmiştir. Bu farklı öncelikler, araştırmacı topluluklarının ve endüstriyel çözümlerin uzun süre ayrı çizgilerde ilerlemesine neden olmuştur. Ayrıca DRM çözümlerinin çoğu kapalı ve ticarî yapılar olup, kaynak kodları, işleyiş prensipleri ve entegrasyon yöntemleri kamuya açık değildir. Patent korumaları, lisans kısıtlamaları ve ticari gizlilik politikaları, akademik toplulukların bu sistemleri derinlemesine inceleyip CDN yapılarıyla bütünleştirmesini zorlaştırmaktadır.

Teknik açıdan da DRM ile CDN entegrasyonu ciddi güçlükler barındırmaktadır. Güvenlik odaklı sistemler çok katmanlı doğrulama süreçleri nedeniyle işlem yoğunluğu ve gecikmeye duyarlıdır. Buna karşın CDN sistemleri veri iletiminde hız ve verimlilik önceliklidir. Bu karşıt performans hedefleri, mimari düzeyde entegre çözümler geliştirmeyi hem karmaşık hem de maliyetli hale getirmektedir. Literatürdeki çalışmaların çoğu, belirli protokollerin veya algoritmaların verimliliğine odaklanmakta; ancak gerçek zamanlı adaptasyon, yüksek eşzamanlı trafik yönetimi ve senaryo çeşitliliği gibi kritik konular görece sınırlı biçimde ele alınmaktadır.

Bu tez çalışması, mevcut literatürdeki söz konusu boşlukları dikkate alarak şekillendirilmiştir. Bu bölümde geliştirilen sistem mimarisinin kavramsal ve teknik temelleriyle ilişkili üç ana araştırma alanı ayrıntılı biçimde incelenmektedir. İlk olarak, içeriklerin yalnızca yetkilendirilmiş kullanıcılar tarafından erişilebilmesini sağlayan sayısal hak yönetimi (DRM) teknolojileri ele alınmakta, bu kapsamda kullanılan yaklaşımlar, standartlar ve güncel akademik çalışmalar değerlendirilmektedir. Ardından, büyük kullanıcı gruplarına performanslı içerik sunumunu hedefleyen içerik dağıtım ağları (CDNs) incelenmekte; mimari yapılanma, önbellekleme stratejileri, kaynak planlama ve yapay zeka destekli yöntemler ışığında mevcut araştırmalar sınıflandırılmaktadır. Son olarak, geliştirilen sistemin performans değerlendirmesinde kullanılan ağ simülasyon sistemleri tartışılmakta; yaygın kullanılan simülasyon araçlarının işlevleri ve sınırlılıkları ortaya konarak, bu tez kapsamında geliştirilen Tree-Based Network Simulator (TBNS) aracının ortaya çıkış motivasyonu açıklanmaktadır. Böylelikle bu bölüm, yalnızca mevcut araştırmaları özetlemekle kalmamakta, aynı zamanda tezin sunduğu çözümün literatürdeki özgün konumunu ve katkısını da net biçimde ortaya koymaktadır.

3.1. Dijital Hak Yönetimi (DRM)

DRM sistemleri, dijital içeriklerin yetkisiz erişim ve çoğaltmaya karşı korunmasında temel güvenlik katmanlarından birini oluşturmaktadır. Bu yapılar, içerik sahibinin belirlediği koşullar çerçevesinde erişimi düzenleyen teknik ve kriptografik bileşenlerden oluşmakta; lisanslama, kimlik doğrulama ve şifreleme gibi süreçleri bütünsel biçimde yürütmektedir. Güncel literatürde, özellikle dağıtım mimarileri, kimlik doğrulama protokolleri, watermarking teknikleri, blockchain çözümleri ve kuantum sonrası güvenlik yaklaşımları öne çıkan araştırma alanlarını temsil etmektedir.

Mishra ve ark. (2024), çoklu içerik sağlayıcıların bulunduğu dağıtım ortamları için gizlilik korumalı bir DRM mimarisi önererek veri sızıntısı ve kimlik açığa çıkma risklerini azaltmayı hedeflemiştir. Yi ve ark. (2023) ise redactable blockchain tabanlı DRM modeli ile perceptual hash tabanlı kopya tespit mekanizmalarını bütünleştirerek manipülasyon direncini artırmıştır. İçerik sahipliği doğrulamasında yaygın kullanılan watermarking teknikleri de gelişimini sürdürmektedir. Frattolillo (2023) web ortamına uygun watermarking protokolleri için rehber nitelikli bir çerçeve sunarken, Kumari ve

ark. (2023) tunicate swarm optimizasyon algoritmasıyla güçlendirilmiş watermarking modeliyle görüntü güvenliğini artırmıştır. Shi ve ark. (2022) ise CDN ortamlarına uyarlanabilir segment bazlı sıfır-watermarking yöntemi geliştirmiştir.

Kimlik doğrulama, DRM sistemlerinde yalnızca kullanıcı yetkilendirmesi değil, aynı zamanda içerik sunucusunun güvenilirliğinin sağlanması açısından da kritik bir rol oynamaktadır. Fan ve ark. (2022), düşük maliyetli ve anonimlik odaklı bir DRM sistemi geliştirirken; Hussain ve ark. (2022), zayıf protokollerin açıklarını gidermeye yönelik ek güvenlik katmanları önermiştir. Rewal ve ark. (2023) ise biyometrik temelli anonim kimlik doğrulama mekanizmasıyla hem güvenliği hem de gizliliği birlikte optimize eden bir yaklaşım sunmuştur.

Kriptografik açıdan, kuantum sonrası güvenliğe yönelik çalışmalar öne çıkmaktadır. Rewal ve ark. (2024), lattice tabanlı anahtar dağıtım modeliyle kuantum saldırılarına dayanıklı DRM çözümleri üretirken; Dadsena ve ark. (2023), mobil DRM için RLWE tabanlı doğrulanmış anahtar değişim protokolleri önermiştir. Liu ve ark. (2023) ise SPNbox yapısına yönelik integral kriptanaliz yöntemleriyle beyaz kutu şifreleme sistemlerinin güvenlik değerlendirmesine katkı sağlamıştır. Beyaz kutu kriptografi uygulamaları, istemci tarafında güvenliği güçlendirmek açısından kritik görülmektedir. Ferro ve ark. (2023), smart legal contracts tabanlı DRM çözümleriyle gerçek zamanlı içerik koruması sağlarken; Schelkunov (2024) hızlı açık anahtarlı beyaz kutu şifreleme yöntemleri geliştirmiştir. Jimoh ve ark. (2024) ise MPEG-DASH temelli üçlü şifreleme yaklaşımıyla video akış performansını artırmayı hedeflemiştir.

Blockchain tabanlı akıllı sözleşmelerin DRM sistemlerine entegrasyonu da son yıllarda dikkat çekici bir araştırma alanı haline gelmiştir. Frattolillo (2024), güvenilir üçüncü taraf (TTP) ihtiyacını ortadan kaldıran kullanıcı dostu çözümler geliştirerek içerik sahipliği süreçlerini basitleştirmiştir. Yuan ve ark. (2022), chameleon hash kullanımıyla yazılım lisanslama sistemlerinde kontrollü alt-lisanslama mekanizmalarının daha etkin uygulanabileceğini göstermiştir. Bununla birlikte, DRM sistemlerinin yalnızca teknik boyutu değil, ekonomik etkileri de araştırma konusu haline gelmiştir. Volckmann (2025), Denuvo yazılımının PC oyunları üzerindeki etkilerini analiz ederek, DRM çözümlerinin korsanlıkla mücadeledeki rolünü ve gelir üzerindeki istatistiksel etkilerini incelemiştir.

Genel olarak, DRM alanındaki çalışmalar içerik güvenliği, erişim kontrolü ve hak doğrulama mekanizmaları bakımından kayda değer ilerlemeler sunmaktadır. Ancak bu araştırmaların çoğu, DRM çözümlerinin içerik dağıtım altyapılarıyla bütünleşik işleyişine yeterince odaklanmamaktadır. Özellikle CDN mimarileriyle DRM sistemlerini bir araya getiren ölçeklenebilir yaklaşımlar son derece sınırlıdır. Bu nedenle, güvenlik ile performans arasındaki dengeyi kurabilen bütünleşik çözümlere duyulan ihtiyaç devam etmektedir. Ayrıca, mevcut literatürde kullanılan simülasyon ortamlarının çoğu sınırlı düğüm sayılarıyla kısıtlıdır; bu da milyonlarca istemcinin eşzamanlı içerik talep ettiği gerçekçi senaryoların modellenmesini zorlaştırmaktadır. Gerçek dünya koşullarına yakın test ortamlarının yokluğu, sistem güvenliği ve performans değerlendirmesinde önemli bir boşluk oluşturmaktadır. Dolayısıyla, DRM mekanizmalarının CDN altyapılarıyla birlikte ele alındığı, ölçeklenebilir ve yüksek trafiğe duyarlı bütüncül çözümler geliştirilmesi alandaki en temel gereksinimlerden biri olarak öne çıkmaktadır.

3.2. İçerik Dağıtım Ağları (CDN)

CDN teknolojileri, internet üzerinden içerik sunumunun verimliliğini artırmak üzere geliştirilen çeşitli mimari ve algoritmik çözümlerle son yıllarda önemli bir evrim geçirmiştir. Bu bölümde, CDN alanındaki güncel çalışmalara odaklanılarak, dağıtım mimarileri, önbellekleme stratejileri, kaynak yerleştirme, yapay zeka destekli yaklaşımlar ve yazılım tanımlı ağlarla olan bütünleşik kullanım boyutları üzerinden bir inceleme sunulmaktadır.

CDN mimarilerinin esnekliği ve etkinliği, önbelleklerin ve içeriklerin ağa optimal şekilde dağıtılmasıyla doğrudan ilişkilidir. Contreras ve ark. (2023), CDN-as-a-service dilimleme senaryolarında sanal önbellek paylaşımının etkili kullanımını incelemiş, bu yapının kaynak verimliliğini artırdığını ortaya koymuştur. Fog tabanlı CDN mimarilerinde, yerleşim ve içerik dağıtımının birlikte optimize edildiği çalışmasında Yadav ve Kar (2024), Voronoi temelli yaklaşım ve doğal dil işleme teknikleriyle etkili çözümler sunmuştur. MEC ortamlarında çalışan bir diğer çalışma ise Liu ve ark. (2023) tarafından sunulmuş; bu çalışma, öğrenme tabanlı planlama ile belirsizlik altında network slice tahsisini optimize etmeyi hedeflemiştir. Benzer biçimde, SDN tabanlı CDN yapıları son dönemde yaygınlaşan bir paradigma olarak karşımıza çıkmaktadır. Bhardwaj ve ark. (2024), IoT bağlamında kullanıcı merkezli içerik

sunumu için SDN tabanlı bir model önerirken; Kumar ve ark. (2022), video akışına uyarlanabilir P2P-CDN yapıları üzerine odaklanmıştır. Yang ve ark. (2023) ise SD-CDN yaklaşımının CDN mimarilerine katkılarını ve açık sorularını kapsamlı bir derleme çalışmasıyla ele almıştır.

Önbellek yönetimi konusunda da derin öğrenme tabanlı yöntemlerin öne çıktığı görülmektedir. Xu ve ark. (2024), açıklayıcı yapay zeka tekniklerini kullanarak kenar servislerinde zekice önbellekleme stratejileri önermiş; Wang ve ark. (2024), takviyeli öğrenme ile önbellek tanımlama ve terfi politikalarını optimize etmiştir. Liu ve ark. (2023, 2024) tarafından önerilen sistem, CDN önbellek kabul politikasını yeniden kullanım süresine dayalı olarak optimize etmiş ve bu alanda etkili bir model sunmuştur. Bu çalışmalar, CDN performansının önemli bir belirleyicisi olan cache hit oranını artırmaya odaklanmıştır. Bunun yanında, kaynak yerleştirme ve iletim yollarının planlanması da CDN performansının diğer kritik unsurlarındandır. Gao ve ark. (2023), MEC tabanlı ağ kenarında video içeriği yerleştirme için merkezi ve dağıtık algoritmalar önerirken; Panigrahy ve ark. (2022), önbelleğe alma politikaları için kuramsal cache hit üst sınırını ortaya koymuştur. Bu tür kuramsal yaklaşımlar, CDN tasarımlarının sınırlarını belirleme açısından önemlidir.

Dağıtım stratejileri tarafında da dikkat çekici gelişmeler vardır. Zhu ve Gu (2022), multi-CDN yapılarında veri odaklı kullanıcı eşleştirme stratejileri önermiş; Khansoltani ve ark. (2022), PROMETHEE algoritmasıyla CDN sunucu seçimini çok kriterli karar mekanizması olarak ele almıştır. Aynı zamanda, gecikmeye duyarlı çözümler CDN performansını optimize etmeyi amaçlamaktadır. Yan ve Li (2022), LA-Cache mekanizmasıyla CDN önbelleklemesini zamanlayıcı temelli bir yaklaşımla gerçekleştirmiş; Farahani ve ark. (2024) ise gecikme ve maliyet odaklı hibrit P2P-CDN mimarisi önermiştir. Güvenlik boyutunda ise Shao ve ark. (2023), blockchain destekli SDN mimarisiyle güvenli içerik sunumunu sağlarken; Venkateswaran ve ark. (2023), gecikme varyansını minimize ederek yedek sunucuların yerleşimini optimize etmiştir. Benzer şekilde, Zhang ve ark. (2022), maksimum güvenilir akış hesaplama algoritmaları üzerinde durmuş ve bu alandaki temel problemlere katkı sunmuştur. Literatürde ayrıca CDN sistemlerine dair derleme çalışmalar da mevcuttur. Ali ve ark. (2025), güncel CDN mimarilerini kapsamlı biçimde sınıflandırırken; Priyanka ve ark. (2022), CDN alanında kullanılan yöntemlerin etkinliğini çeşitli boyutlar üzerinden değerlendirmiştir.

Bu arařtırmaların ortak noktası, CDN sistemlerinin mimari ve algoritmik olarak sürekli eřitlendiđini gstermeleridir. Ancak buna karřın, literatrde oklu CDN senaryolarında yk dengeleme, ierik nceliklendirme ve gerek zamanlı adaptasyon gibi konular halen paralı biimde ele alınmaktadır. Ađ kenarındaki dađıtım stratejilerinin, kullanıcı davranıřları veya cođrafi yođunluk gibi deđiřkenleri yeterince kapsamaması da nemli bir sınırlılıktır. Bu durum, farklı sektrlere uyarlanabilir ve leklenebilir yeni metodolojilere duyulan ihtiya gndeme getirmektedir.

Ađaç tabanlı ierik dađıtım ađları, literatrde ne ıkan gl mimari yaklařımlardan biri olarak deđerlendirilmektedir. Ađaç tabanlı yapılar, ieriklerin hiyerarřik bir dzen aracılıđıyla u kullanıcılara ulařtırılmasını sađlar. Bu mimaride, dđmler sunucuları ya da nbellek noktalarını, kenarlar ise bu dđmler arasındaki bađlantıları temsil eder. İerik, ađaç yapısı boyunca yukarıdan ařađıya dođru dađıtılır. zellikle ok noktaya yayın yntemine olanak tanıyarak, aynı ieriđin eřzamanlı olarak birden fazla kullanıcıya iletilmesini sađlar; bylece bant geniřliđi kullanımı optimize edilir ve dađıtım verimliliđi artırılır (Liu ve ark., 2019). Liu ve arkadaşları, multicast aktarım ađaçlarının bulut tabanlı ierik dađıtım ađlarında (CCDNs) ierik kopyalama gereksinimini en aza indirdiđini ve bu ynyle olduka verimli olduđunu vurgulamaktadır.

Ađaç yapısının sunduđu hiyerarřik dzen, ierik yerleřimi ve eriřim ynetimi aısından da nemli avantajlar sađlar. Dđmlerin sistematik řekilde organize edilmesi, ierik istekleri iin ynlendirme yollarının optimize edilmesini mmkn kılar. Bylece kullanıcılar ieriklere en yakın dđmden eriřebilir; bu da gecikmeyi azaltarak u kullanıcılar aısından daha yksek QoE sađlar. Multicast desteđi, bireysel sunucuların ykn nemli lde azaltır; nk aynı ierik, ayrı veri akıřlarına gerek kalmadan aynı anda ok sayıda kullanıcıya iletilebilir (Lopez-Fuentes, 2012). Bu durum, zellikle spor msabakaları, canlı yayınlar ve eřzamanlı video izleme gibi yksek eřzamanlılık gerektiren uygulamalarda ciddi avantaj sunmaktadır.

Bunun yanı sıra, ađaç tabanlı CDN yapısı hata toleransı ve sistem gvenilirliđi aısından da nemli katkılar sunar. Herhangi bir dđm arızalandıđında, alternatif yolların hızlı bir řekilde oluřturulabilmesi sayesinde ierik iletiminde kesintilerin nne geilir. Heterojen ve deđiřken ađ ortamlarında hizmet srekliiliđinin korunması ihtiyaı, bu yapıların sunduđu yksek hata toleransı sayesinde daha etkin řekilde karřılanabilir (Jedari & Francesco, 2018). Ancak ađaç tabanlı ierik dađıtım ađlarının

karşılaştığı temel zorluklardan biri, ağ topolojisindeki dinamik değişimlerin etkin bir şekilde yönetilmesidir. Khudabukhsh (2018), değişken ağ koşullarının kararlı ağaç yapılarının kurulmasını zorlaştırabileceğini ve bu durumun içerik dağıtım yollarını verimsizleştirebileceğini belirtmektedir. Ayrıca, artan kullanıcı taleplerinin belirli düğümlerde tıkanıklığa yol açması performans düşüşü yaratabilmektedir. Rathod ve Kulkarni (2014), bu sorunları hafifletmek için trafiği sürekli izleyip gerçek zamanlı yönlendirme uyarlaması yapabilen gelişmiş izleme araçlarının gerekliliğine dikkat çekmektedir.

Gelecekte sürdürülebilir iyileştirmeler sağlamak amacıyla, ağaç tabanlı CDN'lerde yapay zeka ve makine öğrenimi gibi ileri teknolojilerin entegrasyonu kritik bir araştırma alanı olarak öne çıkmaktadır. Kullanıcı davranışlarını tahmin ederek içerik yerleşimini optimize eden yapay zeka temelli algoritmalar, bu yapının çevikliğini ve verimliliğini artırabilir. Bunun yanı sıra, P2P mimarilerle bütünleştirilmiş hibrit modeller de giderek daha fazla ilgi görmektedir. Zhang ve ark. (2020), P2P mekanizmalarının ağaç tabanlı CDN'lere entegre edilmesinin ölçeklenebilirlik ve dayanıklılığı artırabileceğini göstermektedir. Sonuç olarak, ağaç tabanlı içerik dağıtım ağları, geniş ölçekli içerik sunumunda sağlam bir yapı sunsa da ağın dinamik doğasına uyum sağlayacak esnek çözümlerle desteklenmediği sürece potansiyelini tam olarak gerçekleştirememektedir.

3.3. Simülasyon Araçları

Bilgisayar ağlarında ölçeklenebilir simülasyon altyapılarının geliştirilmesi, özellikle içerik dağıtım sistemleri gibi yüksek düğüm sayısı gerektiren senaryolarda önemli metodolojik zorluklar barındırmaktadır. Literatürde yaygın olarak kullanılan birçok simülasyon aracı, belirli ağ mimarilerine özgü sınırlamalar nedeniyle geniş ölçekli test senaryolarını desteklemekte yetersiz kalmaktadır.

Özel amaçlı simülasyon ortamları, belirli kullanım senaryolarında etkili olsa da genel CDN testleri için sınırlı kalmaktadır. Örneğin, kuantum anahtar dağıtımı odaklı simülatörler güvenlik temelli mimarilerde başarıyla kullanılabilir (Dervisevic vd., 2024); ancak içerik yayılımı ve kaynak yönetimi gibi parametreleri detaylı biçimde modelleyememektedir. Benzer şekilde, 6TiSCH tabanlı ağlar için geliştirilen simülasyon ortamları (Kubaszek vd., 2024), zaman duyarlılığına odaklanmalarına

rağmen düğüm yoğunluğu yüksek içerik dağıtım senaryolarında ölçeklenebilirlik sağlayamamaktadır.

IoT odaklı simülasyon ortamlarının da benzer kısıtlar barındırdığı görülmektedir. Ramonet vd. (2024), ns-3 gibi yaygın platformların düşük bant genişliği ve enerji tüketimi gibi metrikleri önceliklendirdiğini; buna karşın içerik tabanlı performans analizlerinde yetersiz kaldığını ortaya koymaktadır. SDN tabanlı sağlayıcı ağlar için geliştirilen SDNSandbox gibi modüler ortamlar da kontrol düzeyinde esneklik sunmakla birlikte, çok sayıda istemci-düğüm etkileşimini gerçekçi şekilde modellemekte sınırlıdır (Solomon vd., 2022).

Uydu tabanlı simülasyon sistemlerinde de benzer sınırlamalar dikkat çekmektedir. LEO uydu takımyıldızlarına yönelik ns-3 modülü (Schubert vd., 2022) ve uydu-karasal bütünleşik ağlar için hazırlanan simülasyon araçları (Jiang vd., 2023), fiziksel katman etkileşimlerini modelleme konusunda güçlü olmakla birlikte, yüksek düğüm sayısına sahip CDN senaryolarında performans sorunları göstermektedir. Özellikle zaman hassasiyetine sahip içerik dağıtım uygulamalarında bu kısıtlar daha belirgin hale gelmektedir.

Hareketli ağ topolojilerine odaklanan simülasyon ortamları da benzer şekilde sınırlı genellenebilirlik sunmaktadır. Örneğin, 3D VANET simülasyonu için önerilen Veins 3D tabanlı modeller (Brummer vd., 2023) ya da UAV topolojilerinde bağlantı kontrolü sağlayan yapay zeka destekli çözümler (Yoo vd., 2023), durağan ve yüksek yoğunluklu düğüm tabanlı CDN yapılarıyla doğrudan uyumlu değildir. Benzer biçimde, sağlık nesneleri ağı (IoHT) için önerilen iletişim protokol değişim modelleri (Weqar vd., 2024) ya da akıllı şehirlerde kötü niyetli davranış tespiti amacıyla geliştirilen makine öğrenmesi tabanlı çözümler (Nayak vd., 2023), oldukça özelleşmiş alanlara hitap etmekte ve genel ağ performans analizleri için genişletilebilirlik göstermemektedir.

Genel olarak bakıldığında, yaygın olarak kullanılan ns-3, OMNeT++ ve Mininet gibi simülatörler, genellikle 100 ila 1.000 düğüm arasında stabil performans gösterebilmekte; ancak bu sınır, içerik akışı, erişim denetimi ve dağıtım stratejileri gibi karmaşık mekanizmaların gerçekçi biçimde test edilmesine engel teşkil etmektedir. Literatürde yer alan birçok çalışmada, bu kısıtlar nedeniyle yalnızca küçük ölçekli

örneklemeler yapılabilmiş ve geniş ölçekli performans analizleri yeterince gerçekleştirilememiştir.

Oysa güncel içerik dağıtım ağları, özellikle medya ve IoT gibi kullanıcı tabanı geniş uygulamalarda, on binlerce istemciyi eşzamanlı olarak desteklemek zorundadır. Böyle bir ölçek için gereken simülasyon altyapısı yalnızca yüksek düğüm kapasitesiyle değil, aynı zamanda CDN ve DRM gibi çok bileşenli yapıların birlikte modellenebilmesini sağlayacak esneklikte olmalıdır. Literatürde bu nitelikleri aynı anda karşılayan bir simülasyon aracının bulunmaması, büyük ölçekli ve çok boyutlu dağıtım modellerinin geliştirilmesi ve doğrulanması açısından ciddi bir boşluk oluşturmaktadır.





4. ÖNERİLEN İÇERİK DAĞITIM AĞI MODELİ VE MİMARİSİ

Bu bölüm, dijital varlıkların büyük ölçekli ve dağıtık ortamlarda hem güvenli hem de yüksek performansla dağıtılmasını hedefleyen, tezin temelini oluşturan özgün sistem mimarisini ve bu mimariyi meydana getiren kavramsal modelleri detaylandırmaktadır. Önerilen bütünleşik yaklaşım, literatürde sıklıkla birbiriyle çelişen iki temel gereksinimi (içerik bütünlüğü ve erişim kontrolü ile dağıtım verimliliği ve ölçeklenebilirlik) aynı anda karşılamak üzere tasarlanmıştır. Bölümün devamında, bu mimarinin üç temel bileşeni olan hak yönetimi sistemi (EDU-DRM), hiyerarşik içerik dağıtım ağı (TBCDN) ve bu yapıyı analiz etmeye yönelik simülasyon aracı (TBNS) teknik derinlikleriyle ve birbirleriyle olan ilişkileri çerçevesinde ele alınacaktır.

Dijital içeriklerin artan çeşitliliği ve ölçeği, özellikle yüksek eşzamanlı erişim senaryolarında bir tasarım ikilemini ön plana çıkarmaktadır. Bir tarafta, monolitik güvenlik modelleri üzerine kurulu DRM sistemleri içerik güvenliğini sağlamada başarılı olsa da ani talep artışlarında performans darboğazlarına girerek ölçeklenebilirlik sorunları yaşamaktadır. Diğer tarafta ise, güvenlik katmanından büyük ölçüde bağımsız çalışan CDN yapıları, dağıtım performansını optimize etse de dinamik erişim kontrol mekanizmalarının bütünleşik biçimde uygulanmasında yetersiz kalmaktadır. Artan veri hacmi, kullanıcı yoğunluğu ve bant genişliği üzerindeki baskı, bu iki alanın tekil çözümlerinin ötesinde hibrit ve bütünleşik mimarilere duyulan ihtiyacı açık biçimde ortaya koymaktadır.

Bu kapsamda geliştirilen bütünleşik mimari, söz konusu tasarım ikilemine yeni bir çözüm paradigması sunmaktadır. Önerilen sistem üç temel kavramsal bileşenden oluşmaktadır: Birincisi, içeriğe erişim haklarını çok boyutlu ve rol-tabanlı bir yapıda yöneten bir hak kontrol ve yetkilendirme sistemi; ikincisi, içerik dağıtımını hiyerarşik bir ağ topolojisi üzerinde, özyinelemeli bir yönlendirme algoritması ile optimize eden bir dağıtım altyapısı ve üçüncüsü, bu karmaşık sistemin performansını farklı senaryolar altında analiz etmek için geliştirilen özel bir simülasyon aracıdır. Geliştirilen hesaplama modeli; uçtan-uca erişim süresi, toplam ağ yükü, önbellekleme başarımı ve lisans kontrol süreçlerinin etkinliği gibi temel performans ölçütlerini

sayısal olarak değerlendirmeyi hedeflemektedir. İlk bulgular, önerilen bütünleşmiş mimarinin, geleneksel ayırık sistemlere kıyasla daha istikrarlı ve verimli bir içerik erişim hizmeti sağladığını işaret etmektedir.

Bu mimari, her biri literatürdeki belirli bir zorluğa çözüm üreten, ancak asıl potansiyellerini eşgüdümlü bir entegrasyonla ortaya koyan iki temel kavramsal model üzerine inşa edilmiştir: Birincisi çok boyutlu bir hak yönetimi sistemi, ikincisi ise hiyerarşik bir içerik dağıtım ağıdır. Bu iki sistem, metodolojik olarak hem bağımsız modüller olarak çalışabilecek hem de bütünleşik bir yapıda birbirini tamamlayacak şekilde tasarlanmıştır. Bu modüler yaklaşım, sistemin farklı gereksinimlere uyarlanabilirliğini ve gelecekteki teknolojik gelişmelere karşı genişletilebilirliğini temin etmeyi amaçlamaktadır.

Mimarinin ilk temel bileşeni EDU-DRM, dijital varlıkların yaşam döngüsü boyunca güvenliğini ve erişim kontrolünü sağlayan dijital hak yönetimi sistemidir. Bu sistem, içerik sağlayıcıların dijital varlıklarını şifrelenmiş biçimde sisteme yüklemesine olanak tanır ve bu varlıklara erişimi, önceden tanımlanmış ilkelere göre yönetir. Farklı yetki seviyelerine sahip kullanıcı profilleri (örneğin; son kullanıcı, içerik yöneticisi, sistem admini) için özelleştirilmiş erişim politikaları dinamik olarak tanımlanabilmektedir. Sistemin modüler yapısı, farklı dijital varlık türlerine yönelik özel güvenlik protokollerinin entegrasyonuna imkân tanırken, platformlar arası çalışabilirliği de korumaktadır.

İkinci temel bileşen olan TBCDN, içerik dağıtım sürecinin performansına odaklanan, hiyerarşik bir ağ topolojisine sahip özel içerik dağıtım ağıdır. Bu sistemde dijital varlıklar, topolojik olarak iç içe geçmiş çok seviyeli bir hiyerarşiye göre dağıtılmaktadır (örneğin: Çekirdek Düğüm → Üst-Seviye Dğümleri → ... → Uç Dğümler). Geliştirilen özyinelemeli yönlendirme algoritması, kullanıcı taleplerini hiyerarşinin en alt katmanından (uç düğümden) yukarı doğru yönlendirerek, içeriğin bulunduğu en yakın topolojik düğümün tespit edilmesini sağlar. Bir içerik talep edildiğinde, yanıtlama sürecinde içeriğin bir kopyası talep yolundaki alt katman düğümlerine de yerleştirilir (önbelleklenir). Bu “talep-yolu önbellekleme” yaklaşımı sayesinde, aynı içeriğe yönelik tekrar eden istekler hiyerarşinin daha alt katmanlarından karşılanarak hem ağın çekirdek katmanlarındaki trafik yükü ciddi oranda azaltılır hem de kullanıcıların erişim gecikmesi minimize edilir.

