MULTİMEDYA UYGULAMALARI İÇİN DİNAMİK KOŞULLU ERİŞİM SİSTEMİ TASARIMI

DYNAMIC CONDITIONAL ACCESS SYSTEM DESIGN FOR MULTIMEDIA APPLICATIONS

FAİK ÖZTÜRK

Hacettepe Üniversitesi

Lisansüstü Eğitim – Öğretim ve Sınav Yönetmeliğinin

ELEKTRİK ve ELEKTRONİK Mühendisliği Anabilim Dalı İçin Öngördüğü

YÜKSEK LİSANS TEZİ

olarak hazırlanmıştır.

2012

Fen Bilimleri Enstitüsü Müdürlüğü'ne,

Bu çalışma jürimiz tarafından **ELEKTRİK ve ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI 'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Başkan :.....
Prof. Dr. Hüseyin Selçuk GEÇİM

Üye (Danışman) :.....
Yard. Doç. Dr. Mehmet DEMİRER

Üye :.....
Prof. Dr. Abdullah ÇAVUŞOĞLU

Üye :.....
Doç. Dr. Ali Ziya ALKAR

Üye :.....
Yard. Doç. Dr. Umut SEZEN

ONAY

Bu tez Hacettepe Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği'nin ilgili maddeleri uyarınca yukarıdaki jüri üyeleri tarafından ...../...../..... tarihinde uygun görülmüş ve Enstitü Yönetim Kurulunca ...../...../..... tarihinde kabul edilmiştir.

Prof.Dr. Fatma SEVİN DÜZ
Fen Bilimleri Enstitüsü Müdürü

Aileme ...

MULTİMEDYA UYGULAMALARI İÇİN DİNAMİK KOŞULLU ERİŞİM SİSTEMİ TASARIMI

FAİK ÖZTÜRK

ÖZ

IPTV sistemlerinde, dijital televizyon hizmetinin sunulması işlemi internet protokolünün kullanılması ile gerçekleştirilir. Bu konudaki en önemli ihtiyaçlardan biri de belirli bir yönetim şebekesi üzerinden esnek, güvenli ve kesintisiz bir dijital televizyon hizmetinin çok büyük bir maliyet getirmeden son kullanıcıya hitap edecek şekilde oluşturulmasıdır. Bu yüzden hizmet sağlayıcıları günümüzde kullanılan klasik koşullu erişim teknikleri yerine yeni arayışlar içerisindedirler.

Bu tezde, belirli bir yönetim şebekesi üzerinden VPN şifreleme tekniği kullanılarak koşullu erişimin sağlandığı IPTV hizmetinin modellenmesi amaçlanmıştır. Bahsedilen amaç doğrultusunda, IPTV kavramı araştırılmış ve tezde bu konuyla ilgili özet bilgi verilmiştir. Donanım tabanlı koşullu erişim sistemleri ile yazılım tabanlı koşullu erişim sistemlerinin güvenlik yeterlilikleri karşılaştırılmıştır. Bunun yanında, tez kapsamında üretilmiş olan IPTV yönetim ve son kullanıcı programı ile ilgili tasarım ve kodlama detayları tezde sunulmuştur.

Programın tasarımında nesne tabanlı yaklaşım benimsenerek tasarımda kolay anlaşılırlık, değişime ve gelişime elverişlilik temel prensip olarak alınmıştır. Kod, C# dili kullanılarak Visual Studio .NET ortamında geliştirilmiştir. Veri tabanı yönetimi Microsoft SQL Server ile güvenli ve kesintisiz bir şekilde sağlanmıştır. Sistemin son kullanıcı tarafında oluşturulan IPTV programı, yönetim şebekesi ile entegre bir şekilde çalışmaktadır.

ANAHTAR SÖZCÜKLER: IPTV, akış, VPN, AES, Visual Studio .NET, C#, nesne tabanlı programlama, Microsoft SQL Server, İsteğe Bağlı Video.

Danışman: Yard. Doç. Dr. Mehmet DEMİRER, Hacettepe Üniversitesi, Elektrik ve Elektronik Mühendisliği Anabilim Dalı

DYNAMIC CONDITIONAL ACCESS SYSTEM DESIGN FOR MULTIMEDIA APPLICATIONS

FAİK ÖZTÜRK

ABSTRACT

In the IPTV systems, delivery of digital television service is realized by utilising the Internet protocol. One of the main necessities in this area is to develop a flexible, secure and seamless digital television service via a particular management network, in a way that appeals to the end user without leading big costs. Therefore, service providers search for new prospects other than existing conditional access techniques.

In this thesis, it is aimed to model an IPTV service delivered over conditional access by using VPN encryption technique over a particular management network. In that sense, some information on IPTV concept is provided. Security adequacy for hardware based and software based conditional access systems is discussed and compared. Finally, design and coding details of an IPTV management and end user program created in the frame of this thesis is presented.

An object-oriented approach is adopted during the design of the program, which allows for further change and development making the design easy to understand. The code was developed in Visual Studio .NET platform using C# programming language. Microsoft SQL Server was used for a secure and seamless database management. An IPTV user program has been working in an integrated way with the management network on the other part of the system.

KEYWORDS: IPTV, stream, VPN, AES, Visual Studio. NET, C#, object-oriented programming, Microsoft SQL Server, Video on Demand.

Advisor: Asst. Prof. Dr. Mehmet DEMİRER, Hacettepe University, Department of Electrical and Electronics Engineering

TEŞEKKÜR

Yazar, bu çalışmanın gerçekleşmesinde katkılarından dolayı, aşağıda adı geçen kişi ve kuruluşlara içtenlikle teşekkür eder.

Sayın Yard. Doç. Dr. Mehmet DEMİRER (tez danışmanı), çalışmanın sonuca ulaştırılmasında ve karşılaşılan güçlüklerin aşılmasında yön gösterici olmuştur.

Başta TÜRKSAT A.Ş. (yazarın çalıştığı şirket) Uydu Frekans Gözlem Direktörü Sayın Orhan ULUBEY olmak üzere yazarın çalışma arkadaşları, tezin tamamlanması aşamasında hoşgörü göstererek manevi olarak destek olmuşlardır.

Yazarın ailesi ve arkadaşları, bu çalışmanın gerçekleştirilmesi sırasında hiçbir yardımdan ve fedakârlıktan kaçınmamış, maddi ve manevi destek olmuşlardır.

İÇİNDEKİLER DİZİNİ

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

AES	Gelişmiş Şifreleme Standardı (Advance Encryption Standard)
ADSL	Bakışımsız Sayısal Abone Hattı (Asymmetric Digital Subscriber Line)
API	Uygulama Programlama Arayüzü (Application Programming Interfaces)
ATSC	İleri Televizyon Sistemleri Komitesi (Advanced Television Systems Committee)
AVC	Gelişmiş Video Kodlama (Advanced Video Coding)
Bps	Saniye Başına Düşen Bit (Bit Per Second)
CA	Koşullu Erişim (Conditional Access)
DARPA	İleri Araştırma Projeleri Ajansı (Defense Advanced Research Projects Agency)
DMB	Sayısal Çoklu Ortam Yayıncılığı (Digital Multimedia Broadcasting)
DRM	Sayısal Hakların Korunması (Digital Rights Management)
DSL	Sayısal Abone Hattı (Digital Subscriber Line)
DVB	Sayısal Video Yayıncılığı (Digital Video Broadcasting)
DVB-C	Sayısal Kablo Yayıncılığı (Cable Digital Video Broadcasting)
DVB-S	Sayısal Uydu Yayıncılığı (Satelite Digital Video Broadcasting)
DVB-T	Sayısal Karasal Yayıncılığı (Terrestrial Digital Video Broadcasting)
EPG	Elektronik Program Rehberi (Electronic Program Guide)
FEC	İleri yönlü Hata Denetimi (Forward Error Correction)
FPS	Saniyedeki Kare Sayısı (Frame Per Second)
HDTV	Yüksek Çözünürlüklü Televizyon (High Definition Television)
HTML	Hareketli-Metin İşaretleme Dili (HyperText Markup Language)
Hz	Hertz
IEEE	Elektrik Elektronik Mühendisleri Enstitüsü (The Institute of Electrical and Electronics Engineers)
IP	İnternet Protokolü (Internet Protocol)

IPTV	İnternet Protokollü Televizyon (Internet Protocol Television)
IRD	Tümleşik Alıcı Kod Çözücü (Integrated Receiver Decoder)
ITU	Uluslararası Telekomünikasyon Birliği (International Telecommunications Union)
ITU-T	Uluslararası Telekomünikasyon Birliği Telekomünikasyon Standartlaştırma Birimi (International Telecommunications Union Telecommunication Standardization Sector)
MBMS	Çoklu Ortam Yayın ve Çoklu Dağıtım Servisi (Multimedia Broadcast and Multicast Service)
Mbps	Saniye Başına Düşen Megabit (Mega Bit Per Second)
MD5	Mesaj Özet Algoritması 5 (Message-Digest Algorithm 5)
MHz	Megahertz
MPE	Çoklu Protokol Sarma (Multiprotocol Encapsulation)
MPEG	Hareketli Görüntü Uzmanları Birliği (Moving Pictures Experts Group)
NPVR	Ağ Tabanlı Kişisel İçerik Kaydedici (Network Personal Video Recorder)
NTSC	Ulusal Televizyon Standartları Komitesi (National Television Standards Committee)
PAD	Programlarla İlgili Bilgiler (Program Associated Data)
PVR	Kişisel İçerik Kaydedici (Personal Video Recorder)
SDTV	Standart Çözünürlüklü Televizyon (Standard Definition Television)
SI	Servis Bilgileri (Service İnformation)
STB	Set Üstü Cihaz/Kutu (Set-Top Box)
TCP	Aktarım Denetim Protokolü (Transmission Control Protocol)
TV	Televizyon (Television)
UDP	Kullanıcı Veribloğu İletişim Kuralları (User Datagram Protocol)
vb.	ve benzeri
VoD	Talebe Bağlı Video (Video on Demand)
VoIP	İnternet Telefon Servisi (Voice Over Internet Protocol)
VPN	Sanal Özel Ağ (Virtual Private Network)

EKLER DİZİNİ

Sayfa

1. GİRİŞ

Sosyal yapıdaki ilişkilere paralel olarak gelişim gösteren teknoloji, insanların dünyanın farklı noktalarından ve farklı zaman kesitlerinden bilgi ve beğenilere odaklanmasına imkân tanımaktadır. Yakın zamana kadar geleceğin teknolojisi olarak tanımlanan multimedya ve internet artık günümüz teknolojisi halini almıştır. Karşılıklı etkileşimin oluşturduğu iletişim teknolojileri insan yaşamında vazgeçilmez bir yere sahip olmaya başlamıştır.

İnternetin ortaya çıkışı, Amerikan Federal Hükümeti Savunma Bakanlığı'nın araştırma ve geliştirme kolu olan Savunma İleri Düzey Araştırma Projeleri Kurumu'na dayanmaktadır. 1969 yılında bilgisayar bilimleri ve askeri araştırma projelerini desteklemek için ABD Savunma Bakanlığı ARPANET adında ilk Paket Anahtarlamalı Bilgisayar Ağı'nı oluşturmaya başlamıştır. Bu ağ, ABD'deki üniversite ve araştırma kuruluşlarının değişik tipteki bilgisayarlarını da kapsayarak 1970'li yıllar boyunca Atlantik'ten Pasifik'e uzanarak kıta ölçeğinde genişlemiştir. 1973 yılında ağ için bir protokol seti geliştirmek amacıyla Stanford Üniversitesi'nde, daha sonra BBN'in ve College of London'ın da dahil olduğu ağda çalışma projesi başlatılmıştır. 1978'e kadar İletim Kontrol Protokolü'nün (TCP-Transmission Control Protocol) dört uyarlaması geliştirilmiş ve denenmiştir. 1980 yılında ise bu küme sabitleştirilmiş ve ARPANET'e bağlı bilgisayarlar arasındaki iletişim kolaylaşmıştır. 1983'te tüm ARPANET kullanıcıları İletim Kontrol Protokolü/İnternet Protokolü (TCP/IP Transmission Control Protocol/Internet Protocol) olarak bilinen yeni protokolü kullanmaya başlamıştır. Aynı yıl TCP/IP, ARPANET'i de içeren Savunma Bakanlığı ağında kullanılmak üzere standartlaştırılmıştır. ARPANET 1990 Haziran'ında kullanımdan kaldırılmış ve yerini ABD, Avrupa, Japonya ve Pasifik ülkelerinde ticari ve hükümet işletimindeki omurgalara ağlara bırakmıştır. ARPANET'in kaldırılmasına rağmen TCP/IP protokolü kullanılmaya devam etmiş ve günümüzde internet protokolü adı altında gelişimini sürdürmüştür [1].

Günümüzde web tarzı yaşam, insanların mesafelerin önemi olmaksızın sahip oldukları bilgiyi paylaşabilmelerini, bilgiden faydalanmalarını, farklı topluluklar içinde yer almalarını sağlamaktadır. XXI. Yüzyıl'ın ilk yarısı sona erdiğinde gelişmiş ülkelerdeki ev ve işyerlerinin tamamında bilgisayar olacağı ve çok çeşitli

ev aletlerine de çeşitli yazılımlar yüklenerek iletişim kurulabileceği ya da internet üzerinden araçların yönetileceği sıklıkla ifade edilmektedir.

Uydu, fiber optik ve nanoteknoloji alanlarındaki gelişmeler televizyon yayıncılığının etkileşimsel kapasitesini artırması ve izleyicilere iletim süreci üzerinde daha fazla denetim olanağı vermesi nedeniyle gün geçtikçe gelişen pratik bir gerçeklik haline gelmektedir.

Haberleşme, ulaşım, taşımacılık ve bilgi işlem hizmetlerindeki gelişmeler sonucunda internet, noktadan noktaya iletişim, veri transferi ve enformatik bilgi aktarımı gibi farklı tarzlarda iletişim biçimleri giderek artmıştır. İnternetin diğer hizmetlere yakınsamasını güçlendiren unsur onun bir ağ ortamı olmasıdır. Geniş bant erişim sayesinde, ağlar arasında veri aktarımı geçmişe oranla çok daha hızlı gerçekleşebilmektedir. Ses ve görüntü öğelerinin paylaşılabildiği internet, bu özelliği sayesinde ağ üzerinden televizyon yayınlarına erişimi de olanaklı hale getirmiştir. Televizyon yayınlarının internet ortamından izlenebilmesi, televizyon yayıncılığını ve televizyon izleme biçimini de değiştirmektedir. Yeni nesil IPTV, geniş bant iletişim teknolojisini kullanarak televizyon yayınlarında dönüşüme olanak sağlamıştır [2].

IPTV televizyon ve görüntü sinyallerinin, geniş bant (kablo internet/xDSL) kullanıcısı abonelere veya izleyicilere, internet protokolü üzerinden dağıtıldığı sistemlerdir [3]. Bu sistem genel olarak geniş bant işletmecisi tarafından sağlanan internet bağlantısına paralel olarak, aynı altyapı üzerinden tahsis edilen bir bant genişliğiyle yürütülmektedir. Halen tüm dünyada 100 milyondan fazla evde geniş bant internet bağlantısının kurulu olduğu düşünüldüğünde, IPTV'nin önümüzdeki yıllarda çok büyük bir hızla gelişme göstereceği öngörülmektedir.

Telekomünikasyon ve yayın şirketlerinin yeni gelir kaynakları oluşturmak ve kullanıcı taleplerini karşılamak amacıyla ortaya çıkan IPTV, dünyada hızla yaygınlaşan bir hizmet haline gelmiştir. Yeni nesil şebekeler üzerinden sunulan yeni hizmetlerden biri olarak da değerlendirilebilecek IPTV konusunun, sadece yeni bir medya iletişim ortamı olarak algılanmaması, yeni nesil şebekeler ve bu şebekeler üzerinden sunulabilecek diğer geniş bant hizmetleri için bir başlangıç stratejisi olarak da görülmelidir.

IPTV hizmetinin alternatiflerinden farkı üçlü oyun hizmetidir. Tüketicinin, görüntü, veri ve telefon iletişimini aynı paket içinden alabildiği bu uygulamaya “Üçlü Oyun” (Triple Play) denmektedir. Üçlü Oyun servislerine mobil özelliklerin de eklenerek mobil ortamlar için tasarlanan haline ise “Quad Play” denir [6]. Bir geniş bant hattından tüketiciye üçlü oyun hizmeti sunulabilmesi için işletmecinin hem IPTV hem de internet üzerinden ses iletimi teknolojisini kullanması gereklidir. Kullanıcılar, telefon, geniş bant internet ve etkileşimli televizyon hizmetlerinin bir arada sunulmasına bu hizmetlerin ayrı ayrı sunulmasından daha fazla değer vermektedir. Aynı zamanda firma açısından da bu hizmetleri bir arada sunmak, ayrı ayrı sunmaktan daha az maliyet ortaya çıkarmaktadır.

IPTV mantığıyla çalışan ilk yayın 1994 tarihinde ABC (American Broadcasting Company) tarafından “Cu-SeeMe” adlı video konferans yazılımı yardımıyla yapılmıştır. İlk önemli yatırım ise İngiltere’de hizmet veren Kingston Communications firması tarafından yapılmış ve 1999 yılında ADSL altyapısı kullanılarak IPTV teknolojisi ile hizmet verilmiştir. Bu süreçte ABD’nin en büyük telekomünikasyon sağlayıcısı olan AT&T’nin IPTV’ye ilgisi yoğunlaşmış ve 2006 yılında geniş bant internet altyapısı kullanarak 11 kentte 300′ün üzerinde kanalla hizmet vermeye başlamıştır.

Avrupa’da Fransa, IPTV aboneliğinde bir numaralı ülke konumunda olmuştur. Avrupa ülkelerinin IPTV’de başarılı olmasının en önemli sebebi, fiber ve geniş bant internet erişim altyapısına yaptığı yatırımdır [5].

IPTV’nin geleneksel TV sistemlerine göre en önemli avantajı her kullanıcının ayrı bir yayını izleyebilmesi ve iki yönlü iletişim yeteneğinin olmasıdır. Bu sayede kullanıcının içerik üzerinde denetim (durdurma, ileri, geri sarma, kaydetme vb.) ve dar bant temelli web uygulamalarında olduğu gibi izleyeceği içeriği özgürce seçebilme olanağı bulunmaktadır. Kablosuz iletişim alanında faaliyet gösteren Motorola’nın, Almanya, Fransa, İtalya, İspanya ve İngiltere’de gerçekleştirdiği 2500 geniş bant kullanıcısına yönelik alan araştırması, gelecekte televizyon izleme alışkanlıklarının hızla değişeceğini göstermektedir [2].

Televizyonun yapısı gereği sınırlı bir geri bildirime olanak sağlaması karşısında internetin iki yönlü iletişime olanak sağlayan interaktif yapısı, izleyicinin eğilimlerini

anlamlandırma ve bu eğilimler doğrultusunda mecraları yeniden yapılandırmada önemli katkılar sağlamaktadır. Yine bu durum medya profesyonellerine yayıncılığın yeniden tasarlanması açısından çok önemli fırsatlar sunmaktadır. Konuyu televizyon yayıncılığı açısından değerlendirdiğimizde, tüm bu teknolojik değişim gerçek bir içerik devrimine yol açmaktadır. Yeni başlayan süreçte internet ağ ortamını ve televizyon yayıncılığını bir araya getiren IPTV, teknolojik alt yapının kurulmasıyla birlikte hızla yaygınlaşmakta ve yayıncılığın değişimine katkıda bulunmaktadır. Sayısal teknolojiler, televizyon yayınlarının istatistiki bilgilerini kontrol altına alma ve yorumlama olanağı sağlamaktadır. Yayıncılar tarafından sürekli analiz edilmesi gereken izleyici hangi yayınları hangi sıklıkla izlediği sorusu IPTV ile çözüm bulmaktadır. Reklam verenler ise bu teknoloji sayesinde, kendi ürünlerinin hedef kitlesini çok daha net ve kolay bir biçimde belirlemektedirler. Günümüzde yapılan ölçümlerin ne kadar gerçekçi ve nasıl yapıldığı hala tartışılırken, bu yeni teknolojilerin sağladığı kolaylıklar izleyici kitlenin takibinde dönüşümü hızlandırmaktadır.

Geleneksel TV yayınlarının aksine IPTV teknolojisi istenilen programın istenildiği zaman izlenmesini mümkün kılmakta, bu da günümüzün yoğun iş ve yaşam temposu içerisinde kullanıcıların planlarını TV yayınlarının akışına göre değil, kendi programlarına göre yapmalarına imkân tanımaktadır. Talebe bağlı görüntü (Video on Demand) gittikçe popüler bir kavram haline gelmekte ve IPTV teknolojisi de bu hizmet için en iyi altyapıyı sunmaktadır.

Çağdaş izleyiciler programların seçiminde, çeşitlilik ve tercih esnekliği kazanmak istemektedir. Teknolojik gelişmelerle birlikte, artık insanlar sadece neyi seyretmek istediklerine karar vermemekte, aynı zamanda nasıl ve ne zaman seyretmek istediklerine de kendileri karar vermek istemektedirler. IPTV ile izleyici, program içeriklerini artık kendisi şekillendirmekte ve kendi eğilimlerine göre bir program izleme menüsü tasarlayabilmektedir.

IPTV ile içerik sağlayıcılar, yayıncılar, yapımcılar ve reklamcılar için doğrudan geri besleme de mümkün olmaktadır. İzleyicilerin beğeni ve taleplerini tahmin ederek değil, doğrudan ölçerek anlayabilmek yayıncılık alanında devrimsel bir değişim ve gelişimin önünü açmaktadır [5].

IPTV hizmetini vermek isteyen operatörlerin, ağ ortamında verilen diğer hizmetler gibi yüksek güvenlik gereksinimleri vardır. Bu gereksinimler, kullanılan donanım, yazılım ve en önemlisi sunulan içeriğin korunmasıyla ilgilidir. IPTV hizmetinin sağlanmasıyla ilgili donanım, genel internet trafiğinden ayrı bir şekilde yer alacağı için sistem güvenliğinin üst düzeyde tutulması gerekmektedir [7].

IPTV sistemlerinde ilgi gören ödemeli TV hizmetleri, varlıklarını abonelere değerli ve çekici içerik sağlayabilme yeteneklerine borçludur. Bu içerik, kendi kullanımları veya kendi müşterilerine ucuza satmak için bedava erişim sağlamak isteyen üçüncü şahıslar tarafından sürekli saldırılara maruz olduğundan korunmalıdır. Ödemeli TV işletmecileri donanımsal tabanlı, kart çözümlü koşullu erişim sistemleri kullanarak aşağıdaki güvenlik önlemlerini almaktadır:

- İçeriğe kimin erişebildiği üzerinde sıkı denetim uygulanıp bu erişim ücretlendirilerek, ödemeli TV işletmecilerinin kazançları güvence altına alınmaktadır.

- Ödemeli TV işletmecilerinin sundukları içeriğin güvenliğiyle ilgili içerik sahiplerinin gereksinimleri karşılanıp, yasa dışı kullanım ve dağıtım önlenmeye çalışılmaktadır.

- İşletmecilerin set üstü cihazlara (STB) erişimi denetlenerek, kendi aygıtlarına yaptıkları yatırımı korumaları sağlanmaktadır.

Eskiden beri geleneksel bir noktadan çok noktaya tarzı yayın ağları olan ödemeli TV işletmecilerinin kullandığı donanımsal kart tabanlı koşullu erişim sistemleri, günümüze kadar kullanılan en yaygın koşullu erişim sistemi olmuştur. Fakat günümüzde;

- Sabit yayına dayalı ağlar giderek genişbantlı ağlarla karma hale gelmektedir.

- Gittikçe daha fazla sayıda ödemeli TV ticareti, IP ağlar üzerinden IPTV firmalarınca işletilmektedir.

- Görüntü iletim modlarının ve ilgili aygıtların çeşitliliği giderek artmakta ve doğrusal TV tüketiminin hakimiyeti kaybolmaktadır.

- İçerik hırsızlığı daha çok internet üzerinden içerik dağıtımı veya şifre anahtarlarının paylaşımı şeklinde gerçekleşmektedir.