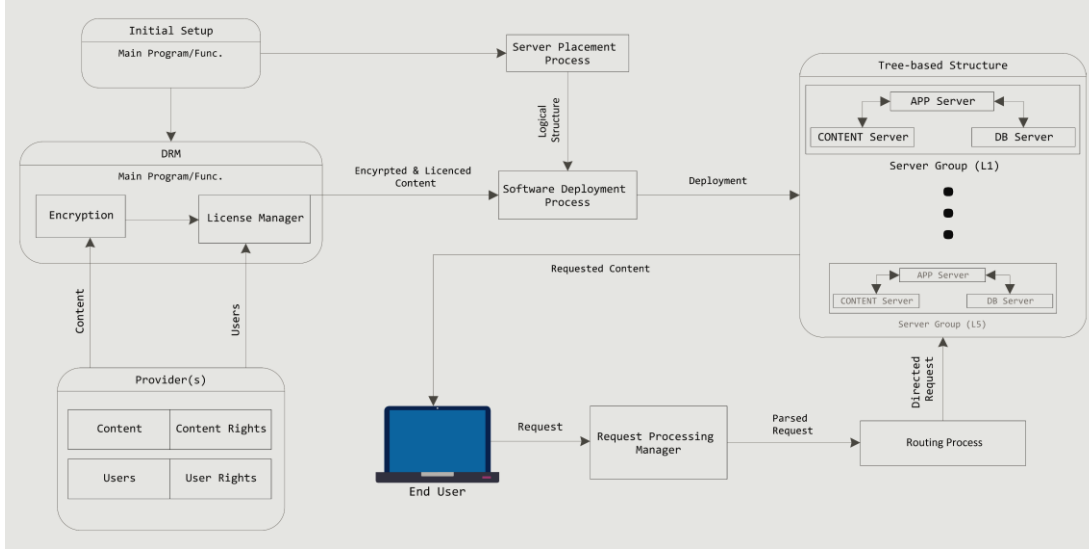
Bu iki sistemin entegrasyonu ile dijital varlıkların yaşam döngüsü aşağıdaki gibi işlemektedir:

- İçerik, sağlayıcı tarafından şifrelenerek hak yönetimi sistemi üzerinden altyapıya yüklenir.
- Erişim politikaları, talepte bulunan kullanıcının profiline ve yetki seviyesine göre dinamik olarak belirlenir.
- Kullanıcı içerik talebinde bulunduğunda, hiyerarşik dağıtım ağı devreye girerek talebi topolojik olarak en verimli düğümden karşılamaya çalışır.
- İçerik, ağ üzerinde her zaman şifreli biçimde taşınır; deşifreleme işlemi yalnızca son kullanıcı cihazında, hak yönetimi sisteminin kontrolü ve denetimi altında anlık ve geçici olarak gerçekleşir.
- İçerik hiçbir aşamada sistem dışına korumasız (açık) biçimde çıkmaz; eş zamanlı olarak, tekrar eden talepler hiyerarşinin uç katmanlarından karşılanarak sistemin genel ölçeklenebilirliği ve performansı artırılır.

Bu bütünleşik yapı, belirli bir uygulama alanına yönelik bir çözüm olmanın ötesinde, güvenlik ve performans gereksinimlerinin kesişim kümesinde yer alan büyük ölçekli dağıtık sistemler için genel bir mimari paradigma sunmaktadır. Özellikle yüksek kullanıcı yoğunluğu, yüksek talep tekrar oranı ve katı güvenlik politikaları gerektiren sistemlerde, sadece güvenliğe veya sadece hıza odaklanan yaklaşımların yetersiz kalacağı açıktır. Bu nedenle, iki temel modelin birlikte tasarlanması, bu tezin temel metodolojik yaklaşımını ve en özgün yönünü oluşturmaktadır.

4.1. Önerilen Sistem Mimarisi ve Bileşenleri

Tez kapsamında geliştirilen bütünleşik sistemin genel mimarisi ve temel iş akışları **Şekil 4.1**'de şematik olarak göstermektedir. Bu mimari, bir dijital içeriğin kaynak sağlayıcıdan (Provider) alınıp son kullanıcıya (End User) ulaştırılmasına kadar olan tüm yaşam döngüsünü kapsayacak şekilde, birbiriyle bütünleşmiş süreçler halinde tasarlanmıştır. Sistemin temel felsefesi, katı güvenlik gereksinimlerini sağlayan Dijital Hak Yönetimi (DRM) süreçleri ile yüksek performans ve ölçeklenebilirlik sunan Ağaç Tabanlı İçerik Dağıtım yapısını tek bir potada eritmektir. Mimarinin işleyişi, içeriğin hazırlanması ve güvenli hale getirilmesi, altyapının stratejik olarak planlanıp kurulması, hiyerarşik sunucu yapısının oluşturulması ve son olarak kullanıcı isteklerinin akıllı bir şekilde karşılanması olmak üzere dört ana fazda incelenebilir.



Şekil 4.1. TBCDN Sistem Mimarisi Şeması

4.1.1. İçerik ve kullanıcı hakları hazırlık süreci

Sistemin başlangıç noktasını, dijital varlıkların ve ilgili yetkilendirme kurallarının tanımlandığı hazırlık süreci teşkil etmektedir. Bu sürecin kaynağı olan Sağlayıcı (Provider) modülü, dağıtılacak olan ham içeriği, bu içeriğin kullanım koşullarını belirleyen içerik haklarını, sisteme erişim potansiyeli olan kullanıcıların listesini ve hangi kullanıcının hangi içeriğe ne tür haklarla erişebileceğini tanımlayan yetkilendirme matrisini barındırmaktadır. Bu ham veriler, sistemin güvenlik kalbi olan DRM modülüne girdi olarak sunulmaktadır. DRM modülü içerisinde, ilk olarak Şifreleme bileşeni ham içeriği AES gibi güçlü kriptografik algoritmalarla şifreleyerek yetkisiz erişime karşı koruma altına alınmaktadır. Sonraki adımda, Lisans Yöneticisi, kullanıcı ve hak bilgilerini esas alarak her bir içerik ve kullanıcı için özel dijital lisanslar oluşturmaktadır. Bu lisanslar, şifrelenmiş içeriği açacak anahtarı ve kullanım kurallarını barındıran güvenli birer dijital jeton görevi görmektedir. Bu sürecin çıktısı olarak, ham içerik artık dağıtımına hazır, güvenli bir paket olan Şifrelenmiş ve Lisanslanmış İçerik haline gelmektedir.

4.1.2. Altyapı kurulum ve dağıtım süreci

İçeriğin güvenli hale getirilmesini takiben, dağıtımın yapılacağı altyapının kurulum süreci başlar. Başlangıç Kurulumu ile tetiklenen bu fazın ilk adımı, stratejik bir öneme sahip olan Sunucu Yerleştirme Süreci'dir. Bu süreçte, kullanıcı yoğunluğu, ağ topolojisi ve hedeflenen gecikme süreleri gibi faktörler analiz edilerek sunucuların ağ üzerinde (coğrafi veya mantıksal olarak) nasıl konumlandırılacağı planlanır. Bu

planlama aşamasının çıktısı, sunucu altyapısının hiyerarşik ve mantıksal bir şeması olan Mantıksal Yapı'dır. Bir sonraki adım olan Yazılım Dağıtım Süreci ise bu mantıksal planı ve DRM modülünden gelen güvenli içerik paketlerini alarak fiziksel veya sanal sunuculara dağıtır (Deployment). Bu otomatize edilmiş dağıtım işlemi sonucunda, tezin özgün katkısını oluşturan canlı ve çalışan Ağaç Tabanlı Yapı hayata geçirilmiş olur.

4.1.3. Ağaç tabanlı sunucu mimarisi

Ağaç Tabanlı Yapı, L1'den L5'e kadar numaralandırılmış hiyerarşik katmanlardan oluşan dağıtık bir sunucu mimarisidir. Her katman, bir veya daha fazla Sunucu Grubu içerir. Bir sunucu grubu, kendi içinde üç temel bileşenden oluşan ve bir bütün olarak çalışan bir mantıksal birimdir. Bu grubun beyni olan Uygulama Sunucusu, kullanıcı kimlik doğrulaması, yetki kontrolü, lisans talepleri ve iş mantığı gibi uygulama katmanı işlemlerini yürütür. Karar verme süreçlerinde ihtiyaç duyduğu veriler için, kullanıcı bilgileri, lisans detayları ve içerik metaverilerini depolayan Veritabanı Sunucusu'na başvurur. Son olarak, şifrelenmiş içerik dosyalarını fiziksel olarak barındıran ve sunan İçerik Sunucusu, Uygulama Sunucusu'ndan gelen talimatlar doğrultusunda içeriği talep eden kullanıcıya gönderir. Bu üçlü yapı, görev ayrılığı ilkesine uygun olarak hem güvenliği hem de yönetilebilirliği artırır.

4.1.4. Son kullanıcı istek ve yönlendirme süreci

Sistemin dinamik işleyişi ise bir Son Kullanıcı'nın içeriğe erişim isteği göndermesiyle başlar. Bu İstek, ilk olarak İstek İşleme Yöneticisi tarafından karşılanır. Bu bileşen, gelen isteği ayrıştırarak hangi içeriğin talep edildiği, kullanıcının kimliği ve diğer oturum bilgileri gibi anlamlı verilere dönüştürür. Ayrıştırılmış bu veri, sistemin akıllı yönlendirme mekanizması olan Yönlendirme Süreci'ne iletilir. Bu süreç, tezin önerdiği özyinelemeli yönlendirme algoritmasını kullanarak, isteği karşılamak için en uygun (örneğin, kullanıcıya en yakın, en az yüklü veya içeriği barındıran en verimli) sunucu grubunu belirler. Bu akıllı karar sonucunda oluşturulan Yönlendirilmiş İstek, Ağaç Tabanlı Yapı içindeki hedef sunucu grubuna (diyagramda L5'e) iletilir. Hedef grup isteği işler, yetkileri doğrular ve son olarak Talep Edilen İçerik'i kullanıcıya geri göndererek döngüyü tamamlar. Bu bütünlük yaklaşım, sistemin hem güvenli hem de yüksek performanslı bir içerik dağıtım hizmeti sunmasını mümkün kılar.

4.2. TBCDN: Ağaç Tabanlı İçerik Dağıtım Sistemi

Geleneksel CDN mimarilerinin, merkezi bir orijin sunucusuna olan bağımlılıkları ve genellikle düz topolojileri, özellikle yüksek eşzamanlılık ve ani talep patlamaları yaşanan dağıtık sistem senaryolarında yapısal performans sınırları ortaya koymaktadır. Bu bölümde detaylandırılacak olan Ağaç Tabanlı İçerik Dağıtım Ağı modeli, söz konusu darboğazları aşmak üzere tasarlanmış özgün bir mimaridir. TBCDN, dijital varlıkların dağıtımını topolojik olarak istemciye en yakın düğümlerden başlatmayı hedefleyen, çok katmanlı hiyerarşik bir yapı ve bu yapı üzerinde çalışan dinamik replikasyon mekanizmaları üzerine kurulmuştur. Bu yaklaşım, hem ağın çekirdek katmanlarındaki yükü azaltmayı hem de son kullanıcıya sunulan hizmet kalitesini artırmayı amaçlamaktadır.

TBCDN mimarisinin dinamik işleyişi, RRR olarak adlandırılan ve bu tez kapsamında geliştirilen özgün bir algoritma tarafından yönetilmektedir. Bu algoritma, geleneksel CDN'lerin doğrudan yönlendirme (direct routing) yaklaşımlarından farklı olarak, talepleri hiyerarşik bir yol üzerinde "tırmandıran" (escalating) bir mantığa dayanır. Bu mekanizmanın temel amacı, bir içeriğe yönelik talebi, ağın çekirdek katmanlarına ulaşmadan, topolojik olarak mümkün olan en alt seviyedeki düğümde çözümlemektir.

Önerilen TBCDN mimarisi, teknik işleyişinin ötesinde, bir sistem olarak sahip olduğu yapısal özelliklerle de öne çıkmaktadır. Mimarinin katmanlı ve dağıtık doğası, ona hem genişletilebilirlik (scalability) hem de esneklik (elasticity) kazandırır. Sistem, yeni düğümlerin hiyerarşinin herhangi bir katmanına kolayca eklenmesiyle yatay olarak; hiyerarşiye yeni katmanlar eklenmesiyle ise dikey olarak genişletilebilir. Bu yapı, artan kullanıcı sayısı veya belirli bir topolojik bölgedeki talep yoğunluğu gibi dinamik değişimlere karşı sistemin kolayca uyum sağlamasını sağlar. RRR algoritmasının otonom karar verme yeteneği ile birleştiğinde, sistem yük değişimlerine karşı elastik bir davranış sergiler.

Performans optimizasyonunun yanı sıra, güvenlik de mimarinin ayrılmaz bir parçası olarak tasarlanmıştır. Bu model, istemci tarafında özel bir yazılım kurulumu gerektirmeksizin, standart web protokolleri üzerinden çalışır. Ancak içeriğin güvenliği, ağ üzerinde daima güçlü kriptografik algoritmalarla (örn. AES-256) şifrelenmiş olarak taşınmasıyla temin edilir. Deşifreleme işlemi, yalnızca yetkilendirilmiş ve kimliği doğrulanmış istemci ortamında, bu tezin ilk bölümünde anlatılan bütünleşik hak yönetimi sisteminin denetimi altında anlık ve geçici olarak

gerçekleşir. Bu yaklaşım, performansı öncelerken güvenlikten ödün vermeyen, bütünsel bir çözüm sunar.

Bu çalışmada modelin etkinliğini göstermek için spesifik bir uygulama senaryosu kullanılmış olsa da TBCDN mimarisi kavramsal bir model olarak genel bir geçerliliğe sahiptir. Modelin temel aldığı hiyerarşik yapı, özyinelemeli yönlendirme ve dinamik talep-yolu önbellekleme prensipleri; dijital yayıncılık, lisanslı medya servisleri, büyük ölçekli yazılım dağıtımı (software distribution) ve yüksek hacimli, erişim kontrollü veri sunumu gerektiren hemen her alanda karşılaşılan performans ve ölçeklenebilirlik sorunlarına uyarlanabilir niteliktedir. Bu nedenle TBCDN, belirli bir probleme yönelik bir çözümden ziyade, dağıtık sistemler literatürüne sunulmuş genel bir mimari paradigma olarak değerlendirilmelidir.

4.2.1. Genel CDN topolojisi ve işleyişi

CDN, dijital içeriğin son kullanıcılara dağıtımında yaşanan gecikme ve ölçeklenebilirlik sorunlarına çözüm olarak geliştirilmiş, coğrafi olarak dağıtık bir sunucu altyapısıdır. Temel amaç, içeriği, talep eden kullanıcıya fiziksel olarak en yakın noktadan sunarak ağ üzerindeki seyahat süresini minimize etmek ve merkezi orijin sunucusu üzerindeki yükü hafifletmektir (Nygard, 2009). Geleneksel bir CDN'in topolojisi ve işleyişi, üç ana bileşen etrafında şekillenir: Orijin Sunucu, Uç Sunucular ve İstek Yönlendirme Sistemi.

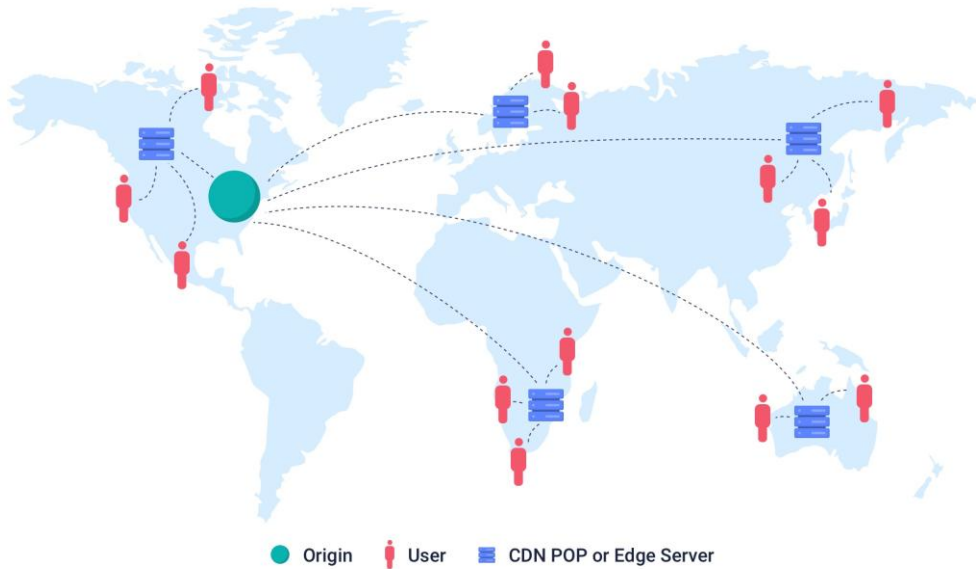
Orijin Sunucu (Origin Server): Tüm içeriğin orijinal ve yetkili kopyasını barındıran merkezi sunucudur. CDN'in diğer bileşenleri, içeriklerinin güncel kopyalarını bu sunucudan çeker.

Uç Sunucular (Edge Servers / Points of Presence - PoP): CDN'in temel gücünü oluşturan, dünya genelinde stratejik coğrafi konumlara (genellikle büyük internet değişim noktalarına yakın) yerleştirilmiş sunucu kümeleridir. Her bir PoP, orijin sunucudan aldığı popüler içeriklerin kopyalarını kendi önbelleğinde (cache) saklar. Bir kullanıcıdan talep geldiğinde, içerik orijin sunucu yerine bu uç sunuculardan birinden sunulur.

İstek Yönlendirme Sistemi (Request Routing System): CDN'in beyni olarak kabul edilen bu mekanizma, bir kullanıcıdan gelen içeriği talebini, o kullanıcı için en "uygun" PoP'a yönlendirmekle görevlidir. "Uygunluk" metriği genellikle en düşük ağ gecikmesi, sunucu yük durumu veya coğrafi yakınlık gibi faktörlere göre belirlenir.

Bu yönlendirme işlemi genellikle DNS tabanlı yönlendirme (DNS-based redirection) veya Anycast gibi ağ protokolleri kullanılarak gerçekleştirilir.

Genel işleyiş mekanizması **Şekil 4.2**'te şematik olarak gösterilmiştir. Bir son kullanıcı (End User) bir içeriğe (örneğin bir video dosyasına) erişmek istediğinde, istek öncelikle CDN'in yönlendirme sistemine ulaşır. Yönlendirme sistemi, kullanıcıyı en optimal Uç Sunucu'ya (PoP) yönlendirir. Talep bu uç sunucuya ulaştığında, sunucu kendi önbelleğini kontrol eder. Eğer talep edilen içerik önbellekte mevcut ise (Önbellek İsabeti - Cache Hit), içerik doğrudan ve hızla kullanıcıya sunulur. Eğer içerik önbellekte mevcut değilse (Önbellek Hatası - Cache Miss), uç sunucu içeriğin orijinal kopyasını Orijin Sunucu'dan çeker, kendi önbelleğine kaydeder ve ardından kullanıcıya sunar. Bu sayede, aynı içeriğe yönelik sonraki talepler doğrudan önbellekten karşılanabilir hale gelir.



Şekil 4.2. Geleneksel CDN Mimarisi

Geleneksel CDN mimarisi, genel amaçlı içerik dağıtımını için son derece etkili olsa da, TBCDN modelinin çözmeyi hedeflediği spesifik problemler karşısında bazı temel farklılıklar ve sınırlılıklar sergilemektedir. TBCDN'in bu genel topolojiden ayrıştığı temel noktalar şunlardır:

Topoloji Yapısı: Geleneksel CDN'ler genellikle tek katmanlı bir uç sunucu ağına (yayımlı topoloji) sahipken, TBCDN, katı ve çok seviyeli bir hiyerarşik (ağaç) yapı sunar. Bu hiyerarşi, içeriğin sadece uç noktalarda değil, ağın ara katmanlarında da organize bir şekilde depolanmasına olanak tanır.

İstek Yönlendirme Mantığı: Geleneksel CDN'lerde yönlendirme, genellikle kullanıcıyı en yakın tek bir uç noktaya doğrudan bağlama ilkesine dayanır. TBCDN'de ise “hiyerarşik istek tırmandırma” adı verilen özyinelemeli bir mekanizma kullanılır. Talep, en alt düğümden başlayarak içerik bulunana kadar hiyerarşi içinde yukarı doğru tırmandırılır.

Önbellekleme Stratejisi: Geleneksel CDN'lerde önbellekleme, büyük ölçüde uç sunucularda gerçekleşir. Bir “Cache Miss” durumunda içerik doğrudan orijinden çekilir. TBCDN ise “talep-yolu önbellekleme” stratejisini benimser. Bu sayede, orijinden dönen bir içerik, sadece talep eden uç düğüme değil, yol üzerindeki tüm ara düğümlere de kopyalanır. Bu, özellikle belirli bir hiyerarşik alt ağda popüler hale gelen içerikler için muazzam bir performans artışı sağlar ve çekirdek ağ üzerindeki yükü minimize eder.

Bu yapısal ve algoritmik farklılıklar, TBCDN'i, özellikle yüksek talep tekrarı ve hiyerarşik erişim desenleri gösteren büyük ölçekli, erişim kontrollü sistemler için geleneksel CDN'lere göre daha verimli ve ölçeklenebilir bir alternatif haline getirmektedir.

4.2.2. TBCDN topolojisi

TBCDN modeli, temelini çok seviyeli bir hiyerarşik mimariden almaktadır. Bu mimari, ağaç veri yapısı prensiplerine uygun olarak organize edilmiş, birbiriyle ebeveyn-çocuk (parent-child) ilişkisi içinde olan düğümlerden (nodes) oluşur. Sistemin en tepesinde, tüm dijital varlıkların orijinal ve yetkili kopyasını barındıran tek bir Çekirdek Düğüm (Root Node) yer alır. Bu düğüm, sistemin nihai doğruluk kaynağı (ultimate source of truth) olarak işlev görür. Çekirdek Düğüm'ün altında, talepleri ve içerikleri dağıtan bir veya daha fazla katmandan oluşan Ara Katman Düğümleri (Intermediate nodes) bulunur. Hiyerarşinin en alt katmanında ise doğrudan istemci (client) isteklerini karşılayan Uç Düğümler (Edge nodes) yer alır.

Bu yapının en temel özelliği, her düğümün yalnızca kendisine doğrudan bağlı olan üst (ebeveyn) düğüm hakkında bilgi sahibi olmasıdır. Bu dağıtık bilgi yapısı, ağ topolojisinin merkezi bir kontrol mekanizmasına ihtiyaç duymaksızın organik olarak genişletilmesini ve yönetilmesini sağlar. Bir düğümün ağdan çıkarılması veya yeni bir düğümün eklenmesi, sadece ilgili ebeveyn ve çocuk düğümleri etkileyerek sistemin genel kararlılığını ve esnekliğini artırır. Bu hiyerarşik yapı içerisinde, Çekirdek

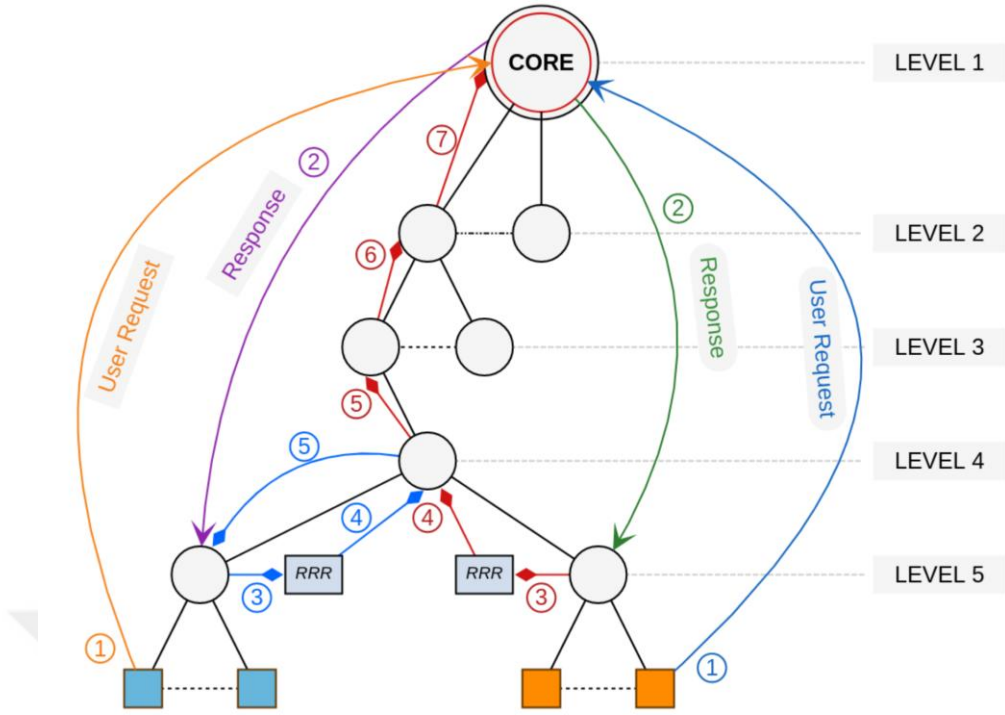
Düğüm dışındaki tüm düğümler, talep yoğunluğuna ve önbellekleme stratejisine bağlı olarak içerikleri dinamik olarak saklayarak yerel birer dağıtım noktası haline gelme potansiyeline sahiptir.

Modelin esnekliği, farklı dağıtım senaryoları için farklı derinlik ve genişlikte topolojiler oluşturulmasına olanak tanır. Örneğin, geniş bir coğrafi alana yayılan bir sistemde, Çekirdek Düğüm'ün altında birden fazla ana bölgeyi temsil eden üst katman ara düğümleri konumlandırılabilir. Bu ana düğümlerin her biri, daha küçük alt bölgeleri veya mantıksal grupları temsil eden alt katman ara düğümlerine bağlanabilir. Hiyerarşi, son kullanıcıya en yakın erişim noktalarını oluşturan Uç Düğümler ile son bulur. Bu katmanlı yapı, her düğümün kendi alt ağacına (subtree) hizmet vermesini sağlayarak, yükün mantıksal ve sistematik bir şekilde dağılmasını garanti eder.

Bu topolojik tasarım, bir sonraki bölümde detaylandırılacak olan RRR ile birleştiğinde, TBCDN'in temel verimlilik prensibini ortaya çıkarır. Talepler, ağaç üzerinde Uç Düğümlerden Çekirdek Düğüm'e doğru tırmandırılırken, yanıtlar hiyerarşide aşağı doğru iner ve bu süreçte içerik uygun ara düğümlerde çoğaltılır. Sonuç olarak, bu katmanlı mimari sadece içerik sunumunu hızlandırmakla kalmaz, aynı zamanda ağ kaynaklarının verimli kullanılmasını ve sistemin genel ölçeklenebilirliğini de temin eder.

4.2.3. Recursive request routing yaklaşımı

TBCDN mimarisinin dinamik işleyişi ve otonom davranışının merkezinde, bu tez kapsamında geliştirilen RRR algoritması yer almaktadır. Bu algoritma, geleneksel CDN'lerin doğrudan yönlendirme (direct routing) yaklaşımlarından farklı olarak, talepleri hiyerarşik bir yol üzerinde "tırmandıran" (escalating) bir mantığa dayanır. RRR'ın temel amacı, bir içeriğe yönelik talebi, ağın çekirdek katmanlarına ulaşmadan, topolojik olarak mümkün olan en alt seviyedeki düğümde çözümlenektir.



Şekil 4.3. Recursive Request Routing Algoritması

Algoritmanın temel iş akışı, **Şekil 4.3**'de şematik olarak gösterildiği üzere, şu adımları takip eder:

İstek Başlatma: Bir istemciden (client) gelen içerik talebi, ilk olarak hiyerarşinin en alt katmanında yer alan ve istemciye topolojik olarak en yakın olan Uç Düğüm (Edge Node) tarafından karşılanır.

Yerel Önbellemek Kontrolü: İsteği alan düğüm, ilk olarak talep edilen dijital varlığın kendi yerel önbelleğinde (local cache) bulunup bulunmadığını kontrol eder. Eğer içerik mevcut ise (Önbellemek İsabeti - Cache Hit), istek döngüsü burada sonlanır ve içerik doğrudan istemciye sunulur.

Özyinelemeli Tırmandırma: Eğer içerik yerel önbellekte mevcut değilse (Önbellemek Hatası - Cache Miss), düğüm talebi reddetmek yerine, hiyerarşik yapıdaki bir üst katmanda bulunan ebeveyn (parent) düğümüne özyinelemeli olarak iletir.

Sürecin Tekrarı: Talep, ebeveyn düğümüne ulaştığında, 2. ve 3. adımlar bu düğüm için tekrarlanır. Bu “kontrol et veya yukarı ilet” döngüsü, içerik hiyerarşi içindeki bir ara düğümde bulunana kadar veya en son olasılıkla, tüm içeriğin bir kopyasının bulunduğu garanti edilen Çekirdek Düğüm’e ulaşılanaya kadar devam eder.

Bu deterministik yönlendirme davranışı sayesinde, sistemde bir talebin karşılanamaması riski ortadan kaldırılırken, yönlendirme kararları tamamen dağıtık bir şekilde, her düğümün yalnızca kendi durumu ve üst düğümü hakkındaki bilgisiyle alınır. Bu yaklaşım, sistemin karmaşıklığını azaltır ve merkezi bir yönlendirme otoritesine olan ihtiyacı ortadan kaldırır.

Bu deterministik yönlendirme davranışı sayesinde, sistemde bir talebin karşılanamaması riski ortadan kaldırılırken, yönlendirme kararları tamamen dağıtık bir şekilde, her düğümün yalnızca kendi durumu ve üst düğümü hakkındaki bilgisiyle alınır.

Bu stratejinin doğrudan bir sonucu olarak iki temel performans avantajı elde edilir:

Çekirdek Ağ Yükünün Azaltılması: Tekrar eden taleplerin hiyerarşinin daha alt katmanlarında, yani uç veya ara düğümlerde karşılanması, ağın en tepesindeki Çekirdek Düğüm'e ve ana internet omurgasına yapılan erişim sayısını dramatik bir şekilde azaltır. Bu durum, özellikle yüksek erişim frekansına sahip popüler dijital varlıklar için ağ kaynaklarının çok daha verimli kullanılmasını sağlar ve gereksiz veri transferini önler.

Erişim Gecikmesinin Minimizasyonu: İçeriğin istemciye topolojik olarak daha yakın bir düğümden sunulması, verinin ağ üzerinde kat etmesi gereken mesafeyi kısaltır. Bu da doğrudan, son kullanıcının deneyimlediği uçtan-uca gecikme (end-to-end latency) süresinin ve içerik indirme süresinin anlamlı ölçüde düşmesi anlamına gelir.

TBCDN'in bottom-up (aşağıdan yukarıya) yönlendirme ve talep-yolu önbellekleme stratejisi, içeriği reaktif olarak değil, taleplerin doğal akışını takip ederek proaktif bir şekilde dağıtır. Bu, sistemi hem daha ölçeklenebilir hem de daha verimli hale getirerek geleneksel CDN mimarilerinin temel sınırlılıklarına etkin bir çözüm sunar.

4.3. EDU-DRM Sistemi: Dijital Hak Yönetimi Süreci

Dijital yayıncılık ve son kullanıcı cihazlarında yaşanan hızlı teknolojik gelişmeler, içerik üretiminden tüketimine kadar tüm süreci köklü bir şekilde dönüştürmektedir. Bu dönüşüm, yalnızca fiziksel içeriklerin dijital ortama aktarılmasıyla sınırlı değildir; aynı zamanda söz konusu içeriklerin gizliliğinin sağlanması, erişim haklarının denetlenmesi ve telif haklarının korunması da dijital içerik yönetiminin vazgeçilmez unsurları haline gelmiştir. Günümüzde dijital içeriklerin farklı cihazlar, platformlar ve

ağ ortamlarında hızla çoğalması, güvenli ve ölçeklenebilir hak yönetim altyapılarının geliştirilmesini zorunlu kılmaktadır.

Bu çerçevede EDU-DRM sistemi, içerik sağlayıcıların dijital varlıklarını şifrelenmiş biçimde sisteme yüklemesine ve bu varlıklara erişimi rol-tabanlı, dinamik politikalar doğrultusunda yönetmesine olanak tanıyan merkezi bir güvenlik katmanı sunmaktadır. Sistem, yalnızca içeriklerin yetkisiz erişime karşı korunmasını değil, aynı zamanda kullanıcı profillerine göre özelleştirilebilir erişim politikalarının uygulanmasını da mümkün kılmaktadır. EDU-DRM'in temelini rol-tabanlı erişim modeli oluşturmaktadır. Bu modelde kullanıcı profilleri, içerik yöneticisi, son kullanıcı ya da sistem yöneticisi gibi farklı seviyelerde tanımlanabilmekte; her profil için erişim hakları ayrı ayrı belirlenebilmektedir. Böylece, farklı kullanıcı grupları için kişiselleştirilmiş, esnek ve ölçeklenebilir bir erişim kontrol mekanizması sağlanmaktadır.

Sistemin güvenlik altyapısı, şifreleme, süre sınırlı lisanslama, üçüncü taraf paylaşımının engellenmesi ve donanım-yazılım tabanlı erişim doğrulama gibi çok katmanlı mekanizmalar üzerine inşa edilmiştir. Bu sayede, içeriklerin yalnızca yetkilendirilmiş cihazlar ve kullanıcılar tarafından erişilmesi garanti altına alınmakta; yetkisiz çoğaltma veya paylaşım girişimleri önlenmektedir. EDU-DRM, yalnızca güvenliği sağlamakla kalmayıp, aynı zamanda farklı ağ koşulları ve kullanıcı yoğunlukları altında ölçeklenebilir performans sunmayı hedeflemektedir. Sistem, artan veri hacmi ve eşzamanlı erişim taleplerine uyum sağlayabilmek için modüler tasarlanmış; bu da farklı içerik türleri, cihaz ekosistemleri ve dağıtım senaryoları için genişletilebilir bir çözüm üretmiştir.

Geliştirilecek sistemin sağlaması gereken başlıca gereksinimler arasında, mobil cihazların dijital içerik ekosistemindeki artan rolü önemli bir yer tutmaktadır. Mobil cihazların yaygınlaşması, içerik tüketim süreçlerini daha etkileşimli ve dinamik hale getirmiştir. Çoklu ortam bileşenlerinin aktif kullanımı sayesinde mobil platformlar, klasik bilgi iletim yöntemlerine kıyasla daha esnek ve sürdürülebilir bir yapı sunmaktadır. Ancak bu eğilim, içeriklerin mobil cihazlar üzerinden dağıtımını zorunlu kılarken, aynı zamanda güvenlik risklerini de beraberinde getirmektedir.

Mobil cihazların doğası gereği dijital altyapıya dayanması, bu cihazlar aracılığıyla dağıtılan içeriklerin izinsiz kopyalanması, çoğaltılması ve yetkisiz paylaşımı gibi

tehditleri artırmaktadır. Bu durum, özellikle telif hakkı taşıyan dijital varlıkların korunmasını kritik hale getirmektedir. İçerik üreticilerinin fikri mülkiyet haklarının korunamaması, sürdürülebilir bir dijital içerik ekosistemi açısından ciddi zafiyetler doğurmaktadır. Bu bağlamda önerilen DRM sistemi, dijital varlıkların yalnızca yetkilendirilmiş kullanıcılar tarafından erişilebilmesini sağlayacak şekilde tasarlanmıştır. Sistem, gerekli durumlarda kişiye özel, ücretli ve süre sınırlı lisanslarla erişim sağlayabilmekte; ayrıca içeriklerin üçüncü taraflarla paylaşımını donanım ve yazılım düzeyinde engelleyecek güvenlik mekanizmaları içermektedir. Kiralama modeliyle sunulan içeriklerin süresi sona erdiğinde otomatik ve geri döndürülemez biçimde silinmesi de sistemin ayrılmaz bir parçasıdır. Böylece hem içerik güvenliği hem de erişim kontrolü, bütüncül ve sürdürülebilir bir dijital hak yönetimi yaklaşımıyla tesis edilmektedir.

Önerilen DRM altyapısında, kullanıcı kimliği, içerik türü ve erişim kuralları arasında dinamik bir ilişki kurulmuştur. Dijital içerik ekosistemlerinde kullanıcı profilleri çeşitlilik göstermekte; her profilin sistem içerisindeki rolü, erişim haklarını doğrudan etkilemektedir. Bu nedenle, DRM sisteminin temelinde rol tabanlı ve kurala dayalı bir erişim modeli yer almakta, kullanıcıların sahip oldukları yetkiler doğrultusunda içeriklerle etkileşimleri sınırlandırılmaktadır.

Kullanıcılar: DRM sistemi içerisinde tanımlı kullanıcı grupları; son kullanıcılar, içerik sağlayıcılar, misafir kullanıcılar ve yöneticilerden oluşmaktadır. Son kullanıcılar, sistemin en geniş grubunu temsil ederek içerik tüketiminde aktif rol oynar. İçerik sağlayıcılar, yeni içerik yükleme, güncelleme ve meta-veri yönetiminden sorumludur. Misafir kullanıcılar, belirli kısıtlamalar altında sisteme geçici erişim hakkı tanınan bireylerden oluşur. Yöneticiler ise içeriklerin ve kullanıcıların meta-verilerini düzenleyebilme, erişim politikalarını tanımlama ve sistem bütünlüğünü koruma yetkisine sahiptir. Tüm kullanıcıların kimlik doğrulama süreçleri, merkezi bir kimlik yönetim altyapısı üzerinden yürütülmekte ve güvenilir erişim sağlanmaktadır.

İçerikler: Sistemde yer alan içerikler, farklı kategorilere ve erişim düzeylerine göre sınıflandırılmıştır. Henüz doğrulama sürecini tamamlamamış içerikler, erişime kapalı bir bekleme alanında tutulur. İçerik sağlayıcılar, yükleme aşamasında tüm meta-veri bilgilerini sisteme kaydetmekle yükümlüdür. Onay sürecinin ardından içerikler, ilgili kategorilere atanarak son kullanıcıların erişimine açılır. Bu yapı, yalnızca onaylı içeriklerin dağıtılmasına imkân tanıyarak içerik güvenliğini güçlendirmektedir.

Kurala Dayalı Yetkilendirme: Sistemin ölçeklenebilirliğini desteklemek için, kullanıcı profilleri ve erişim hakları dinamik biçimde güncellenebilmektedir. Bu amaçla kurala dayalı bir yetkilendirme modülü geliştirilmiş olup, kullanıcıların rol değişiklikleri ya da içeriklerin erişim politikalarındaki güncellemeler otomatik olarak işlenmektedir. Böylece, erişim tabloları sürekli güncel tutulmakta ve rol-tabanlı erişim kontrolü gerçek zamanlı uyarlanabilir hale gelmektedir.

Kullanıcı-İçerik İlişkisi: Kullanıcıların içeriklere erişimi hem kullanıcı rolüne hem de içerik kategorisine bağlı olarak tanımlanmaktadır. Sistem, yöneticilerin farklı içerik seviyelerine erişmesine olanak tanırken, son kullanıcılar yalnızca kendi yetkilendirme kapsamlarındaki içeriklere ulaşabilmektedir. Kullanıcı profillerinde meydana gelen değişiklikler sistem tarafından otomatik işlenmekte ve buna bağlı olarak erişim hakları dinamik biçimde güncellenmektedir.

Sistemin performansını ve esnekliğini artırmak amacıyla erişim hakları veri tabanında bit düzeyinde kodlanan mantıksal bir Rights Expression Language (REL) ile saklanmaktadır. Tüm olası erişim kombinasyonları bu yapıda tanımlanmış ve kullanıcı rollerine göre yetkilendirme tabloları oluşturulmuştur (bkz. **Tablo 4.1** ve **Tablo 4.2**). Bu yöntem sayesinde, yüksek kullanıcı yoğunluğunda dahi erişim kontrol süreçleri verimli bir şekilde yürütülmekte ve sistemin ölçeklenebilirliği korunmaktadır.

Tablo 4.1. EDU-DRM için belirlenmiş erişim türleri.

Access ID	Access Types
1	Edit records
2	Monitor
3	Download
4	Upload
5	View
6	Erase
7	Print

Tablo 4.2. Sistemde tanımlanan roller ve yetkilendirme kodları.

Role ID	Role Name	Authorization Code						
		1	2	3	4	5	6	7
1	Super Admin	1	1	1	1	1	1	1
2	User Admin	1	1	0	0	0	0	0
3	Policy Admin	1	1	0	0	0	0	0
4	Licence Admin	1	1	0	0	0	0	0
5	Content Supervisor	0	1	1	0	1	0	0
6	End-User	0	0	0	0	1	0	0
7	Producer	0	0	0	1	1	0	1
8	Guest	0	0	0	0	1	0	0

Bu yapısal kurgunun, yalnızca teorik erişim modelleriyle sınırlı olmadığı; aynı zamanda bütünleşik sistem mimarisi içerisinde doğrudan işlevselleştirildiği görülmektedir. Kullanıcı grupları ve içerik hakları, EDU-DRM katmanında tanımlanan şifreleme ve lisanslama süreçleriyle güvence altına alınmakta; ardından içerikler, sunucu yerleşim ve yazılım dağıtım mekanizmaları aracılığıyla hiyerarşik TBCDN yapısına aktarılmaktadır. Kullanıcı talepleri, bu hiyerarşik yapı içinde özyinelemeli yönlendirme algoritmalarıyla en yakın uygun düğüme yönlendirilirken, erişim yetkileri REL tabanlı kurallar aracılığıyla gerçek zamanlı olarak doğrulanmaktadır. Böylece, tablolarla tanımlanan erişim türleri ve roller yalnızca statik bir politika seti olmaktan çıkmakta; sistem mimarisinin her aşamasında dinamik ve sürdürülebilir bir erişim kontrol mekanizmasına dönüşmektedir.

4.3.1. Rol tabanlı erişim ve hak modelleri

EDU-DRM sistemi, yalnızca kullanıcıların rollerine göre erişim izni tanımlamakla kalmaz; aynı zamanda her rolün hangi işlevleri ne ölçüde yerine getirebileceğini ayrıntılı olarak sınırlandırır. Bu amaçla sistemde tanımlanmış yedi temel erişim türü, farklı kullanıcı rolleriyle eşleştirilmiş ve bu eşleşmeler sistem veri tabanındaki lisans kayıtları aracılığıyla uygulanabilir hale getirilmiştir. Erişim türlerinin hem güvenlik hem de işlevsellik açısından hassas biçimde tanımlanmış olması, sistemin sürdürülebilirliğini ve denetlenebilirliğini desteklemektedir.

Aşağıda EDU-DRM sisteminde yer alan erişim türleri özetlenmiştir:

Kayıtları Düzenle (Edit Records): Yalnızca yönetici rollerine tanımlıdır. Bu yetki, kullanıcı profilleri ve içerik meta-verileri üzerinde düzenleme yapılmasını sağlar. Ancak yönetici rolleri kendi aralarında da ayrılmaktadır; örneğin, “kullanıcı yöneticisi” içerik profillerine müdahale edemezken, “içerik yöneticisi” kullanıcı verilerine erişemez. Bu erişim türü, otomatik yetkilendirme sürecinde oluşabilecek istisnaların manuel olarak düzeltilmesine de imkan tanır.

İzleme (Monitor): Kullanıcı aktivitelerine ilişkin log verileri üzerinden çeşitli raporların oluşturulmasına olanak tanıyan özel bir yetkidir. Bu sayede örneğin bir öğretmen, öğrencilerinin belirli içeriklere kaç kez eriştiğini sistem üzerinden analiz edebilir.

İndirme (Download): İlgili içeriğin istemci cihaza şifreli olarak indirilmesini sağlar. Bu içerikler diskte yalnızca şifrelenmiş biçimde tutulur. Bu yetki, sistemin mevcut sürümünde henüz aktif değilse de, ilerleyen versiyonlar için uygulanabilir olarak planlanmıştır.

Yükleme (Upload): Sisteme yeni içerik eklemek amacıyla kullanılır ve genellikle içerik üreticilerine tanımlıdır. Yüklenen içerikler öncelikle onay havuzuna alınmakta, ardından uygun sınıf düzeyine aktarılmaktadır.

Görüntüleme (View): İçeriğin doğrudan diske kaydedilmeden, yalnızca istemci belleğinde geçici olarak şifre çözülerek sunulmasını sağlar. Bu erişim modeli, istemci tarafında dijital iz bırakmamakta; ayrıca sunucu tarafı ön bellek engelleme mekanizmalarıyla desteklenmektedir.

Silme (Erase): İçeriğin sistem diskinden kalıcı olarak silinmesini sağlar. Bu yetki, yalnızca yüksek seviye yönetici rollerine atanabilir.

Yazdırma (Print): Görüntülenen içeriğin fiziksel olarak basılmasına veya bu işlemin engellenmesine olanak tanır. Bu tür hem içerik koruması hem de telif kontrolü açısından önemli bir kontrol noktasıdır.

Sistemin lisans veri tabanında, bu erişim türlerine karşılık gelen erişim vektörleri yapılandırılmıştır. **Tablo 4.1**, bu erişim türlerinin listesini; **Tablo 4.2**, rollerle olan eşleşmelerini; **Tablo 4.3** ise lisans kayıtlarında saklanan örnek erişim vektörlerini sunmaktadır. Böylece EDU-DRM, hem roller arası ayrımı teknik düzeyde koruyabilmekte hem de içerik erişimini mikro düzeyde denetleyebilmektedir.

Tablo 4.3. İçeriklere bağlı erişim vektörü örneği.

Content ID	Authorization Vector							
	1	2	3	4	5	6	7	8
234	1	0	0	0	1	1	0	0
34	1	1	0	0	1	1	0	0
245	1	0	0	0	0	0	0	1
171	1	0	0	1	0	0	1	0

Bu erişim modeli, yalnızca roller üzerinden tanımlı yetkilendirme politikalarını değil, aynı zamanda erişim işleminin doğasına göre belirlenmiş çok boyutlu kontrol parametrelerini de içermektedir. Sistem, erişim haklarını veri tabanında bit düzeyinde yapılandırılmış erişim vektörleri şeklinde kodlamakta; bu yaklaşım hem bellek kullanımını minimize etmekte hem de yetkilendirme kararlarının düşük gecikme ile gerçek zamanlı biçimde alınabilmesini sağlamaktadır. Ayrıca, erişim vektörlerinin mantıksal kurallara dönüştürülmesi için özel bir Hak İfade Dili (Rights Expression Language – REL) kullanılmakta, böylece hangi rolün hangi koşullar altında hangi içeriğe erişebileceği denetlenebilir ve sürdürülebilir bir yapıya kavuşturulmaktadır.

EDU-DRM sisteminde rollerle eşleştirilen erişim türleri, kullanıcı profillerine doğrudan yansıtılmaktadır. Her bir kullanıcı rolü için sistemde tanımlanan erişim vektörleri, kullanıcı arayüzünde basitleştirilmiş bir biçimde gösterilmekte ve böylece kullanıcıların sahip oldukları hakları sezgisel olarak takip edebilmeleri mümkün

olmaktadır. Örneğin içerik üreticileri, sisteme yeni materyal yükleyebilme, mevcut içerikleri görüntüleyebilme veya belirli koşullarda çıktısını alabilme gibi yetkilerle sınırlandırılabilir. Bu yapı, erişim vektörlerinin yalnızca lisans veri tabanında değil, aynı zamanda istemci tarafında da güvenli şekilde temsil edilmesini sağlamakta; yöneticilere kullanıcı haklarını merkezi ya da dağıtık biçimde denetleyebilme olanağı sunmaktadır. Böylece EDU-DRM’de erişim kontrol mekanizması hem teknik güvenlik katmanıyla hem de kullanıcı deneyimiyle bütünleşik bir model olarak işler hale gelmektedir.

EDU-DRM sisteminde erişim türlerinin etkin biçimde uygulanabilmesi, kullanıcı rollerine dayalı bir yetkilendirme modeli ile sağlanmaktadır. Sistem genelinde sekiz farklı rol tanımlanmış olup, bu roller klasik veritabanı sistemlerindeki içsel (internal) rollerden ayrılmaktadır. EDU-DRM’de roller ile erişim türleri arasındaki ilişki, bit düzeyinde tanımlanmış erişim vektörleri üzerinden modellenmektedir. Bu yaklaşım sayesinde her bir kullanıcının erişim hakları açık, denetlenebilir ve gerektiğinde dinamik olarak güncellenebilir hale gelmektedir. Böylece, sistemin ölçeklenebilirliği korunurken, kullanıcı profilleri ile erişim yetkileri arasında doğrudan ve sürdürülebilir bir bağ kurulmaktadır.

Aşağıda, her bir rolün sistem içindeki tanımı ve varsayılan erişim yetkileri özetlenmektedir:

Süper Yönetici (Super Admin): Sistem üzerindeki tüm içeriklere ve bileşenlere sınırsız erişim hakkına sahip en yüksek yetki düzeyini temsil eder. Bu rol, genellikle sistemin bütünsel işleyişinden sorumlu olan merkezi yöneticilere atanmakta olup, erişim politikalarının tanımlanması, kullanıcı yetkilerinin düzenlenmesi ve olağan dışı durumlarda manuel müdahale gibi kritik işlevleri yerine getirir.

Kullanıcı Yöneticisi (User Admin): Sistem kullanıcılarının hesaplarını oluşturma, düzenleme ve yönetme sorumluluğunu taşır. Rol, özellikle kullanıcı kimlik bilgilerinin doğrulanması ve güncellenmesi süreçlerinde etkindir. Ancak bu yetki içeriklere doğrudan erişimi kapsamaz; yani kullanıcı yöneticisi içerik üzerinde işlem yapamaz, yalnızca kullanıcı profilleri üzerinden kontrol sağlar.

Erişim Politikası Yöneticisi (Policy Admin): Sistemdeki kullanıcı profillerinin erişim politikalarını tanımlamak ve güncellemekle sorumlu roldür. Özellikle dinamik kullanıcı geçişlerinde (örneğin abonelik yenilenmesi, rol değişikliği, yeni kullanıcı

gruplarının eklenmesi gibi) otomatik yetkilendirme mekanizmasının çözümleyemediği durumları yönetir. Bu rol, merkezi sistem yöneticilerinin altında konumlanan ve erişim politikalarının sürekliliğini sağlayan kritik bir ara katman görevi üstlenir.

Lisans Yöneticisi (License Admin): Sisteme yüklenen içeriklerin doğrulama ve onay süreçlerinden sorumludur. İçeriklerin meta-verilerini ve lisans koşullarını inceleyerek, yalnızca uygun bulunan materyallerin yayımlanmasına izin verir. Bu yönüyle, sistemin güvenilirliğini ve içerik kalitesini sağlayan kritik bir ara kontrol katmanını oluşturur.

İçerik Denetleyici (Content Supervisor): Farklı kategorilerdeki içeriklere erişim iznine sahiptir ve kullanıcı etkileşimlerini izleme, raporlama yetkileriyle donatılmıştır. Örneğin, belirli bir kullanıcı grubunun bir içeriğe erişim sıklığını veya kullanım istatistiklerini analiz edebilir. Bu rol, sistemin hem güvenlik hem de performans boyutunda denetlenebilirliğini artırır ve içerik tüketim dinamiklerinin doğru anlaşılmasına katkı sağlar.

Standart Kullanıcı (End-User): Yalnızca kendisine tanımlı içerik grubuna erişim yetkisine sahiptir. Güvenlik politikaları gereği içerikleri kalıcı olarak indirme yetkisi yoktur; erişim, yalnızca istemci tarafında geçici bellekte şifre çözülerek sağlanır. Bu yaklaşım, yetkisiz paylaşımı önlerken, aynı zamanda kullanıcı deneyimini yüksek tutacak şekilde optimize edilmiştir.

İçerik Üreticisi (Producer): Sisteme yeni içerik yükleme yetkisine sahip kullanıcıları kapsar. Üreticilerin yüklediği içerikler, otomatik şifreleme süreçlerinden geçirilerek geçici depolama alanına kaydedilir. Üreticiler kendi materyallerini görüntüleyebilir veya çıktı alabilir, ancak içeriklerin onaylanması veya yayımlanması süreçlerine doğrudan müdahale edemezler.

Misafir (Guest): Geçici oturum açabilen, sisteme kayıtlı olmayan kullanıcıları temsil eder. Bu kullanıcılar yalnızca “public” biti aktif olan genel içeriklere erişebilirler. Sistem, her misafir oturumu için dinamik bir profil oluşturur ve oturum sona erdiğinde bu profil silinir. Bu yaklaşım, geçici erişim ihtiyaçlarını karşılamakla birlikte sistemin güvenlik bütünlüğünü de korur.

Bu rollerin her biri, sistemdeki belirli erişim türleriyle ilişkilendirilmiş olup, erişim vektörleri üzerinden yetkilendirme motoru tarafından kontrol edilmektedir (bkz.

Tablo 4.2).

Sistemde kullanıcıların içeriklere erişim hakları, bit tabanlı erişim vektörleri aracılığıyla tanımlanmaktadır. Her kullanıcı için oluşturulan profil kaydı, rol tabanlı yetkiler ile içerik seviyelerini aynı anda kodlayan bir bit dizisi biçiminde tutulmaktadır. Bu yaklaşım sayesinde, herhangi bir kullanıcının hangi içeriklere hangi tür erişim hakkına sahip olduğu doğrudan okunabilir ve sistem tarafından düşük gecikmeyle denetlenebilir hale gelmektedir. Profil yapısının bit düzeyinde tasarlanması, milyonlarca kullanıcı ve içerik kaydı altında bile bellek kullanımını minimize ederek ölçeklenebilirlik sağlamaktadır.

Benzer şekilde, içerik kayıtları da lisanslama sürecine tabi tutulmakta ve bu süreç bit düzeyinde işaretlerle yönetilmektedir. Örneğin, sisteme yüklenen bir içerik ilk aşamada “taslak” veya “bekleme havuzu” bitleriyle işaretlenir. Lisans yöneticisi tarafından onaylandığında bu bit sıfırlanır ve içerik, ilgili erişim düzeylerine sahip kullanıcı profilleriyle ilişkilendirilerek aktif hale gelir. Bu mekanizma, içeriklerin onaylanmadan yayına alınmasını engellediği gibi, yetkisiz erişim risklerini de ortadan kaldırır. Ayrıca, içeriklerin yaşam döngüsü boyunca (taslak, onaylı, süreli erişim, iptal edilmiş vb.) farklı bit kombinasyonlarıyla modellenebilmesi, sistemin esnekliğini artıran bir diğer unsurdur.

Bu yapı sayesinde, EDU-DRM sisteminde erişim yönetimi yalnızca rol bazlı değil, aynı zamanda içeriklerin durumuna ve yaşam döngüsüne duyarlı çok boyutlu bir kontrol mekanizması haline gelmektedir. Böylelikle hem kullanıcı profilleri hem de içerik kayıtları, ortak bir bit tabanlı yapı üzerinden yönetilerek sürdürülebilir, ölçeklenebilir ve denetlenebilir bir hak yönetim altyapısı sağlanmaktadır.

İçerik Lisanslama Politikası ve Süreç Yönetimi: Bu yaklaşım, içerik-kullanıcı eşleşmesini sistem düzeyinde sabit kılarak yetkilendirme süreçlerinde kararlılık ve öngörülebilirlik sağlamaktadır. Sistemde bir kullanıcının belirli bir erişim grubuna atanması, yalnızca bu gruba özgü içeriklere erişebilmesi anlamına gelir. Benzer şekilde, bir dijital içeriğin belirli bir erişim seviyesine tanımlanması, o içeriğin sadece ilgili kullanıcı profillerine açık hale gelmesini sağlar.

Kullanıcıların erişim yetkileri, tanımlanan abonelik süresi, organizasyonel rol veya kurumsal politika çerçevesinde sabitlenmiş biçimde yapılandırılabilir. Bu sayede erişim sürekliliği korunurken, dönemsel değişikliklerde (örneğin rol geçişleri, lisans yenilemeleri, kullanıcı profil güncellemeleri gibi) sistem erişim haklarını otomatik

olarak g ncelleyebilir. Bu mekanizma, manuel m dahaleye gerek kalmadan yetkilendirme tablolarının yeniden tanımlanmasını saęlayarak hem y netimsel maliyeti azaltır hem de sistemin  l eklenebilirlięini g  lendirir.

  erikler i in lisanslama s reci, materyalin i erik havuzuna y klenmesiyle bařlatılır ve onay mekanizması  zerinden ilerler. Bu ařamada i erik, alan uzmanı lisans y neticileri tarafından deęerlendirilir; onay verilmesi durumunda i erik kaydındaki “havuz biti” (PL) sıfırlanır ve materyal yayımlanmıř, lisanslı bir varlık haline gelir. Bu iřlem yalnızca i erięin yayınlanma stat s n  deęil, aynı zamanda hangi eriřim grubuna ( rneęin belirli rol veya kategoriye) ait olduęunu da kalıcı bi imde belirler. B ylece i erikler, sistemdeki kullanıcı profilleriyle tanımlanmıř eriřim matrisine otomatik olarak baęlanır.

Bu yaklařımın temel farklılıęı, lisanslama s recinin i erik ile kullanıcı arasında sistemsel ve geri d nd r lemez bir iliřki kurmasıdır.  rneęin, ticari dijital platformlarda ( rneęin Apple iTunes) lisanslama genellikle s reye dayalıdır ve belirlenen s renin sonunda i erik eriřilemez hale gelir. Buna karřılıklı EDU-DRM modeli, s reye deęil, stat ye dayalı bir lisanslama politikası benimsemekte; eriřim haklarını kalıcı ve yapısal stat ler  zerinden tanımlamaktadır. Bu sayede, i eriklerin yařam d ng s  boyunca eriřim s rekliilięi korunur ve sistemin b t nsel iřleyiřinde  ng r lebilirlik saęlanır.

Lisans y neticileri, yalnızca i erik  reticileri tarafından y klenen taslak materyallerin incelenmesi ve deęerlendirilmesinden sorumludur. Bu kullanıcıların, i eriklerin teknik b t nl ę n , g venlik gereksinimlerini ve kullanım senaryolarına uygunluęunu deęerlendirecek uzmanlık d zeyine sahip olmaları beklenir. Reddedilen i erikler sistemden  ıkarılırken, onaylanan i erikler lisanslanarak eriřim matrisine entegre edilir ve ilgili roller i in eriřilebilir hale gelir.

T m lisanslama iřlemleri sistem tarafından otomatik olarak kayıt altına alınmakta ve bu log verileri s per y neticiler tarafından denetlenebilir bi imde saklanmaktadır. Ayrıca sistem, bu logların analizi i in geliřmiř raporlama ara larıyla desteklenmiřtir. B ylece, lisanslama s reci yalnızca bir yetkilendirme mekanizması olmaktan  teye ge erek, i eriklerin izlenebilirlięini, denetlenebilirlięini ve kullanıcı-i erik etkileřiminin řeffaf bi imde raporlanmasını m mk n kılmaktadır.

4.3.2. Modüler mimari: lisans sunucusu, içerik sunucusu, şifreleme

EDU-DRM sisteminin teknik mimarisi, dijital içeriklere güvenli ve kontrollü erişim sağlamak amacıyla çok katmanlı bir yapıda kurgulanmıştır. Bu mimari, bir yandan kullanıcıların taleplerini hızlı ve ölçeklenebilir biçimde karşılamayı hedeflerken, diğer yandan içeriklerin yaşam döngüsü boyunca bütünlüğünü ve güvenliğini korumaya odaklanmaktadır. Sistem tasarımının temelinde, kimlik doğrulama, bütünlük kontrolü, kopya engelleme ve güvenli iletim gibi kritik güvenlik hedeflerini eşzamanlı olarak karşılayan bir erişim altyapısı yer almaktadır.