Bütün bu gelişmeler, görüntü hizmetlerinin giderek daha fazla bağlantılı ortamlarda erişilebilmelerine yol açmaktadır. Bu, ödemeli TV içeriğini üçüncü kişilerden korumada ve dağıtımı güvenli hale getirmede geleneksel yöntemlerin hala uygun olup olmadığı sorusunu daha da belirginleştirmektedir. Bu yüzden donanım tabanlı sistemler yerine yazılım tabanlı koşullu erişim tekniklerini geliştirme çabaları gün geçtikçe artmaktadır.

Sıralanan gelişmeler çerçevesinde bu çalışmada yüksek güvenlik gereksinimlerini sağlamak üzere yazılım tabanlı koşullu erişim tekniği kullanılarak üretilmiş olan IPTV yönetim ve son kullanıcı programı ile bilişim teknolojilerindeki değişim sürecine paralel olarak, televizyon yayıncılığının nasıl dönüşüm geçirdiğinin ve interaktif ortamların süreç içerisinde televizyon yayıncılığına alternatif olma potansiyelinin hangi bağlamlarda anlam kazandığının tartışılması amaçlanarak, konuyla ilgili literatüre katkı sağlanması hedeflenmiştir.

Tezin bundan sonraki bölümleri şu şekildedir. Bölüm 2'de IPTV kavramı açıklanacak ve IPTV sistemlerinin yapısıyla ilgili bilgi verilecektir. Bölüm 3'te IPTV teknolojisinin mevcut teknolojilerle farklılıkları açıklanacaktır. Bölüm 4'te tez kapsamında geliştirilen IPTV koşullu erişim sistemi ile ilgili başlıklar yer alacaktır. Son olarak bölüm 5'te sonuç ve öneriler sunulacaktır.

EK 1'de yapılan benzer tez çalışmalarından örnekler yer almaktadır. Verilen tez örneklerinin bu tezden başlıca farkları, kapsamları ve kullanılan geliştirme ortamlarıdır. Dolayısıyla, bu tez çalışması bahsi geçen biçimde bir IPTV sistemi geliştirilmesini amaçlamakla birlikte, daha sonra üzerinde çalışılmayı gerekli kılan bir ürün ortaya koymaktadır. Bu nedenle tezde üretilen her türlü yapı, kod ve ürün için kolay anlaşılabilirlik asıl hedef olmuştur. Tasarım adımlarında kullanılan yapılar olası değişiklik ve eklemelere müsaade edecek biçimde tasarlanmıştır. Geliştirme ortamı olarak kullanımı yaygın olan Microsoft Visual Studio .NET ve programlama dili olarak yüksek seviye dillerden C# kullanılmıştır. Tez kapsamında oluşturulan veri tabanı için en çok tercih edilen veri tabanı ortamlarından biri olan Microsoft SQL Server kullanılmıştır. IPTV yönetim şebekesi ve son kullanıcı

programı arasındaki üst düzey güvenlik Cisco VPN erişimi ile sağlanmıştır. Tüm kod parçaları açık olup grafik kütüphanesi dışında her türlü kod bu tez kapsamında üretilmiştir.

2. IPTV KAVRAMI

IPTV, televizyon yayınlarının geleneksel şekilde kablo TV, uydu veya karasal yayıncılık ile seyirciye iletimi yerine, internet teknolojileri kullanılarak geniş bant altyapısı üzerinden gerçekleştirilen yayın sistemidir. IPTV, sıradan herhangi bir televizyon programının internet üzerinden yayınlanması şeklinde değildir. Kendi içinde bir özgünlüğü vardır. Yapısı, kapalı ve kişiye özel bir TV sistemi olarak düşünülmelidir. IPTV'nin kullanıcıya dağıtılması, IP tabanlı güvenilir kanallar üzerinden yapılmaktadır [4].

IPTV, kullanıcı seçeneklerinin ve tercihlerinin takibine imkân sağlamaktadır. Hem televizyon hem de video sinyallerinin abonelere ya da izleyicilere ulaştırılması için kullanılan sistemlere verilen genel bir adlandırma olarak IPTV'nin gün geçtikçe kullanımı artmaktadır. Yayıncılar açısından, mevcut uydu, kablo ve karasal sistemler ile etkin bir rekabetçi olma potansiyeline rağmen IPTV bu tür sistemler için tamamlayıcı bir platform olarak görülmektedir.

IPTV, geniş bant erişim sağlayan bir operatör tarafından abonenin internet bağlantısına paralel olarak sunulan bir hizmettir ve internet protokolünü kullanır [8]. Geniş bant internet erişimi ile aynı altyapıyı kullanmaktadır. Ancak bu kullanımda IPTV hizmeti için tahsis edilmiş bir bant genişliği göze çarpmaktadır. Bu yüzden IPTV, abone olmuş kullanıcılara internet protokolünü kullanarak geniş bant bir bağlantı üzerinden dijital televizyon hizmetini sağlayan bir sistem olarak tarif edilebilir. Aşağıda IPTV'nin avantaj ve dezavantajları yer almaktadır.

IPTV Avantajları:

- Çift yönlü iletim vardır.
- Kullanıcıya özel dağıtım yapılır.
- Yüksek çözünürlük ve kaliteli görüntü imkânı sunar.
- Sınırlı internet kullanımı ile zararlı yazılım ve internet tehditlerine karşı güvenli bir teknolojidir.

• Mevcut yayın teknolojileriyle entegre bir şekilde çalışabilmektedir.

IPTV Dezavantajları:

• IPTV görüntü kalitesi tamamen bağlantı hızı ile ilişkilidir. Düşük hızlı bağlantılarda görüntü kayıpları oluşabilir.
• IPTV sistemi kaliteli ve genişbant bağlantı gerektiren yüksek maliyetli bir alt yapıya ihtiyaç duyar.

IPTV teknolojisi ile daha gelişmiş, kullanıcı dostu ve daha yüksek hızlı erişim teknolojileriyle iç içe bir yapıda sunulmaktadır. Çizelge 2.1'de IPTV teknolojisi ile verilen hizmetler yer almaktadır [9].

Çizelge 2.1 IPTV Teknolojisi ile Verilen Hizmetler.

TV Yayını	Dijital Radyo
İsteğe Bağlı Video	Çevrimiçi Oylama
Kişisel Video Kaydı	Video Konferans
İzle ve Öde	İnternet
Yayın Durdurma	Teletext
Elektronik Program Rehberi	Ebeveyn Kontrolü
Etkileşimli Arayüz	e-ticaret
Geriden İzleme	Anlık Mesajlaşma
Kişiselleştirilmiş Reklam	Eğitim
İsteğe Bağlı Müzik	Oyun

TV Yayını: IPTV ile son kullanıcıya, SD ve HD çözünürlükte TV yayınları sunulmaktadır.
İsteğe Bağlı Video: Depolanmış içeriği müşteriye katalog şeklinde sunan ve bu katalogdaki herhangi bir içeriği, müşterinin istediği zaman bir arayüz üzerinden seçerek izleyebilmesine olanak sağlayan hizmettir.

Kişisel Video Kaydı: Kullanıcıların istedikleri TV yayınlarını, daha sonra istedikleri zamanda izlemek üzere EPG üzerinden kaydetmesi sağlanır.

İzle ve Öde: Normal TV yayınının elektronik program rehberi üzerinden seçilerek belli bir süre için ücreti karşılığında izlenmesidir.

Yayın Durdurma: Kullanıcı izlemekte olduğu TV yayının herhangi bir anda “durdur” tuşuna basarak yayının o anında durdurma şansına sahip olabilir. Sonrasında “oynat” tuşuna basarak yayını izlemeye kaldığı yerden devam eder.

Elektronik Program Rehberi (EPG): Elektronik Program Rehberi, kanalların, TV yapımlarının belirli bir süredeki (günlük, haftalık, vb.) yayın akışının gösterilmesini sağlar. Ayrıca isteğe bağlı video içeriğinin gösterilmesi de EPG içerisinde ayrı bir ekranda yapılmaktadır.

Etkileşimli Arayüz: Kullanıcıya, kendisine sunulan bütün hizmetlere erişimini sağlayan bir kullanıcı arayüzü sağlanmaktadır. Bu arayüz, hesap bilgilerine erişme, sistem ayarlarını değiştirme, sık kullanılanları yönetme, ebeveyn kontrolleri gibi müşterinin kendisiyle ilgili işlemleri yapmasına olanak sağlar.

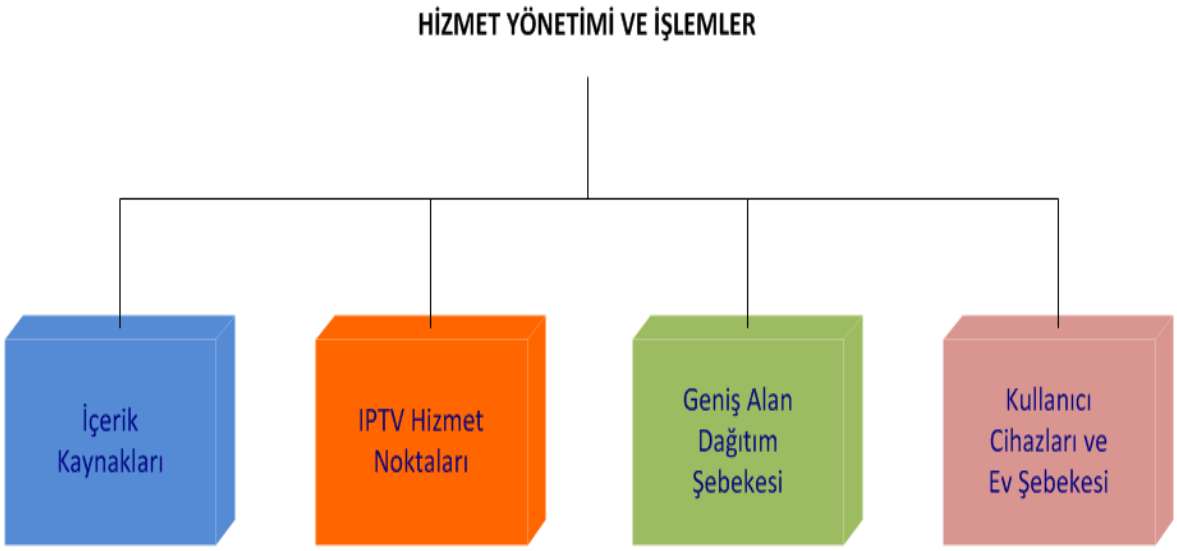
Geriden İzleme: Kullanıcının seçtiği TV kanallarını belli bir süre için kaydetmesi ve müşterinin kaydedilmiş yayınları isteğe bağlı olarak izlemesine olanak sağlayan hizmettir.

Kişiselleştirilmiş Reklam: Kullanıcının tercihlerine göre reklam hizmeti verilmesidir.

Bunun yanında IPTV ile isteğe bağlı müzik, dijital radyo, çevrimiçi oylama, video konferans, internet, teletext, ebeveyn kontrolü, e-ticaret, anlık mesajlaşma, eğitim ve oyun hizmetleri verilmektedir.

2.1. IPTV Mimarisi

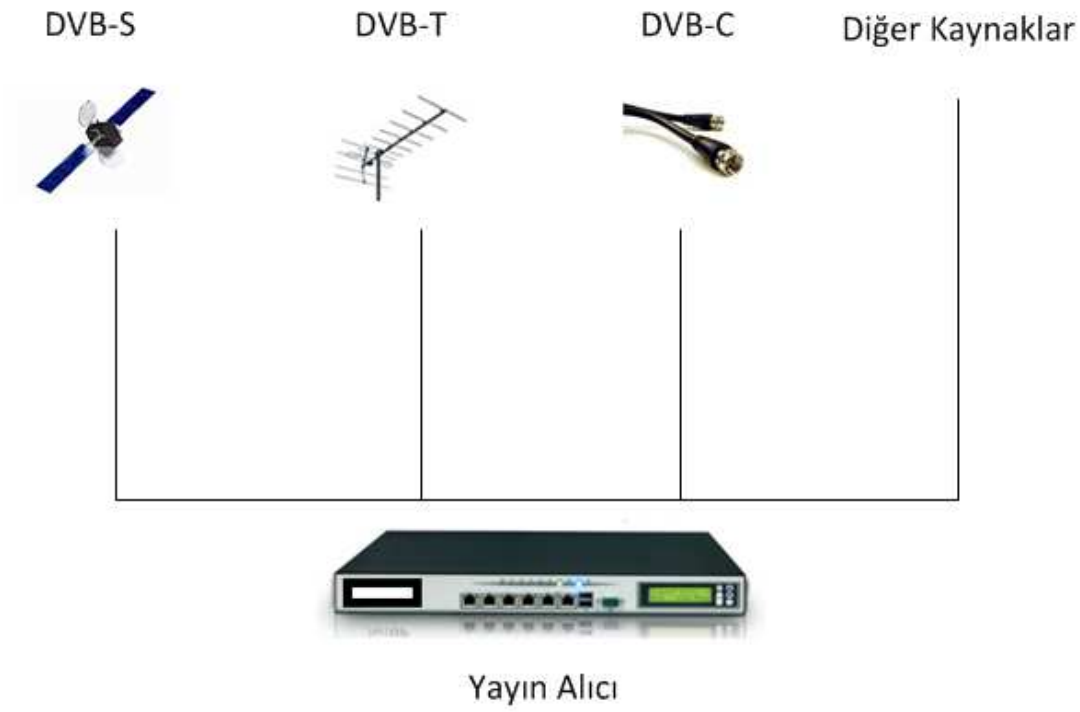
Hizmetin sunulacağı şebeke buna hazır olduğu sürece IPTV çok maliyetli bir iş değildir. Standart analog ya da dijital televizyonla karşılaştırıldığında daha düşük kapasitede bilgi gönderir. Bu yüzden hem operatör için hem de son kullanıcı için daha düşük maliyetlerden söz edilebilmektedir. IPTV mimarisi Şekil 2.1’de verilen bileşenlerden oluşmaktadır [10].



Şekil 2.1 Hizmet Yönetimi ve İşlemler.

2.1.1. İçerik Kaynakları

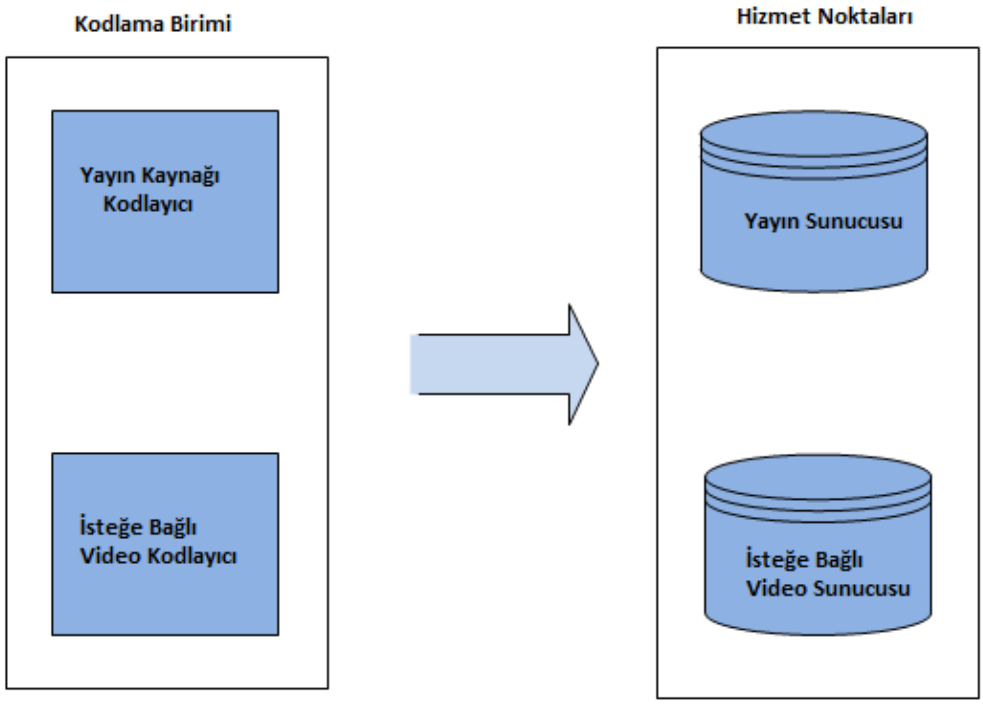
İçerik kaynakları canlı TV yayını veya isteğe bağlı video şeklinde olabilmektedir. Video içeriği yapımcılardan ya da diğer kaynaklardan alınmaktadır. Bu içerikler çözülerek isteğe bağlı video veritabanında depolanmaktadır. Şekil 2.2'de IPTV içerik kaynağını oluşturan bileşenler gösterilmektedir.



Şekil 2.2 IPTV Yayın Kaynakları.

2.1.2. Hizmet Noktaları

“Hizmet Noktası” video akışının farklı formatlarda alınması işlemini belirtmek üzere kullanılır. Farklı formatlardaki bu video akışları daha sonra yeniden formatlanır ve geniş alan dağıtım şebekesine uygun hizmet kalitesini gösteren belirteçlerle birlikte iletim için zarflama işlemine tabi tutulur. Artık video akışı abonelere sunulmaya hazırdır. Şekil 2.3’te hizmet noktası genel yapısı yer almaktadır.



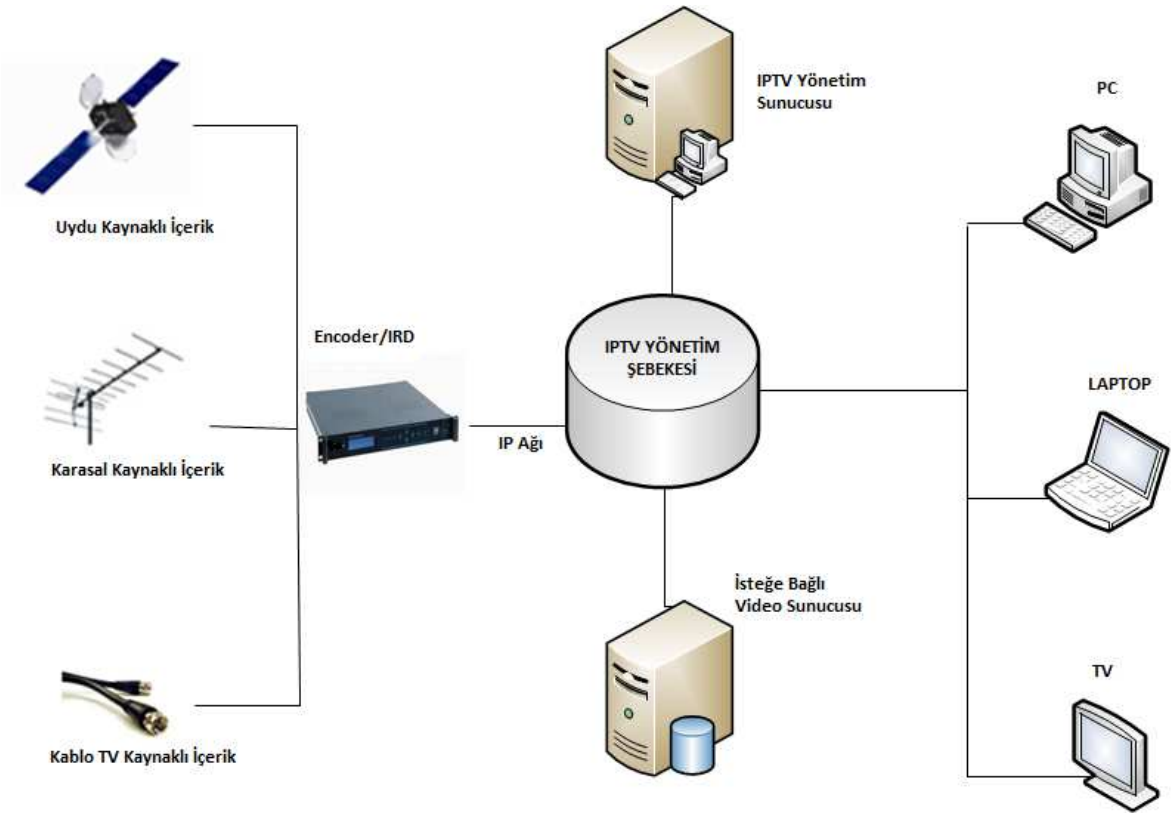
Şekil 2.3 Hizmet Noktası Genel Yapısı.

Hizmetin sunumu açısından hizmet noktaları dijital haklar yönetimi ile de birebir iletişim halindedir.

2.1.3. Geniş Alan Dağıtım Şebekesi

IPTV servisinin verilebilmesi için yayın merkezinden sonra, televizyon yayınlarının genişbant ağlar üzerinden kullanıcıya taşınması gerekmektedir. Genişbant ağlar, omurga ağlar ve erişim ağları şeklinde ikiye ayrılır. Omurga ağlar, IPTV hizmetini veren operatörün şehiriçi ve şehirlerarası ağlarına verilen isimdir. Burada omurga ağını tüm kullanıcılar ortak olarak kullanmaktadırlar. Bu ağlar günümüzde en çok kullanım şekline göre ATM ve IP omurga olarak ikiye ayrılmaktadır. Bu ağlar

üzerinde kullanılan protokoller çeşitli olup, kullanım şekline göre farklılıklar gösterir. Erişim ağları ise IPTV hizmetini veren telekom firmasının son sistem şebekesinden kullanıcının evine kadar bulunan ağlara verilen isimdir. Şekil 2.4'te IPTV geniş alan dağıtım şebekesi yer almaktadır.

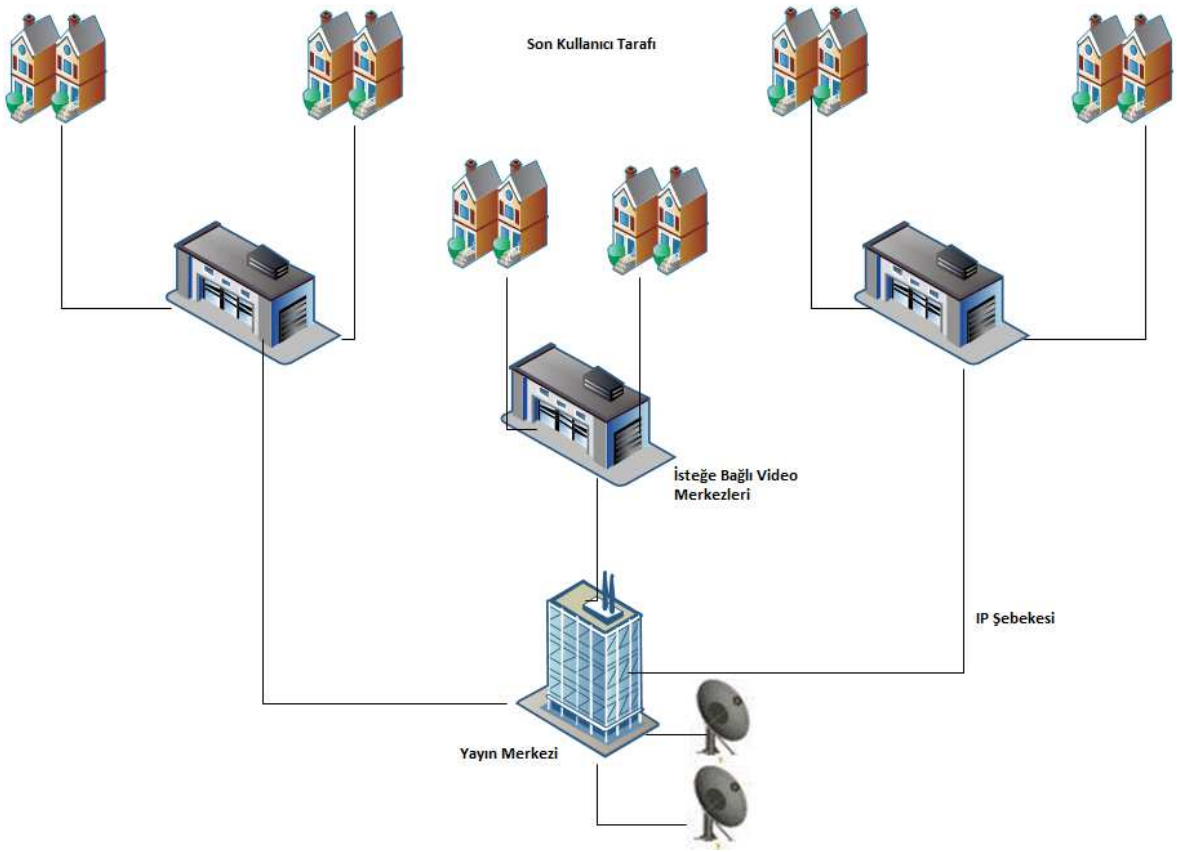


Şekil 2.4 Geniş Alan Dağıtım Şebekesi.

Geniş alan dağıtım şebekesinin üzerinde durduğu temeller, dağıtım yeteneği, dağıtım kapasitesi ve hizmet kalitesidir. IPTV hizmeti sunulması istenen geniş alan dağıtım şebekesinin başka yeterlilikleri de olmalıdır. Multicast yeteneği, hizmet noktalarından abonelerin evlerine kadar IPTV veri akışının güvenilir olarak ve zamanında sağlanması için gereklidir. Kullanılan şebekenin türüne göre şebeke omurgasının dağıtım noktalarında çekirdek yapılar da yer almaktadır. DSL şebekelerinde DSLAM, kablo TV şebekelerinde fiber node sistemi örnek olarak verilebilir.

Kullanıcı erişim hatlarında yüksek hızlı teknolojiler gerekmektedir. Örneğin DSL teknolojiler için ADSL+ ve VDSL teknolojileri örnek verilebilir. Bu tarz bir teknoloji ile kullanıcılara dağıtım, mevcut şebeke ile telefon hatları üzerinden sağlanabilir. Ayrıca hem DSL hem de Kablo TV işletmecileri son kullanıcıya kadar doğrudan

fiber iletimi de gerçekleştirebilirler. Şekil 2.5'te IPTV yönetim merkezi ve son kullanıcı arasındaki iletim yapısı gösterilmiştir.

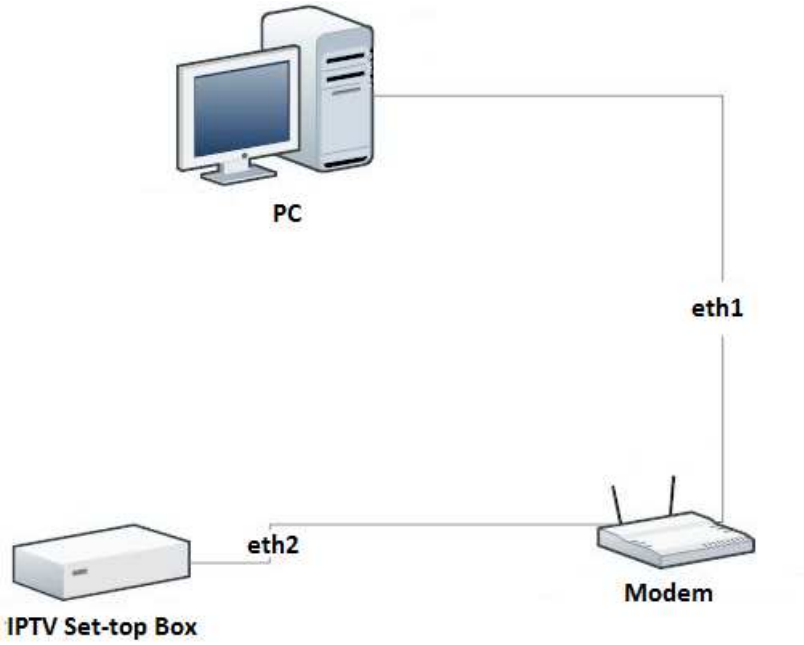


Şekil 2.5 IPTV İletimi.

Bununla birlikte, alınmak istenen en iyi sonuç, hizmet sağlayıcıların sundukları ürünlerin zenginliğine bağlıdır.

2.1.4. Kullanıcı Cihazları ve Ev Şebekesi

Bu cihazlar, son kullanıcının yani abonenin evinde ya da işyerinde bulunan cihazlar olup genişbant şebekenin sonlandığı noktadır. Son kullanıcı cihazları şebekenin sonlandırılması işlevinin yanında, üzerlerine entegre edilmiş başka özellikler de taşıyabilirler. Örneğin; routing gateway, set-top box ya da ev içi şebeke oluşturma olarak sıralanabilir. İşlevi, hizmet noktası ile kaliteli bağlantı yapısının kurulması, video akışındaki kodlamanın çözülmesi, kanal değiştirilmesinin sağlanması, kullanıcı ekranın kontrolü ve kullanıcının evindeki standart çözünürlükte ya da yüksek çözünürlükteki televizyon ya da monitörle bağlantının sağlanmasıdır. Şekil 2.6'da IPTV alıcı cihazları yer almaktadır.



Şekil 2.6 IPTV Alıcısı.

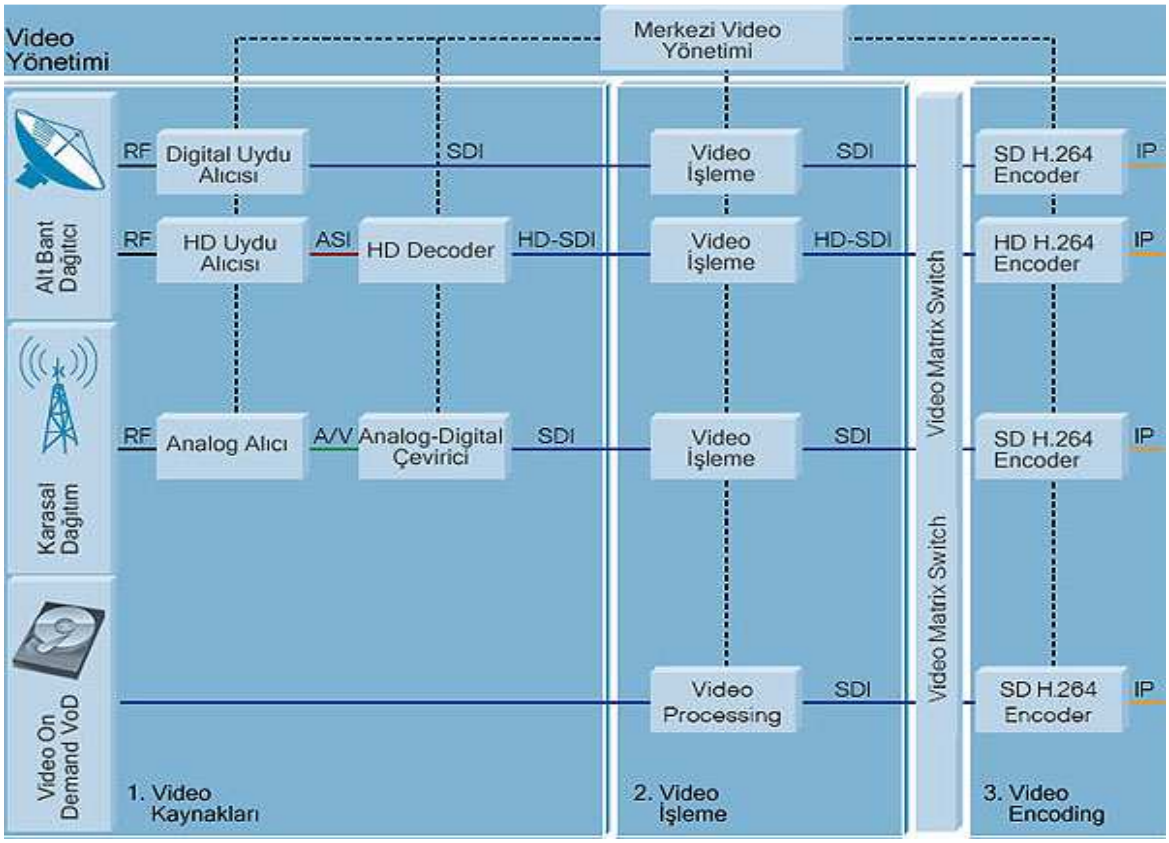
IPTV alıcısı receiver/set-top box tarzı bir cihaz olabileceği gibi PC tabanlı sistemlerde IPTV kullanımı için geliştirilmiş özel yazılımlar, IPTV alıcısı şeklinde çalışabilmektedir.

2.2. Yayın Merkezi

IPTV platformunda yer alacak içeriklerin IP şebekesi üzerinden yayınlanabilmesi için bir yayın merkezine ihtiyaç vardır. Yayın merkezi temel anlamda diğer sayısal televizyon yayın teknolojilerinin yayın merkezlerine benzemektedir. Ancak IPTV yayın merkezinde televizyon sinyalleri IP paketlerine dönüştürüldüğü için, IP protokolünün sağladığı etkileşimli teknolojileri ve katma değerli servisleri sağlamaktadır [11].

Yayın merkezi içerisinde öncelikle canlı yayını uydu ve diğer iletişim yolları üzerinden alıp IP paketlerine dönüştüren kodlayıcı cihazlar bulunmaktadır. İsteğe bağlı video yayını yapacak ve film içeriklerini sağlayacak olan video sunucuları, güvenliği sağlayacak olan cihazlar, her müşteri için tanımlamaların yapıldığı ve kişisel bilgilerinin tutulduğu ara yazılım ve tüm sistemin kontrolünün yapılacağı yönetim sistemi, yayın merkezi içinde bulunabilecek diğer cihazlardır [15]. Bu cihazların tümünün yayın merkezinde olması beklenmemelidir. Verilecek servislere

göre bunlardan bazıları yayın merkezine konulabilir. Yayın merkezinin genel bir yapısı Şekil 2.7'de gösterilmektedir.



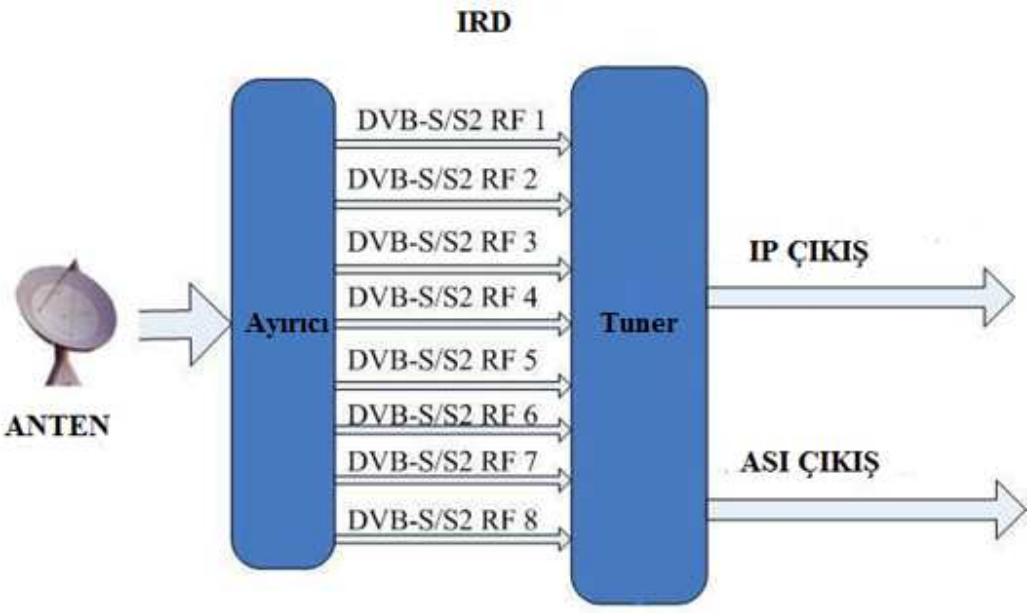
Şekil 2.7 Yayın Merkezi [15].

Yayın merkezi, uydudan veya stüdyodan alınan televizyon yayınlarını MPEG kodlama teknolojileri yardımıyla kodlar. Dolayısıyla içerik verisini sıkıştırarak bant genişliğinin azaltılması yoluyla, genişbant ağlara aktarılması görevini yerine getirir. Yayın merkezi aşağıdaki bileşenlerden oluşmaktadır.

- TV Yayını Alıcı Sistemleri (IRD, receiver)
- Kodlayıcı (Encoder)
- Ara Yazılım (Middleware)
- Güvenlik (CA/Sayısal Telif Yönetimi)
- İsteğe Bağlı Video (Video on Demand)

2.2.1. Yayın Alıcı Sistemleri

Farklı kaynaklar üzerinden gelen yayınları alan ve yayınların kodlayıcılara aktarılmasını sağlayan ekipmanlardır. Canlı TV kanalları doğrudan çanak antenden (DVB-S, DVB-S2), karasal antenden (DVB-T) veya kablodan (DVB-C) alınabilmektedir. Şekil 2.8'de yayın alıcı sistemi yer almaktadır.

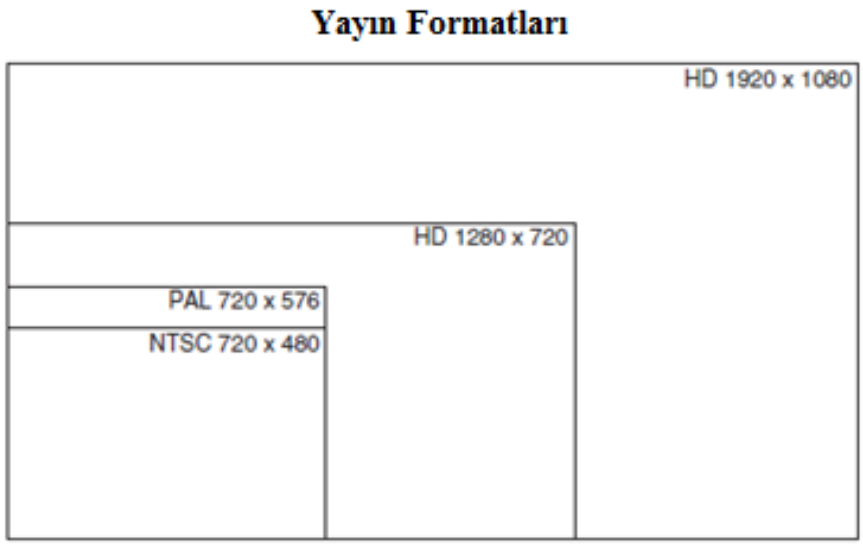


Şekil 2.8 Yayın Alıcı Sistemi.

2.2.2. Kodlayıcılar

Uydu üzerinden veya karasal olarak gelen yayınların IRD vasıtasıyla toplanmasından sonra, kodlayıcı uygun bir kodlama tekniği kullanarak yayınları sıkıştırılmış sayısal veriye dönüştürür ve IP paketleri içerisine yerleştirir. Daha sonra sayısal olarak sıkıştırılmış formatta IP paketleri içerisine yerleştirilen veriyi şebekeye gönderir. Kodlayıcılar üzerinde kodlama modülü bulunur ve genellikle her bir modül bir kanalı kodlar. MPEG-2, MPEG-4 (H.264) ve Windows Media 9 kodlayıcılar üzerinde kullanılan kodlama tekniklerinden bazılarıdır. Windows Media 9 ise Microsoft tarafından geliştirilmiş yaklaşık olarak MPEG-4 kadar bir sıkıştırma sağlayabilen formattır. Bant genişliği avantajı sağlaması nedeni ile MPEG-4 kullanımı yaygınlaşmaktadır. MPEG-4 ile H.264 aynı kodlama tekniği olup, ISO MPEG-4 ile isimlendirirken, ITU ise aynı kodlama tekniğini H.264 olarak isimlendirmektedir. Windows Media 9 ile MPEG-4/H.264 kodlama tekniklerinin

sıkıştırma oranları aynıdır [12]. Şekil 2.9'da HD ve SD formatlı yayınların karşılaştırması verilmiştir.



Şekil 2.9 HD ve SD Yayın Formatları ([26],fig.3.6'dan değiştirilerek).

MPEG-2 sıkıştırma formatıyla kodlanmış SDTV (Standart Definition TV) kanallar 4 Mbps veri hızına ihtiyaç duyarken, HDTV (High Definition TV) kanalların ihtiyaç duyduğu veri hızı ise 19 Mbps'dir. Bu video sıkıştırma formatı yerini yavaş yavaş MPEG-4'e bırakmaktadır. MPEG-4 (H.264) sıkıştırma formatıyla kodlanmış SDTV kanallar ise ortalama 1-3 Mbps veri hızına ihtiyaç duyarken, HDTV kanallar 5-6 Mbps veri hızına ihtiyaç duymaktadır [16]. Çizelge 2.2'de HD ve SD yayınlar için gerekli olan veri hızları karşılaştırmalı olarak verilmiştir.

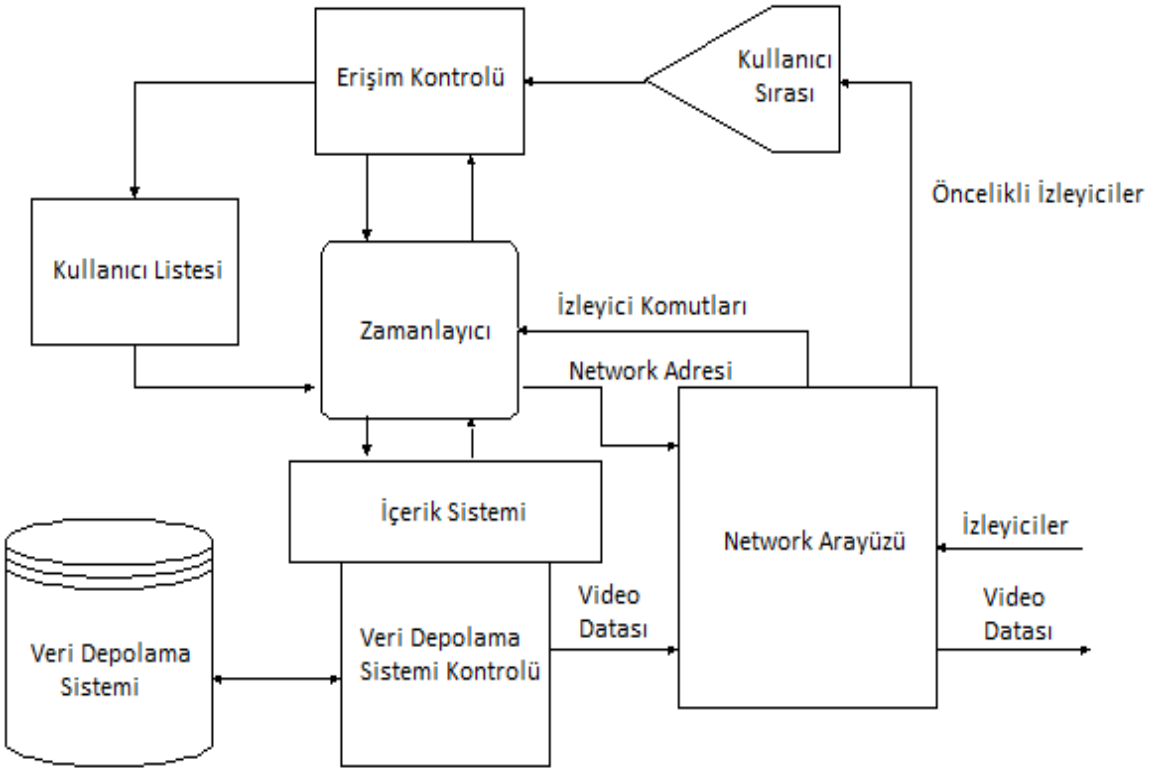
Çizelge 2.2 HD ve SD Yayınların Veri Hızları.

Format	**Çözünürlük**	**H.264 Veri Hızları**
SDTV	720x480	1-3 Mbps
HDTV	1280x720	5-6 Mbps
	1920x1080	7-9 Mbps

2.2.3. Ara Yazılım

Ara yazılım tüm IPTV servisinde birlikte çalışmayı sağlayan yazılım katmanıdır ve sistem içinde çalışan tüm cihazlara hizmet verebilecek yeteneklere sahiptir. Ara yazılım, servis sağlayıcının yönetim sistemi üzerinde müşteri oluşturulmasından, faturalama sistemi üzerinde fatura üretilmesine kadar ayrıntılı olarak sistemler arasındaki veri geçişini içeren program arayüzlerini sağlar. Ayrıca IPTV sisteminin başından sonuna kadar tüm iş akışının yürütülmesini kontrol eder.

Ara yazılım, IPTV platformu için operasyonel destek sistemi gibi düşünülebilecek bir yazılım unsurudur. Ara yazılım faturalama, kimlik doğrulaması, kullanım raporları ve abone arabirimleri gibi birçok fonksiyonu kontrol eden karmaşık bir yazılım bütünüdür. Ara yazılım hem yayın merkezinde, hem de müşteri STB'si üzerinde aktif bir rol oynar. Ayrıca ara yazılım, IPTV network elemanları arasında birlikte çalışmayı da sağlar [3]. Şekil 2.10'da IPTV hizmet için kullanılan ara yazılım blok diyagramı verilmiştir.



Şekil 2.10 Ara yazılım.

Ara yazılım uygulamaları şunları içerir:

- Müşteri yönetimi ve ücretlendirme arabirimi, yeni müşterilerin oluşturulması ve tüm müşterilerin aktivitelerinin yönetilmesi.

- Program takvimi, isteğe bağlı video ve tüm diğer IPTV uygulamalarını içeren program rehberi.

- Müşterilerin ve arabirimlerin tüm işlemlerini faturalama ve ücretleme sistemleri ile birlikte yönetilmesi.

- IPTV ağındaki aktiviteleri izleyip kaydederek kullanım raporlarını çıkartılması.

- Tüm müşterilerin başlattığı uygulamaların kontrol edilmesi.

- Şebeke güvenlik sistemi ile kimlik doğrulama sistemleri arasında birliktelik sağlanması.

- Diğer veri tabanında tutulan faturalama, vb. ilişki kurulması.

Ara yazılımın çalışmasına örnek olarak, IPTV servisini kullanan bir müşterinin ön karşılama ve uğurlama işlemleri sırasında yapılanlar aşağıda verilmiştir.

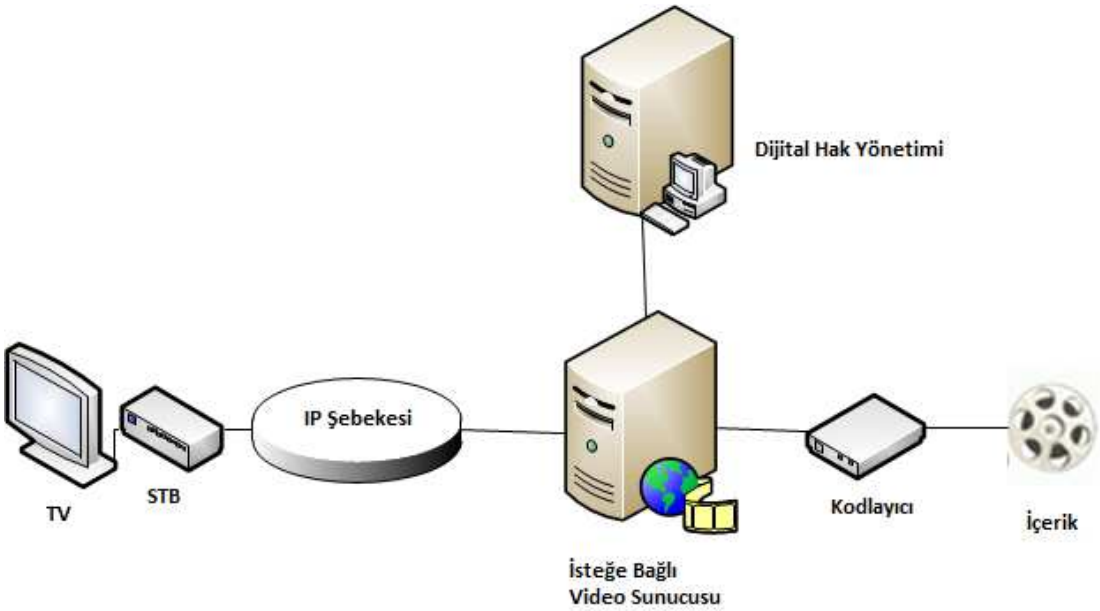
Ön Karşılamada; kullanıcı geçmişi kontrol edilerek, elektronik program rehberi, izle-öde, video kaydedebilme, isteğe bağlı video gibi servislerin ara yüzü ve ekranda bir kullanıcı ID'si oluşturulur. Ebeveyn kontrolü, müşteriye uyarlanmış kanal listesi, e-mail adresi vb. kişiselleştirme ayarları yapılır. Uğurlamada ise; isteğe bağlı video şifresi kontrol edilerek, isteğe bağlı video içeriği kataloglar halinde saklanır ve acil alarmların görünmesi ve istenen içerik için kredi yeterliliğinin doğrulanması sağlanır [3].