Bu çerçevede, ilk olarak erişim talebinde bulunan her kullanıcının kimliğinin güvenilir biçimde doğrulanması zorunludur. Bu süreç, yalnızca yetkili kullanıcıların sisteme giriş yapabilmesini sağlamakta ve kimlik sahteciliğine karşı temel bir güvenlik katmanı oluşturmaktadır. İkinci olarak, dağıtılan tüm dijital içeriklerin bütünlüğünün korunması esastır. İçerikler, yükleme ve dağıtım aşamalarında bütünlük kontrol mekanizmalarıyla doğrulanarak yetkisiz değişikliklerin engellenmesi hedeflenmektedir.

Üçüncü olarak, sistem mimarisi içeriklerin izinsiz kopyalanmasına karşı koruma sağlamaktadır. Bu bağlamda, istemci tarafındaki erişim yalnızca geçici ve şifrelenmiş oturumlarla sınırlandırılmakta; içeriklerin kalıcı olarak çoğaltılması veya farklı platformlara aktarılması engellenmektedir. Son olarak, ağ üzerindeki iletim süreci güvenli iletişim protokolleri aracılığıyla korunmakta; böylece yetkisiz kişilerin iletim halindeki verilere erişimi ya da müdahalesi önlenmektedir.

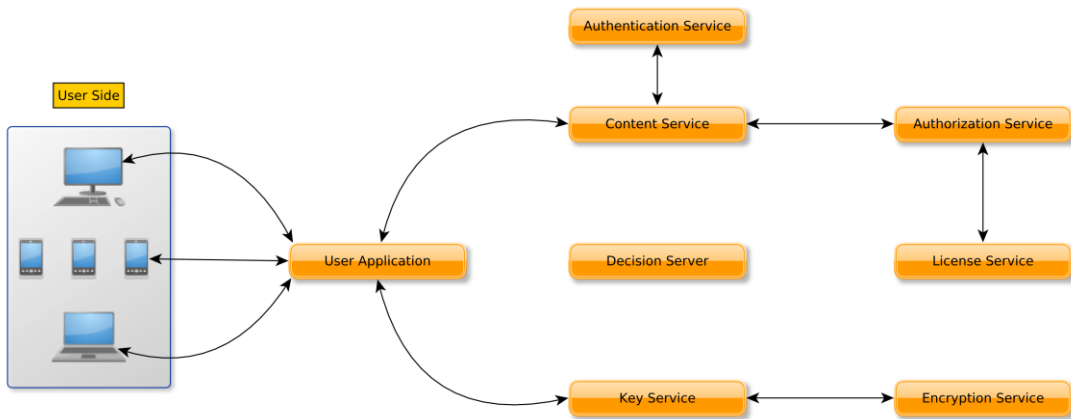
EDU-DRM mimarisinde içerik yükleme süreci, istemci tarafındaki kullanıcı etkileşim arayüzü üzerinden başlatılmaktadır. Bu arayüz, içerik üreticilerinin sisteme aktaracakları materyale ait temel meta-verileri tanımlamalarına (örneğin içerik adı, kategori bilgisi, erişim düzeyi) ve ilgili dosyayı seçmelerine imkân tanımaktadır. Varsayılan güvenlik politikası gereği her içerik yükleme işlemi şifreleme katmanıyla bütünlük olarak gerçekleşmekte; böylece sisteme aktarılan materyallerin tamamı depolama anından itibaren koruma altına alınmaktadır.

Yükleme sırasında içerik, sistemin şifreleme modülü tarafından gerçek zamanlı olarak işlenmekte ve yalnızca şifrelenmiş haliyle veri tabanına kaydedilmektedir. Bu sayede içerikler, dağıtım sürecinde yetkisiz erişimlere karşı korunaklı hale gelir. Uygulama tasarımında farklı içerik türleri desteklenebilmekle birlikte, mevcut prototipte yalnızca

belirli dosya türleri (örneğin PDF belgeleri) istemci tarafında güvenli biçimde görüntülenebilmektedir.

Mimari yapı, yerel bir doküman sunucusu ile bu sunucuya bağlı bir uygulama sunucusundan oluşmaktadır. İçerikler, şifrelenmemiş halleriyle yalnızca internet bağlantısı bulunmayan yerel depolama alanında tutulur. Bir istemci içerik talebinde bulunduğu anda, doküman uygulama sunucusuna aktarılmakta ve burada dinamik olarak üretilen 1024-bitlik bir oturum anahtarıyla şifrelenmektedir. Elde edilen oturum anahtarı, istemcinin açık anahtarıyla şifrelenir ve şifreli içerikle birlikte güvenli iletim protokolleri (örn. SSL/TLS) üzerinden kullanıcıya gönderilir.

İstemci tarafında, kullanıcı yeniden kimlik doğrulamasından geçirilir, ardından veri bütünlüğü denetimi yapılır. Doğrulama adımları başarıyla tamamlandığında, istemcinin gizli anahtarı aracılığıyla oturum anahtarı çözülür ve içerik erişime açılır. Bu çok katmanlı süreç hem depolama hem de iletim sırasında verilerin güvenliğini garanti altına almakta, hem de kimlik doğrulama, şifreleme ve erişim kontrolü arasındaki bütünleşik işleyişi sağlamaktadır.



Şekil 4.4. EDU-DRM Sisteminin Servis Tabanlı Mimarisi

Şekil 4.4., sistemde kullanıcı tarafı uygulaması ile sunucu tabanlı servisler arasındaki etkileşimi gösteren servis odaklı mimariyi temsil etmektedir. Kullanıcı tarafından başlatılan her erişim talebi, karar sunucusu üzerinden ilgili servislerle iletişime geçirilmekte; bu süreçte kimlik doğrulama, yetkilendirme, lisans kontrolü, içerik sunumu, şifreleme ve anahtar yönetimi adımları bütünleşik bir akış içerisinde yürütülmektedir. Bu yapı, sistemin ölçeklenebilirliğini artırırken aynı zamanda bileşenlerin bağımsız şekilde yönetilebilmesine ve güncellenebilmesine olanak sağlamaktadır.

Mimari, yalnızca yetkilendirilmiş kullanıcıların içeriklere erişimini garanti altına almakla kalmaz; aynı zamanda şifreli verinin üçüncü taraflarca ele geçirilmesi durumunda dahi anlamsız hale gelmesini sağlar. Örneğin, ağ trafiğini izleyen yetkisiz bir kullanıcı yalnızca şifreli veriyi elde edebilir; ancak oturum anahtarı ve kullanıcıya özgü gizli anahtar olmadan bu veriyi çözümlemesi mümkün değildir. Ayrıca, şifrelenmiş bir doküman farklı bir kullanıcıya aktarılsa bile, yalnızca orijinal ve yetkilendirilmiş kullanıcıya ait anahtar ile çözülebileceği için sistem dışı kullanım teknik olarak engellenmektedir.

Modüler ve servis tabanlı güvenlik mimarisi, dijital içeriklerin güvenli depolanmasının ötesinde, kullanıcı düzeyinde erişim kontrollerinin hassasiyetle uygulanmasını mümkün kılmaktadır. Bu yapı, özellikle yüksek ölçekli ve heterojen kullanıcı gruplarının bulunduğu dağıtık ortamlarda hem veri güvenliği hem de operasyonel sürdürülebilirlik açısından stratejik bir avantaj sunmaktadır.

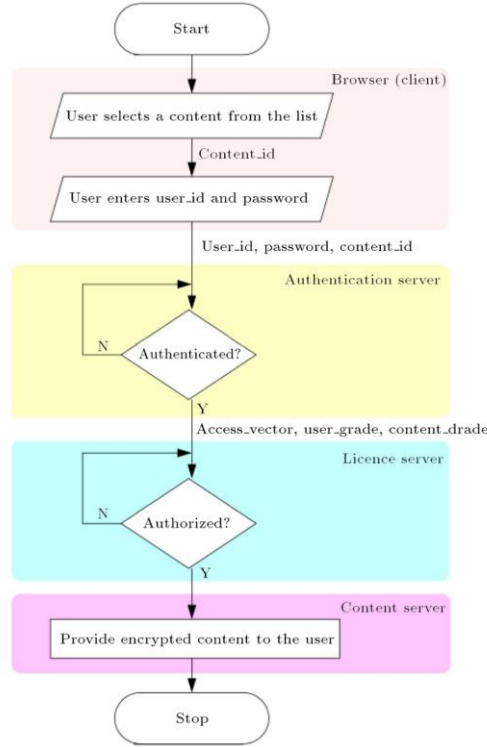
Sisteminin bütüncül güvenlik yaklaşımı, yalnızca şifreleme ve yetkilendirme tekniklerinin uygulanmasıyla sınırlı değildir; aynı zamanda bu işlevlerin modüler biçimde ayrıştırılmış sunucu bileşenleri aracılığıyla yürütülmesini esas almaktadır. Mimari, görev ayrımı ilkesine dayalı olarak yapılandırılmış ve her biri belirli işlem türlerinden sorumlu olacak şekilde tanımlanmış dört temel sunucu modülü üzerine inşa edilmiştir. Bu ayrım, sistemin ölçeklenebilirliğini artırmakta, yönetim süreçlerini kolaylaştırmakta ve güvenlik katmanlarını birbirinden izole ederek olası tehditlerin sınırlandırılmasını sağlamaktadır.

Sistem Modülleri ve İşlevsel Bileşenler: Güvenlik temelli görev ayrımı prensibine dayalı dört temel sunucu modülünden oluşmaktadır: Kimlik Doğrulama Sunucusu, Lisans (Yetkilendirme) Sunucusu, İçerik Sunucusu ve İzleme Sunucusu. Bu modüler yapı sayesinde sistem, kimlik doğrulama, erişim kontrolü, içerik saklama, veri bütünlüğü ve kullanıcı etkileşimi gibi kritik işlevleri ayrıştırılmış, esnek ve ölçeklenebilir bir çerçevede gerçekleştirebilmektedir.

Kimlik Doğrulama Sunucusu (Authentication Server): Bu bileşen, sisteme erişim talebinde bulunan kullanıcıların kimlik bilgilerinin doğrulanmasından sorumludur. Tüm kullanıcı profilleri merkezi bir kimlik veritabanında saklanmakta ve kullanıcı girişleri, güçlü kimlik doğrulama protokolleri üzerinden kontrol edilmektedir. Kimlik doğrulama sürecinde, kullanıcı adı ve parola gibi temel bilgilerin yanında, çok faktörlü

doğrulama (MFA) veya elektronik kimlik altyapıları gibi gelişmiş yöntemlerin de entegre edilmesi mümkündür. Doğrulama sürecinde başarısız olan kullanıcılar, sistemde “misafir” statüsünde tanımlanır ve yalnızca genel nitelikli, kısıtlı erişim içeriğine ulaşabilirler. Bu yaklaşım hem kullanıcı deneyiminin sürekliliğini sağlamakta hem de yetkisiz erişim risklerini sınırlamaktadır.

Lisans (Yetkilendirme) Sunucusu (Authorization Server): Kimliği doğrulanan kullanıcıların hangi içeriklere hangi koşullar altında erişebileceğini belirlemek üzere yapılandırılmıştır. Yetkilendirme kararları, rol tabanlı erişim kontrolü (RBAC) ile içeriklerin lisanslama kayıtlarında tanımlanmış erişim vektörleri üzerinden alınmaktadır. Böylece her erişim talebi, sistemde kayıtlı rol–yetki eşleşmeleri ve içerik–lisans tabloları ile çapraz kontrol edilmekte; yalnızca ilgili haklara sahip kullanıcıların erişimine izin verilmektedir. Bu sunucu, erişim kontrolünün merkezi bir karar noktası olarak çalışmakta ve her içerik talebi için güvenlik politikalarının istikrarlı biçimde uygulanmasını garanti altına almaktadır. **Şekil 4.5**’de bir kullanıcının içerik talebine ilişkin süreç akışı özetlenmektedir. Kullanıcı önce içerik seçimini yapar ve kimlik bilgilerini girer. Ardından kimlik doğrulama sunucusu, kullanıcıyı merkezi kimlik veritabanına göre kontrol eder. Başarılı doğrulama sonrası, talep edilen içerik bilgisi ve kullanıcı profili lisans sunucusuna iletilir. Lisans sunucusu erişim vektörleriyle uyumlu bir hak denetimi gerçekleştirdikten sonra, yetkilendirme başarılı ise içerik sunucusuna yönlendirme yapılır. Son aşamada içerik, şifrelenmiş biçimde kullanıcıya iletilir.



Şekil 4.5. Bir kullanıcının içerik talebine ilişkin akış diyagramı.

İçerik Sunucusu (Content Server): Dijital varlıkların depolanması, işlenmesi ve istemcilere güvenli biçimde iletilmesinden sorumludur. Sisteme yüklenen her içerik, öncelikle benzersiz bir içerik kimliği (CID) ile tanımlanır. Bu süreç, dijital nesnelerin yapısal tanımlanmasında uluslararası kabul gören MPEG-21 DID (Digital Item Declaration) standardı ile uyumlu olarak yürütülmektedir (Burnett vd., 2005). Yükleme aşamasında içerikler sistem tarafından otomatik olarak şifrelenir; böylece içeriklerin bütünlüğü ve gizliliği, depolama katmanında dahi korunmuş olur. İçerik sunucusu aynı zamanda şifreleme anahtarlarının yönetiminden sorumlu olup, gerekli durumlarda ilgili anahtarları çözerek istemci uygulamalara güvenli aktarımını sağlar. Bu işlev, sistemin güvenlik katmanları arasındaki kritik köprü görevini üstlenmektedir.

İzleme Sunucusu (Monitoring Server): Kullanıcıların sistem içindeki tüm etkileşimlerini kayıt altına alır ve erişim güvenliğinin sürdürülebilir biçimde denetlenmesine olanak tanır. Üretilen log verileri, yalnızca güvenlik ihlallerinin tespiti için değil, aynı zamanda sistem performansının optimizasyonu ve kullanıcı davranışlarının analizi için de kullanılmaktadır. Bu kapsamda, erişim yoğunluğu, içerik talep sıklığı ve yetkisiz erişim denemeleri gibi metrikler sistematik biçimde izlenir. Elde edilen veriler, hem yönetsel karar destek sistemlerine girdi sağlamakta hem de olası saldırı senaryolarının önceden tespit edilmesine katkı sunmaktadır.

Böylece izleme süreci, yalnızca pasif bir loglama işlevi değil, aynı zamanda aktif bir güvenlik katmanı olarak işlev görmektedir.

Şifreleme Altyapısı ve Anahtar Yönetimi: EDU-DRM sisteminde kullanılan şifreleme altyapısı, hibrit kriptografi yaklaşımına dayalıdır. Sistem kurulumu sırasında RSA algoritması ile 4096 bit uzunluğunda açık (public) ve gizli (private) anahtar çiftleri üretilmekte; gizli anahtar yalnızca root seviyesinde erişilebilir özel bir alanda güvenli biçimde saklanmaktadır. Her içerik için ayrıca rastgele oluşturulan 256 bitlik simetrik bir “content key” kullanılmakta, bu anahtar RSA ile şifrelenerek veritabanında saklanmaktadır. Bu sayede, simetrik şifrelemenin performans avantajı ile asimetrik şifrelemenin güvenlik gücü bir arada kullanılmaktadır. İçeriklerin sisteme yüklenmeden önce bütünlük kontrolleri de gerçekleştirilmektedir: SHA-1 ve/veya MD5 algoritmalarıyla üretilen özet (hash) değerleri, veritabanında saklanarak gelecekteki bütünlük doğrulamaları için referans alınmaktadır. Bu çok katmanlı kriptografik yapı, içeriklerin hem depolama aşamasında hem de iletim sürecinde yetkisiz erişimlere karşı korunmasını sağlamaktadır.

İçerik Yükleme Süreci (Upload): Kimlik doğrulama ve yetkilendirme aşamalarını başarıyla geçen içerik sağlayıcılar, sistem menüsü üzerinden “yükleme” seçeneğini kullanarak içerik aktarımını gerçekleştirir. Bu aşamada sağlayıcı, materyalin tanımlayıcı meta-verilerini girer ve dosyanın sistemdeki konumunu belirler. Metadata, uluslararası kabul görmüş MPEG-21 DID (Digital Item Declaration) standardına uygun biçimde oluşturularak veritabanına kaydedilir. Yüklenen dosya türlerinde herhangi bir sınırlama bulunmamakla birlikte, sistem öncelikli olarak PDF ve metin tabanlı içeriklerin yönetimine odaklanmıştır. İçerikler yükleme esnasında gerçek zamanlı olarak şifrelenir ve yalnızca şifreli biçimleri içerik sunucusunda saklanır.

İçerik Görüntüleme Süreci (View): Yetkilendirilmiş kullanıcıların içeriklere erişimi, istemci ile sunucu arasında kurulan güvenli ve şifreli oturumlar üzerinden sağlanır. Sunucu tarafında, veritabanında saklanan şifreli content-key alınır ve root düzeyinde çözümlenir. Ardından içerik, gerekli kontrol betikleri (örn. JavaScript tabanlı güvenlik bileşenleri) ile HTTPS protokolü üzerinden istemciye aktarılır. İstemci tarafında çalışan bu betikler, içerik görüntülenirken kopyalama, yazdırma veya yerel diske kaydetme gibi işlemleri engeller. Ayrıca content-key, güvenlik gerekçesiyle istemci diskine asla kaydedilmez; yalnızca geçici bellekte tutulur ve oturum kapandığında otomatik olarak silinir.

Bu yapısal ayırım, EDU-DRM sisteminin içerik yükleme, saklama, erişim denetimi ve görüntüleme süreçlerini güvenli, yönetilebilir ve sürdürülebilir biçimde birbirinden ayırmasını mümkün kılmaktadır. Böylece sistem, bir yandan yüksek güvenlik standartlarında veri işleme ve saklama imkânı sunarken, diğer yandan kullanıcı etkileşimini esnek ve kontrollü bir çerçevede sürdürmektedir. Bu yaklaşım, geniş ölçekli dijital içerik dağıtım ekosistemlerinde hem operasyonel verimlilik hem de fikri mülkiyetin korunması açısından bütüncül bir dijital hak yönetim altyapısı sağlamaktadır.

4.3.3. Güvenlik katmanları ve erişim denetimi

Önerilen sistem mimarisi, dijital içeriklerin yalnızca yetkilendirilmiş kullanıcılar tarafından erişilebilmesini ve erişim süreci boyunca veri bütünlüğünün korunmasını esas alan çok katmanlı bir güvenlik modeli ile desteklenmektedir. EDU-DRM ve TBCDN bileşenleri, farklı güvenlik düzeylerini birbirini tamamlayacak biçimde uygulayarak hem istemci tarafında hem de dağıtım ağı genelinde içerik güvenliğini sürdürülebilir kılmaktadır.

Kimlik Doğrulama (Authentication): Sisteme giriş yapan her kullanıcının kimliği, merkezi kimlik doğrulama altyapısı üzerinden çok faktörlü yöntemlerle kontrol edilmektedir. Bu süreçte kullanıcı kimlik bilgileri, cihaz kimliği ve oturum parametreleri birlikte doğrulanır. Başarılı kimlik doğrulama, ilgili kullanıcıya ait erişim vektörünün aktifleşmesi ile sonuçlanır ve sistemin diğer güvenlik katmanları için temel teşkil eder.

Erişim Yetkilendirme (Authorization): Bit tabanlı erişim vektörleri aracılığıyla içerik düzeyinde yetkilendirme gerçekleştirilmektedir. Her dijital nesne, kullanıcı rolü ve erişim politikalarıyla ilişkilendirilmiş erişim matrisine göre şifrelenmiş olarak saklanır. Bu sayede kullanıcılar yalnızca kendilerine tanımlı içeriklere erişebilir. Ayrıca, içerik üzerinde gerçekleştirilebilecek işlemler (örneğin indirme, yazdırma, paylaşma) erişim vektörleri üzerinden ayrıntılı biçimde denetlenir.

Uçtan Uca Şifreleme (End-to-End Encryption): İçerikler TBCDN sistemine yüklenmeden önce AES-256 standardında şifrelenir ve aktarım süreci boyunca TLS 1.3 protokolü üzerinden güvenli iletim sağlanır. Dağıtım ağı üzerinde her ara düğüm, yalnızca kendi yetkili özel anahtarı ile çözümlenebilecek şifreli blokları iletir. Böylece içeriklerin ağ içerisinde yetkisiz şekilde açığa çıkması teknik olarak imkânsız hale

getirilir. Bu yaklaşım hem merkezî hem de dağıtık güvenlik risklerine karşı etkin bir koruma sağlamaktadır.

Veri Bütünlüğü ve Geri İzlenebilirlik: Her içerik dosyası, SHA-512 tabanlı dijital özet (hash) değerleri ile imzalanmakta ve istemci tarafında erişim sırasında bütünlük doğrulaması yapılmaktadır. Böylece, iletim veya depolama sırasında içerikte en ufak bir değişiklik gerçekleşmişse sistem bunu anında tespit edebilmektedir. Ayrıca, tüm erişim işlemleri kimlik bilgisi, zaman damgası, IP adresi ve içerik ID'si ile günlüklenmektedir. Bu kayıtlar yalnızca adli analiz süreçlerinde değil, aynı zamanda erişim politikasının ihlal edilmesi durumlarında da denetim ve izleme imkânı sunmaktadır.

Cihaz Denetimi ve Oturum Sınırlamaları: Kullanıcıların tanımlı cihazları dışından erişim talepleri sınırlandırılmakta; her cihaz için içerik erişim hakkı oturum bazlı olarak yönetilmektedir. Oturumlar belirli bir zaman aşımı (timeout) politikasına tabidir ve pasif durumda kalan bağlantılar otomatik olarak sonlandırılmaktadır. Aynı anda birden fazla cihazdan içerik erişimi engellenerek, yetkisiz çoğaltma ve paylaşım senaryolarının önüne geçilmektedir.

Replikasyon Güvenliği ve CDN Düğüm Denetimi: İçerikler, TBCDN mimarisi kapsamında yalnızca şifreli biçimde düğümler arasında aktarılmaktadır. Düğümler arası bağlantılar mutual TLS (mTLS) protokolü ile kurulmakta; bu sayede hem istemci hem de sunucu tarafı kimlik doğrulaması sağlanmaktadır. İçerik replikasyonu yalnızca EDU-DRM erişim kurallarını içeren yetkilendirilmiş düğümler arasında gerçekleştirildiğinden, dağıtım zincirinde yetkisiz çoğaltma riski ortadan kaldırılmaktadır.

Bu bütünlük yapısı, yalnızca içerik erişim haklarını denetlemekle kalmaz; aynı zamanda istemci tarafı veri manipülasyonu, lisanssız çoğaltma ve yetkisiz erişim gibi tehdit senaryolarını da teknik düzeyde engeller. Böylece EDU-DRM ve TBCDN sistemleri, güvenlik, gizlilik ve lisans bütünlüğü gereksinimlerini eşzamanlı olarak karşılayan ölçeklenebilir ve denetlenebilir bir güvenlik mimarisi sunmaktadır.

4.4. Toplam Uçtan Uca Ağ Gecikmesi

Gerçek IP ağlarında veri paketleri genellikle sabit boyutlu segmentlere bölünerek farklı ağ rotaları üzerinden iletilir. Ancak bu iletim her zaman coğrafi olarak en kısa

yol üzerinden gerçekleşmeyebilir. Örneğin İstanbul'dan Sakarya'ya iletilen bir paket, ağ yoğunluğu veya kullanılan yönlendirme protokollerine (ör. BGP) bağlı olarak İstanbul → Kocaeli → Sakarya rotası yerine daha dolaylı ve uzun bir iletim hattına sahip olan İstanbul → Yalova → Bursa → Ankara → Düzce → Sakarya gibi dolaylı rotaları izleyebilir. Bu tür alternatif rotalar, her yeni düğümde yeni bir gecikme bileşeni yaratır ve toplam gecikmenin artmasına neden olur. Bu nedenle toplam uçtan uca gecikme, ağın o anki durumu ve izlenen rota doğrultusunda dinamik olarak değişmektedir.

Gerçek ağlarda tıkanıklık, tampon taşmaları veya iletim hataları nedeniyle paket kayıpları yaşanabilmektedir. TCP gibi güvenilir protokoller, bu kayıpları zaman aşımı mekanizmaları veya yinelenen onay paketleri (ACK) aracılığıyla algılar ve kaybolan paketlerin yeniden iletimini başlatır. Ancak her yeniden iletim en az bir ek gidiş-dönüş süresi (RTT – Round Trip Time) gecikmesi yaratır. Özellikle yüksek kayıp oranı veya uzak mesafeli iletimlerde bu ek gecikmeler, uçtan uca performansı ciddi ölçüde etkileyebilir.

Bu çalışmada paket kaybı, yeniden iletim ve hata düzeltme gibi dinamikler kapsam dışında tutulmuştur. Geliştirilen analitik model, yalnızca içerik iletimine ilişkin sabit yapısal gecikme bileşenlerine odaklanmakta ve ideal ağ koşullarını varsaymaktadır. Bununla birlikte, ileride yapılacak çalışmalarda paket kaybı, jitter ve yeniden iletim etkilerinin ayrı birer parametre olarak dahil edilmesi, daha gerçekçi bir modelleme sunacaktır.

Server-Client ve Cache-Proxy gibi merkezi yapılarda, özellikle eşzamanlı veya patlamalı trafik artışlarının görüldüğü senaryolarda sunucular aşırı yük altında kalabilmektedir. Bu durumda, kök sunucularda işlem ve kuyruklama gecikmeleri birikerek sistemin yanıt veremez hale gelmesine yol açar. Kuyruk gecikmesinin, ağ yükü arttıkça logaritmik olarak büyüdüğü literatürde yaygın biçimde rapor edilmiştir. Dolayısıyla, uçtan uca gecikmenin doğru anlaşılabilmesi için her bir düğümde oluşan gecikme bileşenlerinin ayrıştırılması kritik öneme sahiptir.

Bir iletişim yolundaki toplam düğüm gecikmesi aşağıdaki formül ile ifade edilmektedir:

$$d_{\text{nodal}} = (N - 1) \cdot (T_{\text{processing}} + T_{\text{queuing}} + T_{\text{propagation}} + T_{\text{transfer}}) \quad (4.1)$$

Burada (N), verinin geçtiği ara düğüm sayısını (yönlendirici, anahtar ya da önbellek noktaları gibi); ($N - 1$) terimi ise bu düğümleri birbirine bağlayan yolların, yani geçiş (hop) sayısını ifade eder. Her hop bir düğüm geçişi gibi görünse de gecikme aslında iki düğüm arasındaki iletim hattında oluşur. Bu nedenle gecikmenin temel belirleyicisi düğüm sayısı değil, bağlantı sayısıdır. Bu formülasyon, içerik dağıtım yapılarındaki ağ katmanını gecikmelerinin hassas biçimde modellenmesini sağlamaktadır.

Bu çalışmada yayılım gecikmesi ($T_{\text{propagation}}$), işlem gecikmesi ($T_{\text{processing}}$) ve kuyruk gecikmesi (T_{queuing}) ihmal edilmiştir. Bunun temel nedeni, bu bileşenlerin ağ topolojisi, trafik yoğunluğu, yönlendirici yapısı ve zamana bağlı değişkenlik gibi faktörlere göre yüksek oranda değişkenlik göstermesidir. Özellikle yayılım gecikmesi, geniş alan ağlarında düğümler arası fiziksel mesafeye bağlı olsa da çoğu durumda iletim gecikmesine kıyasla daha düşük kalmaktadır. İşleme gecikmeleri ise modern donanımlarda milisaniyenin altında gerçekleşmekte ve toplam gecikme üzerinde belirleyici etkisi azalmaktadır. Kuyruk gecikmesi, yalnızca aşırı trafik yükü veya patlamalı istek durumlarında öne çıkmakta olup, bu tür sınır durumlar bu çalışmanın kapsamı dışında bırakılmıştır.

Bu sebeplerle, analizde yalnızca iletim gecikmesi (T_{transfer}) temel alınmış ve yapısal farkların karşılaştırılmasına odaklanılmıştır. Bununla birlikte, söz konusu bileşenler daha ileri çalışmalar kapsamında modele eklenerek bütüncül bir analiz yapılabilir.

4.4.1. TBCDN mimarisinde gecikme modellemesi ve karşılaştırmalı analiz

Ağ tabanlı içerik dağıtım sistemlerinin performansını belirleyen en kritik ölçütlerden biri, uçtan uca toplam gecikmedir. Özellikle geniş ölçekli ve çok katmanlı mimarilerde, içeriklerin hangi rotalar üzerinden, kaç ara düğümden geçerek son kullanıcıya ulaştığı bu toplam gecikmenin boyutunu doğrudan etkiler. Bu nedenle, klasik sunucu-istemci (SC), önbellek-proxy (CP), geleneksel CDN ve önerilen ağaç tabanlı CDN (TBCDN) yapılarının gecikme davranışlarının karşılaştırmalı olarak incelenmesi önemlidir.