Ara yazılım teknik özellikleri ikiye ayrılabilir. Bunlar müşteriler için ve servis sağlayıcılar için desteklenen özelliklerdir. Standart TV yayını, izle ve öde, isteğe bağlı video, kişisel video kaydı ve elektronik program rehberi müşteriler için desteklenen özelliklerdir. Kullanıcı yazılım konfigürasyonu, uygulama programı arayüzü, kullanıcı takibi, denetim, servis yönetimi, müşteri yönetimi ve müşterinin anlık olarak talep yapabilmesi ise servis sağlayıcıları için desteklenen özelliklerdir.

2.2.4. İsteğe Bağlı Video Yönetimi

İsteğe bağlı video hizmeti, müşterinin televizyonu üzerinden istediği zaman, istediği içeriği seçip izleyebilmesine imkân vermektedir. İsteğe bağlı video servisinin temel parçaları, videoları depolayan ve erişimi sağlayan video sunucuları, müşteri ile bağlantıyı sağlayan şebeke ve son kullanıcıya ait olan set-top box'tır. Video sunuculara yüklenmiş olan videolar sıkıştırılmış ve kodlanmış bir format içerisinde iletilir. Herhangi bir video talebi durumunda kullanıcı tarafında bu formatta gelen içerik çözülerek kullanıcıya gösterilmelidir. Bir isteğe bağlı video müşterisi, seyrettiği videoyu sanki kendi video cihazından seyrediyormuş gibi ileri, geri, yayın dondurma gibi fonksiyonları yapabilmelidir [12].

Basit olarak bir isteğe bağlı video hizmetinde çeşitli kaynaklardan elde edilen içerik Şekil 2.11'de gösterildiği üzere, depolama ünitelerinde şifrelenmiş olarak saklanır. Kullanıcı tarafından istenen içerik video sunucular aracılığıyla şebeke üzerinden unicast olarak ilgili kullanıcıya ulaştırılır ve burada çözülen içerik kullanıcı televizyonu, PC vb. görüntülenir.



Şekil 2.11 İsteğe Bağlı Video Yönetimi.

Her video sunucusunun belli bir kapasitesi bulunmaktadır. Bu yüzden bir sunucu ile istenilen sayıda aboneye hizmet vermek mümkün değildir. Dolayısıyla bir sunucudan değil, paralel olarak çalışabilen ve gelen istekleri cevaplayabilecek bir

sunucu grubundan bahsetmek gerekir. Bir video sunucusu için en önemli parametre eş zamanlı istekleri karşılayabilme kapasitesidir. Örneğin bir video sunucu üzerinde 8 slot ve her bir slottaki medya kartlarının 1 Gbps bant genişliğinde eş zamanlı yayın yapabildiğini ve içeriğin de yaklaşık 2 Mbps'lik MPEG-4 (H.264) formatıyla sıkıştırıldığı varsayıldığında bu video sunucu eş zamanlı olarak yaklaşık 4000 adet kullanıcı isteğine cevap verebilir. Bu varsayım altında bir video yayın merkezine 4000'den daha fazla video isteği geliyorsa buradaki sunucu sayısı artırılmalıdır. Böyle bir durumda bir depolama ünitesine bağlı video sunucu grubundan bahsedilebilir.

Geniş bir coğrafya üzerindeki tüm abonelere tek bir merkez üzerinden hizmet vermek, hem yukarıda anlatılan sebeplerden dolayı müşteri sayısı arttıkça video sunucuları merkezde ölçeklendirmenin zor olması, hem de her video isteğinin unicast olarak müşteriye ulaştırılmasından dolayı video akışının şebekeye aşırı yük getirmesi sebebiyle pek olası değildir. Bunun yerine dağınık bir yapı tercih edilmelidir. Dağınık mimaride merkez ve uç noktalar olmak üzere iki aşamalı ya da merkez, hub ve uç servis noktaları olmak üzere üç aşamalı yapılar kurmak mümkündür.

2.3. Güvenlik

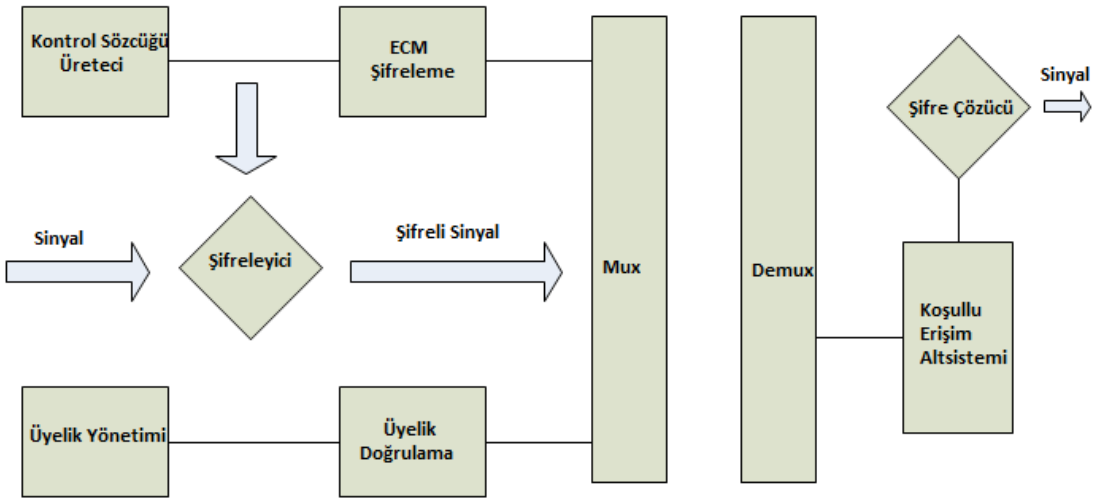
IPTV hizmetini vermek isteyen operatörlerin, ağ ortamında verilen diğer hizmetler gibi yüksek güvenlik gereksinimleri vardır. Bu gereksinimler kullanılan donanım, yazılım ve en önemlisi sunulan içeriğin korunmasıyla ilgilidir.

IPTV içeriği, diğer IP hizmetleri gibi içeriğin çalınması, kullanıcının taklit edilmesi, spam ve diğer saldırılarla karşı karşıyadır. Bunların engellenmesi ve içeriğin güvenli bir şekilde son kullanıcıya kadar iletilebilmesi için uçtan uca bir güvenlik sistemine gereksinim vardır. Burada önemli nokta, telekom operatörlerinin IPTV hizmetini sunabilmek için içeriğe ihtiyaç duyduğu ve bu içeriği sağlayıcılardan alabilmek için de yeterli bir güvenlik seviyesini elde edebilmesi gerektiğidir.

2.3.1. Koşullu Erişim

Koşullu erişim, abonelerin IPTV içeriğine erişiminin yönetilebilmesini sağlayan şifreleme/şifre çözme tekniğidir. Bu yöntem sayesinde bir abonenin gerçekten

hedeflenen kullanıcı olduğu belirlenmektedir. Ayrıca abonelerin STB üzerinde belli içeriğe erişebilmelerine olanak sağlayan koşullu erişim yöntemlerine sahiptir [7]. Şekil 2.12'de koşullu erişim yapısı gösterilmektedir.



Şekil 2.12 Koşullu Erişim Prensibi.

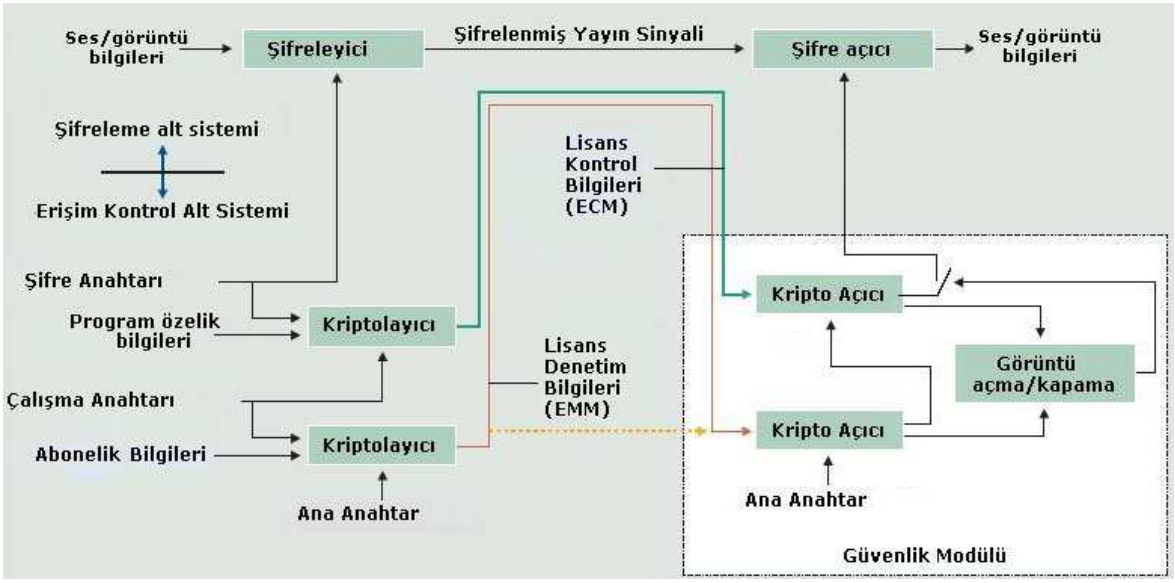
Koşullu erişim için donanım tabanlı veya yazılım tabanlı koşullu erişim olmak üzere iki yöntem kullanılmaktadır. Donanım tabanlı sistemlerde genellikle smart kart çözümleri kullanılmaktadır. Smart kart yönteminde kullanıcının kimliğini doğrulayacak bilgiler, kullanıcıya STB ile birlikte verilen elektronik devrelere yazılmıştır ve buradan okunarak doğrulanır. Yazılım temelli koşullu erişim yönteminde ise, şifreli bağlantı üzerinden kullanıcıya verilen bir kullanıcı ismi ve parola kullanılarak kimliği doğrulanmaktadır.

Esas olarak bir koşullu erişim sistemi, güvenli bir yöntemle kullanıcının yetkilerine bağlı olarak içerik sağlamayı açıp kapatmak için tasarlanan bir anahtardır. Bir DVB ortamında yayın sinyalini oluşturan dijital veri, kontrol sözcüğü olarak bilinen 8 baytlık bir güvenlik anahtarı kullanılarak iletimden hemen önce şifrelenerek okunamaz hale getirilir. Bu güvenlik anahtarı otomatik ve rastgele üretilerek sık sık değiştirilir ve tahmin edilememesi sağlanır.

Kart tabanlı bir koşullu erişim sisteminde set üstü cihazın güvenlik işlemcisi etkin rol oynar ve yayının şifresinin çözülmesi için bu kontrol sözcüklerinin değişen değerlerinin güncel tutulması gerekir. Bu işlem, STB aygıtlarına veri yayınlayarak yapılır [14]. Ancak bu veri değiştirilebildiğinden veya gizliyse anlaşılabileceğinden

dolayı korunmalıdır. Koruma işlemi, koşullu erişim sistemine özel bir şekilde gerektiği yerde mesajların imzalanması ve verinin şifrelenmesi tekniklerinin birlikte kullanılmasıyla yapılır. Bu güvenli mesajlara, yayını izlemek için STB'ye hangi yetkilerin gerektiğini bildiren fazladan bilgiler de eklenir. Sonuçta oluşan veri kümeleri, yetki denetim mesajları (ECM – Entitlement Control Messages) olarak bilinir.

Yetki yönetim mesajları (EMM – Entitlement Management Messages) olarak adlandırılan ayrık korumalı bilgi yığınları ise paralel olarak gönderilir. Bunlar STB'ye hangi yetkilerin gerektiğini söyleyen ECM'lerin tersine, STB'ye o anda hangi yetkilere sahip olduğunu söyler ve böylece hangi programların şifresiz seyredilebileceğini denetlemektedir [13]. Şekil 2.13'te gösterildiği üzere hem ECM'ler hem de EMM'ler yayın sinyalinin bir parçası olarak iletilirler ve kart tarafından işlenirler. Bu mesajları işlemek, şifreleme algoritmalarını ve anahtarlarını yönetmek için koşullu erişim kartı tarafından kullanılan mekanizmalar her koşullu erişim sistemine özel olup patentlidir.



Şekil 2.13 Geleneksel Koşullu Erişim Süreci ([42],fig.2.1'den değiştirilerek).

Yukarıda açıklanan DVB tekniğinin bir zayıflığı vardır. İçeriği okunamaz hale getirmek için kullanılan şifreleme algoritması ve karşılığı olan şifre çözücü algoritma standarttır. Başka bir deyişle şifre çözme işlevi tüm DVB STB'lerde aynıdır ve hiçbir şekilde ne koşullu erişim kartı başına ne de STB başına çeşitlendirilmemiştir. Böylece bu net ve çeşitlendirilmemiş kontrol sözcüklerinin

engellenebildiği STB'de daima fiziksel bir yer olur. Bu, standart şifre çözücüyle haberleştikleri noktadır. Bu yüzden DVB şifre çözücü algoritmanın diğer standart uygulanışlarıyla olduğu gibi yeniden kullanılabilirler ve şifrelenmiş içeriğe erişim sağlayabilirler. Bu risk geniş bandın yaygınlaşmasından önce pek önemli değilse de, bugün birçok koşullu erişim sistemi, kontrol sözcüğü paylaşımı kullanan bu tip saldırılardan dolayı risk altındadır. Böyle bir durumda üçüncü kişilerce ele geçirilen bir STB, internet üzerinden çok sayıda istenmeyen aygıta kontrol sözcüklerinin içinde bir sinyal akışı yaymak için kullanılır. Bunun için sadece yasa dışı olarak değerli içeriğe erişebilen DVB standartlı bir şifre çözücü sistemi gerekir. Ele geçirilen bu cihazın izini sürmek son derece zordur.

Bu tip koşullu erişim sürecinde savunmasızlık set üstü cihazdadır. Bir koşullu erişim sistemi için, STB donanımının koşullu erişim kartı ile şifre çözücü arasındaki arayüzünü korumada sağladığı güvenlik seviyesi, kullandığı şifreleme mekanizması ve smart kartın varlığı kadar önemlidir. Bu nedenle DVB ortamında çalışan tüm koşullu erişim sistemlerinin genel güvenliği için smart kart ile DVB şifre çözücünün devreleri arasındaki bağlantı kanalının saydam olmaması son derece önemlidir. Bu durumda kontrol sözcüklerine girilme olanağı en aza indirilmektedir. Kontrol sözcüklerinin internet üzerinden tüm dünyaya yayılması için sadece tek bir aygıta kaçak girilmesi gerektiğinden, potansiyel olarak koşullu erişim sistemini taşıyan tüm aygıtlarda bu seviyede güvenliğin % 100 garantilenmesi gerekir.

Uydu veya karasal yayın ağları gibi geleneksel TV ağları, servis sağlayıcıdan STB cihazına "tek yönlü" kanal kuran sistemler olarak tanımlanabilir [18]. STB bazen aramalı veya geniş bant bağlantıda olduğu gibi ters yönde bir geri dönüş yoluna erişebilse de, ağ işletmecileri bunun sürekli erişilebilirliğine güvenememektedir. Bu durum kablo modemle bütünleşik STB donanımı olmayan kablolu TV ağları için de geçerlidir. Bu tip ağlarda işletmeciler hizmetlerinin büyük kısmını ve işlemlerinin çoğunu STB cihazlarının tamamen geri dönüş bağlantısız olduğunu kabul ederek yapılandırmalıdır. Smart kart tabanlı yaklaşımın avantaj ve dezavantajları aşağıda sunulmuştur.

Smart kart yapısının avantajları:

- Smart kartın değiştirilebilir olması, ihtiyaç olduğunda set üstü cihazın kendisini değiştirmeden donanım ve yazılım değişikliklerine imkân vermektedir.
- Çıkarılabildiği için, piyasada yaygın satılan STB'lerde bile güvenlik donanımında kolayca değişikliklere imkân vermektedir.
- İzinsiz erişime dayanıklı tasarlanmıştır.
- Dahili etkinliklerini gizleyecek şekilde tasarlanmıştır.
- Donanım ve yazılım mimarilerinin eşsiz ve gizli yapılabilir olması şifre çözülmesini zorlaştırır.
- Çoğaltmayı zorlaştıracak şekilde tasarlanırlar.

Smart kart yapısının dezavantajları:

- Daha önce açıklanan kontrol sözcüğünün güvenlik zaafiyeti, smart kart ile STB arasındaki arabağlantı, kontrol sözcüklerinin geçtiği kanalın içerisindedir. Bu nedenle koşullu erişim sistemleri üreticilerinin tüm STB'lerde çok yüksek seviyede müdahaleye dayanıklı uygulamaları yeterli olmamakla birlikte, koşullu erişim kartı ile STB arasında yüksek güvenlik sağlayabilen haberleşmeyi de garantilemeleri gerekir.
- Smart kart üretim, dağıtım ve depolama, işletmeciye dağıtım zincirinin her noktasında sürekli uygulanması gereken sıkı güvenlik aşamaları gerekmektedir.
- Smart kartların tedarik edilmeleri işletmeciler için önemli bir maliyet getirir ve bazen işletmecilerin de smart kartların sıkı denetimini, miktarını ve yerlerini incelemeleri gerekir.
- Güvenlikte risk oluşursa koşullu erişim kartlarının değiştirilmeleri zaman alır ve maliyet getirir.
- Smart kartların sınırlı boyutları, eklenen smart kart çipinin yeteneklerini ve bu yüzden kullanılabilecek güvenlik teknolojilerini azaltır.

- Sürekli teknolojik yenilikler sayesinde en güvenli smart kartlar bile kullanılmaz hale gelip değiştirme ihtiyacı gerektirebilir.

- Smart kartlar birbirinden farklı, karşılıklı çalışma uyumu olmayan koşullu erişim sistemleri kullandıkları için abonelerin rakip işletmecilerden çok sayıda hizmet almalarını zorlaştırır. Rakip işletmeciler farklı koşullu erişim sistemlerine hitap eden iki veya daha fazla ECM/EMM akışının işletmecinin yayın sinyallerine iliştirildiği ortak bir SimulCrypt tekniği yer almaz ise, birden fazla STB veya bir DVB ortak arayüzü (DVB-CI) ile birlikte ilgili koşullu erişim birimlerini içeren STB olmak zorundadır. Bu durum ek maliyet gerektirir ve kullanıcının işletmeciler arasında geçiş yapabilmesi için koşullu erişim birimlerini değiştirmesi gerekir.

Smart kart kullanılarak sağlanan koşullu erişim, günümüzde klasik dijital uydu alıcıları ve şifreli kanal operatörleri tarafından da kullanılan yöntemdir. Burada kart üzerindeki şifrelerin çözülebilmesi durumunda koşullu erişim yöntemi başarısızlığa uğrayabilecektir.

Yazılım temelli koşullu erişim yöntemlerinde ise dışarıdan yetkisiz erişimi engelleyecek bir koşullu erişim yapısı önerilmektedir. Yayın kaynağında şifrelenerek son kullanıcı set-top box'ına gönderilen içerik smart kart kullanımı gerekmeksizin her kullanıcıya özel şifre anahtarı ile çözülerek üst düzey güvenlik sağlanmaktadır.

Yazılım tabanlı sistemlerin geleneksek smart kart tabanlı sistemlere göre avantajları;

- Koşullu erişim sistemi yapısında smart kart kullanımına ihtiyaç yoktur.

- Smart kart üretim, değişim vb. maliyetler olmadığından dolayı set-top box dizayn maliyetlerinin ucuzlamasıyla birlikte %60'a kadar daha ucuz çözümler sunulabilmektedir.

- Kullanılan şifreleme algoritmaları herhangi bir donanıma bağımlı olmadığı için güvenlik teknolojilerinde bir sınırlama yoktur.

- Koşullu erişim güncelleme veya değişim işlemlerinde herhangi bir donanım değişikliği gerektirmemektedir.

- Mevcut yöntemlerden farklı olarak kullanıcının işletmeler arasında geçiş yapması durumunda kart veya donanım birim değişikliği gerektirmemektedir.

Son yapılan araştırmalar, yeni nesil IPTV operatörlerinin yazılım temelli koşullu erişim sistemlerini tercih ettiklerini göstermektedir.

2.3.2. Kopyalamanın Engellenmesi

Daha önceden de belirtildiği gibi içeriğin yayın merkezindeyken, iletilirken veya iletildikten sonra kullanıcının elindeyken kopyalanması engellenmelidir. Yayın merkezi içerisindeyken içeriğin kopyalanması, burada alınan güvenlik önlemleriyle engellenmektedir [23]. İçeriğin aktarımdayken korunması için ise, şifreleme yöntemleri kullanılmaktadır. İçerik, kullanıcı STB cihazı üzerine geldiğindeyse, artık STB çıkışındaki analog koruma yöntemleri sayesinde korunmaktadır. Bu yöntemler tam olarak görüntünün kopyalanmasını engellememekte, ancak kopyalama sırasında elde edilen görüntünün kalitesini düşürerek değersiz hale gelmesini sağlamaktadır.

Kopyalanmanın engellenmesini sağlamanın bir diğer yolu da, kopyalama işlemine karşı caydırıcılık sağlayacak olan işaretleme (watermarking) yöntemidir. Bu yöntem sayesinde kopyalama engellenmemekte ancak kopyalanan içeriğe kullanıcısı hakkında gizli bir veri eklenmektedir. Bu sayede içeriği kimin kopyaladığı kolaylıkla belirlenebilmektedir. Bu da yetkisiz kopyalama karşısında caydırıcı bir örnek olabilmektedir.

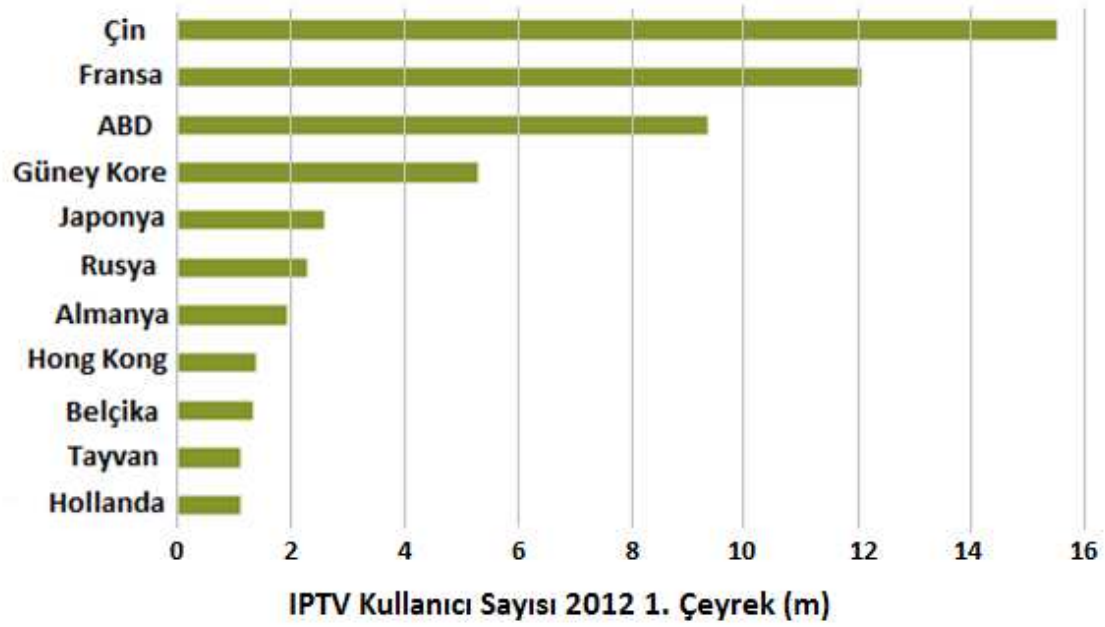
Diğer taraftan kopyalamanın engellenmesi günümüz şifreleme yöntemleri ile oluşturulan şifreleme algoritmalarıyla sağlanabilmektedir. Şifre algoritmalarıyla içerik şifrelenerek üst düzey güvenlik sağlanmaktadır. Üçüncü kişi şifrelenmiş bilgiye sahip olsa bile şifre çözülemediğinden dolayı içeriğe ulaşılamamaktadır.