$D_A(N)$, mimari A' 'da N düğüm üzerinden geçen bir isteğin toplam düğümsel gecikmesini ifade etsin. Tekrarlayan içerik istekleri için şu eşitsizlik sağlanır:

$$d_{\text{nodal}} = (N - 1) \cdot (T_{\text{processing}} + T_{\text{queuing}} + T_{\text{propagation}} + T_{\text{transfer}}) \quad (4.2)$$

$$D_{TBCDN}(N_T) < D_{CDN}(N_C) < D_{CP}(N_P) < D_{SC}(N_S) \quad (4.3)$$

Her düğümde yaşanan gecikme şu bileşenlerden oluşur:

$$D_{\text{düğüm}} = (T_{\text{processing}} + T_{\text{queuing}} + T_{\text{propagation}} + T_{\text{transfer}}) \quad (4.4)$$

Toplam gecikme, N düğüm için yaklaşık olarak:

$$D_A(N) = \sum_{i=1}^{N-1} \frac{D_{\text{node}}}{1-p_i} \approx (N-1) \cdot D_{\text{node}} \quad (\text{eğer } p_i \approx 0) \quad (4.5)$$

Eğer paket kaybı oranı düşükse eğer $p_i \approx 0$ kabulüyle sadeleşir:

$$D_A(N) \approx (N-1) \cdot D_{\text{node}} \quad (4.6)$$

Bu yaklaşık ifade, kayıpsız veya düşük kayıplı ağlar için geçerlidir.

Hiyerarşik yapı, kök düğümden başlayarak aracı katmanlar üzerinden uç düğümlere uzanan beş seviyeli bir organizasyon göstermektedir; dolayısıyla mimarinin derinliği $d = 5$ seviyedir:

$$N_S = d + 1 = 6 \quad (4.7)$$

$$N_P = 1(\text{önbellekten}), = N_S(\text{önbelleksiz}) \quad (4.8)$$

$$N_C \in [2, d + 2] \quad (\text{eş düğüm mesafesine bağlı}) \quad (4.9)$$

$$N_T = 2 \text{ veya } 3(\text{öz yinelemeli istek yönlendirme}) \quad (4.10)$$

Yukarıda verilenler her bir yöntem için ele alındığında aşağıdaki gibi bir sonuç elde edilmektedir:

$$D_{SC} = d \cdot D_{\text{node}} = 5 \cdot D_{\text{node}} \quad (4.11)$$

$$D_{CP} \approx D_{\text{node}} \quad \text{veya} \quad D_{CP} = D_{SC} \quad (4.12)$$

$$D_{CDN} \in [2, 6] \cdot D_{\text{node}} \quad (4.13)$$

$$D_{TBCDN} = (1 \text{ veya } 2) \cdot D_{\text{node}} \quad (4.14)$$

Dolayısıyla:

$$D_{TBCDN} < D_{CDN} < D_{CP} < D_{SC} \quad (4.15)$$

$$D_{TBCDN}(N_T) < D_{CDN}(N_C) < D_{CP}(N_P) < D_{SC}(N_S) \quad (4.16)$$

TBCDN mimarisi, özyinelemeli ve yerleştirilmiş yönlendirme yapısı sayesinde, tekrarlayan içerik isteklerini genellikle yalnızca 1 veya 2 düğüm üzerinden karşılamaktadır. Bu mimari yapı, iletim, işlem ve kuyruk gecikmelerini asgariye indirirken, içerik yayılımını yalnızca ilgili düğümlerle sınırlandırarak ağ üzerindeki

toplam yükü azaltmaktadır. Dolayısıyla, sabit düğüm gecikmesi varsayımı altında ve çok katmanlı hiyerarşik ağ topolojilerinde, TBCDN mimarisi toplam gecikmeyi minimize eden yapısal olarak üstün bir çözüm sunmaktadır.



5. DENEYSEL ORTAM, BULGULAR VE DEĞERLENDİRME

Bu bölümde, önerilen bütünleşik mimarinin (EDU-DRM ve TBCDN bileşenleri) deneysel gerçekleştirme süreci, kurulum ayrıntıları ve performans analizleri ele alınmaktadır. Deneysel ortam, hem yazılım hem de donanım bileşenlerini kapsayacak şekilde uçtan uca tanımlanmış; ağ topolojisi, düğüm yerleşimi ve bileşen etkileşimleri ayrıntılı biçimde açıklanmıştır. Ardından, iş yükü modeli, performans ölçütleri ve karşılaştırmalı yöntemler sistematik olarak ortaya konmuştur.

Değerlendirme süreci üç aşamada yapılandırılmıştır: İlk olarak, deneysel kurulumun teknik bileşenleri (donanım, yazılım yığını, ağ altyapısı) detaylandırılmış; ikinci aşamada, test senaryoları ve ölçüm yöntemleri tanımlanmış; üçüncü aşamada ise elde edilen bulgular analitik olarak değerlendirilmiş ve klasik yaklaşımlarla karşılaştırılmıştır.

Bu deneysel çalışma, özellikle önerilen mimarinin ölçeklenebilirlik, erişim gecikmesi, lisans yönetimi verimliliği ve güvenlik açısından etkinliğini test etmeyi hedeflemektedir. Bulgular yalnızca sistemin performansını ortaya koymakla kalmayacak; aynı zamanda kavramsal modelin pratik uygulanabilirliğini de ortaya koyacaktır.

Son olarak, deneysel sonuçların geçerliği üzerine metodolojik bir tartışma sunulmuş; sistemin sınırlılıkları ve gelecekteki geliştirme alanları değerlendirilmiştir. Böylece, önerilen mimarinin akademik katkısı ve gerçek dünya uygulamalarına yönelik potansiyeli bütüncül bir bakış açısıyla ortaya konmuştur.

Bu bölümdeki deneysel değerlendirme, bölüm 4.3'te tanımlanan hak modeli ve mimari akışın üzerine inşa edilmiştir; kavramsal tanımlar yinelenmemiş, yalnızca test ortamına özgü yerleşim ve ölçüm sonuçları sunulmuştur.

5.1. Prototip Sistem Kurulumu ve Test Ortamı

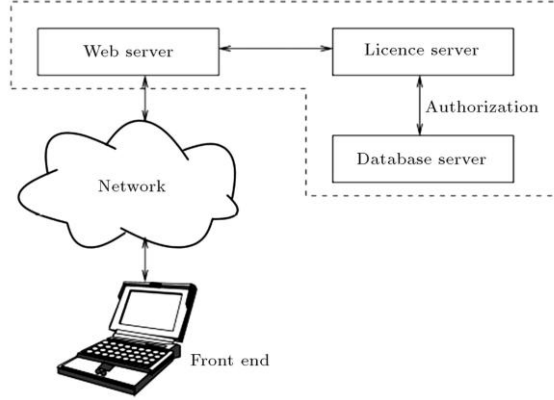
Önerilen DRM tabanlı güvenlik katmanı ile ağaç-tabanlı içerik dağıtım mimarisinin (TBCDN) bütünleşik performansını değerlendirmek amacıyla, tam işlevli bir prototip sistem Sakarya Üniversitesi bünyesinde kurulmuş ve kontrollü bir test ortamında

çalıştırılmıştır. Kurulum, hem lisanslama–yetkilendirme sürecinin hem de dağıtım altyapısının gerçekçi koşullar altında ölçümlenmesine olanak tanıyacak biçimde yapılandırılmıştır. Ayrıca, karşılaştırmalı değerlendirme için sistem mimarisine alternatif bir XML tabanlı yetkilendirme modülü entegre edilmiş ve web servisleri aracılığıyla aynı ortamda test edilmiştir.

Yetkilendirme sürecinde kullanılan belgeler, Polo vd. (2004) tarafından tanımlanan XML şeması temel alınarak uyarlanmıştır. Ortalama belge boyutu yaklaşık 1 KB olmakla birlikte, sistemin farklı senaryolardaki duyarlılığını ölçmek amacıyla daha büyük boyutlu belgeler de kullanılmıştır. Böylece hem hafif hem de yoğun kurallı erişim politikaları altında sistemin davranışı gözlemlenmiş; özellikle yetkilendirme gecikmesi ile uçtan uca erişim gecikmesine etkileri ayrıntılı olarak değerlendirilmiştir.

Yük üretimi ve yanıt sürelerinin ölçülmesi için Apache Bench (ab) aracı kullanılmıştır (Prokofyeva & Boltunova, 2017). Araç, farklı eşzamanlı istemci seviyeleri ve değişken toplam istek hacimleriyle prototip üzerinde yük oluşturacak şekilde yapılandırılmıştır. Her test senaryosu çoklu tekrarlarla yürütülmüş ve varyans analizi yapılarak gözlemlerin istatistiksel güvenilirliği sağlanmıştır. Ölçümler sırasında istemci tarafı bekleme süreleri, sunucu yanıt süreleri, hata oranları ve başarılı işlem yüzdeleri kaydedilmiştir. Bu metrikler daha sonra server–client, cache–proxy, geleneksel CDN ve önerilen TBCDN senaryoları ile karşılaştırmalı olarak raporlanmıştır.

Test yatağı **Şekil 5.1**'de şematik olarak sunulmaktadır. Ön uç istemciler, ağ üzerinden web sunucusuna erişmekte; web sunucusu, lisans sunucusuyla ve yetkilendirme akışını yöneten veritabanı sunucusuyla etkileşmektedir. Bu yapı, içerik sunumu, lisans doğrulama ve erişim haklarının uygulanmasını ayırık servisler olarak konumlandırmakta; böylece her bir bileşenin sistem genelindeki performansa katkısı bağımsız biçimde ölçülebilmektedir.



Şekil 5.1. Bit ve XML tabanlı yetkilendirme yöntemleri test diyagramı

Fiziksel altyapı, VMware vSphere 6.0 sanallaştırma platformu üzerinde çalışan yüksek performanslı bıçak sunuculara dayalıdır. Web sunucusu, lisans sunucusu ve veritabanı sunucusu aynı fiziksel havuz üzerinde birbirinden ayrılmış sanal makineler olarak yapılandırılmış, böylece hem kaynak paylaşımı optimize edilmiş hem de servis izolasyonu sağlanmıştır. Kullanılan bıçak sunucuların donanım yapılandırmaları aşağıdaki gibidir:

Blade 1: 6 × Intel Xeon E5-2630 v4, 2.20 GHz, 10 çekirdek

Blade 2: 2 × Intel Xeon E5-2640 v4, 2.40 GHz, 10 çekirdek

Blade 3: 2 × Intel Xeon E5-2650 v4, 2.40 GHz, 10 çekirdek

Blade 4: 1 × Intel Xeon X5650 v4, 2.66 GHz, 6 çekirdek

Sistem genelinde toplam 2.47 TB RAM sağlanmıştır. Depolama altyapısı, çok katmanlı disk havuzlarını (SSD, SAS, NL-SAS, SATA) destekleyen Hitachi HUS130 hibrit depolama sistemi üzerinde, toplam 100.78 TB kapasite ile yapılandırılmıştır. Bu sayede, farklı I/O yoğunluklarına sahip süreçler için uyarlanabilir performans elde edilmiştir. Ağ omurgası, sunucular arası 10 GbE bağlantılar ve dış erişim için 40 Gbps fiber uplink ile sağlanmıştır. Deneysel çalışmalarda, tüm bileşenler aynı L2 segmentinde izole edilerek arka plan gürültüsü minimize edilmiş, böylece ölçümlerin yalnızca sistemsel faktörlerden etkilenmesi sağlanmıştır.

Kurulum, yeniden üretilebilirlik ilkesi gözetilerek sürüm sabitleme yaklaşımıyla gerçekleştirilmiştir. Tüm hizmet süreçleri ve konfigürasyon betikleri sürüm kontrol altında tutulmuş, deneyler sırasında sistem kararlılığı ve tekrarlanabilirlik garanti altına alınmıştır. Zaman eşgüdümü için ağ zaman protokolü kullanılmış; ölçümlerin

senkronizasyonu ve sistemin gözlemlenebilirliği için telemetrik veriler toplanmıştır. Ayrıca, güvenli iletişim gereksinimleri saklı tutulmuş; yetkilendirme ve lisans doğrulama trafiği veri bütünlüğünü koruyan şifreli kanallar üzerinden yürütülmüştür.

5.2. EDU-DRM Gerçekleme Süreci

Önerilen mimaride hakların uygulanması dağıtım yolundan ayrık fakat onunla sıkı bağlı bir erişim katmanı olarak tasarlanmıştır. Amaç, yüksek eşzamanlılık altında yetkilendirme gecikmesini minimize ederken, içerik güvenliğini ve birlikte çalışabilirliği korumaktır. Bu kapsamda sistem; içerik paketleme ve şifreleme, lisans üretimi ve doğrulama, politika değerlendirme ve istemci-ucunda zorunlu kılma bileşenlerinden oluşan uçtan uca bir boru hattı olarak gerçekleşmiştir. Karşılaştırmalı temel olarak, EDU-DRM'in bit tabanlı yetkilendirme modeli ile XML tabanlı bir yetkilendirme modülü aynı servis mimarisi içinde konumlandırılmış ve ölçümler 5.4.1'de sunulmuştur.

5.2.1. Sağlayıcılar, kullanıcı – içerik dijital hak tanımlamaları

Bu alt bölümde, genel mimariyle uyumlu olarak ekosistemdeki başlıca varlıkların (sağlayıcılar, kullanıcılar ve içerik nesneleri) nasıl temsil edildiği ve dijital hakların nasıl tanımlandığı ortaya konulmaktadır. Amaç, DRM katmanında yürütülecek yetkilendirme ile 5.2.3'te açıklanan dağıtım sürecinin üzerinde çalışacağı tutarlı bir veri modelinin tesis edilmesidir.

Kullanıcı modeli, Bölüm 4'te tanımlanan 8 bitlik (tek bayt) bir yetkilendirme vektörüne dayanmaktadır. Bu vektör ile kullanıcıya atanan rol ve kabiliyetler sıkıştırılmış biçimde temsil edilmekte ve sabit zamanda değerlendirilebilmektedir. Vektör, kullanıcı sisteme ilk kaydolduğunda oluşturulmakta; sağlayıcıların izin hizmetinde kullanıcı kimliği, durum (aktif/askıda/süresi dolmuş), geçerlilik aralığı ve gerekirse cihaz bağlarıyla birlikte sürümlü olarak tutulmaktadır. Böylelikle ilerleyen aşamalarda gerçekleştirilecek yetki yükseltme ya da geri alma işlemleri, veri modeli değiştirilmeksizin izlenebilmektedir.

İçerik modeli, her içerik nesnesinin sağlayıcı tarafından sisteme alınması sırasında oluşturulan tanımlayıcı üstveri kümesine ve o nesneye özgü bir hak vektörüne dayanmaktadır. Üstveri; içerik kimliği, sürüm, bütünlük özeti, boyut, format türü ve dağıtım sınıfı gibi alanları kapsamaktadır. Hak vektörü bit tabanlı olarak

tanımlanmakta ve kullanıcı vektörü ile aynı bit konumlandırması kullanılmaktadır; bu sayede 5.2.2’de ele alınacak karar sürecinde herhangi bir dönüşüm gerekmez doğrudan bit düzeyinde karşılaştırma yapılabilir. Aynı başlığın farklı edisyonları veya dönemsel sürümleri için özgül hak vektörleri atanabilmekte ve böylece nesne düzeyinde hassas denetim sağlanmaktadır.

Bit konumları, platformdan bağımsız temel ayrıcalık alanlarını temsil edecek şekilde yapılandırılmaktadır. Bu alanlar; çevrimiçi görüntüleme/akış, kontrollü indirme, süre sınırlı çevrimdışı kullanım, yazdırma kotası, not veya işaretleme izni, cihaz bağlama, kurum içi paylaşım ve ekran yakalama/otomatik kayıt koruması gibi farklı kullanım senaryolarını kapsayacak biçimde tanımlanabilmektedir. Kullanılmayan bitler, sistem gereksinimlerine göre genişletilebilir; ancak bit anlamlarının sistem genelinde tutarlı kalması hem geriye dönük uyumluluk hem de sabit zamanda gerçekleştirilen hak değerlendirmeleri açısından kritik öneme sahiptir.

Hak tanımlarının yönetimi, sağlayıcı bünyesinde sürdürülen iki temel kayıt üzerinden yürütülmektedir: kullanıcı dizini ve içerik sicili. Kullanıcı dizini, kimlik belirteci, durum (aktif/askıda/süresi dolmuş), geçerlilik aralığı, cihaz bağları ve tek baytlık hak vektörünü içerirken; içerik sicili, her nesneye ait tanımlayıcı bilgileri, hak vektörünü ve sürüm geçmişini barındırmaktadır. Politika şablonları, içerik kategorileri (örneğin genel erişimli, lisanslı, kurumsal kullanım, araştırma verisi) için varsayılan hakları belirlerken; nesneye özgü sapmalar ilgili kayıtlarda işaretlenmekte ve politika yönetimi bu sayede esnek biçimde sürdürülebilmektedir. Böylelikle içerik paketleri veya dağıtım topolojisi değiştirilmeden hak politikaları güncellenebilir.

Hakların içerik nesneleriyle bağlanması, içeriğin sisteme kabulü sırasında gerçekleşmektedir. Bu aşamada, nesneye ait tanımlayıcı üstveri ile hak vektörü ilişkilendirilmekte ve ileride lisans nesnesi oluşturulurken kullanılmak üzere güvenli biçimde saklanmaktadır. İçerik dağıtımı sırasında CDN düğümlerinde herhangi bir hak değerlendirmesi yapılmamakta; CDN yalnızca şifreli yükü ve yönlendirme için gerekli üstveriyi barındırmaktadır. Böylece ayrıcalıkların belirlenmesi DRM katmanında sınırlandırılmakta, dağıtım katmanı ise hak durumlarından bağımsız ve ölçeklenebilir bir önbellekleme mantığıyla işletilmektedir.

Veri yapıları yalın ama işlevsel olacak şekilde tasarlanmıştır. Bir kullanıcı kaydı; kimlik belirteci, 8 bitlik hak vektörü, durum bilgisi, geçerlilik süresi ve (varsa) cihaz

bağlarını içerirken; bir içerik kaydı, içerik kimliği, sürüm ve bütünlük özeti, format, dağıtım sınıfı, hak vektörü ve yerleşim ipuçlarını barındırmaktadır. Bu minimal şema, 5.2.2’de açıklanacak lisanslama süreci ve 5.2.3’te ele alınacak dağıtım akışlarının gerektirdiği kontrolleri desteklemekte; aynı zamanda gereksiz karmaşıklıkların oluşmasını önlemektedir.

Sonuç olarak, kullanıcıların tek baytlık vektörlerle; içeriklerin ise nesneye özgü bit tabanlı hak vektörleriyle temsil edilmesi, mimaride bileşenler arasında açık bir sorumluluk ayrımı sağlamaktadır. Böylece yetkilendirme kararları DRM katmanında sabit zamanda alınabilmekte; ağaç tabanlı CDN ise hak durumlarından bağımsız, yüksek verimli bir dağıtım katmanı olarak işletilebilmektedir. Bu yapı, sistemin hem güvenlik hem de ölçeklenebilirlik boyutlarını bütüncül biçimde desteklemektedir.

5.2.2. Yetkilendirme, lisanslama

Bu bölüm, genel mimaride DRM sınırında gerçekleşen yetkilendirme ve lisanslama işlevlerinin bütünleşik biçimde nasıl çalıştığını açıklamaktadır. Kullanıcılar, Bölüm 4’te tanımlandığı üzere sekiz bitlik kompakt vektörlerle temsil edilmekte; içerik nesnelerinin hakları ise sağlayıcı tarafından her nesneye özgü olarak yine bit tabanlı biçimde kodlanmaktadır. Yetkilendirme kararı, istem anında kullanıcıya ait vektör ile içerik nesnesine ait hak vektörünün doğrudan bit düzeyinde karşılaştırılmasıyla verilir. Bu yaklaşım, karar süresini sabit zamanda tutmayı mümkün kılarken, değerlendirme işleminin tamamen DRM katmanında gerçekleştirilmesi sayesinde dağıtım altyapısının erişim ayrıcalıklarından bağımsız, ölçeklenebilir bir önbellekleme modeliyle çalışmasına imkân tanır.

Yetkilendirme akışı şu şekilde işlemektedir: İstek İşleme Yöneticisi, kullanıcıya ait vektörü sağlayıcı dizininden; içeriğe ait hak vektörünü ise içerik sicilinden çeker. Bu iki veri kümesi, Lisans Yöneticisi üzerinde tanımlanmış politika şablonlarıyla birlikte değerlendirilir. Değerlendirme sonucunda etkinleşen bitler; çevrimiçi görüntüleme veya akış, kontrollü indirme, süre sınırlı çevrimdışı kullanım, yazdırma kotası, açıklama ekleme, cihaz bağlama, kurumsal paylaşım ve ekran yakalama/otomatik kayıt koruması gibi ayrıcalıkları temsil eder. Kararın CDN’den önce alınması, ara sunucularda hak çıkarımının yapılmasını engeller ve anahtar gizliliğini korur; bu da mimarinin güvenlik bütünlüğü açısından kritik bir fayda sağlar.

Elde edilen karar, yürütülebilir bir temsil olan lisans nesnesi aracılığıyla uç noktaya iletilir. Lisans nesnesi; etkin bit kümesi, geçerlilik aralığı, kota ve cihaz kısıtları, denetim göstergeleri ile içerik anahtarının sarılı (encrypted) hali gibi bileşenleri içerir. Kısa ömürlü olacak şekilde tasarlanan lisanslar, yenileme sürecinde yeniden değerlendirilerek güncellenir. Bu sayede erişim iptali veya yetki düşürme işlemleri, içeriğin yeniden paketlenmesine gerek kalmadan anında uygulanabilir. Böylece, önbelleklerde depolanan şifreli içerikler durağan kalırken, erişim durumu dinamik olarak güncellenebilir.

Sistemin güvenilirliği ve düzenlemelere uyumu açısından lisans yaşam döngüsü boyunca tam denetlenebilirlik gözetilmektedir. Lisans Yöneticisi; kullanıcıya ait takma adlı kimlik, içerik kimliği, etkin bit kümesi, veriliş ve sona erme zamanları gibi bilgileri içeren değiştirilemez günlük kayıtları üretir. İçerik anahtarları yalnızca uç noktada çözümlenebildiğinden, ara bileşenler yetkilendirme sonucunu gözlemleyebilir ancak anahtar veya açık içerik üzerinde herhangi bir tasarrufta bulunamaz. Bu yapısal ayırım, gizlilik riskini minimize etmekte ve mimarinin uçtan uca güvenlik hedefiyle tam uyumlu bir çözüm ortaya koymaktadır.

5.2.3. İçerik dağıtım süreci ile etkileşim

Bu bölüm, DRM katmanında gerçekleşen yetkilendirme–lisanslama mekanizmasının ağaç tabanlı CDN (TBCDN) ile etkileşimini ve uçtan uca güvenlik düzenini açıklamaktadır. İçerik, sağlayıcı tarafında paketlenirken her nesne veya akış parçası için rastgele oluşturulan bir simetrik anahtar ile şifrelenir. Nesneye ait hak vektörü ve tanımlayıcı üstveri, lisans şablonuna bağlanarak dağıtım sürecinde kullanılacak kontrol noktalarını belirler. Bu yapı sayesinde CDN düğümleri yalnızca şifreli yük ve yönlendirme için gerekli üstveriyi taşıyabilmekte; hak değerlendirme veya anahtar çözme işlevleri tamamen DRM sınırında tutulmaktadır. Böylece önbellekler, farklı kullanıcı ayrıcalıklarından bağımsız olarak aynı şifreli nesneyi hizmete sunabilmektedir.

İstemci tarafındaki akış şu şekilde işlemektedir: Kullanıcı, içerik talebini İstek İşleme Yöneticisine iletir. Başarılı yetkilendirme sonrasında, istemciye ilgili lisans nesnesi ve içerik konum bilgisi döndürülür. Yönlendirme süreci, isteği hiyerarşik ağ yapısındaki en yakın uygun düğüme yönlendirir ve şifreli nesne istemciye teslim edilir. İstemci tarafındaki oynatıcı/okuyucu, lisansın içinde sarılı biçimde gönderilen anahtarı çözer ve etkin bit kümelerine göre tanımlanmış ayrıcalıkları (örneğin görüntüleme, kontrollü

indirme, çevrimdışı kullanım süresi, yazdırma kotası, cihaz bağlama veya paylaşım sınırlamaları) zorunlu kılar. Bu mimari tercih, erişim kontrolünün yalnızca uç noktada uygulanmasını sağlayarak ara sunucuların içerik haklarına dair herhangi bir bilgi edinmesini engeller.

Model, süre duyarlı senaryolarda düşük gecikmeli lisans yenileme ve erişim iptali desteği sunmaktadır. Lisans nesnelerinin kısa ömürlü tasarlanması, erişim iptalinin bir sonraki yenileme çevriminde etkinleşmesini mümkün kılar. Bu yaklaşım, şifreli nesnelerin CDN katmanında değiştirilmesini gerektirmediğinden, yayılım gecikmesini ortadan kaldırır ve sistemin bütünsel tutarlılığını korur. İçeriğin yeni bir sürümle güncellenmesi durumunda, yeni nesne farklı bir anahtar ve hak vektörüyle paketlenir; yönlendirme ipuçları ağacın üst seviyelerinden aşağıya doğru yeniden dağıtılır ve talep yoğunluğu doğrultusunda kopyalar çoğaltılır. Bu yöntem hem yüksek ön bellek isabet oranı hem de tutarlı hak icrası sağlamaktadır.

Akış tabanlı dağıtım senaryolarında (örneğin segmentli video), her segmentin ayrı şifrelenmesi, hata toleransını artırmakta ve kesintisiz oynatmayı desteklemektedir. Lisansın geçerlilik penceresi boyunca alınan segmentler çözülebilir; geçerlilik dışına çıkan istekler ise Lisans Yöneticisi tarafından reddedilmekte veya lisans yenileme sürecine yönlendirilmektedir. Çevrimdışı kullanım senaryosunda ise lisans nesnesi, istemci tarafında güvenli bir depoda saklanır ve yalnızca geçerlilik süresi boyunca izin verilen işlemler uygulanır.

Bu bütünleşik model; yetkilendirme, lisanslama ve dağıtım bileşenleri arasında açık sorumluluk ayrımı sağlamakta; güvenlik, ölçeklenebilirlik ve operasyonel basitliği aynı anda temin etmektedir. Böylelikle DRM katmanında tanımlanan haklar, TBCDN altyapısının performans avantajları ile uçtan uca güvenilir bir içerik dağıtım mekanizmasına dönüştürülmektedir.

5.3. Ağaç Tabanlı İçerik Dağıtım Ağı Gerçekleme Süreci

Önerilen TBCDN mimarisinin gerçekleşmesi, yalnızca teorik gecikme analizleriyle sınırlı kalmayıp, deneysel ölçümlerle de desteklenmiştir. Bu kapsamda, mimarinin hiyerarşik yapısı, yönlendirme yöntemleri ve içerik yerleşim stratejileri test yatağında uygulanmış ve elde edilen ölçümler sistematik biçimde kaydedilmiştir. Bu bölümde öncelikle kullanılan veri setinin özellikleri açıklanmakta, ardından 5.4 bölümünde

ayrıntılı sonuçların analizine temel oluşturacak yöntemsel hazırlık ortaya konulmaktadır.

5.3.1. Veri seti

Deneylerde kullanılan veri seti, gerçekçi talep davranışı ile hiyerarşik topoloji üzerinde oluşan ölçümlerin bütünleşik biçimde ele alınabilmesi için tasarlanmıştır. Veri şeması; RecordID, RequestID, CaseCode, MethodID, TransferTime, ContentSize, ContentID, LSID, L4ID, L3ID, L2ID alanlarından oluşmaktadır.

RecordID her kaydı benzersiz olarak tanımlar, RequestID aynı isteme ait ölçümlerin birleştirilmesine olanak sağlar. CaseCode topoloji derinliği, yük profili ve içerik sınıfı gibi faktörleri kodlayan birleşik bir tanımlayıcıdır. MethodID uygulanan yönlendirme/yerleştirme stratejisinin kimliğini gösterir ve dört farklı yöntemi ayırt etmek için kullanılır. (1) Sunucu–İstemci, (2) Cache Proxy, (3) CDN, (4) Ağaç-tabanlı CDN (özyinelemeli istek yönlendirme).

Bu yapı sayesinde, aynı RequestID–ContentID kombinasyonu sabit tutulmakta ve her yöntem için ayrı ayrı ölçüm yapılabilmektedir. Böylece yöntemler arası adil ve doğrudan kıyaslama sağlanmaktadır.

TransferTime, uçtan uca aktarım süresini (ms) kaydederken; ContentSize, içerik boyutunu (byte) belirtmektedir. ContentID nesnelerin kimliğini temsil etmekte; LSID, L4ID, L3ID, L2ID ise hiyerarşik topolojide izlenen yolu göstermektedir. Bu alanlar sayesinde her isteğin hangi ağ seviyelerinden geçtiği izlenebilmekte, böylece topoloji–gecikme ilişkisi ayrıntılı biçimde analiz edilebilmektedir. Veri gizliliği açısından içerik ve sunucu kimlikleri anonimize edilmiş, yalnızca ilişkisel bütünlük korunmuştur. Eksik veya aykırı değerler için sınır kontrolleri uygulanmış, birim dönüşümleri normalize edilmiştir (ör. ms/byte).

Veri seti iki kaynaktan beslenmektedir. Birinci kaynak, TBNS üzerinde çalıştırılan izleme modülünden elde edilen simülasyon izleridir; burada trafik Poisson tabanlı geliş süreçleri ve Zipf dağılımlı içerik popülerliği ile üretilmektedir. İkinci kaynak, küçük ölçekli saha kurulumundan toplanan örnek uçtan uca ölçümlerdir; bu ölçümler, simülasyon parametrelerinin kalibrasyonunda referans olarak kullanılmaktadır. Her iki kaynak aynı şemaya dönüştürülmekte ve birleştirilmiş veri kümesi üzerinden analizler yürütülmektedir.