3. IPTV TEKNOLOJİ ANALİZİ

3.1. IPTV Mevcut Durum

IPTV teknolojisine birçok farklı sektör ilgi duymaktadır. Telekom Operatörleri müşterilerine yeni katma değerli servisler sunmak amacındayken, içerik üreticileri yeni satış kanallarına ulaşmaya çalışmaktadır. TV yayıncıları ise müşteri

portföylerine sundukları hizmetleri çeşitlendirmeye çalışırken, birçok yeni şirket ise TV sektörüne girmek için IPTV'nin önemli bir fırsat olduğunu düşünmektedir. IPTV yayınının kullanıcıya ulaşabilmesi için gerekli bant genişliğini sağlayan DSL aboneleri arttıkça, IPTV uygulamaları da paralel olarak yaygınlaşmaktadır. 2007 yılında dünya genelinde abone sayısı 13.5 milyon civarında olan IPTV hizmetlerinden yararlanan abone sayısı 2012 yılı itibariyle 54 milyona ulaşmıştır [24]. Şekil 3.1'de 2012 birinci çeyrek itibariyle değişik ülkelere göre IPTV kullanıcı sayısı verilmiştir.



Şekil 3.1 IPTV Kullanıcı Sayısı ([24],fig.1'den değiştirilerek).

Video pazarındaki rekabet seviyesi göz önüne alındığında IPTV'nin sabit telekomünikasyon hizmeti sağlayıcılarının gelir beklentilerini kısa vadede karşılamasının zor olacağı değerlendirilmektedir. Hizmet gelirlerinin 2014 yılında ise 24 milyar dolar olması öngörülmektedir. Uzun dönem karlılık oranları için IPTV'nin stratejik bir hizmet olacağı açıktır.

Pazar araştırma şirketi Gartner'in Eylül 2010'da açıkladığı rapor 2008-2014 yılları arasındaki IPTV pazar paylarını ve gelir tahminlerini ortaya koymaktadır. Gartner tarafından yapılan araştırmalarda, Çizelge 3.1'de gösterildiği üzere 2008 yılında 19 milyon olan abone sayısının, 2014 yılında 74 milyona çıkacağı tahmin edilmektedir [5].

Çizelge 3.1 IPTV Hizmet Gelirleri 2008-2014 [5].

	2008	2009	2010	2011	2012	2013	2014	2009-2014
IPTV Abone Sayısı (Bin Kişi)	**19.266**	**27.736**	**35.721**	**44.456**	**53.569**	**63.413**	**74.124**	**21,7%**
Büyüme		44,0%	28,8%	24,5%	20,5%	18,4%	16,9%	-
Ev Penetrasyon	1,0%	1,5%	1,9%	2,3%	2,7%	3,1%	3,6%	-
IPTV Genişbant	6,4%	8,1%	9,2%	10,4%	11,6%	12,7%	13,9%	-
Kullanıcı Başına Ortalama Gelir (Aylık) ABD Doları	**23,77**	**25,89**	**26,60**	**27,50**	**28,55**	**29,41**	**30,13**	**3,1%**
Büyüme		8,9%	2,7%	3,4%	3,8%	3,0%	2,5%	-
IPTV Hizmeti Gelirleri (Milyon Dolar)	**4.411**	**7.302**	**10.128**	**13.229**	**16.791**	**20.643**	**24.691**	**27,6%**
Büyüme		65,5%	38,7%	30,6%	26,9%	22,9%	20,5%	-

Türkiye'de ise IPTV çalışmaları 2008 yılında başlamıştır. Türk Telekom'un yaptığı çalışmalar ile 2011'in başında IPTV 30 ilde hizmete girmiştir. 2010 yılı sonunda ise genişbant internet abonesi 8 milyonu aşmıştır [5]. IPTV hizmetinin verilebilmesi açısından bu rakamlar önemlidir.

Ayrıca IPTV hizmeti, içerik sağlayıcılar ve televizyon kanalları için de yeni teknolojik imkânlar doğurmaktadır. İzleyici alışkanlıklarının değişmesi televizyon kanallarını yeni arayışlara itmektedir. IPTV araştırma şirketleri tarafından duyurulan raporlara göre hizmet sağlayıcıları, şebekelerinin gelecek nesil televizyon servislerine uyumluluğu için yoğun bir çalışma içerisindedirler [25]. Kablo işletmecileri diğer telekom hizmet işletmecilerinin telefon ve internetten elde ettikleri pastadan bir pay alabilmek; telekom hizmet işletmecileri de büyük TV pazarına ortak olabilmek için gerekli yatırımları yapmaktadırlar.

3.2. IPTV ve İnternet Televizyonu Karşılaştırması

IPTV ve internet televizyonu birbirinden farklı yapılardır. IPTV, kapalı ve kişiye özel bir TV sistemini temsil etmektedir. IP tabanlı güvenlikli kanallar ile kullanıcıya sunulmaktadır. Sonuç olarak, içeriğin dağıtılmasında kontrol çok fazladır. İnternet

televizyonu ise açık bir çerçevede, birçok küçük ya da orta ölçekli pek çok sayıda video yapımcısı tarafından sunulan bir yapıdadır [26].

İnternet TV, diğer adıyla Web TV, internete bağlanılan her yerden bilgisayar aracılığı ile canlı TV yayınına ve video içeriğine erişim sağlayan bir yapıdır. Görüntü kalitesi garanti edilmemekte ve internet hızına göre kalite belirlenmektedir. İnternete açık bir sunucu üzerinden görüntü aktarılır ve kalite sunucunun ve internet bağlantısının kalitesiyle birebir ilişkilidir.

IPTV sistemleri dijital televizyon yayını ve seçimli video hizmetinin sağlanması içindir. Böyle bir uygulama hizmet sağlayıcısına aynı zamanda video, ses ve verinin sunulduğu bir ortam da sağlamaktadır. Çizelge 3.2'de IPTV ve İnternet TV karşılaştırılması yer almaktadır.

Çizelge 3.2 IPTV ve İnternet TV Karşılaştırması.

	IPTV	**Internet TV**
Kapsama Alanı	Operatörün kapsama bölgesi	Dünya geneli
Kullanıcılar	IP adresi ve yeri belli bilinen müşteriler	Genellikle bilinmeyen herhangi kullanıcı
Görüntü Kalitesi	Yayın (broadcast) TV kalitesi, Yüksek QoS	Şartlara bağlı kalite, QoS garantisi yok
Bağlantı Bant Genişliği	1 – 4 Mbit/s	Genellikle 1Mbit/s nin altında
Görüntü Formatı	MPEG-2, MPEG-4 Part 2, MPEG-4 Part 10 (AVC), Microsoft VC-1	Windows Media, RealNetworks, Quick Time Flash, …..
Alıcı Cihaz	Set Üstü Kutusu (STB) eklenmiş TV	PC
Çözünürlük	Tam TV ekranı (Full TV display)	QCIF/CIF
Güvenlik	Kullanıcılar yetkilendirilmiş ve korunmuştur	Güvenli değil
Telif	Telif hakları gözetilmektedir	Genellikle telif ödenmemiştir
Diğer Servisler	EPG, PVR	
Müşteri İlişkileri	Desteklenmektedir	Genellikle destek yoktur
Kablo, Uydu ve Karasal Yayınlarla Bütünleşme	Potansiyel olarak ortak STB kullanmak mümkündür	Ön izleme ve talebe bağlı düşük kaliteli hizmetler

3.3. Maliyet

Günümüzde IPTV hizmeti vermek isteyen bir kuruluş, talep yönünden, arz yönünden ve müşteriyle hizmet sağlayıcı arasındaki ilişki yönünden farklı koşullarla karşı karşıya olacaktır.

Talep açısından bakıldığında, çevrim içi İnternet TV'nin yaygınlaşması, sınırlı bir kesim için olsa bile televizyon izleme alışkanlıklarını değiştirmiştir. Bir yandan etkileşimli televizyon hizmetlerine ilişkin talep artarken, bir yandan da televizyon başında geçirilen süre azalmaktadır. IPTV hizmeti verecek bir firma bu iki koşulu da lehine kullanacak bir iş modeli geliştirmelidir.

Arz tarafında ise frekans bandının az bulunan bir kaynak olması artık yayıncılık sektörü için en önemli sorun olmaktan çıkacaktır. Geleneksel yayıncılıkta, tüm TV kanalları birlikte ve gerçek zamanlı olarak izleyiciye ulaştırılmaktadır. IPTV hizmetlerinde ise DSL sınırlı bant genişliği nedeniyle herhangi bir anda alıcıya sadece tek bir TV kanalı ulaştırılabilir.

Geleneksel bir yayıncı, 24 saatlik yayın üretir ve geleneksel yayıncılık teknolojilerinde 24 saat boyunca bütün TV kanallarını kullanıcıya ulaştırır. Ortalama bir kullanıcının günde 3-5 saat boyunca televizyon izlediği varsayılırsa, talep miktarına bakılmaksızın arz sabit kalmaktadır [25]. Oysa IPTV'de sadece talep edilen veri iletilmektedir.

Bu yapının bir uzantısı olarak IPTV, kullanıcılarla hizmet sunucular arasındaki ilişkiyi de değiştirmektedir. Yayıncılık sektöründe gün geçtikçe kullanıcının hareket alanı artacağı değerlendirilmektedir. İçerik türlerinin gün içinde nasıl yerleştirileceği geleneksel bir yayıncının elindeki en büyük silahlardan ve farklılaştırma unsurlarından birisidir. Ancak artık kullanıcı herhangi bir içeriğe günün istediği saatinde ulaşmaktadır. Dolayısıyla izlenme oranının en yüksek olduğu zamanlarda yayınlanacak bir içeriğe yüksek ücretle reklam yerleştirmek artık kullanılabilir bir gelir modeli olmaktan çıkacaktır [27].

Kullanıcı doğrusal televizyon yayınlarından başka bir içeriğe ulaşmayı tercih etmese bile, içeriği etkileyerek doğrusal reklamlardan kurtulmak artık daha kolay olacaktır. Kullanıcılar, gönderilen içeriği izlemek ve seçmek dışında kendi içeriklerini oluşturarak da IPTV değer zinciri ile etkileşime girebilirler. IPTV hizmeti verecek bir kuruluş, kullanıcıya sağlanacak bu imkânları bir tehdit olarak değil kendisi için de bir imkân olarak görmeli ve ona göre bir iş modeli tasarlamalıdır.

IPTV söz konusu olduğunda değer zincirine yeni halkalar da katılmaktadır. Frekans bandı kısıtlaması ortadan kalktığı için daha çeşitli içerik arz ve talep

edilecektir. Piyasada çok sayıda ufak içerik üreticisinin oluşması durumunda, ana görevi bu içerikleri bir araya getirmek olan işletmeler doğabilir. İçerik birleştirme faaliyeti, belirli bir kaliteye ya da belirli bir konuya spor, sanat, teknoloji, mesleki eğitim vb. odaklanmayı garanti etmektedir.

İçerik oluşturanlar, içerik birleştiriciler ve doğrusal yayınlar gibi çeşitli kaynaklardan alınan içerik paketlenerek, IP üzerinden iletilecek hale gelir. Bu aşamada sayısal olmayan görüntüler için sayısal dönüşüm yapılır. İçerikler etiketlenir ve IPTV sistemine uygun standart veriler haline getirilir. Daha sonra bu veriler, çoklu gönderimle iletilecek doğrusal yayın olarak ya da tek yönlü gönderimle iletilecek video verisi olarak depolanır. Sunucularda depolanan veri IP ağlarıyla kullanıcıya ulaştırılır [24].

Yayın merkezi ve dağıtım ağının kurulması için yapılan altyapı yatırımı en büyük maliyet kalemidir. Dağıtım ağıyla beraber set üstü kutular, kullanıcı başına maliyeti arttıran unsurlardır. Düzenli içerik temin edilmesi ve altyapının bakımı, işletimi iş modelinin değişken maliyetleridir. En büyük maliyet kalemi kullanıcı başına sabit maliyettir.

3.4. Adreslenebilir Reklamcılık ve Sayısal Telif Yönetimi

Analog içerikten sayısal içeriğe doğru yaşanan geçiş, teknolojiden pazarlamaya, içerik oluşturmadan, küresel dağıtıma kadar pazarın her aşamasını etkilemektedir. Teknolojik gelişimler ve teknolojiyi yönlendiren yeni yatırımlar, yeni içerik formlarının ortaya çıkarılmasını ve yeni gelişmiş medya deneyimlerini yaşanmasını sağlamaktadır.

Adreslenebilir reklamcılık kişiye özgü reklamcılığın yapılmasına dayanmaktadır. Bu sayede bir reklam kampanyasının başarı derecesi de rahatlıkla ölçülebilmektedir. Kullanıcının IPTV'sini açmasıyla birlikte, IPTV sistemi, kayıtlı kullanıcılar arasından kendi ismini seçmek isteyip istemediğini sorabilir. Kullanıcının kayıtlı kullanıcılar arasından kendi ismini seçmesiyle kullanıcı daha önceden oluşturduğu kendi tercihlerini ve profilini seçmiş olur. Tercih etmiş olduğu reklamlar, mesajlar, e-postalar, program kılavuzları, favori kanalları vb. çok çeşitli seçenekler yer almaktadır [29]. IPTV'nin sağladığı etkileşimle birlikte verilere

anında ulaşılarak analiz imkânı bulunmakta ve tüketicinin eğilimine yönelik etkin reklamcılık hizmetleri oluşturulabilmektedir.

Adreslenebilir reklamcılık sayesinde, klasik yayıncılık ve reklamcılık anlayışıyla yapılan reklamcılıkta elde edilen gelirlerin 10 ila 100 katına kadar daha fazla gelirin elde edilmesi mümkün olabilir. Belirli müşterilere, belirli sayıda reklamın gönderilmesiyle de reklam şirketleri, sabit bir reklam harcaması planı yapabilir. Adreslenebilir reklamcılık, aynı coğrafyada olmalarına rağmen, kullanıcılara farklı reklamların sunulmasına da imkân sağlamaktadır [23].

Sayısal telif yönetimi ise sayısal veri (yazılım, müzik, video vb.) ve donanıma erişim için daha önceden belirlenmiş kuralların uygulanması için kullanılan teknolojilerin genel ismidir. Daha teknik bir tanımlama yapılırsa sayısal telif yönetimi, sayısal bir emeğin kullanım kısıtlamalarına ait tanımlama, katmanlama, analiz, değerleme, ticaret, izleme ve uygulama gibi işlemleri ele alır.

Sayısal telif yönetimi ilk olarak müzik alanında ortaya çıkmıştır. Aslında sayısal telif yönetimi de bir koşullu erişim çözümüdür. Sayısal telif yönetimi, dosyaların sadece belli koşullar sağlandığında indirilebilmesine izin verir.

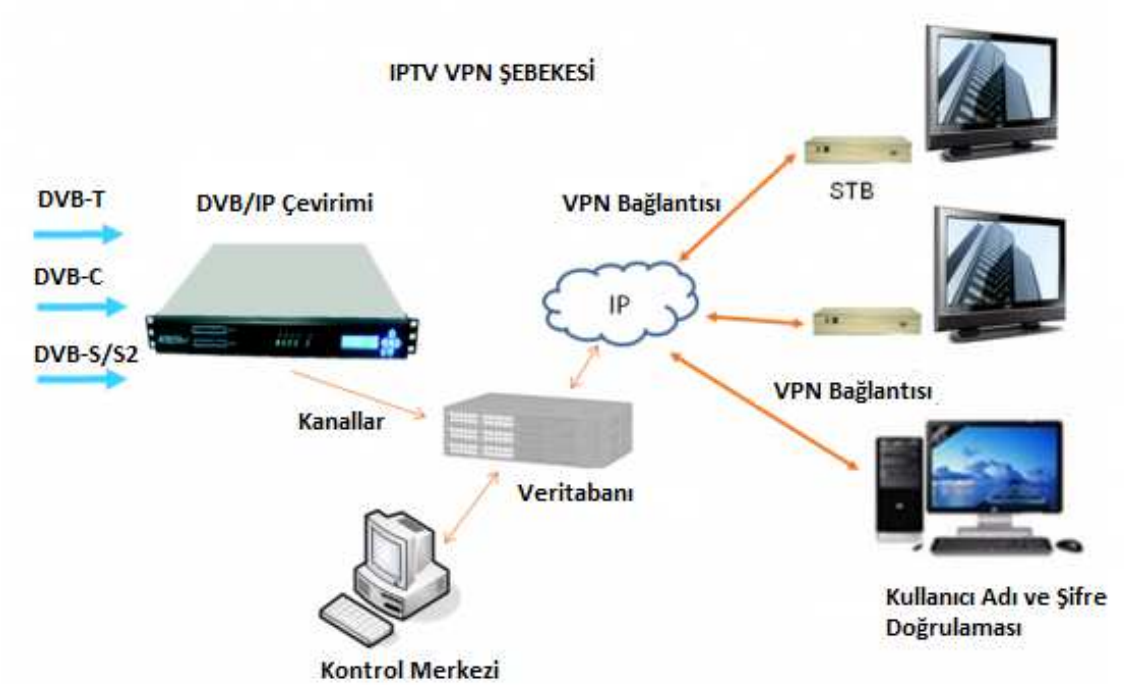
Sayısal telif yönetimi kavramını IPTV için ele alınırsa, içeriğin sadece istenen müşterilere iletildiğinden ve hiçbir şekilde kopyalanıp çoğaltılmadığının garanti edilmesi şeklinde tanımlanabilir. Ayrıca konu içerik sağlayıcının bakış açısından değerlendirildiğinde, operatöre verilen içeriğin belirlenen sayıdaki müşteriye dağıtılması ve içeriğin belirlenen süre zarfında müşteriye sunulması gibi konuların garanti edilmesi de sayısal telif yönetimi kapsamında ele alınabilir.

4. KOŞULLU ERİŞİM SİSTEMİ TASARIMI

4.1. Tasarım Bilgileri

Günümüzde IPTV uygulamaları dünya genelinde hızlı bir şekilde artmakta ve sistemin kurulumundan son kullanıcıya iletimine kadar çok büyük güvenlik gereksinimi ortaya çıkmaktadır. Bu tez kapsamında IPTV alanında standart uygulamaların haricinde geleneksel koşullu erişim sistemlerinden farklı olarak yazılımsal tabanlı, CI kart modüle vb. cihazlar kullanılmadan VPN şifreleme tekniği

kullanılarak güvenlik düzeyi en üst seviyede olacak şekilde, her kullanıcıya ID ve şifre verilmesi suretiyle IPTV sisteminin gerçekleştirilmesi amaçlanmıştır. Şekil 4.1'de IPTV VPN bağlantı şeması gösterilmiştir.



Şekil 4.1 IPTV VPN Bağlantı Mimarisi.

Bu amaçla yayın merkezi tarafında uydu üzerinden alınan kanallar IRD vasıtasıyla çözülerek her kanala bir IP atanması suretiyle multicast akış verileri elde edilmiştir. Multicast akış verileri yayın merkezinde toplanarak, kapsüller halinde udp formatında IPTV ağı üzerinden iletilmeye hazır hale getirilmektedir.

Yayın merkezindeki veri tabanındaki IPTV ağı içerisindeki tüm kullanıcıların bilgileri şifrelenerek saklanmaktadır. Son kullanıcının sürekli olarak veri tabanı bigileri güncel tutularak hangi paketlere üye olduğu, fatura bilgileri, izleme alışkanlıkları vb. bilgileri anlık olarak tutulmaktadır. Bunun yanında son kullanıcı tarafından gelen isteğe bağlı video talepleri veya farklı paketlere geçiş talepleri veri tabanına aktarılmakta ve kullanıcı istekleri alınarak yönlendirilmesi yapılmaktadır.

IPTV ağının yayın merkezi tarafı ve son kullanıcı arasında güvenli bir şekilde iletişim kurarak içeriğin korunması, VPN şifreleme tekniği vasıtasıyla gerçekleştirilmektedir. Yayın merkezindeki son kullanıcıya iletilecek canlı yayın multicast akış verileri veya isteğe bağlı videolar, VPN şifreleme tekniği ile koruma altına alınarak son kullanıcıya iletimi sağlanmaktadır. IPTV ağında her kullanıcının

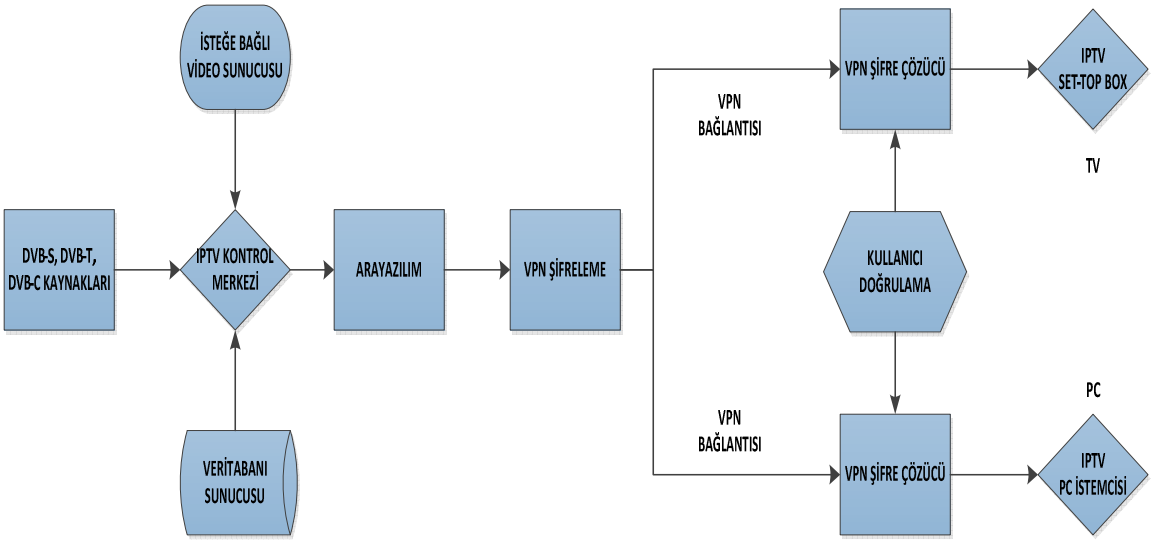
IPTV kullanıcı yazılımının kurulu olduğu cihazın fiziksel adresi (MAC) adresine özgü sabit bir kullanıcı adı ve şifre verilmektedir. Son kullanıcının geçerli bir VPN bağlantı imkânı olsa dahi IPTV yayın merkezi ile iletişim ancak eşleşmiş MAC adresi, kullanıcı adresi ve şifre ile mümkün olabilmektedir.

IPTV ile sunulan içeriğin VPN ile şifrelenerek yayın merkezi tarafından kişiye özel verilen VPN ID ve şifresi ile bağlantıya imkân tanınmaktadır. Bu şekilde VPN şifreleme tekniği ile gönderilen içerik korunmuş olmakta, son kullanıcı dışında yetkisiz kişilerce içeriğe erişim engellenmektedir.

Son kullanıcı tarafında IPTV PC kullanıcı yazılımı oluşturulmuştur. Bu yazılım ile son kullanıcı için IPTV hizmeti verilmektedir. İstemci yazılımında kişinin üye olduğu paket kapsamında izleyebileceği kanallar ve isteğe bağlı videoların gösterimi yapılmaktadır. Bunun yanında yeni paketlere üyelik başvurusu ve isteğe bağlı video talepleri bu yazılım üzerindeki sekmeler yardımıyla yapılabilmektedir.

4.2. Geliştirme Platformu

IPTV geliştirme platformu tüm içerik sistemini yöneten ve işleten tek nokta olma özelliğini taşımaktadır. Ses/görüntü sinyallerini DVD kalitesinde LAN ve WAN üzerine aktarabilen bir platformdur. Şekil 4.2'de tez kapsamında oluşturulan IPTV platformu tasarım aşamaları gösterilmektedir.



Şekil 4.2 IPTV Tasarım Aşamaları.

Geliştirme platformunda H.264 kodlama tekniği, bitrate desteği, şifreli ve şifresiz SD ve HD kanal içerik iletimi özellikleri yer almaktadır.

4.2.1. IPTV Yayın Akış Sistemi

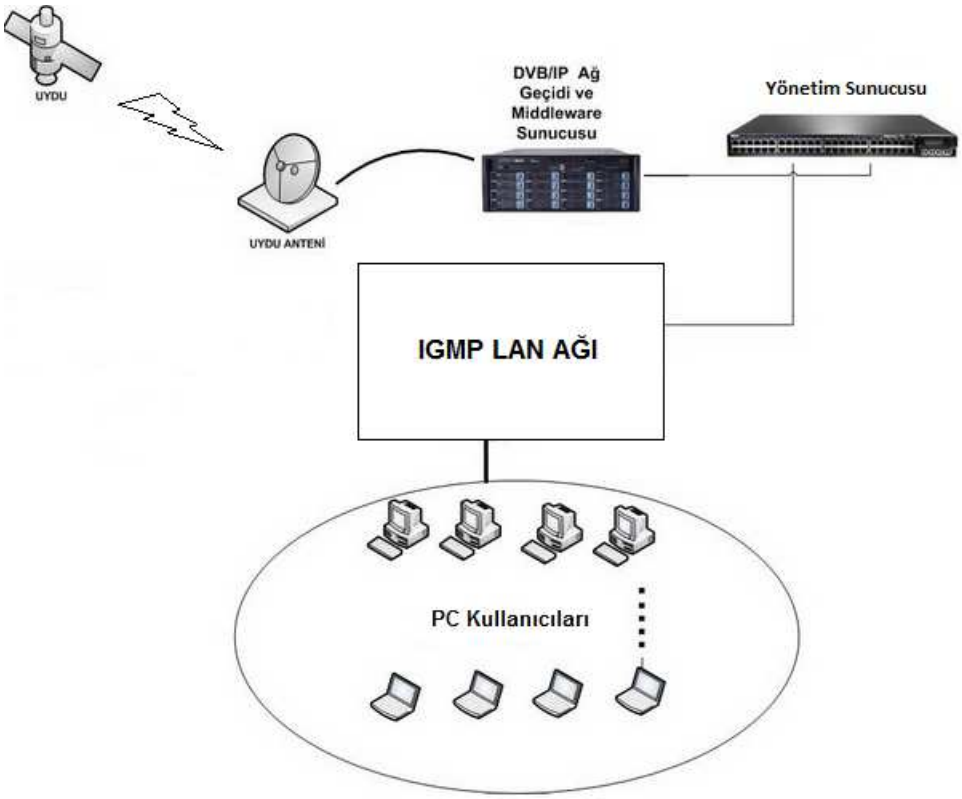
TV kanalları ve videolar çeşitli kaynaklardan alınarak yayın merkezinde kodlama işleminden sonra IP paketlerine dönüştürülmektedir. IP protokolü LAN, internet ya da WAN gibi IP tabanlı ağ üzerinden video ve ses taşınmasına imkân vermektedir. Video ve ses kaynakları ağ üzerinden PC'lere ya da set-top box aracılığıyla TV'lere aktarılır [30].

IPTV kaynak verilerinin iletiminde uygun kodlama teknikleri kullanılmaktadır. IPTV için kullanılan görüntü sıkıştırma formatları MPEG-2, H.264, WMV (Windows Media Video 9 ve VC1), XviD, DivX, ve Ogg bulunmaktadır [16]. Tez kapsamında video kodlaması H.264 sıkıştırma formatında yapılmaktadır. Video akışı VLC sunucusuyla iletilmektedir. IP akış verilerinin iletimi iki farklı metotla gerçekleştirilmektedir.

IPTV multicast ya da unicast yapıda olabilir. Unicast, paketin tek bir hedefe gönderilmesini sağlar. Sınıf A, B ve C IP hedef adreslerini kullanır ve noktadan noktaya bağlantıyı tanımlar. Her bir bağlantı ayrı bant genişliği kullanır. Multicast ise paketin farklı alt ağlar üzerinde yer alan, fakat bir multicast grup üyesi olarak tanımlanmış kullanıcılara gönderilmesini sağlar. Sınıf D grup adres formatı ile tek noktadan çok noktaya bağlantıya olanak sağlar. Çoğullama, istek yapana en yakın noktada yapılır [9].

Multicast bir akış verisi için bant genişliği anlamında en efektif kullanımı sağlar. Bu tür bir yayında aynı kaynak çok sayıda kullanıcı tarafından datarate düşürülmeden erişilebilir. Örneğin bir video akışı 2 Mbps ise düzgün bir ağ yapılandırmasıyla kullanıcı sayısı artsa da 2 Mbps tüketir. Bu şekilde dağıtım yükü kullanıcılar arasında paylaştırılabilmektedir. Unicast de ise 100 kişi tarafından farklı zamanlarda erişim sağlandığı düşünüldüğünde, ayrı ayrı aktarım yapılacağından 100x2=200 Mbps datarate gerekecektir. IPTV uygulamalarında veri trafiği yükü, internet veya LAN bağlantıları için tasarlanmış normal veri şebekelerinden çok daha fazla olduğu düşünüldüğünde multicast yapının kullanılması önem arz etmektedir.

Son kullanıcı tarafı ile DSL ağı arasında kullanılacak olan multicast grup üyelik protokolü IGMP olarak tanımlanır. PIM-SM–IP/MPLS omurgada yer alacak bileşenler için kullanılacak olan multicast routing protokolüdür [31]. Şekil 4.3'te IPTV omurga erişim yapısı gösterilmiştir.



Şekil 4.3 IPTV Omurga Erişim Yapısı.

Kaliteli bir IPTV şebekesinin olması için veri geliş ve gidiş hızlarının birbirine eşit olması istenir. Geliş hızından kasıt video dosyası açılmak istendiği andaki sunucu bilgisayarının bu video paketlerini gönderdiği hızdır. Aksi takdirde sunucu bize saniyede 512 Kbps'lık bilgi gönderirken bizim internete bağlanma hızımız 256 Kbps ise bu durumda video geliş hızımız 256 Kbps demektir. Video gidiş hızı olarak kastettiğimiz ise video akış dosyasının hangi veri hızında dönüştürüldüğüdür. Eğer izlediğimiz dosya 512 Kbps hızında akış formatına dönüştürülmüşse, video oynatıcı program saniyede 512 KB'lık paketleri işler. Geliş ve gidiş hızı birbirine eşit ise bir problem çıkmamaktadır.

IPTV video akışı oluşturmak için VLC oynatıcı yazılımında yer alan akış özellikleri kullanılmaktadır [43]. Çizelge 4.1'de örnek bir sunucu kaynağının son kullanıcıya iletilecek şekilde akış işleminin gerçekleştirilmesi detaylarıyla açıklanmıştır.

Çizelge 4.1 Ağ Akışı Adımları.

	İşlem Sırası	**Açıklamalar**
Adım 1	**Ağ Akışı Açma;** Medya>Ağ Akışı	Akış protokolü olarak udp seçilir ve adres olarak multicast grubundan bir kanalın ip adresi atanır. Örnek multicast ip adres: udp://225.1.2:5003.
Adım 2	**Kaynak IP Girişi;** Ağ Akışı>Akış	Akış listesine eklenecek verinin kaynak IP adresi girilmektedir.
Adım 3	**Kapsülleme;** Profil>Kapsülleme	Kapsülleme işlemi yapılacak videonun çözünürlüğü, yayınının iletilme durumundaki veri hızı ayarlanabilmektedir. Bu çalışmada kapsülleme aralığını verimli kullanmak için MPEG4 seçilmiştir.
Adım 4	**Video Kodlama;** Profil>Görüntü Kodeği	Kaynak olarak eklenen verinin kodlama yapısı, bit hızı, kare hızı ve görüntünün en boy oranları ayarlanarak istenilen çözünürlükte verilebilmektedir. VLC oynatıcıda kodlama verimini artırmak için H.264 seçilmiştir.
Adım 5	**Ses Kodlama;** Profil>Ses Kodeği	Görüntü özellikleri belirlenen akışın ses kodeği sekmesi kullanılarak ses iletim özellikleri belirlenmektedir. Çalışma kapsamında MPEG 4 ses kodeği ve 128 kb/s bit hızı kullanılmıştır.

IP şebekeleri için UDP (User Datagram Protocol - Kullanıcı Veribloğu İletişim Kuralları) dizayn edilmiştir. Bu protokol unicast ve multicast dağıtım yapabilen, aynı zamanda TCP (Transmission Control Protocol - İletişim Denetim Protokolü) protokollerini destekleyen, ayrıca internet üzerinden ses ve görüntü yayınlarının yapılmasını sağlayan bir protokoldür. İletimi yapılacak görüntü ve ses bileşeni UDP formatında akış olarak iletilmeye hazır hale getirilir [26].

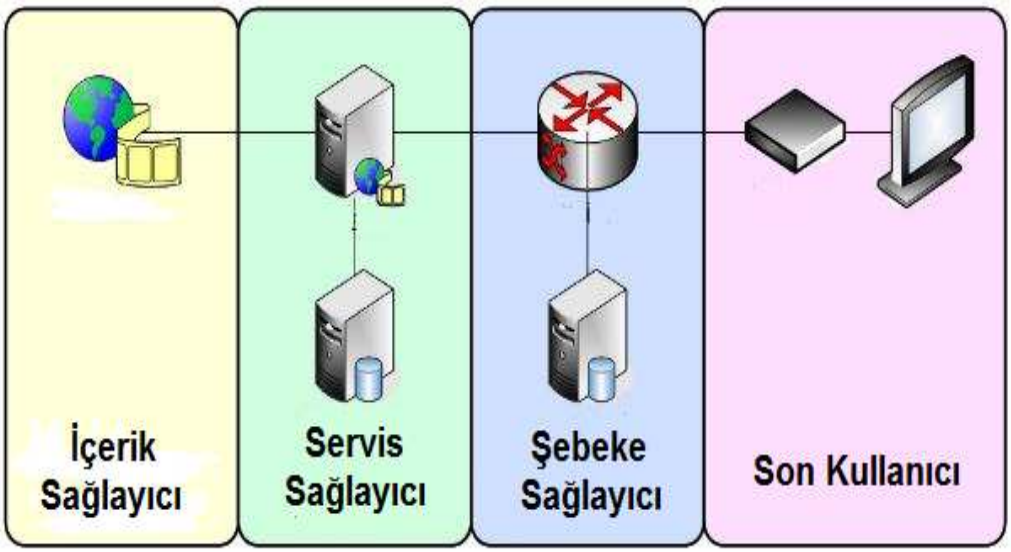
Geniş alan ağlarında ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımlarında UDP kullanılır. UDP'yi kullanan protokollerden bazıları DNS, TFTP, ve SNMP protokolleridir.

İsteğe bağlı video akış işlemi iki ayrı bölümde gerçekleşir: Birincisi video dosyalarını doğru formatta oluşturmak, ikincisi ise bu dosyaları bir video sunucusundan akış edecek şekilde düzenlemektir.

Video içeriğinin aynen multicast video gibi önceden kodlanması gerekir. Günümüzde birçok firmanın yazılım kodlayıcıları, çoğu formattaki MPG, AVI, MOV vb. videoları kolayca sıkıştırarak H.264'e dönüştürebilmektedir. Video içeriğinin unicast şekilde iletimesinden dolayı, hizmet verilmesi sırasında ortaya çıkacak gerekli bant genişliği sunucu grupları kullanılarak karşılanmaktadır.

4.2.2. Kullanım Bilgileri ve Çalışma Şekli

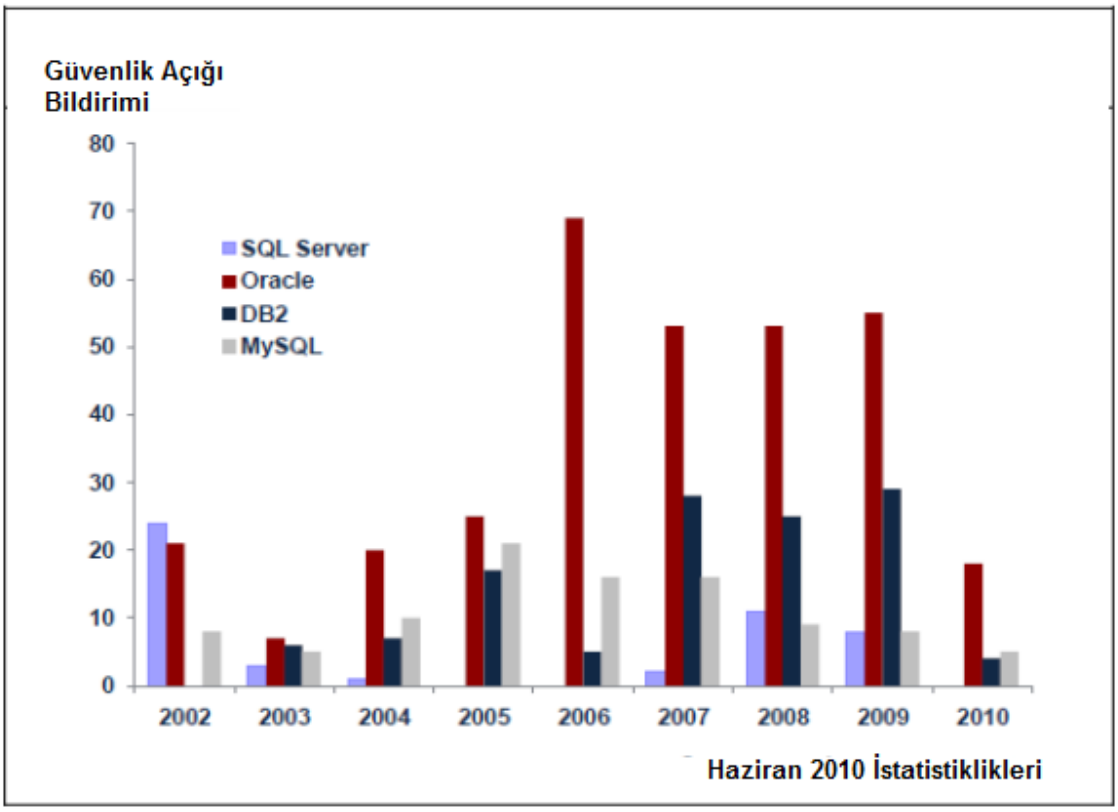
IPTV sisteminde son kullanıcının ilgisini çekecek içeriğin belirlenmesi ve temin edilmesi şarttır. Bahsedilen içeriğin son kullanıcıya kaliteli ve görsel olarak zengin bir şekilde iletilebilmesini destekleyecek bir altyapıya sahip olunması gereklidir. Bunun yanında son kullanıcının kesintisiz ve kaliteli bir hizmet alabilmesi için platformda yer alan içeriğin güvenliğinin sağlanarak omurga ve erişim altyapısında gerekli iyileştirmelerin yapılması önem arz etmektedir. Hizmetin sunumunda kullanıcı dostu ve basit arayüzler kullanılması gerekmektedir. Şekil 4.4'de IPTV hizmetinin sunum aşamaları gösterilmektedir.



Şekil 4.4 IPTV Hizmet Sunumu.

4.2.3. Yayın Merkezi Veritabanı

Bu çalışma kapsamında oluşturulan veritabanı Microsoft SQL 2008 R2 plaformu kullanılarak hazırlanmıştır. Şekil 4.5'de gösterildiği üzere Birleşik Amerika'da teknoloji, tedarikçi ve ürün bazında güvenlik kırılganlıklarını takip eden bağımsız bir kamu kurumu olan National Institute of Standards and Technology NIST'in, Haziran 2010 döneminde veritabanı teknolojisi üzerinde yaptığı istatistikler doğrultusunda SQL Server en güvenli veri tabanından biri olarak ortaya çıkmaktadır [32]. SQL Server 2008 R2, SQL Server 2008'e ek olarak ana veri birimleri ve hiyerarşi yönetimi sağlayan "Master Data Services" olarak adı geçen yeni bir ana veri yönetim sistemine sahiptir. Ayrıca çoklu SQL Server oluşumlarını yönetmeye yarayan çoklu sunucu yönetimi, raporlama servisi, analiz ve integrasyon servisleri ve excel eklenen yeni özellikler arasındadır.



Şekil 4.5 Veritabanı Güvenlik Karşılaştırması ([32],fig.1'den değiştirilerek).

IPTV yayın merkezi için oluşturulan veri tabanında kullanıcıların üyelik, şifre, paket kullanımı ve fatura bilgileri saklanmaktadır. Bu işlem veri tabanında oluşturulan abone yönetim sistemi ile son kullanıcı aktivitelerini entegre eden müşteri servisleri

ile gerçekleştirilmektedir. Diğer taraftan isteğe bağlı video arşivi, kullanıcı izleme alışkanlıkları istatiksel verileri veri tabanı aracılığıyla tutulmaktadır.

Veri tabanı üzerindeki bu bilgilerin güncellenmesi, belirli komutlarla çağrılması ara yazılım kullanılarak gerçekleştirilmektedir. Ara yazılım kullanıcıdan taleplerin alındığı ve veri tabanına iletildiği platformdur. Aynı şekilde veri tabanında yer alan kullanıcıya gönderilecek bilgiler ara yazılım aracılığıyla iletilmektedir. Ara yazılım ve veri tabanı arasındaki bu döngü kod etkileşimleri ve işleyişi bölümünde detaylı olarak verilmiştir.

4.2.4. Veritabanı MD 5 Şifreleme Yapısı

Sistem veri tabanında kullanıcı bilgilerinin güvenliğinin sağlanması amacıyla MD5 şifreleme tekniği kullanılmaktadır. MD5 (Message Digest algorithm 5), MD4 üzerine geliştirilmiş hash algoritmasına dayalı bir fonksiyondur. 128 bit'lik çıktı üreten ve tek yönlü bir şifreleme sistemi olan MD5 fonksiyonu transfer edilmiş bilgilerin doğru ve eksiksiz bir şekilde yerine ulaşıp ulaşmadığının kontrol edilmesinde ve public-key şifrelemesinde kullanılır.

Tez kapsamında oluşturulan veri tabanında tanımlanan her aboneye bir ID verilmiştir. Bu ID'ler emsalsiz yapıda tanımlanmıştır. Kullanıcı ID'leri veri tabanında saklanırken MD5 şifreleme tekniği kullanılarak kullanıcı bilgilerinin güvenliğinin üst düzeye çıkarılması sağlanmıştır.

Matematiksel bir model üzerine kurulan MD5′in kırılamazlığı, input olarak aldığı değerin uzunluğuyla orantılıdır. Özellikle veri tabanı işlemlerinde kullanıcılara ait özel bilgilerin MD5 ile şifrelenerek tutulması yaygındır. Bu veriler kötü niyetli kişiler tarafından çalınsa bile geri döndürülemediği için ciddi bir tehlike oluşturmamaktadır. Aşağıda MD5 şifreleme algoritmasının bu çalışmada seçilmesinin nedenleri sunulmuştur.

- MD5 algoritması tek yönlü çalışmaktadır. Şifreleme yapar, ancak şifre çözüm işlemi yapılamaz.

- MD5 algoritması, üzerinde işlem yapılan dosyada aktarma vb. herhangi bir değişiklik olup olmadığını tespit etmektedir. Eğer bir değişiklik yapılmışsa, yeni

dosyanın MD5 algoritmasından çıkan sonuç ile ilk dosyanın MD5 sonucu birbirinden farklı olmaktadır.

- MD5 algoritması bir alt sürümü olan MD4'e göre yavaş çalışmakta, ancak şifrelendirme sistemi çok daha karışık ve çözülmesi güçtür.

- Algoritmanın en önemli kısmı sıkıştırma fonksiyonunun olduğu kısımdır. Eş. 4.1 - 4.4'de gösterilen (F-G-H-I) genel olarak 4 farklı aşamalı bir sisteme sahiptir. Her aşama birbirinden farklı işleyişe sahip olup 16'şar basamaktan oluşmuştur. Bir MD5 şifreleme işleminde Şekil 4.6'daki algoritmadan 64 tane gerçekleşmektedir [33]. Bu kadar işlemin gerçekleşmesinin sebebi simetriliği engelleme isteğinden doğmaktadır.

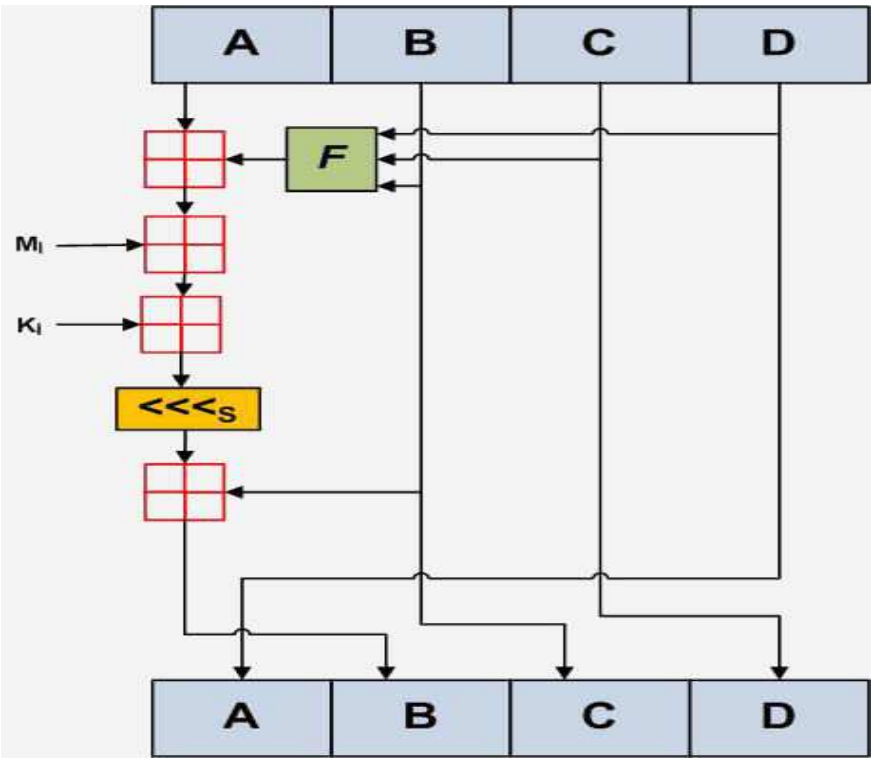
$$F(X, Y, Z) = (X \wedge Y) \vee (\neg X \wedge Z) \quad (4.1)$$

$$G(X, Y, Z) = (X \wedge Z) \vee (Y \wedge \neg Z) \quad (4.2)$$

$$H(X, Y, Z) = (X \oplus Y \oplus Z) \quad (4.3)$$

$$I(X, Y, Z) = Y \oplus (X \vee \neg Z) \quad (4.4)$$

$\oplus$, $\wedge$, $\vee$, $\neg$: Sırasıyla XOR, AND, OR ve NOT işlemlerini temsil etmektedir.



Şekil 4.6 MD5 Şifreleme Yapısı [33].

Başlangıçta değerleri sabit olan, A,B,C,D diye adlandırılan 32 bitlik dört değişken bulunur. Bu değişkenlerin değerleri her 512 bitlik blok işleme girdiğinde değişir ve algoritma sonunda değerler yan yana geldiğinde 128 bitlik şifrelenmiş veri elde edilir. Bütünlük denetiminde ve güvenli şifre saklama sistemlerinde kullanılmaktadır. .NET teknolojisi ile yazılım geliştirilmesi durumunda herhangi bir veride şifreleme yapmak için .NET Framework içerisinde yer alan "System.Security.Cryptography" kütüphanesi kullanılmalıdır. Bu kütüphane içerisinde yer alan fonksiyonlar sayesinde, yazılımcı istediği platformda güvenli bir şekilde veri şifreleme ve şifre çözümleme yapabilmektedir. Yazılım geliştiricinin MD5 algoritmasını kullanarak şifreleme yapabilmesi için "MD5CryptoServiceProvider" sınıfını kullanması gerekmektedir.

Veri tabanında string şeklinde girilen veri, "System.Text.UnicodeEncoding" kütüphanesi yardımıyla UTF-16 karakter sınıfından oluşan bir diziye çevrilmektedir. Yeni oluşan dizinin MD5 hash değeri, "System.Security.Cryptography.MD5CryptoServiceProvide" yardımıyla elde edilir. Elde edilen MD5 hash değeri bir bit dizisi olduğundan string hale döndürülmesi gerekmektedir. Bu işlem de "System.BitConverter.ToString(hash)" yardımıyla yapılır. Çizelge 4.2'de MD5 şifresinin hash fonksiyonu verilmiştir.

Çizelge 4.2 MD5 Şifre Örneği.