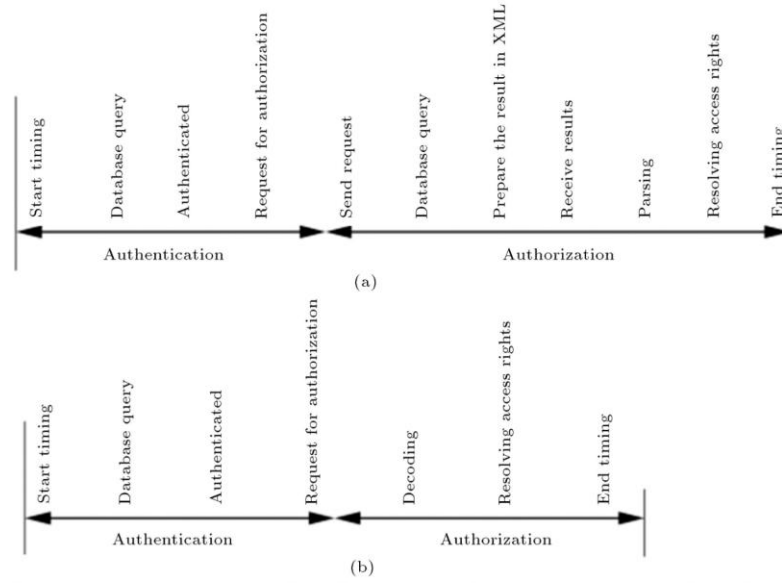
Tablo 5.1. Veri seti örneği

Record ID	Request ID	Case Code	Method ID	Transfer Time	Content Size	Content ID	L5 ID	L4 ID	L3 ID	L2 ID
513	1	211-5	1	12414,51424	38795357	3	14352	9	33	3
514	1	212-10	2	73574,832	306561800	17	16088	31	34	1
515	1	211-5	3	2866,1468	7165367	2	12368	1	28	4
516	1	213-20	4	9937,956	41408150	5	10263	5	23	6
517	2	214-40	1	35915,16896	112234903	4	22413	6	46	7
518	2	215-80	2	14541,97992	60591583	8	19514	13	41	5
519	2	212-10	3	24852,3832	31065479	11	25254	21	52	2
520	2	484-120	4	12426,1916	99368924	6	34224	18	80	1
521	3	560-40	1	24953,58592	77979956	1	16270	20	44	4

5.3.2. Performans ölçütleri ve metodoloji

EDU-DRM sisteminin performans analizi hem erişim altyapısının yanıt süresi hem de alternatif yetkilendirme mekanizmalarının kaynak tüketimi açısından değerlendirilmiştir. Bu kapsamda, özellikle bit tabanlı yetkilendirme modeli ile XML tabanlı yetkilendirme modülü karşılaştırmalı olarak test edilmiştir.

Testlerde kullanılan ölçüm aracı olan Apache Benchmark (ab), sistemin farklı eşzamanlı istemci yükleri altında nasıl davrandığını ölçmek için yapılandırılmıştır. Her bir testte 100, 1.000, 5.000 ve 10.000 eşzamanlı istek sisteme yönlendirilmiş ve sistemin bu istekleri işleme süresi milisaniye (ms) cinsinden kayıt altına alınmıştır. Yanıt süreleri, istemcinin erişim isteğinde bulunduğu andan içeriğe erişimin tamamlandığı ana kadar geçen tüm işlem süresini kapsamaktadır.



Şekil 5.2. XML ve Bit bazlı Kimlik Doğrulama ve Yetkilendirme Olayları

Testlerde XML tabanlı yetkilendirme modelinin, birlikte çalışabilirlik (interoperability) gereksinimlerini karşılamak için daha fazla işlem adımı içerdiği ve dolayısıyla kaynak tüketiminin daha yüksek olduğu gözlemlenmiştir. Şekil 5.2’de, bit tabanlı ve XML tabanlı yetkilendirme modellerinde, işlem adımlarının zaman damgalarına göre ayrıştığı görülmektedir. Bit tabanlı yapı, erişim kontrol kararlarını doğrudan içerik anahtarlarına ve rollerle ilişkilendirilmiş erişim vektörlerine dayanarak verdiği için daha kısa işlem süresine sahiptir.

Bit tabanlı yapı ile XML tabanlı yapının işlem adımları ayrıştırıldıktan sonra, karşılaştırmalı bulgular 5.4.1 alt bölümünde ayrıntılı olarak sunulmaktadır; burada gecikme bileşenleri olay çizelgesine göre raporlanmakta, yük düzeylerine bağlı değişimler güven aralıklarıyla değerlendirilmektedir. Bu bağlamda, her iki yetkilendirme yaklaşımının mimariye etkisi sabit tutulmakta ve yalnızca yetkilendirme katmanı kaynaklı farkların uçtan uca yanıt süresine katkısı izole edilmektedir.

Ağaç tabanlı ölçüm modelinde içerik iletimine odaklanıldığından, yayılım (propagation), işlem (processing) ve kuyruk (queuing) gecikmeleri tüm yöntemlerde aynı donanım/ağ altında sabit kabul edilmekte ve analizde ihmal edilmektedir; karşılaştırma etkisi aktarımı (transfer) belirleyen yol uzunluğu ile içerik boyutuna odaklanarak izole edilmektedir. Böylece TransferTime ölçümü, temelde kat edilen yol (geçilen kenar sayısı) ve ContentSize/bağlantı hızı bileşenleriyle belirlenmektedir.

Karşılaştırma, her yöntemin bir isteği karşılamak için ağacın üzerinde ne kadar yol kat ettirdiğini özetleyen yol çarpanı (κ) üzerinden yürütülmektedir. κ , aynı içerik ve aynı istem noktası için kat edilen mesafenin “en yakın düğümden tek yönlü getirme” göre göreceli katsayısı olarak tanımlanmaktadır. Ölçümler L5ID/L4ID/L3ID/L2ID alanlarından türetilmekte, her kayıt için geçilen seviye sayısı elde edilmekte ve aşağıdaki davranışlar raporlanmaktadır:

Sunucu-İstemci (MethodID=1): Tüm istekler merkez (kök) sunucudan karşılanmaktadır. Veri, kökten istemciye kadar tek yön aktarılmakta; dolayısıyla κ , istemcinin ağaç derinliği ile orantılı olmaktadır. İlk ve sonraki isteklerde davranış değişmemektedir.

Cache Proxy (MethodID=2): İlk istek merkezden getirilmekte, içerik erişim ağındaki proxy üzerinde önbelleğe alınmaktadır. Sonraki istekler proxy’den karşılanmakta; beklenen yol çarpanı $E[\kappa] = (1-h) \cdot \kappa_{\text{kök}} + h \cdot \kappa_{\text{proxy}}$ olacak şekilde hesaplanmaktadır, burada h ölçülen proxy isabet oranını ifade etmektedir (κ_{proxy} tipik olarak 1 hop kabul edilmektedir).

CDN (MethodID=3): Ağaç yapısında aynı seviye yapraklar arasında doğrudan yol bulunmadığından, içerik başka bir yaprakta ise istek bir üst düğüme yükseltilmekte ve oradan en yakın kopyaya yönlendirilmektedir. Bu nedenle gidiş + dönüş etkisiyle yaklaşık $2 \times$ yol kat edilmekte; $\kappa_{\text{CDN}} \approx 2 \cdot \kappa_{\text{kök}}$ davranışı gözlemlenmektedir. İçerik, yalnızca yetkilendirilen CDN düğümlerinde saklandığından geri dönüş yolunda tüm seviyelere yayılma gerçekleşmemektedir.

Ağaç-tabanlı CDN (MethodID=4, recursive): İstek en yakın düğümden başlatılmakta, içerik bulununcaya kadar birer seviye yukarı çıkarılmakta ve bulunan kopya geri dönüşte geçilen tüm düğümlere kopyalanmaktadır. Böylece ilk karşılamada tek yön ($1 \times$) yol kat edilmekte ($\kappa_{\text{TBCDN}} \approx 1 \cdot \kappa_{\text{kök}}$); sonrasında aynı alt ağaçtaki istekler yerel isabet ile daha da kısa yoldan karşılanmaktadır. Bu davranış, klasik CDN’e kıyasla $2 \times \rightarrow 1 \times$ yol avantajını sağlamaktadır.

Bu tanımlar ile, dört yöntemin tamamı aynı ağaç topolojisi üzerinde ve aynı donanım koşullarında koşturulmakta; fark, içeriğe ulaşmak için kat ettirilen yol ve kopyalama politikası üzerinden nicelleştirilmektedir. Recursive ağaç-tabanlı yaklaşımın $1 \times$ yol ve geri dönüşte yayılma özellikleri sayesinde, klasik CDN’in $2 \times$ yol davranışına karşı

ölçülebilir üstünlük sağladığı bu ölçütlerle ortaya konulmaktadır. 5.4.2.1 bölümünde ayrıntılı olarak ele alınmaktadır.

5.3.3. TBNS: tree-based network simulator

Önerilen TBCDN mimarisinin gerçekçi koşullar altında nicel olarak değerlendirilebilmesi, mevcut açık kaynaklı (NS-2, NS-3, OMNeT++) ve ticari (OPNET, NetSim) simülatörlerin ötesinde, yüksek hacimli eşzamanlı kullanıcı taleplerini senkronize biçimde modelleyebilecek özel bir altyapıyı gerektirmiştir. Bu ihtiyacı karşılamak üzere geliştirilen Tree-Based Network Simulator (TBNS), önerilen mimarinin özgün yönlendirme algoritması ve katmanlı yapısıyla tam uyumlu olacak biçimde tasarlanmıştır.

TBNS, yalnızca TBCDN'in performansını ölçmekle sınırlı değildir; aynı zamanda istemci-sunucu, önbellek-proxy ve geleneksel CDN mimarilerini de karşılaştırmalı olarak test edebilecek parametrik bir deney ortamı sunar. Bu yapı, farklı trafik yoğunlukları, içerik türleri ve aktarım stratejileri altında sistem davranışının gözlemlenmesine olanak tanımakta; böylece önerilen çözümün yalnızca teorik açıklamalarla değil, uygulamaya dönük koşullarda da sayısal olarak sınanmasını sağlamaktadır.

Alanında yaygın kullanılan simülatörler çoğunlukla düşük yoğunluklu ve sabit yapıli trafik senaryolarına odaklandığından, içerik dağıtım ağlarının dinamik ve ölçeklenebilir yapısını gerçeğe yakın şekilde temsil etmekte sınırlı kalmaktadır. Bu boşluğu dolduran TBNS, çok katmanlı CDN yapıları altında çalışabilen özelleştirilmiş bir çerçeve sunmakta; ağaç derinliği, kullanıcı sayısı ve içerik çeşitliliği gibi parametrelerin dinamik olarak tanımlanabildiği esnek bir kontrol altyapısı içermektedir.

Bu sayede, ağ yükü, ortalama aktarım süresi ve uçtan uca gecikme gibi kritik performans metrikleri üzerinden kapsamlı ve tekrar üretilebilir analizler yürütülebilmektedir. TBNS'in sunduğu bu bütüncül yaklaşım, önerilen TBCDN mimarisinin hem performans hem de ölçeklenebilirlik açısından metodolojik olarak güvenilir biçimde sınanmasını mümkün kılmaktadır.

5.3.3.1. TBNS'in geliştirilme gerekçesi ve kapsamı

Mevcut ağ simülasyon araçlarının büyük bir bölümü, düşük düzeyli protokol davranışlarının modellenmesine odaklanmakta; ancak gerçek dünyada içerik dağıtım

ağlarında gözlemlenen ani ve yüksek hacimli kullanıcı taleplerini ölçeklenebilir ve senkronize biçimde temsil etmede sınırlı kalmaktadır. Özellikle trafik yoğunluğunun ani artış gösterdiği patlama senaryolarında, geleneksel simülatörlerin işlemci/bellek kısıtları ve olay zamanlayıcı tasarımları doğruluk kaybına yol açmaktadır. Buna ek olarak, klasik simülasyon ortamlarının çoğu CDN katmanlarının hiyerarşik topolojisini ve üst–alt düğüm etkileşimlerini doğal olarak temsil edememekte; bu durum, mimariye özgü yönlendirme algoritmalarının test edilmesini güçleştirmektedir.

Bu eksiklikleri gidermek amacıyla geliştirilen Tree-Based Network Simulator (TBNS), önerilen TBCDN mimarisiyle doğrudan uyumlu olacak şekilde, hiyerarşik ağ yapısı ve Recursive Request Routing (RRR) algoritmasını içerecek biçimde tasarlanmıştır. TBNS yalnızca TBCDN modelinin performansını ölçmekle sınırlı değildir; aynı zamanda istemci–sunucu, önbellek–proxy ve klasik CDN mimarilerinin karşılaştırmalı değerlendirmelerine de olanak tanıyan parametrik bir çerçeve sunmaktadır. Bu yönüyle, TBNS içerik dağıtım sistemlerinin yapısal özelliklerini benzetim ortamına yüksek doğrulukla taşıyan, ölçülebilir ve genişletilebilir bir test altyapısı olarak öne çıkmaktadır.

Simülatör; dağıtım mimarisinin farklı derinlik seviyelerindeki davranışlarını gözlemleme, ölçek arttıkça oluşan ağ yükünü hesaplama ve uçtan uca erişim gecikmesi üzerindeki etkileri ölçme gibi işlevleri desteklemektedir. Bunun yanı sıra, farklı trafik senaryoları, dosya çeşitliliği ve kullanıcı sayısı gibi değişkenlerin sistem performansı üzerindeki duyarlılıklarını incelemeye imkan tanımaktadır. Bu esneklik, TBNS’i yalnızca mimari doğrulama aracı olmanın ötesinde, aynı zamanda performans optimizasyonu ve stratejik karşılaştırmalar için etkin bir araştırma ortamı haline getirmektedir.

5.3.3.2. Arayüz özellikleri ve parametre tanımı

TBNS (Tree-Based Network Simulator), deneysel senaryoların esnek biçimde tasarlanabilmesi için grafiksel kullanıcı arayüzü (GUI) destekli bir kontrol paneli sunmaktadır. Bu arayüz, kullanıcıların ağ topolojisi, trafik profili ve içerik özellikleri gibi parametreleri doğrudan tanımlayabilmesine olanak tanımakta; böylece simülasyon süreci hem kullanıcı dostu bir etkileşimle yürütülmekte hem de deneysel senaryoların tekrarlanabilirliği güvence altına alınmaktadır.

Parametre giriş alanları, minimum–maksimum aralıklar ve varsayılan değerler gözetilerek tasarlanmıştır. Bu yaklaşım, araştırmacının farklı deneysel konfigürasyonları sistematik olarak denemesine imkan tanırken, aynı senaryoların farklı zamanlarda veya farklı kullanıcılar tarafından yeniden üretilmesini de mümkün kılmaktadır.

Tanımlanabilen temel parametreler arasında şunlar yer almaktadır:

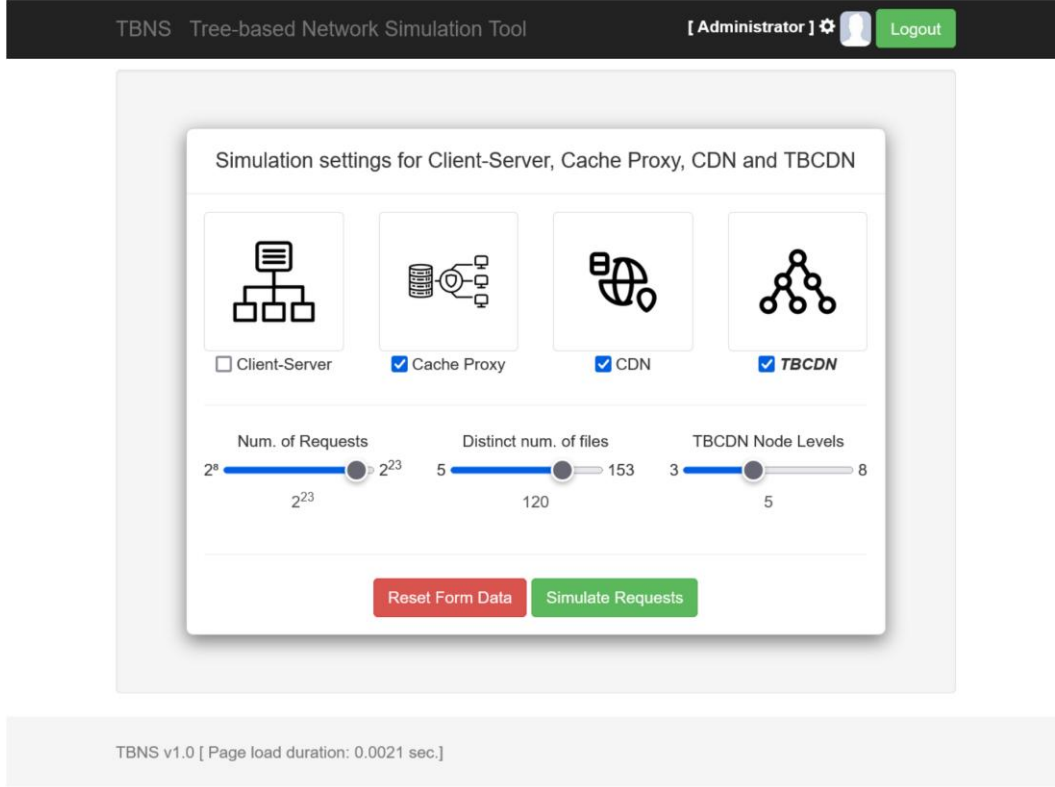
Ağaç derinliği (node levels): Önerilen TBCDN yapısının hiyerarşik seviyelerini belirlemektedir. Bu parametre aracılığıyla farklı topoloji derinlikleri altında performans farklılıkları gözlemlenebilmektedir.

Yöntem seçimi: Simülasyona dahil edilecek karşılaştırmalı yöntemler (ör. istemci–sunucu, cache-proxy, geleneksel CDN, TBCDN) kullanıcı tarafından seçilebilmekte, böylece aynı koşullar altında yöntemler arası doğrudan kıyaslama yapılabilmektedir

İstek sayısı (num. of requests): Kullanıcı yükünü tanımlamakta, farklı eşzamanlılık düzeyleri altında sistemin tepkisinin analiz edilmesine olanak tanımaktadır.

Dosya sayısı (distinct num. of files): İçerik evreninin büyüklüğünü belirleyerek, popülerlik dağılımlarının (ör. Zipf) etkisini gözleme imkânı sunmaktadır.

Bu parametrelerin farklı kombinasyonları aracılığıyla geniş ölçekli senaryo matrisleri oluşturulabilmekte; sistem davranışı, yük profili ve içerik çeşitliliği gibi faktörler altında sistematik biçimde incelenebilmektedir.



Şekil 5.3. TBNS Simülör Arayüzü

Şekil 5.3’de, TBNS arayüzünün parametre giriş panelini ve temel yapılandırma bileşenlerini göstermektedir. Bu yapılandırma, deneysel senaryoların hem kontrollü hem de gerçekçi koşullar altında yürütülmesini sağlayarak, sonraki bölümlerde sunulan karşılaştırmalı performans analizlerinin temelini oluşturmaktadır.

5.3.3.3. Simülasyon ortamı ve yazılım yığını

Tüm simülasyonlar, 64-bit Ubuntu 20.04 LTS üzerinde, Intel Core i7-11700 (8 çekirdek, 2.50 GHz), 32 GB RAM ve Python 3.10 ortamında yürütülmüştür. TBNS, Python tabanlı modüler bir simülasyon motoru ile PyQt5 destekli bir grafik arayüzden oluşur; kullanıcıdan alınan parametrelerle senaryoları yapılandırır ve çalıştırır. Çıktılar CSV olarak üretilip Pandas ve Matplotlib ile görselleştirilmiştir. Donanım/sürüm bilgileri, tekrar üretilebilirliği sağlamak ve 5.4’te sunulan sonuçların araç-bağımlı önyargılarını tartışmak üzere raporlanmaktadır.

5.4. Deneysel Çalışma Sonuçları ve Değerlendirme

Bu bölümde, önerilen bütünleşik mimarinin deneysel performans çıktıları sistematik olarak sunulmaktadır. Amaç, bölüm 5.2 ve 5.3’te açıklanan yetkilendirme–lisanslama

akışı ile ağaç tabanlı içerik dağıtım mekanizmasının, farklı yöntemlerle kıyaslandığında ne ölçüde üstünlük sağladığını ortaya koymaktır.

Deneysel değerlendirmeler iki ekseninde yürütülmüştür:

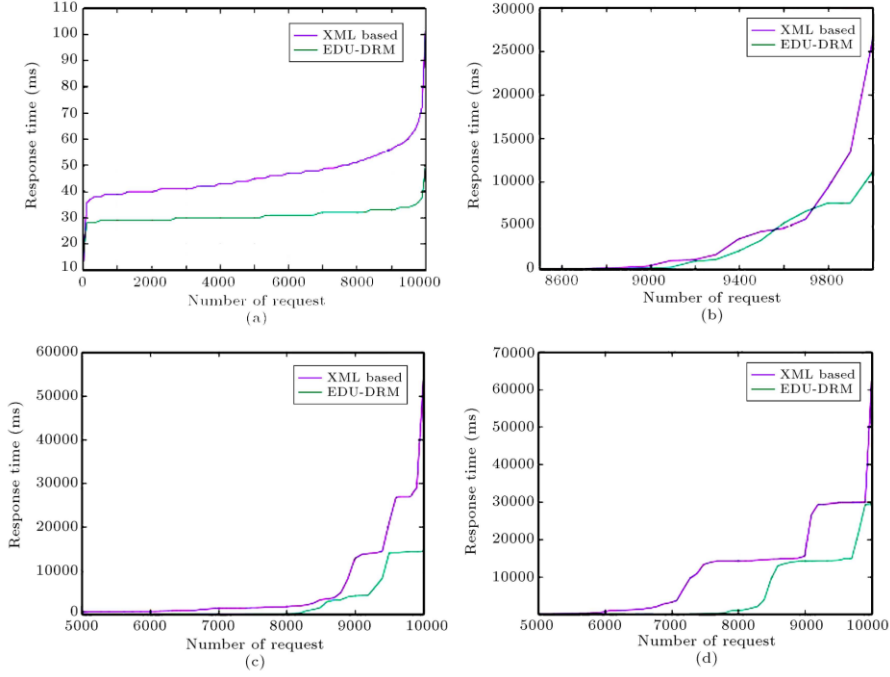
Yetkilendirme Katmanı Performansı: XML tabanlı ve bit tabanlı modeller, işlem gecikmesi, CPU tüketimi ve günlük üretim yükü gibi ölçütler üzerinden karşılaştırılmıştır. Böylelikle, birlikte çalışabilirlik odaklı ağırlaştırılmış yöntemler ile hafif ve sabit-zamanlı değerlendirme sağlayan önerilen yaklaşım arasındaki farklar ortaya konulmuştur (bkz. Bölüm 5.4.1).

Dağıtım Katmanı Performansı: İçerik transfer süresi, farklı yönlendirme ve yerleştirme stratejileri (İstemci–Sunucu, Cache Proxy, CDN, TBCDN) altında ölçülmüş; hem küçük ölçekli kontrollü senaryolar (mini senaryo) hem de milyonlarca isteğin işlendiği geniş ölçekli deneyler ile değerlendirilmiştir. Bu karşılaştırmalar, önerilen TBCDN mimarisinin düşük gecikme, yüksek isabet oranı ve ölçeklenebilirlik açısından sunduğu avantajları görünür kılmaktadır (bkz. Bölüm 5.4.2).

Elde edilen sonuçlar, EDU-DRM ve TBCDN bileşenlerinin bütünleşik olarak çalışmasının hem erişim kontrolünde hem de içerik dağıtımında daha güvenli, verimli ve ölçeklenebilir bir yapı sunduğunu göstermektedir. Bulgular, yalnızca performans kazanımlarını değil, aynı zamanda sistem tasarımında benimsenen modüler yaklaşımın yönetilebilirlik ve sürdürülebilirlik açısından yarattığı stratejik katkıları da doğrulamaktadır.

5.4.1. XML – bit tabanlı kullanıcı yetkilendirme karşılaştırmaları

Bu alt bölümde, **Şekil 5.2**'de betimlenen olay akışları temel alınarak XML tabanlı ve bit tabanlı yetkilendirme mekanizmalarının gecikme ve kaynak kullanımı özellikleri karşılaştırılmaktadır. Test ortamı ve yük profili 5.3.2'de tanımlandığı biçimde korunmakta; her bir yöntem için oturum başlatma, kimlik doğrulama, yetkilendirme, lisans üretimi ve lisansın istemciye iletilmesi adımlarında oluşan zaman damgaları toplanmaktadır. Karşılaştırmalar; medyan ve yüzde 95 gecikmeler, istek başına CPU zamanı ve sunucu/uygulama günlüğünde üretilen olay sayısı üzerinden raporlanmaktadır. Böylelikle, birlikte çalışabilirliğin sağladığı esneklik ile yürütme maliyeti arasında oluşan denge nesnel olarak ortaya konulmaktadır.



Şekil 5.4. EDU-DRM ile XML tabanlı yetkilendirme karşılaştırmalı sonuçları

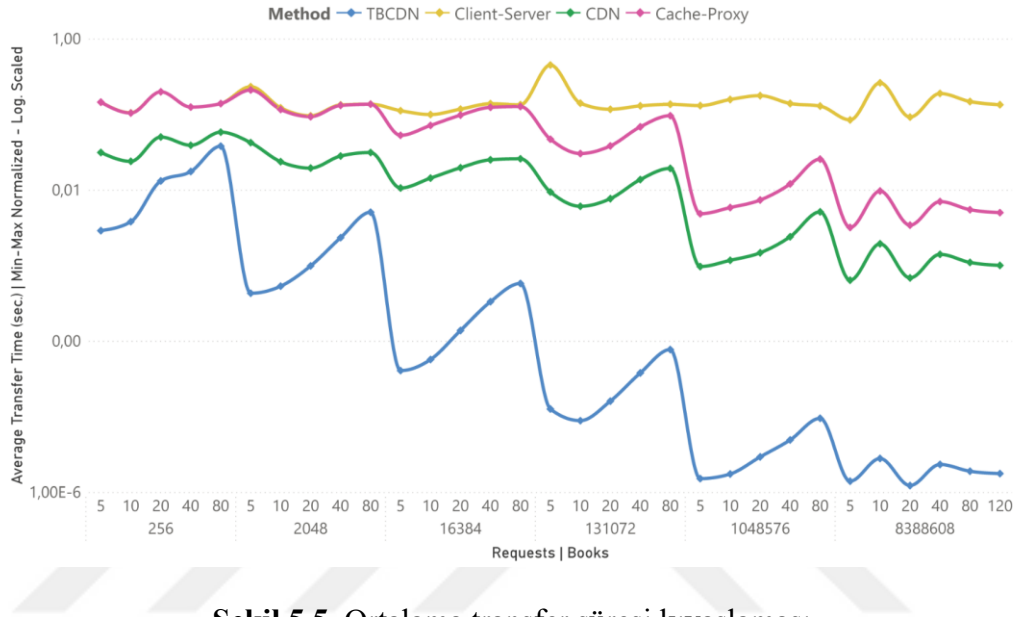
Şekil 5.4, testlerin sonuçlarını grafiksel olarak sunmaktadır. Dört farklı senaryo altında yapılan yük testleri, bit tabanlı yetkilendirme modelinin, özellikle yüksek eşzamanlılık durumlarında XML tabanlı modele göre daha düşük ortalama yanıt süreleri verdiğini göstermiştir. Örneğin, 10.000 eşzamanlı erişim isteği altında bit tabanlı yapı 25–40 ms aralığında yanıt üretirken, XML tabanlı yapı 60–90 ms arasında işlem süresi gerektirmiştir. Bu sonuç, EDU-DRM sisteminin performans optimizasyonu açısından bit tabanlı erişim yapısının daha uygun bir çözüm olduğunu ortaya koymaktadır.

Bu test sonuçları, EDU-DRM sisteminin yüksek kullanıcı yoğunluklarında dahi işlevsel kararlılığını sürdürebildiğini ve ölçeklenebilir dijital hak yönetim sistemleri için uygun bir mimari sağladığını göstermektedir. Ayrıca, alternatif yetkilendirme modellerinin performans maliyetlerinin somut verilerle karşılaştırılması, sistem tasarımı açısından kritik tercih noktalarına veri temelli dayanak oluşturmaktadır.

5.4.2. İçerik dağıtım ağı transfer süresi karşılaştırmaları

Gerçekleştirilen simülasyonlar sonucunda, dört farklı içerik dağıtım yönteminin (istemci-sunucu, cache-proxy, geleneksel CDN ve önerilen TBCDN) performansları hem içerik aktarım süresi hem de toplam ağ yükü bakımından karşılaştırılmıştır. Bulgular, sistemin ölçeklenebilirliği, verimliliği ve kaynak kullanım etkinliği açısından önemli farklar ortaya koymaktadır.

Şekil 5.5'de sunulan sonuçlara göre, istemci-sunucu yapısı artan istek hacmine karşı oldukça sınırlı bir yanıt süresi göstermektedir. İstek sayısı ve içerik çeşitliliği artsa da, merkezi sunucunun işlem kapasitesi ve ağ üzerindeki tıkanıklıklar nedeniyle aktarım süresi lineer biçimde yükselmektedir. Cache-proxy yöntemi, özellikle sık erişilen içeriklerin ara sunucular üzerinden temin edilmesi sayesinde aktarım süresinde anlamlı bir azalma sağlamaktadır; ancak içerik çeşitliliği arttıkça bu avantaj zayıflamaktadır.



Şekil 5.5. Ortalama transfer süresi kıyaslaması

Geleneksel CDN yöntemi, içerikleri coğrafi olarak dağıtarak aktarım sürelerini düşürme konusunda önemli kazanımlar sunmakta; bu yöntemle birlikte yükün farklı sunucular arasında paylaşılması gecikmeleri azaltmaktadır. Önerilen TBCDN mimarisi ise, hiyerarşik ağ yapısı ve recursive yönlendirme algoritması sayesinde, özellikle yüksek kullanıcı yoğunluklarında en düşük aktarım sürelerini sağlamaktadır. Özellikle 1 milyon ve üzeri istek seviyelerinde TBCDN'in geleneksel CDN'e göre %12 ila %21 arasında daha düşük aktarım süreleri ürettiği gözlemlenmiştir.