Şifre	**MD5 Hash**
1234	81dc9bdb52d04dc20036dbd8313ed055

Microsoft .NET framework'te MD5, kendisi gibi soyut bir sınıf olan "HashAlgoritm" sınıfından türeyen MD5 sınıfı ile tanımlanmıştır. "MD5CryptoServiceProvider" MD5 algoritmasını gerçekleyen sınıftır. Microsoft .NET framework'te, MD5 algoritması için hash boyutu 128 bittir. "MD5CryptoServiceProvider" sınıfı MD5 soyut sınıfından türemektedir. MD5 soyut sınıfının erişilebilir özellikleri şu şekilde tanımlanır;

- CanReuseTransform, şu an ki dönüşümün tekrar kullanılıp kullanılmayacağını belirtir, varsayılan değeri true'dur.

- CanTransformMultipleBlocks, aynı anda bir çok veri bloğunun dönüştürülüp dönüştürülemeyeceğini belirtir, varsayılan değeri true'dur.
- Hash, hesaplanan hash değerini verir.
- HashSize, hesaplanan hash değerinin bit olarak büyüklüğünü gösterir. Varsayılan değeri 128 bittir.
- InputBlockSize, kullanılan veri bloğunun bit olarak büyüklüğünü gösterir. Varsayılan değeri 1 bittir.
- OutputBlockSize, algoritma sonunda oluşacak veri bloğunun bit olarak büyüklüğünü gösterir. Varsayılan değeri 1 bittir. Bu sınıfın erişilebilir metotları ise şunlardır;
- Clear, MD5 algoritması tarafından kullanılan kaynakları sisteme geri yükler.
- ComputeHash, kullanılan veri bloğu için hash değerini hesaplar.
- Create, MD5 algoritmasını gerçekleştirecek bir nesne üretir.
- Equals, iki nesnenin birbirine eşit olup olmadığını kontrol eder.
- GetHashCode, bellekteki o nesneye özgü bir hash kodu üretir.
- GetType, bu nesnenin tipini verir.
- Initialize, MD5 nesnesinin ilk değerlerini ayarlar.
- ToString, şu an ki nesneyi ifade eden bir metin oluşturur.
- TransformBlock, belirtilen veri bloğundaki alan için hash değerini hesaplar ve belirtilen sonuç veri bloğunun belirtilen alanına hesaplanan bu hash değerini kopyalar.
- TransformFinalBlock, belirtilen byte dizisindeki alan için hash değerini hesaplar.

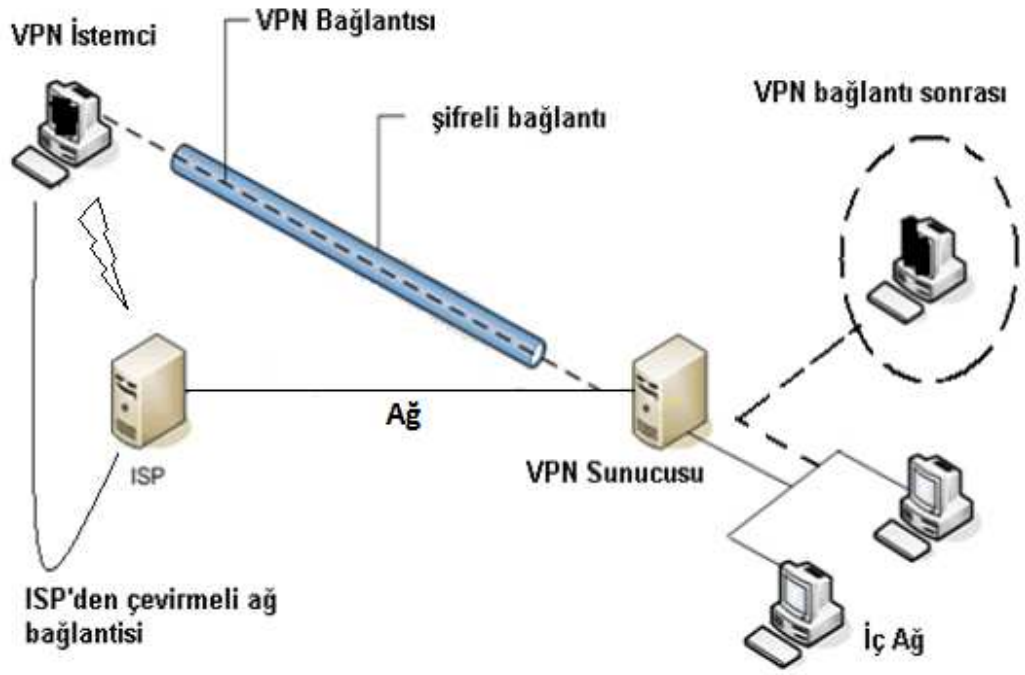
4.2.5. Koşullu Erişim ve VPN

VPN (Virtual Private Network) ağa bağlı olan kullanıcıların, yazılım veya donanım desteği ile güvenli bilgi alışverişine olanak veren uygulamaların genel adıdır. Bu

çalışma kapsamında oluşturulan IPTV yayın merkezi ve son kullanıcı arasında içeriğin şifrelenmesi VPN şifreleme tekniği kullanılarak gerçekleştirilmiştir.

VPN'in en geniş kullanım alanı ise, filtrelenen içeriğe erişim sağlanmasıdır. Güvenlik duvarları ve web filtrelerini aşarak, kısıtlanan noktalara ulaşma imkânı sağlamaktadır. VPN, komşu ağlar arasında gizli ve özel bir bilgi akışını sağlamaya yönelik kurulur. İnternet gibi halka açık telekomünikasyon altyapılarını kullanarak, kullanıcıları uzak ortamdaki yerel bilgisayar ağına güvenli bir şekilde eriştirmeyi sağlamak için geliştirilmiş sanal bilgisayar ağı yapısıdır. Güvenli veri taşıma, yetkilendirme, şifreleme yoluyla bilgi aktarımı ve üçüncü şahısların aktarılan bilgiye erişimini engelleme gibi özelliklere sahiptir.

VPN, aynı özel ağda bulunmayan bir veya daha fazla network cihazı arasında güvenli bir şifreleme metodu kullanılarak kapsüllenmiş veri transferi yapmaktadır. Güvenli şifreleme metodunun kullanım amacı verinin özel ya da kamusal alandaki diğer network cihazlarından gizlenmesidir. Bu yapı genel olarak, uzak noktadaki kullanıcılar için noktadan noktaya hatlar yerine standart bağlantılar üzerinden daha düşük sahip olma maliyetleri ile aynı hizmeti sağlar. Bu şekilde kullanıcıya sanki fiziksel olarak yerel ağ içerisindeymiş gibi çalışma imkânı sağlamaktadır. Şekil 4.7'de VPN bağlantı yapısı gösterilmiştir.



Şekil 4.7 VPN Bağlantı Yapısı.

Güvenli bir VPN bağlantısı gönderici kimlik doğrulaması yoluyla kimlik taklidine engel olma ve yollanan ağ mesajlarının değiştirilmesini engelleme gibi yöntemlerde tutarlılık sağlamalıdır. Güvenli bir VPN bağlantısında kimlik doğrulama işlemini zorunludur. Kullanıcıların erişimi için oluşturulan VPN bağlantı yapılarında kullanıcı adı, şifre, biyometrik doğrulama ve diğer kriptolama teknikleri kullanılabilmektedir.

Ağdan ağa kurulan VPN bağlantılarında erişim, şifreler veya dijital sertifikalar gibi sunucuda sabit halde durmakta olan bilgilerin çift yönlü doğrulaması ile mümkün olabilmektedir. Gelişmiş VPN uygulamaları, sertifika geçerliliği, kullanıcı adı ve parolası yöntemlerini bir arada kullanmaktadır.

VPN herkese açık ağda oluşturulan bir tünelleme tekniğidir. Bu amaçla kullanılan tünelleme protokolleri vardır. L2TP tünelleme protokolü Cisco'nun ürünü olan L2F ile Microsoft'un PPTP protokolünün birlikteliğinden doğmuştur. Microsoft hem PPTP'yi, hem de L2TP'yi de günümüzde desteklemektedir. Cisco'nun GRE tünelleme protokolü ise daha çok IPX, CLNP gibi ve diğer IP olmayan paketleri IP içinden taşımak için kullanılan bir tünelleme tekniğidir. L2TP ve GRE tek başına bir şifreleme yapmaz ve verinin bütünlüğünü garanti etmemektedir. Ayrıca sağladıkları tüneldeki veri monitör edilebilir. Bu eksiklikler her iki tünelllemenin üzerinde ayrıca IPSec kullanılması ile kapatılmıştır [36]. PPTP, L2TP/IPsec ve SSTP kullanan VPN bağlantıları aşağıdaki özelliklere sahiptir:

- Kapsülleme
- Kimlik doğrulama
- Veri şifreleme

Kapsülleme: VPN teknolojisinde özel veriler, geçiş ağını çapraz şekilde geçmelerine izin verecek yönlendirme bilgilerini içeren bir üstbilgiyle kapsüllenmektedir.

Kimlik doğrulama: VPN bağlantılarında kimlik doğrulama üç farklı biçimde yapılır;

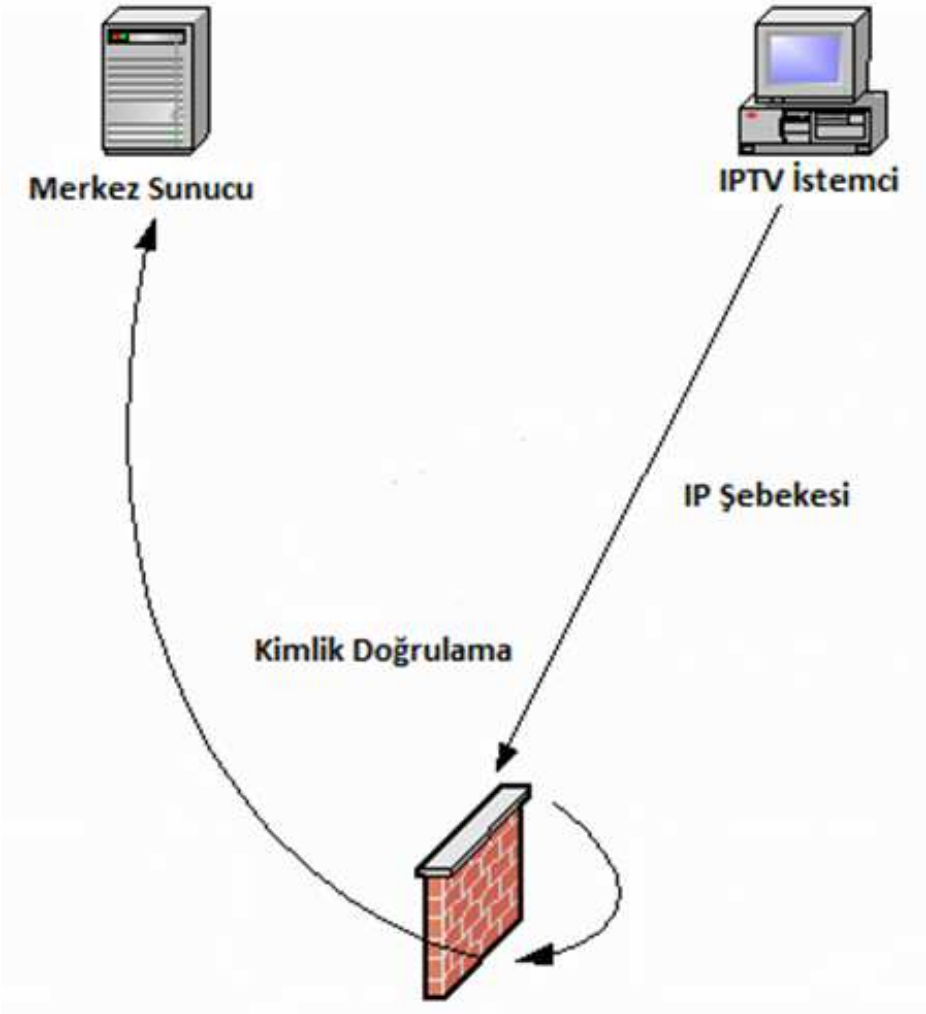
- PPP kimlik doğrulama kullanılarak kullanıcı düzeyinde kimlik doğrulama: VPN bağlantısı oluşturmak için, VPN sunucusu bağlanmayı deneyen VPN istemcisinin

kimliğini, Noktadan Noktaya Protokolü (PPP) kullanıcı düzeyinde kimlik doğrulama yöntemi ile doğrular ve VPN istemcisinin uygun yetkilendirmeye sahip olduğunu onaylar. Karşılıklı kimlik doğrulama kullanılırsa, VPN istemcisi de VPN sunucusunun kimliğini doğrular. Bu şekilde kendilerini VPN sunucuları gibi tanıtan bilgisayarlara karşı koruma sağlanır.

- İnternet Anahtar Değişimi (IKE) kullanarak bilgisayar düzeyinde kimlik doğrulama: İnternet protokolü güvenliği (IPsec) güvenlik ilişkisi oluşturmak üzere VPN istemcisi ve VPN sunucusu, bilgisayar sertifikaları veya önceden paylaşılan bir anahtar değişimi için IKE protokolünü kullanır. Her iki durumda da VPN istemcisi ve sunucusu, birbirlerinin kimliklerini bilgisayar düzeyinde doğrular. Bilgisayar sertifikası kimlik doğrulaması çok daha güçlü bir kimlik doğrulama yöntemi olduğundan daha fazla önerilmektedir. Bilgisayar düzeyinde kimlik doğrulama yalnızca L2TP/IPsec bağlantıları için uygulanır.

Veri kaynağı için kimlik doğrulama ve veri bütünlüğü: VPN bağlantısı üzerinden gönderilen verinin, bağlantının diğer ucundan gönderilmiş olduğunu ve aktarım sırasında değiştirilmediğini onaylamak için veride yalnızca gönderenin ve alanın bildiği bir şifreleme anahtarına dayalı şifreleme sağlama toplamı bulunur. Veri kaynağı için kimlik doğrulama ve veri bütünlüğü yalnızca L2TP/IPsec bağlantılarında kullanılabilir.

IPSec, internet üzerinden veri taşınması işleminde; tünelleme, şifreleme ve kimlik doğrulama için kullanılan standart bir güvenlik protokolüdür. IPSec protokolü herkes tarafından ortak kullanılabilen bir protokoldür. Network seviyesinde çalıştığı için uygulamadan bağımsız olarak her veriyi şifreler ve şifre sonrası oluşturduğu başlık ile verinin internette yolculuk edebilmesi sağlanır. Bu yüzden de günümüzde VPN teknolojisinin altyapısını oluşturmaktadır [26]. Şekil 4.8’de VPN kimlik doğrulaması gösterilmiştir.



Şekil 4.8 VPN Kimlik Doğrulaması.

Veri şifreleme: Veriler, paylaşılan veya ortak geçiş ağından geçerken gizliliğinin sağlanması amacıyla gönderen tarafından şifrelenir ve alıcı tarafından çözülür. Şifreleme ve şifre çözme işlemleri gönderenin ve alanın ortak kullandığı bir şifreleme anahtarına bağlıdır.

VPN bağlantısı üzerinden geçiş ağında gönderilen paketler ele geçirildiğinde, ortak şifreleme anahtarı olmadan üçüncü kişiler için bir anlam ifade etmemektedir. Şifreleme anahtarının uzunluğu çok önemli bir güvenlik parametresidir.

Kriptolama amaçlı olan şifreleme algoritmaları simetrik ve asimetrik olarak ikiye ayrılabilmektedir. Aynı anahtarla şifrelenen veri yine aynı anahtarla açılabiliyorsa simetrik bir şifreleme algoritması kullanılıyor demektir. Buna örnek AES, DES, 3DES, Idea, Blowfish, RC2, RC4 verilebilir [38]. Veri, alıcı tarafından eğer ancak

bir başka anahtarla açılabiliyor ise bu durumda asimetrik bir algoritma kullanılmış demektir. Burada bir çift anahtar kullanılır. Buna örnek RSA, DH (Diffie-Hellman) verilebilir.

Şifreleme algoritması, anahtarı kendi fonksiyonuna katarak hem fonksiyonun özelleştirilmesi sağlanır hem de bu anahtara bağımlı olan fonksiyondan geçirilen veriler karşıya güvenli şekilde iletilir. Alıcı taraf simetrik anahtarı kullanır ve içindeki veriye ulaşır. AES şifreleme standardı bu alanda en çok kullanılan yöntemlerden biridir. AES (Advanced Encryption Standard; Gelişmiş Şifreleme Standardı), elektronik verinin şifrelenmesi için sunulan bir standarttır. AES, Değiştirme-Karıştırma olarak bilinen tasarım temeline dayanır.

AES'in hem yazılım hem de donanım performansı yüksektir. 128'lik girdi bloğu, 128, 192 ve 256 bit anahtar uzunluğuna sahiptir. AES'in temel alındığı Rijndael ise 128-256 bit arasında 32'nin katı olan girdi blok uzunluklarını ve 128 bitten büyük anahtar uzunluklarını desteklemektedir. Dolayısıyla, standartlaşma sürecinde anahtar ve girdi blok uzunluklarında kısıtlamaya gidilmiştir.

AES, durum denilen 4x4 sütun öncelikli bayt matrisi üzerinde çalışmaktadır. Matristeki işlemler de özel bir sonlu cisim üzerinde yapılmaktadır. Algoritma belirli sayıda tekrar eden girdi açık metni, çıktı şifreli metne dönüştüren özdeş dönüşüm çevirimlerinden oluşmaktadır. Her çevirim, son çevirim hariç dört adımdan oluşmaktadır. Şifreli metni çözmek için bu çevirimler ters sıra ile uygulanır. Çizelge 4.3'te gösterildiği üzere çevirimlerin tekrar sayıları 128-bit, 192-bit ve 256-bit anahtar uzunlukları için sırası ile 10, 12 ve 14'tür.

Çizelge 4.3 Tur Sayısının Anahtar Uzunluğuna Göre Değişimi.

	Kelime Uzunluğu	**Tur Sayısı**
AES-128	4	10
AES-192	6	12
AES-256	8	14

VPN algoritması aşağıdaki sıra ile oluşturulmaktadır:

Anahtar Oluştur: Esas anahtar kullanılarak algoritmada kullanılacak çevirim anahtarları oluşturulur.

İlk çevirim:

1. *Anahtar Ekle:* Durum, ilk çevirim anahtarı ile XOR'lanır.

Diğer çevirimler:

1. *Bayt Değiştir*: Durum matrisindeki her bayt bir tabloya göre ve doğrusal olmayan bir dönüşümle güncellenir.
2. *Satır Kaydır:* Her satır belirli bir sayıda çembersel olarak kaydırılır.
3. *Sütun Karıştır:* Her bir sütundaki dört bayt, birbirleri ile karıştırılır. Bu adımda her sütundaki dört bayt değeri tersi olan doğrusal bir dönüşüm kullanılarak birbirleriyle karıştırılır. SütunKarıştır fonksiyonu 4 bayt girdi alıp 4 bayt çıktı verir ve girdideki her baytın çıktıdaki her bayt değerini etkilemesini sağlar. SütunKarıştır işlemi, her sütunun sabit bir matrisle çarpılması işleminden oluşur. Bu sabit matris Eş. 4.5'te verilmiştir:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}. \tag{4.5}$$

4. *Anahtar Ekle*

Son Çevirim:

1. *Bayt Değiştir*
2. *Satır Kaydır*
3. *Anahtar Ekle*

32 ya da daha büyük kelime uzunluğuna sahip sistemlerde "BaytDeğiştir" ve "SatırKaydır" adımlarını "SütunKarıştır" adımı ile birleştirip bir tablo oluşturarak hızlanma sağlamak mümkündür. Bu işlem, toplam 4 KiloBayt (4069 bayt) hafıza kullanan 32-bitlik 256 girdili dört tablo gerektirir. Bu iyileştirme sayesinde her

çevirim 16 tablo okuması ve 12 32-bit XOR işlemini takip eden “AhahtarEkle”, 4 32-bit XOR adımı ile gerçekleştirilebilir.

Hedef platformun 4 kilobaytlık tabloların gömülmesine izin vermediği durumlarda ise tek bir tablo kullanılabilir. Bu durumda 32-bitlik 256 girdisi olan bir tablo (1 kilobayt) oluşturulur ve tablodaki değerler çembersel kaydırma yardımıyla çevirimlerde kullanılabilir. Ayrıca bayt tabanlı bir yaklaşımla da “BaytDeğiştir”, “SatırKaydır” ve “SütunKarıştır” adımları tek bir adımda birleştirilebilir [35].

Kriptografların bakış açısından bir algoritmanın kriptografik olarak kırılması, anahtarın ya da anahtarın bazı parçalarının olası tüm anahtarların denendiği kaba kuvvet saldırısından daha hızlı bir şekilde elde edilmesi anlamına gelir. Bu açıdan, 256-bit anahtar uzunluğuna sahip AES algoritması için 2^{200} işlem gerektiren bir saldırı algoritmanın kırılması olarak kabul edilirken, 2^{200} mertebesindeki bir işlem, şu an için evrenin yaşından daha uzun bir süre gerektirmektedir.

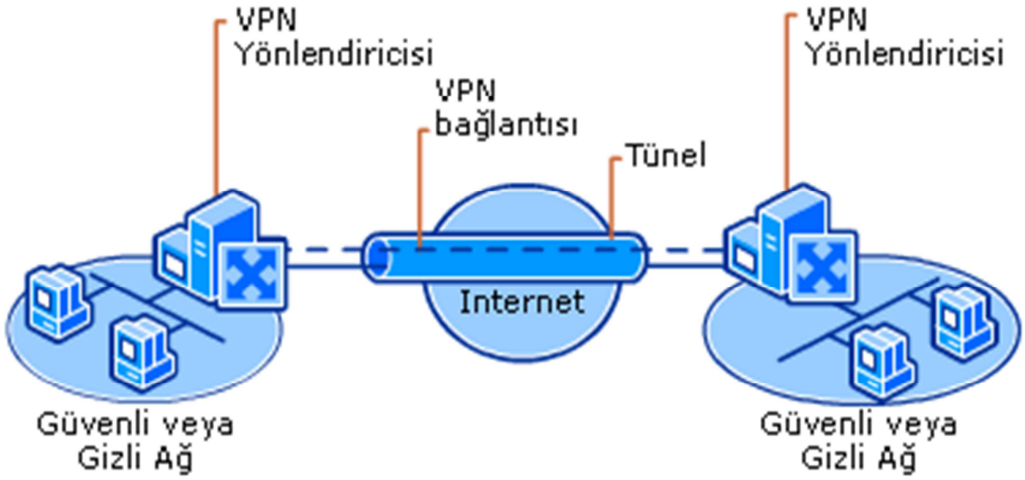
İki tür VPN bağlantısı kullanılmaktadır:

- Uzaktan erişim VPN
- Siteden siteye VPN

Uzaktan erişim VPN: Uzaktan erişim VPN bağlantıları, uzak kullanıcıların internet gibi ortak bir ağ tarafından sağlanan altyapıyı kullanarak özel ağ üzerindeki bir sunucuya erişmelerine olanak verir. Kullanıcı açısından bakıldığında VPN, VPN istemcisi ile kuruluşun sunucusu arasında noktadan noktaya bir bağlantıdır. Mantıksal olarak veriler, adanmış bir özel ağ üzerinden gönderiliyormuş gibi göründüğünden paylaşılan veya ortak ağın gerçek altyapısı önemli değildir.

Siteden siteye VPN: Siteden siteye VPN bağlantıları yönlendiriciden yönlendiriciye VPN bağlantıları olarak da bilinir. Kuruluşların farklı noktalar arasında veya diğer kuruluşlarla ortak bir ağ üzerinden yönlendirilmiş bağlantılar kullanabilmelerine olanak verirken, iletişim güvenliğinin sağlanmasına da yardımcı olur. İnternet üzerinden yönlendirilmiş VPN bağlantısı, mantıksal olarak adanmış geniş alan ağı bağlantısı gibi çalışır. Şekil 4.9’da gösterildiği gibi, ağlar internet üzerinden bağlandıklarında bir yönlendirici, paketleri VPN bağlantısı üzerinde başka bir

yönlendiriciye iletir. Yönlendiriciler açısından VPN bağlantıları veri bağlantısı katmanı olarak işlev görür [39].



Şekil 4.9 VPN Bağlantı Şeması.

Siteden siteye VPN bağlantısı özel bir ağın iki bölümünü birbirine bağlar. VPN sunucusu, bağlı bulunduğu ağa yönlendirilmiş bağlantı sağlar. VPN sunucusu, VPN istemcisi kimliğini doğrular ve karşılıklı kimlik doğrulama amacıyla sunucu da istemcinin kimliğini doğrular.