Şekil 5.6'de sunulan alan grafiklerine göre, istemci-sunucu yöntemi her istek için ayrı bir içerik iletimi gerçekleştirdiğinden sistemde en yüksek ağ yükünü oluşturmaktadır. Cache-proxy yöntemi, ağ yükünü azaltmakla birlikte, talep edilen içerik sayısı arttıkça önbellek etkinliği zayıfladığı için toplam veri taşınımı artmaktadır. Geleneksel CDN yöntemi bu yükü belirli ölçüde dengelemektedir, ancak yüksek içerik çeşitliliğinde merkezi sunuculara olan başvuru oranı halen yük bindirmektedir.



Şekil 5.6. Ağ Yüğü Analizi ve Karşılaştırması

TBCDN mimarisi, içeriği yerel düğümlerde tutarak ve istekleri en yakın noktada çözmeye çalışarak tüm rakip yöntemlerden daha düşük ağ yükü üretmektedir. Özellikle istek sayısının 2^{20} (yaklaşık 1 milyon) düzeyini aştığı durumlarda, uç sunucularda içerik replikalarının bulunma olasılığı çok yüksek olduğundan, veri merkezi üzerindeki yük %40'a varan oranda azalmıştır. Bu bulgular, önerilen mimarinin hem aktarım sürelerini optimize ettiğini hem de altyapı üzerindeki yükü minimize ettiğini göstermektedir.

5.4.2.1. Mini senaryo: 2^3 istek, 3 içerik

Önerilen TBCDN mimarisinin geleneksel yöntemlerle karşılaştırmalı davranışını daha somut şekilde göstermek amacıyla küçük ölçekli bir mini senaryo yürütülmüştür. Senaryoda toplam 8 kullanıcı isteği ve üç farklı içerik nesnesi (A, B, C) modellenmiştir. İstekler, dört farklı yaklaşım (sunucu–istemci, önbellek–proxy, klasik CDN ve TBCDN) altında aynı koşullarda simüle edilmiştir.

Simülasyon sırasında her bir isteğin ağ topolojisi üzerinde kat ettiği yol ve bu yol boyunca oluşan aktarım süresi adım adım izlenmiş, sonuçlar görsel olarak Şekil 5.2'de özetlenmiştir. Sunucu–istemci modelinde tüm talepler kök düğüme yönlendirilmiş ve her isteğin aynı merkezi noktadan karşılanması, yüksek tekrarlar ve gecikmeye neden olmuştur. Önbellek–proxy yaklaşımı, bazı tekrar eden içeriklerin daha alt seviyelerden karşılanmasını sağlamış olsa da, ölçek büyüdükçe düzensiz yük dağılımı ve proxy düğümlerinde yoğunlaşma gözlenmiştir. Klasik CDN mimarisinde içerikler,

istemci taleplerini karşılamak üzere en yakın düğümden sunulmaktadır. Ancak en yakın düğümler arasında doğrudan bağlantı bulunmadığında istek, bir üst seviyedeki düğüm üzerinden yönlendirilmekte ve içerik aynı seviyedeki başka bir düğümden aktarılmaktadır. Bu durum, özellikle alt seviyelerde yol uzunluğunu TBCDN'e kıyasla yaklaşık iki katına çıkarırken, üst seviyelere çıkıldıkça aradaki farkın daha da arttığı gözlemlenmektedir.

TBCDN mimarisinde ise özyinelemeli yönlendirme algoritması sayesinde istekler en yakın üst düğümlerde yanıtlanmış; böylece hem toplam kat edilen yol uzunluğu hem de uçtan uca aktarım süresi anlamlı ölçüde kısalmıştır. Mini senaryonun çıktıları, TBCDN'in özellikle tekrarlayan isteklerde 1–2 düğüm üzerinden içerik sunarak hem transfer zamanını düşürdüğünü hem de ağ yükünü dengelediğini göstermektedir. Bu sonuç, yüksek ölçekli deneylerde gözlenen kazanımların küçük ölçekte de açık biçimde doğrulandığını ortaya koymaktadır.

5.4.2.2. Gerçek hayat senaryosu: $\sim 2^{23}$ istek, $5^1 - 5^3$ içerik

Gerçekçi senaryolar, TBCDN mimarisinin ve karşılaştırmaya konu edilen alternatif içerik dağıtım yöntemlerinin (istemci–sunucu, cache–proxy, geleneksel CDN) uçtan uca aktarım süresi (Transfer Time) ve toplam ağ yükü (Network Load) açısından nasıl performans gösterdiğini sistematik biçimde değerlendirmek amacıyla kurgulanmıştır.

Deneysel veri kümesi, farklı boyut ve popülerlik derecelerine sahip dijital içeriklerden oluşturulmuş; sanal düğümler hiyerarşik bir dağıtım topolojisine yerleştirilmiştir. Her düğüm, yalnızca sınırlı bir içerik portföyüne sahip olacak biçimde yapılandırılmış; böylece sistemin bölgesel taleplere nasıl tepki verdiği gözlemlenebilmiştir.

Kullanıcı istekleri, sistemin ölçeklenebilirlik limitlerini gözlemlemek amacıyla logaritmik olarak artan değerlerde yapılandırılmıştır. Başlangıçta 28 adet olan istek sayısı, her aşamada iki katına çıkarılarak 2^{23} 'e (8.388.608 istek) kadar artırılmıştır. İçerik çeşitliliği sağlanırken dosya boyutları, 4 MB ile 90 MB arasında değişen boyutlarda olup; 5, 10, 20, 40, 80 ve 120 farklı nesne düzeyinde sınanmıştır. Bu yapı, hem düşük çeşitlilik–yüksek yoğunluk hem de yüksek çeşitlilik–düşük yoğunluk senaryolarını değerlendirmeyi mümkün kılmıştır.

Her yöntem için parametreler optimize edilmiş, istekler tekrarlanabilir koşullar altında TBNS üzerinde yürütülmüştür. Ölçümler yalnızca transfer süresi ve ağ trafik yükü metrikleri üzerinden raporlanmıştır.

Transfer süresi, istemci ile en yakın içerik kaynağı arasındaki uçtan uca gecikmeyi göstermektedir. Bu metrik, özellikle özyinelemeli yönlendirme yaklaşımının gecikme üzerindeki etkisini sayısal olarak ortaya koymaktadır.

Ağ trafik yükü, talebin karşılanması için ağ üzerinde üretilen toplam trafik miktarını temsil etmektedir. Bu metrik ise mimarilerin bant genişliği verimliliğini ve ağ kaynaklarının kullanımındaki etkinliğini karşılaştırmalı biçimde ortaya koymaktadır.



6. SONUÇLAR VE ÖNERİLER

Bu çalışmada, dijital hak yönetimi (DRM) ve içerik dağıtım ağları (CDN) alanındaki temel sorunlar bütüncül bir bakış açısıyla ele alınmış ve hem güvenlik hem de ölçeklenebilirliği eşzamanlı olarak hedefleyen özgün bir mimari önerilmiştir. Geliştirilen EDU-DRM ve ağaç tabanlı CDN (TBCDN) bileşenlerinin bütünleşik yapısı, bir yandan içeriklere yalnızca yetkilendirilmiş kullanıcıların erişmesini garanti ederken, diğer yandan yoğun trafik altında bile düşük gecikme ve kontrollü ağ yükü sağlamaktadır. Böylece tez, hem akademik literatüre teorik katkılar sunmakta hem de gerçek dünyada uygulanabilir nitelikte pratik bir çözüm önermektedir.

EDU-DRM tarafında geliştirilen bit tabanlı erişim vektörleri, yetkilendirme kararlarını sabit zamanda gerçekleştirebilmekte; bu özellik XML tabanlı geleneksel yöntemlere kıyasla işlem maliyetini kayda değer ölçüde azaltmaktadır. Deneysel sonuçlar, XML tabanlı lisanslama senaryolarına göre %40'a varan gecikme azalımı sağlandığını ve CPU kullanımında belirgin bir düşüş elde edildiğini göstermektedir. Bu durum, büyük ölçekli kullanıcı tabanına sahip ortamlarda sistemin yanıt verebilirliğini doğrudan artırmaktadır.

TBCDN tarafında ise, klasik CDN ve önbellek-proxy mimarilerine kıyasla çok daha düşük toplam uçtan uca gecikme değerleri elde edilmiştir. Tezde önerilen özyinelemeli istek yönlendirme algoritması, tekrarlayan içerik isteklerinin yalnızca 1–2 düğüm üzerinden karşılanmasını sağlamış; bu da geleneksel CDN mimarilerinde gözlemlenen 3–6 düğümlük yol uzunluklarına göre belirgin bir avantaj yaratmıştır. Deneysel sonuçlar, ortalama transfer süresinde %25–35 oranında azalma sağlandığını; aynı zamanda ağ yükünün eşit dağıtılması sayesinde toplam trafik hacminin %40'a kadar azaldığını ortaya koymuştur. Böylece TBCDN, yalnızca içerik iletimini hızlandırmakla kalmamış; aynı zamanda ağ trafik yükü optimizasyonu açısından da en dengeli ve verimli yaklaşım olduğunu kanıtlamıştır.

Gerçekleştirilen karşılaştırmalı testlerde dört farklı yöntem (sunucu–istemci, cache–proxy, klasik CDN ve önerilen TBCDN) değerlendirilmiştir. Sunucu–istemci modeli, düşük ölçekli isteklerde kabul edilebilir performans göstermiş, ancak eşzamanlı

kullanıcı sayısı arttığında hem gecikme hem de ağ yükü bakımından ciddi darboğazlar üretmiştir. Cache-proxy yaklaşımı, tekrarlayan isteklerde belirli kazançlar sağlamakla birlikte, ölçek büyüdükçe yönetimsel karmaşıklık ve eşit olmayan yük dağılımı nedeniyle etkinliğini yitirmiştir. Klasik CDN mimarisi, yükü dağıtmakta başarılı olsa da içeriklerin yetkilendirme-lisanslama süreçlerinden bağımsız kopyalanabilmesi, güvenlik ve bütünlük açısından zafiyet yaratmıştır. Buna karşılık önerilen TBCDN mimarisi hem ağ yükünü dengelemiş hem de en düşük uçtan uca gecikmeyi sağlamıştır. Özellikle 8 milyona yakın isteğin işlendiği yüksek yoğunluklu senaryolarda dahi istikrarlı performans göstermesi, mimarinin ölçeklenebilirliğini açıkça ortaya koymuştur.

Bu tezde öne çıkan katkılar arasında, bit tabanlı yetkilendirme modeli ile sabit zamanda, düşük maliyetli ve denetlenebilir erişim kontrolünün sağlanması yer almaktadır. Ayrıca, süreye bağlı kısıtların ötesine geçerek kullanıcı-içerik bağımlı sistemsel ve kalıcı bir ilişki ile güvence altına alan statüye dayalı lisanslama yaklaşımı önemli bir yenilik sunmaktadır. Bunun yanında, TBCDN yönlendirme algoritması, hiyerarşik topolojilerde toplam gecikmeyi minimize eden yapısal bir çözüm olarak geleneksel yöntemlere kıyasla hem hız hem de kaynak kullanımı açısından üstünlük sağlamıştır. Son olarak, EDU-DRM ve TBCDN'in ayrıştırılmış fakat bütünleşik tasarımı sayesinde güvenlik, ölçeklenebilirlik ve performans dengesi aynı anda gözetilmiş ve bütüncül bir çözüm ortaya konulmuştur.

Bununla birlikte, çalışmanın bazı sınırlılıkları da bulunmaktadır. Deneysel testler belirli donanım ve yazılım konfigürasyonlarıyla yürütülmüştür; donanım hızlandırmalı kriptografi ya da farklı ağ altyapılarında farklı sonuçlar elde edilebilir. Ayrıca simülasyonlar, Poisson tabanlı trafik modelleri ve Zipf dağılımlı içerik popülerliği üzerinden yürütülmüş olup, gerçek dünyada farklı kullanıcı davranışları altında ek testlere ihtiyaç vardır.

İlerleyen çalışmalarda, TBCDN mimarisine yapay zekâ tabanlı adaptif önbellekleme ve yönlendirme algoritmalarının entegre edilmesi, performansın daha da iyileştirilmesine katkı sağlayabilir. DRM tarafında ise blockchain tabanlı lisanslama, sıfır bilgi ispatları ve homomorfik şifreleme gibi yenilikçi yaklaşımların eklenmesi, güvenlik ve denetlenebilirliği artırabilir. Ayrıca farklı coğrafi bölgelerde yapılacak saha testleri, sistemin ölçeklenebilirliğini ve ağ çeşitliliği altındaki davranışını ortaya koyacaktır.

Bu tez dijital hak yönetimi ve içerik dağıtım ağlarını bütünleşik biçimde ele alan, teorik temeli güçlü ve deneysel olarak doğrulanmış özgün bir mimari ortaya koymuştur. EDU-DRM ve TBCDN birleşimi, içerik güvenliği ile performansı aynı potada eriterek hem akademik literatürde hem de pratik uygulamalarda kullanılabilecek stratejik bir çözüm sunmaktadır.





KAYNAKLAR

- Adhikari, V., S. Jain, and Y. Chen. 2012. "Vivisecting Youtube: An Active Measurement Study." <https://doi.org/10.1109/incom.2012.6195644>.
- Ahvar, S., J. Sahoo, E. Ahvar, M. Dieye, R. Glitho, H. Elbiaze, and N. Crespi. 2018. "Pcpv: Pattern-Based Cost-Efficient Proactive Vnf Placement and Chaining for Value-Added Services in Content Delivery Networks." <https://doi.org/10.1109/netsoft.2018.8459986>.
- Alghamdi, F., S. Mahfoudh, and A. Barnawi. 2019. "A Novel Fog Computing Based Architecture to Improve the Performance in Content Delivery Networks." *Wireless Communications and Mobile Computing* 2019: 1–13. <https://doi.org/10.1155/2019/7864094>.
- Ali, W., Fang, C., & Khan, A. (2025). A survey on the state-of-the-art CDN architectures and future directions. *Journal of Network and Computer Applications*, 236, 104106. <https://doi.org/10.1016/j.jnca.2025.104106>
- Amoozegar, M., & Nezamabadi-pour, H. (2015). A multiobjective approach to model-driven performance bottlenecks mitigation. *Scientia Iranica*, 22(3), 1018–1030.
- Arrufat, M., Torres-Hernández, N., & Pessôa, T. (2019). Competence of future teachers in the digital security area. *Comunicar*, 27(61), 57–67. <https://doi.org/10.3916/C61-2019-05>
- Arrufat, M., Torres-Hernández, N., & Pessôa, T. (2021). Competence of future teachers in the digital security area. *OSF Preprints*. <https://doi.org/10.31219/osf.io/hgxwn>
- Arumaithurai, M., Seedorf, J., Paragliela, G., Pilarski, M., & Niccolini, S. (2013). Evaluation of alto-enhanced request routing for cdn interconnection.. <https://doi.org/10.1109/icc.2013.6655096>
- Austerberry, D. (2012). *Digital asset management* (2nd ed., pp. 283–306). Taylor & Francis.
- Balachandran, A., V. Sekar, A. Akella, and S. Seshan. 2013. "Analyzing the Potential Benefits of Cdn Augmentation Strategies for Internet Video Workloads." <https://doi.org/10.1145/2504730.2504743>.
- Barakova, A., Ussatova, O., Zhubankuzova, I., Nurbekova, A., & Момбеков, С. (2024). Development and study of content protection models for online courses. *E-Learning and Digital Media*, 22(3), 247–262. <https://doi.org/10.1177/20427530241239410>
- Barbir, A., Cain, B., G.Nair, R., & Spatscheck, O. (2003). Known content network (cn) request-routing mechanisms.. <https://doi.org/10.17487/rfc3568>
- Becker, E., Buhse, W., Gunnewig, D., & Rump, N. (2003). *Digital rights management: Technological, economic, legal and political aspects*. Springer.

- Bhardwaj, S., Harit, S., & Verma, S. (2025). There is mathematics for that!: A formal verification of privacy and simulative analysis of consumer centric content delivery in IoT. *Transactions on Emerging Telecommunications Technologies*, 36(2). <https://doi.org/10.1002/ett.70059>
- Bhardwaj, S., Harit, S., & Yadav, A. (2024). Towards a software-defined networking model for consumer-centric content delivery network for IoT. **Transactions on Emerging Telecommunications Technologies**, *35*(1). <https://doi.org/10.1002/ett.4903>
- Bhatt, S., Sion, R., & Carbutar, B. (2009). A personal mobile DRM manager for smartphones. *Computers & Security*, 28(6), 327–340.
- Boriboon, A. & Pongpadpinit, S. (2016). Optimized routing protocol for broadband hybrid satellite constellation communication IP network system. *EURASIP Journal on Wireless Communications and Networking*, 2016(1). <https://doi.org/10.1186/s13638-016-0616-2>
- Boros, T., Bencel, R., & Kotuliak, I. (2019). Transparent redirections in content delivery networks. *Applied Sciences*, 9(24), 5418. <https://doi.org/10.3390/app9245418>
- Brummer, A., German, R., & Djanatliev, A. (2023). Methodology and performance assessment of three-dimensional vehicular ad-hoc network simulation. *IEEE Access*, 11, 36349–36364. <https://doi.org/10.1109/ACCESS.2023.3264668>
- Burnett, I., Davis, S., & Drury, G. (2005). MPEG-21 digital item declaration and identification principles and compression. *IEEE Transactions on Multimedia*, 7(3), 400–407.
- Carbutaru, C., Teo, Y., & Leong, B. (2011). A performance study of peer-assisted file distribution with heterogeneous swarms. In *Proceedings of the 36th IEEE Conference on Local Computer Networks* (pp. 568–575). <https://doi.org/10.1109/lcn.2011.6115314>
- Chakraborty, D., Rabbi, M., Hossain, M., Khaled, S., Oishi, M., & Alam, M. (2022). Deep learning based predictive analytics for decentralized content caching in hierarchical edge networks. In *Proceedings of the International Conference on Computational Intelligence and Data Science* (pp. 113–121). https://doi.org/10.1007/978-3-031-21753-1_12
- Chang, C. C., Chang, S. C., & Yang, J. H. (2013). A practical secure and efficient enterprise digital rights management mechanism suitable for mobile environment. *Security and Communication Networks*, 6(8), 972–984.
- Chang, C. C., Yang, J. H., & Wang, D. W. (2010). An efficient and reliable e-DRM scheme for mobile environments. *Expert Systems with Applications*, 37(9), 6176–6181.
- Chen, C. L. (2008). A secure and traceable e-DRM system based on mobile device. *Expert Systems with Applications*, 35(3), 878–886.
- Chen, S. 2015. “A Survey on Security in Named Data Networking.” <https://doi.org/10.48550/arxiv.1512.04127>.
- Chen, S., and Z. Li. 2022. “An Evolutionary Framework for Server Placement Optimization of Large-Scale Online Media Services System.” <https://doi.org/10.21203/rs.3.rs-446639/v1>.

- Choi, J., Aiken, W., Ryoo, J., & Kim, H. (2016). Bypassing the integrity checking of rights objects in OMA DRM. In *Proceedings of the 21st ACM Symposium on Access Control Models and Technologies* (pp. 133–136). <https://doi.org/10.1145/2857546.2857609>
- Cicalese, D., Giordano, D., Finamore, A., Mellia, M., Munafò, M., Rossi, D., ... & Jounblatt, D. (2015). A first look at anycast cdn traffic.. <https://doi.org/10.48550/arxiv.1505.00946>
- Contreras, L. M., Solano, A., Cano, F., & Folgueira, J. (2023). Analysis of network function sharing in Content Delivery Network-as-a-service slicing scenarios. **International Journal of Network Management**, *33*(4). <https://doi.org/10.1002/nem.2221>
- Dadsena, P. K., Jain, J., Rana, S., & Dharminder, D. (2023). A construction of post quantum secure authenticated key agreement design for mobile digital rights management system. **Multimedia Tools and Applications*, 82*(17), 26643–26660. <https://doi.org/10.1007/s11042-023-14937-6>
- Das, A. K., Mishra, D., & Mukhopadhyay, S. (2015). An anonymous and secure biometric-based enterprise digital rights management system for mobile environment. *Security and Communication Networks*, 8(18), 3383–3404.
- Delgado, J., Dias, M. S., & Serrao, C. (2005). Using webservices to manage and control access to multimedia content. In *Proceedings of The International Symposium on Web Services and Applications* (pp. 23–28). Las Vegas, Nevada, USA.
- Delgado, J., Torres, V., Llorente, S., & Rodriguez, E. (2011). Rights management in architectures for distributed multimedia content applications. In *Trustworthy Internet* (pp. 335–347).
- Dervisevic, E., Voznak, M., & Mehic, M. (2024). Large-scale quantum key distribution network simulator. *Journal of Optical Communications and Networking*, 16(4), 449–462. <https://doi.org/10.1364/JOCN.503356>
- Deti, A., Pomposini, M., Blefari-Melazzi, N., & Salsano, S. (2012). Supporting the web with an information centric network that routes by name. *Computer Networks*, 56(17), 3705–3722. <https://doi.org/10.1016/j.comnet.2012.08.006>
- Dharmapal, P. 2023. “A Novel Cost-Based Replica Server Placement for Optimal Service Quality in Cloud-Based Content Delivery Network.” *International Journal of Electrical and Computer Engineering (Ijece)* 13: 5588. <https://doi.org/10.11591/ijece.v13i5.pp5588-5598>.
- Dieye, M., S. Ahvar, J. Sahoo, E. Ahvar, R. Glitho, H. Elbiaze, and N. Crespi. 2018. “Cpvnf: Cost-Efficient Proactive Vnf Placement and Chaining for Value-Added Services in Content Delivery Networks.” *Ieee Transactions on Network and Service Management* 15: 774–86. <https://doi.org/10.1109/tnsm.2018.2815986>.
- Elkhameesy, N., and H. Mohamed. 2013. “A Proposed Model for Web Proxy Caching Techniques to Improve Computer Networks Performance.” *International Journal of Information Technology and Computer Science* 5: 42–53. <https://doi.org/10.5815/ijitcs.2013.11.05>.

- Famaey, J., F. Iterbeke, T. Wauters, and F. Turck. 2013. "Towards a Predictive Cache Replacement Strategy for Multimedia Content." *Journal of Network and Computer Applications* 36: 219–27. <https://doi.org/10.1016/j.jnca.2012.08.014>.
- Famaey, J., T. Wauters, and F. Turck. 2011. "On the Merits of Popularity Prediction in Multimedia Content Caching," 17–24. <https://doi.org/10.1109/inm.2011.5990669>.
- Fan, Q., Chen, J. H., Wen, Y. H., & Luo, M. (2022). Eland: An efficient lightweight anonymous authentication protocol applied to digital rights management system. **Journal of Internet Technology*, 23*(2), 267–278. <https://doi.org/10.53106/160792642022032302007>
- Fan, Q., H. Yin, G. Min, P. Yang, Y. Luo, Y. Lyu, H. Huang, and L. Jiao. 2018. "Video Delivery Networks: Challenges, Solutions and Future Directions." *Computers & Electrical Engineering* 66: 332–41. <https://doi.org/10.1016/j.compeleceng.2017.04.011>.
- Farahani, R., Çetinkaya, E., Timmerer, C., Shojafar, M., Ghanbari, M., & Hellwagner, H. (2024). ALIVE: A latency- and cost-aware hybrid P2P-CDN framework for live video streaming. **IEEE Transactions on Network and Service Management**, 21*(2), 1561–1580. <https://doi.org/10.1109/TNSM.2023.3335190>
- Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R., Cavallaro, A., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. **Blockchain: Research and Applications*, 4*(3), 100142. <https://doi.org/10.1016/j.bcra.2023.100142>
- Fortino, G., & Mastroianni, C. (2009). Special section: Content management and delivery through P2P-based content networks. *Multiagent and Grid Systems*, 5(2), 133–135. <https://doi.org/10.3233/mgs-2009-0123>
- Frangoudis, P., L. Yala, and A. Ksentini. 2017. "Cdn-as-a-Service Provision over a Telecom Operator's Cloud." *Ieee Transactions on Network and Service Management* 14: 702–16. <https://doi.org/10.1109/tnsm.2017.2710300>.
- Frattolillo, F. (2023). Watermarking protocols: A short guide for beginners. **Future Internet*, 15*(5), 163. <https://doi.org/10.3390/fi15050163>
- Frattolillo, F. (2024). Blockchain and smart contracts for digital copyright protection. **Future Internet*, 16*(5), 169. <https://doi.org/10.3390/fi16050169>
- Gao, Y. A., Yang, S., Li, F., Trajanovski, S., Zhou, P., Hui, P., & Fu, X. M. (2023). Video content placement at the network edge: Centralized and distributed algorithms. **IEEE Transactions on Mobile Computing**, 22*(11), 6843–6859. <https://doi.org/10.1109/TMC.2022.3200401>
- Garmehi, M. and Analoui, M. (2015). Envy-free resource allocation and request routing in hybrid cdn-p2p networks. *Journal of Network and Systems Management*, 24(4), 884–915. <https://doi.org/10.1007/s10922-015-9359-3>
- Garmehi, M., Analoui, M., Pathan, M., & Buyya, R. (2015). An economic mechanism for request routing and resource allocation in hybrid cdn-p2p networks. *International Journal of Network Management*, 25(6), 375–393. <https://doi.org/10.1002/nem.1891>

- Gebeyew, A., Regasa, Z., Muluneh, A., Shibabaw, A., Walle, A., Tizie, S., ... Butta, F. (2024). Attitudes of health professionals toward digital health data security in northwest Ethiopia: Cross-sectional study. *Online Journal of Public Health Informatics*, 16, e57764. <https://doi.org/10.2196/57764>
- Gettys, J. & Nichols, K. (2011). Bufferbloat: Dark buffers in the Internet. *Queue*, 9(11), 40–54. <https://doi.org/10.1145/2063166.2071893>
- Ghareeb, M., S. Rouibia, B. Parrein, M. Raad, and C. Thareau. 2013. “P2pweb: A Client/Server and P2p Hybrid Architecture for Content Delivery over Internet.” <https://doi.org/10.1109/iccitechnology.2013.6579542>.
- Ghorbel, A., M. Kobayashi, and S. Yang. 2016. “Content Delivery in Erasure Broadcast Channels with Cache and Feedback.” <https://doi.org/10.1109/isit.2016.7541416>.
- Giura, P., and G. Reyes. 2011. “The Security Cost of Content Distribution Network Architectures.” <https://doi.org/10.1109/compsacw.2011.31>.
- Goudarzi, P. and Mousavinejad, M. (2019). A lyapunov optimization approach to energy-efficient content delivery networks. *Simulation*, 96(3), 269-280. <https://doi.org/10.1177/0037549719862023>
- Grégoire, J., and A. Hamel. 2014. “On Scheduling Live Media Streaming in the Cloud — a Study,” 1–6. <https://doi.org/10.1109/wowmom.2014.6919000>.
- Giuliano, L., Lenart, C. & Adam, R. (2025, Ocak). TreeDN: Tree-based content delivery network (CDN) for live streaming to mass audiences (RFC 9706). Internet Engineering Task Force. <https://doi.org/10.17487/RFC9706>
- Guo, R., W. Li, B. Liu, S. Hao, Z. Jia, H. Duan, K. Sheng, J. Chen, and Y. Liu. 2020. “Cdn Judo: Breaking the Cdn Dos Protection with Itself.” <https://doi.org/10.14722/ndss.2020.24411>.
- Gupta, M., and A. Garg. 2015. “A Comparative Analysis of Content Delivery Network and Other Techniques for Web Content Delivery.” *International Journal of Service Science Management Engineering and Technology* 6: 43–58. <https://doi.org/10.4018/ijssmet.2015100104>.
- Han, L., & Liu, M. (2024). Digital rights management (DRM) technologies and legal research: Applications and regulations of encryption, digital watermarking, and copyright protection systems. *Applied and Computational Engineering*, 82(1), 106–111. <https://doi.org/10.54254/2755-2721/82/20240957>
- Henderson, T. R., Ahn, G.-S., Brian, L., Lim, Y. S., Ryu, K.-H., Jacobson, V., ve ark. (2018). The ns-3 network simulator. In *Proceedings of the 43rd IEEE Conference on Local Computer Networks (LCN)* (ss. 695–703).
- Henderson, T. R., Lacage, M., Riley, G. F., Dowell, C., & Kopena, J. (2008). Network simulations with the ns-3 simulator. *SIGCOMM Demonstration*, 14(14), 527.
- Herbaut, N., D. Negru, P. Frangoudis, and A. Ksentini. 2016. “Content Delivery Networks as a Virtual Network Function: A Win-Win Isp-Cdn Collaboration,” 1–6. <https://doi.org/10.1109/glocom.2016.7841689>.

- Heverin, T., Lilholt, A., & Woodward, E. (2024). Evaluating cybersecurity class activities based on the cognitive continuum theory: An exploratory case study. *Proceedings of the European Conference on Cyber Warfare and Security*, 23(1), 205–213. <https://doi.org/10.34190/eccws.23.1.2371>
- Hosanagar, K., Han, P., & Tan, Y. (2010). Diffusion models for peer-to-peer (P2P) media distribution: On the impact of decentralized, constrained supply. *Information Systems Research*, 21(2), 271–287. <https://doi.org/10.1287/isre.1080.0221>
- Hussain, S., Bin Zikria, Y., Mallah, G. A., Chen, C. M., Alshehri, M. D., Ishmanov, F., & Chaudhry, S. A. (2022). An improved authentication scheme for digital rights management system. **Wireless Communications & Mobile Computing*, 2022*, 1041880. <https://doi.org/10.1155/2022/1041880>
- Iannella, R. (2004). The Open Digital Rights Language: XML for digital rights management. *Information Security Technical Report*, 9(3), 47–55.
- IETF/GEANT. (2025, April 11). TreeDN discussion [Zoom meeting].
- International Organization for Standardization. (2004). Information technology—Multimedia framework (MPEG-21) Part 5: Rights Expression Language (ISO/IEC 21000-5). Geneva, Switzerland.
- Irwin, J. (2004). Digital rights management: The Open Mobile Alliance DRM specifications. *Information Security Technical Report*, 9(4), 22–31.
- Jedari, B., and M. Francesco. 2018. “Delay Analysis of Layered Video Caching in Crowdsourced Heterogeneous Wireless Networks.” <https://doi.org/10.1109/glocom.2018.8647205>.
- Jiang, W. W., Han, H. Y., He, M., & Gu, W. X. (2024). Network simulation tools for unmanned aerial vehicle communications: A survey. *International Journal of Communication Systems*, 37(15). <https://doi.org/10.1002/dac.5878>
- Jimoh, R. G., Awotunde, J. B., Ogundokun, R. O., & Adeoti, D. S. (2024). A randomized encryption algorithm for the MPEG-DASH digital rights management. **Information Security Journal*, 33*(5), 473–485. <https://doi.org/10.1080/19393555.2024.2334764>
- Jin, Y., Y. Wen, and W. Zhang. 2014. “Content Routing and Lookup Schemes Using Global Bloom Filter for Content-Delivery-as-a-Service.” *Ieee Systems Journal* 8: 268–78. <https://doi.org/10.1109/jsyst.2013.2253041>.
- Kabir, M. H., Islam, S., Hossain, M. J., & Hossain, S. (2014). Detail comparison of network simulators. *International Journal of Scientific & Engineering Research*, 5(10), 203–218.
- Kalker, T., Carey, K., Lacy, J., & Rosner, M. (2007). The Coral DRM interoperability framework. In *Consumer Communications and Networking Conference* (pp. 930–934). Las Vegas, NV, USA.
- Karaata, M., A. Almutairi, and S. Alsubaihi. 2022. “Multipath Routing over Star Overlays for Quality of Service Enhancement in Hybrid Content Distribution Peer-to-Peer Networks.” *Ieee Access* 10: 7042–58. <https://doi.org/10.1109/access.2021.3139936>.

- Karpouzis, K., Maglogiannis, I., Papaioannou, E., Vergados, D., & Rouskas, A. (2007). MPEG-21 digital items to support integration of heterogeneous multimedia content. *Computer Communications*, 30(3), 592–607.
- Ke, C. K., & Lin, Z. H. (2015). An approach for secure data exchange: Experiments on Android-based mobile device. *Scientia Iranica*, 22(4), 1586–1593.
- Khan, K. 2023. “The Protocol Play: Dashing Ahead or Hlsing Back?” *International Journal for Multidisciplinary Research* 5. <https://doi.org/10.36948/ijfmr.2023.v05i06.11176>.
- Khansoltani, A., Jamali, S., & Fotohi, R. (2022). A request redirection algorithm in content delivery network: Using PROMETHEE approach. **Wireless Personal Communications**, *126*(2), 1145–1175. <https://doi.org/10.1007/s11277-022-09786-9>
- Khare, V. and Zhang, B. (2011). Making cdn and isp routings symbiotic.. <https://doi.org/10.1109/icdcs.2011.89>
- KhudaBukhsh, W. 2018. “A Comprehensive Analysis of Swarming-Based Live Streaming to Leverage Client Heterogeneity.” <https://doi.org/10.48550/arxiv.1812.11439>.
- Kim, J., Lee, G., & Choi, J. (2014). Popularity-based adaptive content delivery scheme with in-network caching. *Etri Journal*, 36(5), 819-828. <https://doi.org/10.4218/etrij.14.0113.0090>
- Koenen, R. (2001). Intellectual property management and protection in MPEG standards. In *Workshop on Digital Rights Management for the Web* (pp. 22–23). Sophia Antipolis, France.
- Kovvali, S., and C. Boyle. 2014. “Ran-Aware Content Delivery, Proxy Optimizations, and Offload in Cellular Wireless Networks.” <https://doi.org/10.1109/latincom.2014.7041874>.
- Krishanmoorthy, S., Wei, Z., Zhang, Y., Jin, H., & Dong, H. (2020). A study on optimization of network latency and packet loss rate. *IOP Conference Series: Materials Science and Engineering*, 937(1), 012054. <https://doi.org/10.1088/1757-899x/937/1/012054>
- Krishnan, S., and R. Sitaraman. 2013. “Video Stream Quality Impacts Viewer Behavior: Inferring Causality Using Quasi-Experimental Designs.” *Ieee/Acm Transactions on Networking* 21: 2001–14. <https://doi.org/10.1109/tnet.2013.2281542>.
- Kubaszek, M., Macheta, J., Krzak, L., & Worek, C. (2024). Bit-exact simulation of 6TiSCH networks. *International Journal of Electronics and Telecommunications*, 70(4), 1071–1079. <https://doi.org/10.24425/ijet.2024.152362>
- Kubesch, A., & Wicker, S. (2015). Digital rights management: The cost to consumers [Point of View]. *Proceedings of the IEEE*, 103(5), 726–733. <https://doi.org/10.1109/JPROC.2015.2418457>
- Kumar, A., Banerjee, S., Jain, R., & Pandey, M. (2022). Software-defined content delivery network at the edge for adaptive video streaming. **International Journal of Network Management**, *32*(6), e2210. <https://doi.org/10.1002/nem.2210>

- Kumar, M., & Professor, S. (2023). Peer-to-peer networking for content distribution and sharing. *Turkish Online Journal of Qualitative Inquiry*, 11(4), 10022. <https://doi.org/10.52783/tojq.v11i4.10022>
- Kumari, M. R. R., Kumar, V. V., & Naidu, K. R. (2023). Digital image watermarking using DWT-SVD with enhanced tunicate swarm optimization algorithm. **Multimedia Tools and Applications*, 82*(18), 28259–28279. <https://doi.org/10.1007/s11042-023-14618-4>
- Kuo, W., and Y. Lin. 2016. “Resource-Saving File Management Scheme for Online Video Provisioning on Content Delivery Networks.” *Ieee Transactions on Computers* 65: 1910–20. <https://doi.org/10.1109/tc.2015.2456018>.
- Kurose, J. F., & Ross, K. W. (2017). *Computer networking: A top-down approach* (6. baskı, ss. 65–69). Addison-Wesley.
- La, H.-L., Tran, A.-T. N., Yoshimi, M., Nakajima, T., & Thoai, N. (2021). CDNet: A content delivery network emulator. In *2021 International Symposium on Networks Computers and Communications (ISNCC)* (ss. 1–7).
- Lei, L., L. You, G. Dai, T. Vu, D. Yuan, and S. Chatzinotas. 2017. “A Deep Learning Approach for Optimizing Content Delivering in Cache-Enabled Hetnet.” <https://doi.org/10.1109/iswcs.2017.8108157>.
- Li, G., Yuchi, J., Yang, H., & Li, K. (2019). A network delay factor model based on the hidden Markov model and latent Dirichlet allocation. *IEEE Access*, 7, 133136–133144. <https://doi.org/10.1109/access.2019.2940636>
- Li, J. S., Hsieh, C. J., & Hung, C. F. (2010). A novel DRM framework for peer-to-peer music content delivery. *Journal of Systems and Software*, 83(10), 1689–1700.
- Li, Z., and G. Simon. 2013. “In a Telco-Cdn, Pushing Content Makes Sense.” *Ieee Transactions on Network and Service Management* 10: 300–311. <https://doi.org/10.1109/tnsm.2013.043013.130474>.
- Liu, J. (2008). A primer for real-time simulation of large-scale networks. In *41st Annual Simulation Symposium (ANSS-41 2008)* (ss. 85–94).
- Liu, J. Y., Yao, W. B., Wang, C., & Yang, Q. H. (2023). Provisioning network slice for mobile content delivery in uncertain MEC environment. **Computer Networks**, *224*, 109629. <https://doi.org/10.1016/j.comnet.2023.109629>
- Liu, J., Wang, D. C., Hu, Y. P., Chen, J., & Wang, B. C. (2023). Improved integral cryptanalysis of SPNbox in digital rights management systems. **IET Information Security*, 17*(1), 147–158. <https://doi.org/10.1049/ise2.12087>
- Liu, K., Wu, K., Wang, H., Zhou, K., Wang, P., Zhang, J., & Li, C. (2024). SLAP: Segmented reuse-time-label based admission policy for content delivery network caching. **ACM Transactions on Architecture and Code Optimization**, *21*(2), 32. <https://doi.org/10.1145/3646550>
- Liu, Y., D. Lu, G. Zhang, J. Tian, and W. Xu. 2019. “Q-Learning Based Content Placement Method for Dynamic Cloud Content Delivery Networks.” *Ieee Access* 7: 66384–94. <https://doi.org/10.1109/access.2019.2917564>.
- Lopez-Fuentes, F. 2012. “Performance Comparison of Peer-to-Peer Content Distribution Schemes,” 88–93. <https://doi.org/10.1109/bwcca.2012.24>.

- Ma, G., Z. Wang, M. Zhang, J. Ye, M. Chen, and W. Zhu. 2017. "Understanding Performance of Edge Content Caching for Mobile Video Streaming." *Ieee Journal on Selected Areas in Communications* 35: 1076–89. <https://doi.org/10.1109/jsac.2017.2680958>.
- Macedo, R., Paulo, J., Pereira, J., & Bessani, A. (2020). A survey and classification of software-defined storage systems. *ACM Computing Surveys*, 53(3), 1–38. <https://doi.org/10.1145/3385896>
- Maddah-Ali, M., and U. Niesen. 2015. "Decentralized Coded Caching Attains Order-Optimal Memory-Rate Tradeoff." *Ieee/Acm Transactions on Networking* 23: 1029–40. <https://doi.org/10.1109/tnet.2014.2317316>.
- Maillé, P., G. Simon, and B. Tuffin. 2015. "Impact of Revenue-Driven Cdn on the Competition Among Network Operators," 163–67. <https://doi.org/10.1109/cnsm.2015.7367353>.
- Makhkamov, B. 2023. "A Survey of Cache Placement Algorithms in Content Delivery Networks." *E3s Web of Conferences* 458: 09004. <https://doi.org/10.1051/e3sconf/202345809004>.
- Mandal, U., C. Lange, A. Gladisch, P. Chowdhury, and B. Mukherjee. 2011. "Energy-Efficient Content Distribution over Telecom Network Infrastructure." <https://doi.org/10.1109/ictn.2011.5971047>.
- Mangili, M., F. Martignon, and A. Capone. 2014. "Stochastic Planning for Content Delivery: Unveiling the Benefits of Network Functions Virtualization." <https://doi.org/10.1109/icnp.2014.56>.
- McCanne, S. (1997). The LBNL network simulator. Erişim adresi: <http://www-mash.cs.berkeley.edu/ns/>
- Medina, M., & Tnibar-Harrus, C. (2023). Digital security in educational training programs: A study based on future teachers' perceptions. *Information Technologies and Learning Tools*, 95(3), 102–111. <https://doi.org/10.33407/itlt.v95i3.5204>
- Michiels, S., Joosen, W., Truyen, E., & Verslype, K. (2005). Digital rights management: A survey of existing technologies (Report CW 428). K. U. Leuven, Department of Computer Science.
- Mishra, A., Obaidat, M. S., & Mishra, D. (2024). Privacy preserving content distribution framework for multi-distributor DRM systems. **Security and Privacy*, 7*(1). <https://doi.org/10.1002/spy2.327>
- Mittal, S. (2012). Opnet: An integrated design paradigm for simulations. *Software Engineering: An International Journal*, 2(2), 57–67.
- Mittal, S. (2012). Opnet: An integrated design paradigm for simulations. *Software Engineering: An International Journal*, 2(2), 57–67.
- Miura, H. and Yamamoto, M. Evaluation of integration effect of content location and request routing in content distribution networks., 88-100. https://doi.org/10.1007/978-3-540-71500-9_7

- Monsao, A., S. Corrêa, A. Viana, and K. Cardoso. 2022. "Combining Resource-Aware Recommendation and Caching in the Era of Mec for Improving the Experience of Video Streaming Users." *Ieee Transactions on Services Computing*, 1–14. <https://doi.org/10.1109/tsc.2022.3205482>.
- Musa, A., & Awan, I. (2022). Functional and performance analysis of discrete event network simulation tools. *Simulation Modelling Practice and Theory*, 116, 102470.
- Nam, H., K. Kim, D. Calin, and H. Schulzrinne. 2014. "Towards Dynamic Network Condition-Aware Video Server Selection Algorithms over Wireless Networks." <https://doi.org/10.1109/iscc.2014.6912523>.
- Nayak, R. P., Sethi, S., Bhoi, S. K., Sahoo, K. S., & Nayyar, A. (2023). ML-MDS: Machine learning based misbehavior detection system for cognitive software-defined multimedia VANETs (CSDMV) in smart cities. *Multimedia Tools and Applications*, 82(3), 3931–3951. <https://doi.org/10.1007/s11042-022-13440-8>
- Ng, K., Ong, B., Neagle, R., Ebinger, P., Schmucker, M., Bruno, I., & Nesi, P. (2005). AXMEDIS framework for programme and publication and on-demand production. In *Proceedings of the First International Conference on Automated Production of CrossMedia Content for Multi-Channel Distribution* (pp. 247–250). Washington, DC, USA.
- Özmen, A., Şanslı, A., & Şahin, H. (2019). EDU-DRM: A digital rights management (DRM) system for K-12 education. *Scientia Iranica*, 26(Special Issue on: Socio-Cognitive Engineering), 103–113. <https://doi.org/10.24200/sci.2018.5345.1219>.
- Panigrahy, N. K., Nain, P., Neglia, G., & Towsley, D. (2022). A new upper bound on cache hit probability for non-anticipative caching policies. **ACM Transactions on Modeling and Performance Evaluation of Computing Systems**, *7*(2-4), 5. <https://doi.org/10.1145/3547332>
- Pasupuleti, M. (2025). Decentralized creativity: AI-infused blockchain for secure and transparent digital innovation. *New Era Scientific Exchange*, 12(2), 45–59. <https://doi.org/10.62311/nesx/rrvi125>
- Poese, I., Frank, B., Ager, B., Smaragdakis, G., & Feldmann, A. (2010). Improving content delivery using provider-aided distance information.. <https://doi.org/10.1145/1879141.1879145>
- Polo, J., Prados, J., & Delgado, J. (2004). Interoperability between ODRL and MPEG-21 REL. In *ODRL Workshop* (pp. 65–76). Vienna, Austria.
- Priyanka, D., Channakrishnaraju, & Chethan, B. K. (2022). Insights on effectiveness towards research approaches deployed in content delivery network. **Software Engineering Perspectives in Systems*, Vol. 1*, *501*, 224–243. https://doi.org/10.1007/978-3-031-09070-7_20
- Prokofyeva, N., & Boltunova, V. (2017). Analysis and practical application of PHP frameworks in development of web information systems. *Procedia Computer Science*, 104, 51–56.
- Ramonet, A. G., Pecorella, T., Picano, B., & Kinoshita, K. (2024). Perspectives on IoT-oriented network simulation systems. *Computer Networks*, 253, 110749. <https://doi.org/10.1016/j.comnet.2024.110749>

- Rathod, A., and P. Kulkarni. 2014. "An Aimd Distributed Control Law for Load Balancing in Content Delivery Networks." *International Journal of Computer Applications* 108: 5–8. <https://doi.org/10.5120/19009-0458>.
- Rewal, P., Mishra, D., Mishra, A., & Rana, S. (2023). Enhancing security of biometrics based authentication framework for DRM system. **Multimedia Tools and Applications*, 82*(26), 40857–40871. <https://doi.org/10.1007/s11042-023-14891-3>
- Rewal, P., Pursharthi, K., & Mishra, D. (2024). Quantum-secure content key delivery mechanism for DRM system. **Multimedia Tools and Applications.** <https://doi.org/10.1007/s11042-024-18834-4>
- Rodrigues, M., S. Fernandes, J. Kelner, and D. Sadok. 2014. "An Analytical View of Multiple Cdns Collaboration." <https://doi.org/10.1109/aina.2014.49>.
- Sahoo, J., M. Salahuddin, R. Glitho, H. Elbiaze, and W. Ajib. 2017. "A Survey on Replica Server Placement Algorithms for Content Delivery Networks." *Ieee Communications Surveys & Tutorials* 19: 1002–26. <https://doi.org/10.1109/comst.2016.2626384>.
- Şanslı, A., & Taşçı, T. (2023). TBNS: A novel tool for simulating and analyzing bursty user requests in large-scale networks. In *Proceedings of the 2023 16th International Conference on Information Security and Cryptology (ISCTürkiye)* (pp. 1–5). IEEE. <https://doi.org/10.1109/ISCTrkiye61151.2023.10336108>.
- Schelkunov, D. (2024). An approach for designing fast public key encryption systems using white-box cryptography techniques. **Journal of Computer Virology and Hacking Techniques*, 20*(3), 441–445. <https://doi.org/10.1007/s11416-023-00511-z>
- Schubert, T., Wolf, L., & Kulau, U. (2022). ns-3-leo: Evaluation tool for satellite swarm communication protocols. *IEEE Access*, 10, 11527–11537. <https://doi.org/10.1109/ACCESS.2022.3146770>
- Serrao, C. (2004). Open secure infrastructure to control user access to multimedia content. In *Proceedings of the Fourth International Conference on Web Delivering of Music* (pp. 62–69). Barcelona, Spain.
- Shao, S. J., Gong, W. C., Yang, H. F., Guo, S. Y., Chen, L. D., & Xiong, A. (2023). Data trusted sharing delivery: A blockchain-assisted software-defined content delivery network. **IEEE Internet of Things Journal**, *10*(14), 11949–11959. <https://doi.org/10.1109/JIOT.2021.3124091>
- Shen, Z., Wang, H., Wei, M., & Wang, P. (2023). Research on global deterministic direct forwarding and scheduling of mixed flow based on time-sensitive network in substation. *Electronics*, 12(19), 4101. <https://doi.org/10.3390/electronics12194101>
- Shi, H., Li, Y. N., Hu, B. Y., Chen, M. H., & Ren, Y. G. (2022). A robust and secure zero-watermarking copyright authentication scheme based on visual cryptography and block G-H feature. **Multimedia Tools and Applications*, 81*(26), 38019–38051. <https://doi.org/10.1007/s11042-022-13136-z>

- Shi, L., Z. Wang, Y. Yao, and L. Wei. 2011. "Streaming Media Caching Model Based on Knapsack Problem." *Journal of Networks* 6. <https://doi.org/10.4304/jnw.6.9.1379-1386>.
- Solomon, Y., Mokryn, O., & Kuflik, T. (2022). SDNSandbox – Enabling learning-based innovation in provider networks. *Computer Networks*, 219, 109446. <https://doi.org/10.1016/j.comnet.2022.109446>
- Stamos, K., Pallis, G., Vakali, A., Katsaros, D., Sidiropoulos, A., & Manolopoulos, Y. (2010). CDNSim: A simulation tool for content distribution networks. *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, 20(2), 1–40.
- Sugirtham, R. (2021). Impact of queuing disciplines on the performance of multi-class traffic in a network. *Information Technology in Industry*, 9(1), 698–703. <https://doi.org/10.17762/itii.v9i1.189>
- Tueno, S., Tabue, R., Jiechieu, F., Ndonga, Y., Zafack, B., Feuyan, A., ... & Mbinkeu, R. (2019). Pear2Pear (on WiFi): A data sharing protocol over WiFi through a peer to peer network. *arXiv preprint*. <https://doi.org/10.48550/arxiv.1904.05316>
- Tuncer, D., M. Charalambides, R. Landa, and G. Pavlou. 2013. "More Control over Network Resources: An Isp Caching Perspective," 26–33. <https://doi.org/10.1109/cnsm.2013.6727806>.
- Varga, A., & Hornig, R. (2008). An overview of the OMNeT++ simulation environment. In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications Networks and Systems & Workshops* (ss. 1–10).
- Veith, T. L., Kobza, J. E., & Koelling, C. P. (1999). NetSim: Java™-based simulation for the World Wide Web. *Computers & Operations Research*, 26(6), 607–621.
- Venkateswaran, V., Huang, C. T., & Ravindran, K. (2023). Security management in content distribution networks: A delay-variance reduction approach for content mirror site placement. **2023 15th International Conference on Communication Systems & Networks (COMSNETS)**. <https://doi.org/10.1109/COMSNETS56262.2023.10041417>
- Volckmann, W. M. II. (2025). Revenue effects of Denuvo digital rights management on PC video games. **Entertainment Computing*, 52*, 100885. <https://doi.org/10.1016/j.entcom.2024.100885>
- Wang, H., & Padmanabhan, V. N. (2000). Cache proxy: A performance evaluation. *IEEE Transactions on Computers*, 49(7), 678–693.
- Wang, L., Pai, V., & Peterson, L. (2002). The effectiveness of request redirection on cdn robustness. *Acm Sigops Operating Systems Review*, 36(SI), 345–360. <https://doi.org/10.1145/844128.844160>
- Wang, Y. Z., Zhao, D., Guo, Z. X., Gao, T., Ma, H. D., & Du, Y. (2024). CEL: Cost-aware edge-assisted livecast via optimization with Shapley value. **IEEE Internet of Things Journal**, *11*(5), 7805–7816. <https://doi.org/10.1109/JIOT.2023.3320442>
- Weingartner, E., vom Lehn, H., & Wehrle, K. (2009). A performance comparison of recent network simulators. In *2009 IEEE International Conference on Communications* (ss. 1–5).

- Wen, Y., Chen, Y., Shao, M.-L., Guo, J.-L., & Liu, J. (2020). An efficient content distribution network architecture using heterogeneous channels. *IEEE Access*, 8, 210988–211006.
- Weqar, M., Mehruz, S., Gupta, D., & Urooj, S. (2024). Adaptive switching based data-communication model for Internet of Healthcare Things networks. *IEEE Access*, 12, 11530–11548. <https://doi.org/10.1109/ACCESS.2024.3354722>
- Wolman, A., Dongarra, J. J., Gadgil, U. K., Heymann, M., Krishnamurthy, B., Li, M., & Veer, (2000). Web caching and content distribution: A view from the interior. *ACM Transactions on Internet Technology (TOIT)*, 1(1), 1–19.
- Xu, C., Feng, J., Zhou, Z., Wu, J., & Perera, C. (2019). Cross-layer optimization for cooperative content distribution in multihop device-to-device networks. *IEEE Internet of Things Journal*, 6(1), 278–287. <https://doi.org/10.1109/jiot.2017.2741718>
- Xu, K., X. Li, S. Bose, and G. Shen. 2018. “Joint Replica Server Placement, Content Caching, and Request Load Assignment in Content Delivery Networks.” *Ieee Access* 6: 17968–81. <https://doi.org/10.1109/access.2018.2817646>.
- Xu, X. L., Wu, F., Bilal, M., Xia, X. Y., Dou, W. C., Yao, L. N., & Zhong, W. Y. (2024). XRL-SHAP-Cache: An explainable reinforcement learning approach for intelligent edge service caching in content delivery networks. **Science China Information Sciences**, 67(7), 170303. <https://doi.org/10.1007/s11432-023-3987-y>
- Yadav, P., & Kar, S. (2024). Efficient content distribution in fog-based CDN: A joint optimization algorithm for fog-düğüm placement and content delivery. **IEEE Internet of Things Journal**, 11(9), 16578–16590. <https://doi.org/10.1109/JIOT.2024.3355468>
- Yan, C., Q. Nguyễn, I. Benkacem, D. Okabe, A. Nakao, T. Tsuda, C. Safitri, T. Taleb, and T. Sato. 2019. “Design and Implementation of Integrated Icn and Cdn as a Video Streaming Service,” 194–206. https://doi.org/10.1007/978-3-030-30523-9_16.
- Yan, G., & Li, J. (2022). Towards latency awareness for content delivery network caching. **Proceedings of the 2022 USENIX Annual Technical Conference**, 789–803.
- Yang, H. X., Pan, H. L., & Ma, L. (2023). A review on software-defined content delivery network: A novel combination of CDN and SDN. **IEEE Access**, 11, 43822–43843. <https://doi.org/10.1109/ACCESS.2023.3267737>
- Yang, Q., and D. Gündüz. 2018. “Coded Caching and Content Delivery with Heterogeneous Distortion Requirements.” *Ieee Transactions on Information Theory* 64: 4347–64. <https://doi.org/10.1109/tit.2018.2805331>.
- Yi, X. Y., Zhou, Y. P., Lin, Y. Q., Xie, B., Chen, J. J., & Wang, C. Y. (2023). Digital rights management scheme based on redactable blockchain and perceptual hash. **Peer-to-Peer Networking and Applications*, 16(5), 2630–2648. <https://doi.org/10.1007/s12083-023-01552-3>
- Yoo, T., Lee, S. M., Yoo, K., & Kim, H. (2023). Reinforcement learning based topology control for UAV networks. *Sensors*, 23(2), 921. <https://doi.org/10.3390/s23020921>

- Yuan, M. L., Mu, Y., Rezaeibagha, F., Xu, L., & Huang, X. Y. (2022). Controllable software licensing system for sub-licensing. **Journal of Information Security and Applications*, 64*, 103061. <https://doi.org/10.1016/j.jisa.2021.103061>
- Zarrad, A., & Alsmadi, I. (2017). Evaluating network test scenarios for network simulator systems. *International Journal of Distributed Sensor Networks*, 13(10), 1550147717738216.
- Zhang, B. L., Ling, K. K., Zhang, P., Zhang, Z., & Zhong, M. J. (2022). Algorithms to calculate the most reliable maximum flow in content delivery network. **Computer Systems Science and Engineering**, 41*(2), 699–715. <https://doi.org/10.32604/csse.2022.020193>
- Zhang, F. 2015. “Comparing Alternative Approaches for Mobile Content Delivery in Information-Centric Networking.” <https://doi.org/10.1109/wowmom.2015.7158151>.
- Zhang, H., Rao, S., & Towsley, D. (1998). Cache proxy: A scalable and efficient way to deliver internet content. *IEEE Network*, 12(1), 8–17.
- Zhang, H., Zhang, X., Fan, B., & Shao, L. (2010). Adaptive fast TCP. <https://doi.org/10.1109/icfn.2010.43>
- Zhang, Q., Zhang, S., Lin, J., Bannazadeh, H., & Leon Garcia, A. (2015). Kaleidoscope: Real-time content delivery in software defined infrastructures. <https://doi.org/10.1109/inm.2015.7140356>
- Zhang, T., Y. Wang, W. Yi, Y. Liu, C. Feng, and A. Nallanathan. 2022. “Two Time-Scale Caching Placement and User Association in Dynamic Cellular Networks.” *Ieee Transactions on Communications* 70: 2561–74. <https://doi.org/10.1109/tcomm.2022.3152265>.
- Zhang, Z., J. Dai, M. Zeng, D. Liu, and S. Mao. 2020. “Scalable Video Caching for Information Centric Wireless Networks.” *Ieee Access* 8: 77272–84. <https://doi.org/10.1109/access.2020.2989532>.
- Zheng, L. 2024. “Reqsminer: Automated Discovery of Cdn Forwarding Request Inconsistencies and Dos Attacks with Grammar-Based Fuzzing.” <https://doi.org/10.14722/ndss.2024.24031>.
- Zhu, G. W., & Gu, W. X. (2022). User mapping strategy in multi-CDN streaming: A data-driven approach. **IEEE Internet of Things Journal**, 9*(9), 6638–6649. <https://doi.org/10.1109/JIOT.2021.3112561>.

ÖZGEÇMİŞ

Ad-Soyad : Ahmet ŞANSLI

ÖĞRENİM DURUMU:

- **Lisans** : 2005, Sakarya Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği
- **Yüksek Lisans** : 2007, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar ve Bilişim Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği
- **Doktora** : 2025, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar ve Bilişim Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği

MESLEKİ DENEYİM VE ÖDÜLLER:

- 2022 – ..., Öğretim Görevlisi, Bilgisayar Mühendisliği Bölümü, SAÜ
- 2022 – ..., Yönetim Kurulu Üyesi, Uzaktan Eğitim Araş. ve Uyg. Merkezi, SAÜ
- 2018 – 2023, Müdür Yrd., Bilgisayar Araştırma ve Uygulama Merkezi, SAÜ
- 2005 yılından itibaren Sakarya Üniversitesi'nde görev yapmaktadır.

TEZDEN TÜRETİLEN ESERLER:

- Özmen, A., Şanslı, A., & Şahin, H. (2019). EDU-DRM: A digital rights management (DRM) system for K-12 education. Scientia Iranica, 26(Special Issue on: Socio-Cognitive Engineering), 103–113. <https://doi.org/10.24200/sci.2018.5345.1219>.
- Şanslı, A., & Taşcı, T. (2023). TBNS: A novel tool for simulating and analyzing bursty user requests in large-scale networks. In Proceedings of the 2023 16th International Conference on Information Security and Cryptology (ISCTürkiye) (pp. 1–5). IEEE. <https://doi.org/10.1109/ISCTrkiye61151.2023.10336108>.

DİĞER ESERLER:

- Varan, M., Akgül, A., Kurugöllü, F., Şanslı, A., & Smith, K. (2021). A novel security methodology for smart grids: A case study of microcomputer-based encryption for PMU devices. *Complexity*, 2021, Article ID 2798534. <https://doi.org/10.1155/2021/2798534>.
- Canay, Ö., Şanslı, A., Durdu, A., Darga, S., & Varan, M. (2012, June 5–7). Bologna süreci çerçevesinde hazırlanan eğitim öğretim bilgi sisteminde ders bilgileri modülü tasarımı. *Proceedings of the 6th National Educational Technologies Conference*, Ankara, Türkiye.
- Küçüker, A., Yüzkollar, C., Şanslı, A., & Şen, F. (2006). Speaker recognition using Mel-frequency cepstrum coefficients and artificial neural network for security systems. *Electronic Letters on Science and Engineering*, 2, 8.