IPTV yayın merkezinde oluşturulan içerikler şifreleme sunucularından geçirilerek şifrelenir. Şifreli olarak taşınması gereken kanallar, IP paketleri, IP/MPLS omurga üzerinden multicast iletim tekniğiyle IPsec protokolü kullanılan VPN bağlantısı üzerinden son kullanıcıya kesintisiz bir şekilde iletilmektedir.

Yukarıda açıklanan şekilde IP paketleri şifrelenir ve hedefte aynı algoritmalar yardımıyla şifrelenen paket açılmaktadır. Veri paketi hedefe ulaştığında şifrelenen veri paketi açılır ve kullanılabilir hale getirilir. Çeşitli matematiksel algoritmalar kullanılarak gönderilen veri paketine bir numara verilir. Daha sonra veri paketi hedefe ulaştığında aynı algoritma kullanılarak verilen numara tespit edilmeye çalışılır. Gönderilen veri paketi ağ üzerinde herhangi bir değişikliğe ve veri kaybına uğramışsa numara farklı olacağından veri paketi kabul edilmemektedir.

IPTV içeriğinin VPN yöntemi ile şifrelenerek son kullanıcıya ulaştırılması, üçüncü kişilerin yetkisiz erişimini engellemiş olmaktadır. Geleneksel şifreleme yöntemleri ile karşılaştırıldığında yazılımsal olarak tasarlandığı için decoder ve smart kart

çözümlerine gerek kalmamaktadır. Bu tür harici donanımlar kullanılmadan daha uygun maliyetli ve kullanımı kolay koşullu erişim metodu ile üst düzey güvenlik sağlanmaktadır.

Sonuç olarak VPN verilerinin gizliliğini, bütünlüğünü ve kimden geldiğinden emin olunmasını sağlar. VPN ile her lokasyon, diğer lokasyonlarla arasındaki bağlantıyı internet üzerinden kesintisiz ve yüksek hızla gerçekleştirir.

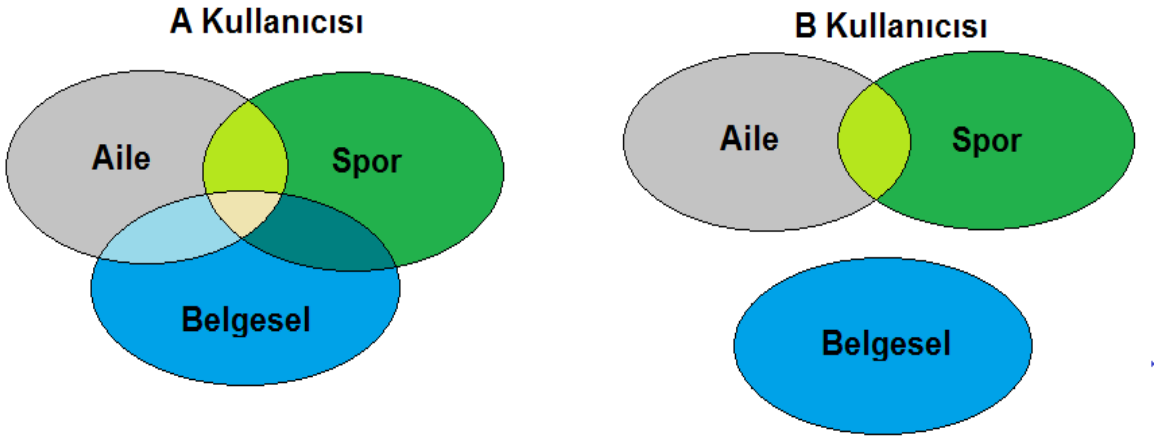
4.2.6. IPTV PC Kullanıcı Yazılımı

IPTV PC kullanıcı yazılımı IPTV hizmetine erişim için gerekli olup, bilgisayar kullanılarak IPTV kompleksine tüm interaktif hizmetleri sağlamak üzere geliştirilmiştir. Sadece canlı TV kanallarının izlenmesine olanak sağlamaz, aynı zamanda talep üzerine video, EPG ve diğer interaktif servislerden faydalanılmasına da imkân vermektedir. Şekil 4.10'da IPTV PC kullanıcı yazılımı verilmiştir. Kullanıcı arayüzü sade bir şekilde tasarlanmıştır ve seyredilmek istenen TV kanalı arayüz kullanılarak seçilebilmektedir.

Şekil 4.10 IPTV PC Kullanıcı Yazılımı.

IPTV kullanıcı yazılımında kullanıcı istek taleplerinin iletilebildiği sekme ile kullanıcı taleplerinin karşılanması mümkündür. Kullanıcının talep ettiği içerik, video veya

farklı bir kanal talebinin hızlı bir şekilde IPTV yönetim merkezine ulaştırılması sağlanmaktadır. Şekil 4.11'de A ve B IPTV son kullanıcıların tercihleri verilmiştir.

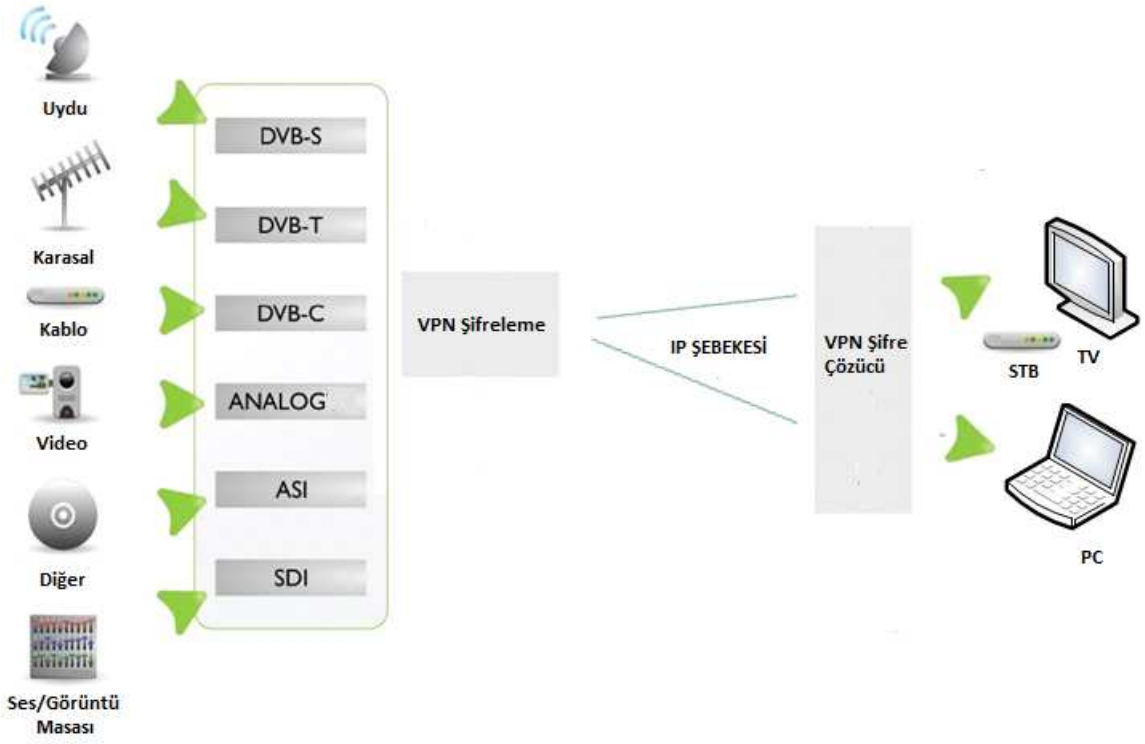


Şekil 4.11 Kullanıcı Tercihleri.

IPTV kullanıcı yazılımı C#.NET üzerinde yazılmış olup IPTV veritabanıyla birebir uyumlu çalışmaktadır. Bu yönüyle çift yönlü bir iletim sağlayarak kullanıcı tercihlerinin anlık olarak alınarak karşılanabilmesi sağlanır. Geliştirilen yazılım PC üzerinde çalıştırılarak bütün test süreçleri IPTV kullanıcı yazılımı üzerinde başarıyla gerçekleştirilmiştir.

4.2.7. IPTV Set-top Box

IPTV'nin teknolojik yapısı gereği etkileşimli olması ve kişiselleştirmeye müsait olması da ayrı bir değerdir. IPTV STB'leri kullanıcı hesabı oluşturacak şekilde tasarlanabilir. Bu sayede aynı STB, aynı evde yaşayan birden fazla kişi için kişiselleştirilmiş etkileşimli televizyon deneyimi sağlayabilmektedir. Televizyonu açan kişi önce kendi kullanıcı hesabını seçebilir. Bu sayede kişinin daha önce girilmiş bilgilerine ve önceki televizyon izleme alışkanlıklarına göre içerik önerilmesi ya da reklam gönderilmesi söz konusu olabilmektedir. Tez kapsamında IPTV set-top box tasarımı yapılmış, set-top box için gerekli yazılım hazırlanarak STB'ye uygulanmak üzere hazır hale getirilmiştir. Şekil 4.12'de IPTV set-top box ve PC kullanıcı yazılımı çalışma yapısı verilmiştir.



Şekil 4.12 IPTV Set Top Box ve PC Kullanıcı Yazılımı Çalışma Yapısı.

4.3. Kod Yapısı

.NET framework'ün alt yapısı sayesinde .NET derleyicisi olan herhangi bir programlama dili ile .NET framework üzerinde uygulama geliştirilebilmektedir. Bu dillerin sayısı ne kadar fazla olsa da .NET framework üzerine uygulama geliştiren kullanıcıların tümüne yakını Visual Basic.NET veya C# ile uygulama geliştirmektedir.

C#, güçlü, modern, nesne tabanlı ve aynı zaman “type-safe” bir programlama dilidir. C#, C++'ın gücünden, visual basic'in kolaylığından ve java 'nın da özelliklerinden faydalanarak tasarlanmış bir dildir. Bilindiği gibi C#, nesne yönelimli bir dildir. Nesne yönelimli programlamanın en önemli özelliklerinden biri de kuşkusuz kalıtım yapısıdır. Bu yapı ile var olan sınıflar genişletilerek, sınıflara kullanım amacımıza hizmet eden yeni işlevsellikler kazandırılır. Nesne tabanlı programlamada belirli bir sınıfa ihtiyacımız doğrultusunda yeni metotlar kazandırmanın tek yolu budur. Sınıflar içinde de yapı, numaralandırma, yordam gibi üyeler bulunur.

Tez kapsamında C# .Net framework kullanılarak IPTV yönetim merkezi ve IPTV PC kullanıcı programı geliştirilmiştir. .NET altyapısı kullanılarak kod üretme, derleme ve çalıştırma süreçleri adım adım gerçekleştirilmiştir.

4.4. Kod Etkileşimleri ve İşleyişi

IPTV sistemi oluşturulurken yönetim merkezi ve kullanıcı tarafı olmak üzere iki ayrı programlama yapısı düşünülmüştür. Her iki kod bloğu da kullanımı kolaylaştırmak adına arayüz kullanılarak beklenen işlemleri yapmaktadır. Arayüz bölümünün yapması gereken, girilen bilgiler ışığında veri tabanına güncel bilgileri işlemektir. Veri tabanı da arayüz bölümünün ihtiyaç duyduğu fonksiyonları sağlamakla yükümlüdür. Yönetim programı sürekli olarak veri tabanı üzerinden herhangi bir kullanıcının bilgilerinde ve izleyebileceği kanallarda güncelleme olup olmadığını denetlemektedir.

IPTV yönetim merkezi, C# .Net framework ile windows form application kullanılarak oluşturulmuştur. Kod bloğu oluşturulurken sayfalar arasındaki geçişleri sağlamak için tab kontrol kullanılmıştır. Tab kontrol içerisinde sekmelerin oluşturulması için 6 adet tab sayfası kullanılmıştır. Aşağıda 6 adet IPTV yönetim arayüzü sekmesi yer almaktadır.

- Kullanıcılar
- Kanallar
- Kategori Oluşturma
- Kategori Ekle
- Kullanıcı İzinleri
- Mesajlar

Kullanıcılar: Bu sekme yardımı ile yönetim merkezinde yeni kullanıcı ekleme, güncelleme ve parola güncelleme işlemleri yapılmaktadır. Şekil 4.13’te kullanıcı bilgilerinin düzenlendiği sekme verilmiştir.

Şekil 4.13 IPTV Sunucu Kullanıcı Bilgileri.

Kullanıcı sekmesi bir adet kombo box, 4adet text box ve 3 adet buton kullanılarak hazırlanmıştır. Kullanıcıdan adı, telefonu, mac adresi ve açıklama bilgisi alındıktan sonra yönetim programı kullanıcı için eşsiz ID ve parola üreterek veri tabanında kaydetmektedir. Her kullanıcının MD5 olarak kodlanan 8 karakter ile oluşturulan şifresi veri tabanında saklanmaktadır.

Kullanıcı güncelle butonu seçilen kullanıcının bilgileri üzerinde değişiklik yapılması için kullanılır. Kullanıcı parolasının MD5 ile üretildiği için şifrenin geri çözülerek kullanılma şansı yoktur. Parola sıfırla sekmesi ile sistemde şifresini unutan kullanıcının bilgileri teyit edilerek yeni parola oluşturulur.

Kanallar: Kanallar sekmesi ile kanal adı ve IP adresi ekleme, güncelleme ve silme işlemleri yapılmaktadır. Şekil 4.14'de IPTV yönetim merkezi arayüzünde kanal akış bilgilerinin oluşturulması gösterilmiştir.

Şekil 4.14 IPTV Sunucu Kanal Bilgileri.

Kanallar sekmesi içerisinde bir adet kombo box, 2 adet text box ve 3 adet buton kullanılmıştır. Kanal adı ve IP bilgisi yönetim programına girilerek kanal ekle butonu sayesinde veritabanına eklenir. Güncelleme ve silme butonları ile gerektiğinde düzenleme işlemleri yapılmaktadır.

Kategori Oluşturma: Haber, Belgesel, Spor gibi kategorilerin eklenmesi güncellenmesi ve silinmesi için kullanılır. Şekil 4.15'te kategori oluşturma sekmesi gösterilmiştir.

Şekil 4.15 IPTV Sunucu Kategori Oluşturma.

Kategori oluşturma sekmesi içerisinde bir adet kombo box, 1 adet text box ve 3 adet buton tanımlanmıştır. İzleyici hedef kitlesine göre kategoriler oluşturularak düzenleme yapılmaktadır.

Kategori Ekle: Bu sekme ile istenilen kanal istenilen kategoriye eklenebilir ve silinebilir. Şekil 4.16'da kanalların istenen kategori ile eşleştirilmesi gösterilmektedir.

Şekil 4.16 IPTV Sunucu Kategori Ekleme.

Kategori ekle sekmesi içerisinde iki adet kombo box, bir adet list view ve 2 adet buton hazırlanmıştır. Bu sekme ile kanallar belirli kategorilere ayrılarak son kullanıcıya sunulabilmektedir.

Kullanıcı İzinleri: Kullanıcıların izleyebileceği belirli kategorideki seçilen kanallar tanımlanmaktadır. Bunun yanında izlenebilecek kanalların kullanıcıya ne kadar süre ile açık olduğu tanımlanabilmektedir. Şekil 4.17'de IPTV yönetim merkezi tarafından verilen kullanıcı izinleri gösterilmektedir.

Şekil 4.17 IPTV Sunucu Kullanıcı İzinleri.

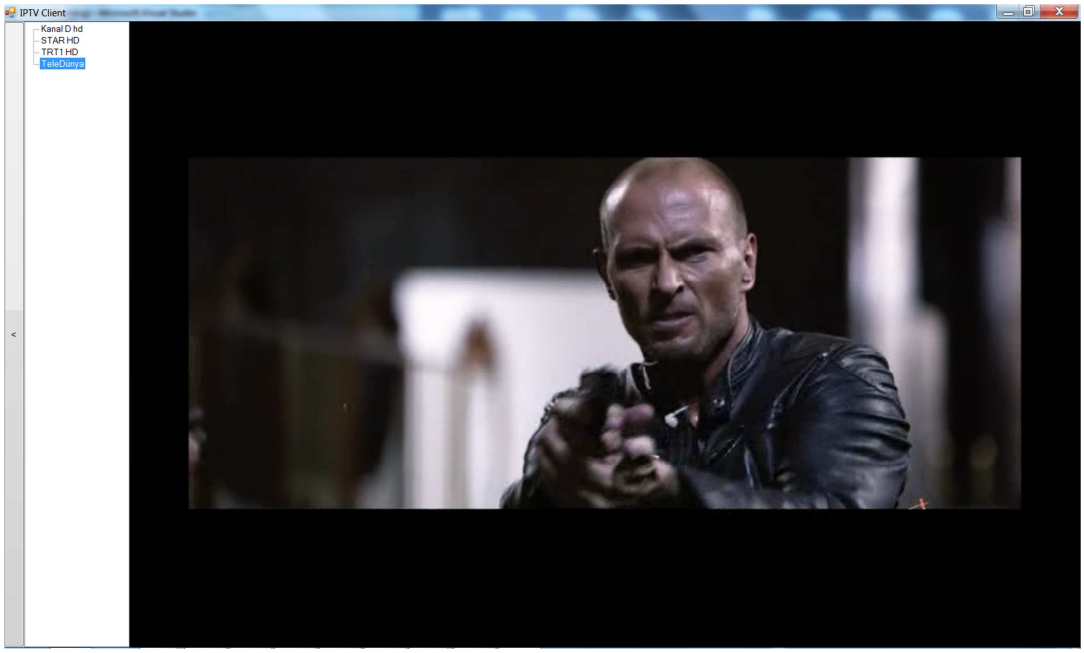
Kullanıcı izinler sekmesi iki adet kombo box, 2 adet mask text box, bir adet list view ve 2 adet buton ile hazırlanmıştır. Kullanıcı izinleri ile ilgili tüm düzenlemeler bu sekme yardımı ile yapılmaktadır.

Mesajlar: IPTV sisteminde son kullanıcıların içerik talebinde bulunması için mesajlar sekmesi kullanılmaktadır. Bu sekme yardımı ile hızlı bir şekilde kullanıcı talepleri alınarak çeşitli içerik sunumu yapılabilmektedir. Şekil 4.18'de IPTV kullanıcı mesaj bölümü gösterilmiştir.

Şekil 4.18 IPTV Kullanıcı Mesaj Bölümü.

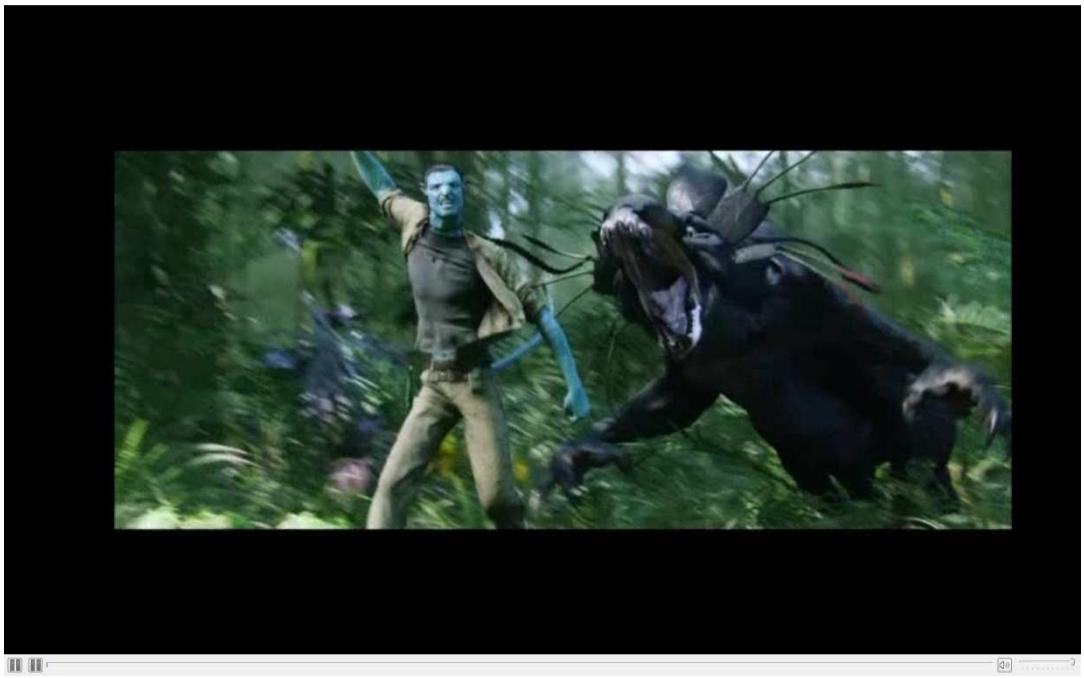
IPTV kullanıcı mesaj bölümü bir adet kombo box, 2 adet text box ve 1 adet buton kullanılarak oluşturulmuştur. Mesaj sekmesi her iki yönde de çalışarak kullanıcılar ve yönetim merkezi arasında anlık iletişimi sağlamaktadır.

Kullanıcı tarafı ise kullanıcı parola kontrol sayfası ve görüntüleme sayfası olmak üzere iki formdan oluşmaktadır. Parola ekranında parola girilip giriş butonuna basıldıktan sonra bilgisayarın MAC adresi alınarak girilen parola MD5 olarak kodlanır. Bu mac adresi ve parolaya sahip kullanıcı doğrulandığında bu kullanıcı girişi onaylanır. Sonrasında kullanıcının izleme hakkına sahip olduğu içerik ekranı görüntülenir. Kullanıcı kanal değiştirdiğinde veri tabanında ilgili kullanıcının izlemek istediği kanal bilgisi iletilerek sunucu tarafında seçilen kanal için akış değişikliği yapılarak kullanıcıya sunulur. Bu işlem yaklaşık olarak 1 sn içerisinde gerçekleşmektedir. Şekil 4.19'da IPTV PC kullanıcı yazılımı kanal listesi verilmiştir.



Şekil 4.19 IPTV PC Kullanıcı Yazılımı Kanal Listesi.

IPTV PC kullanıcı yazılımı içerisine VLC player dll dosyası eklenmiştir. Diğer taraftan kullanıcı kanal değiştirdiğinde ara yazılım aracılığıyla yönetim tarafındaki sunucu üzerine komut gönderilerek diğer kanalın gösterilmesi sağlanmaktadır. Şekil 4.20'de IPTV kullanıcı programı tam ekran görüntüsü verilmiştir.



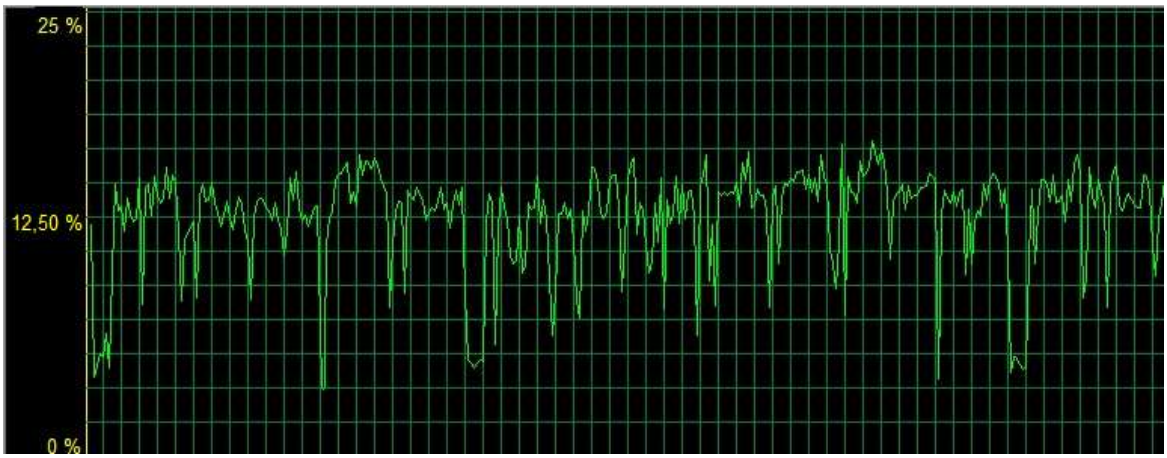
Şekil 4.20 IPTV PC Kullanıcı Programı Tam Ekran Görüntüsü.

Görüntünün PC üzerinden HDMI, VGA veya DVI bağlantı aracılığıyla TV ekranına verilmesi sağlanabilmektedir.

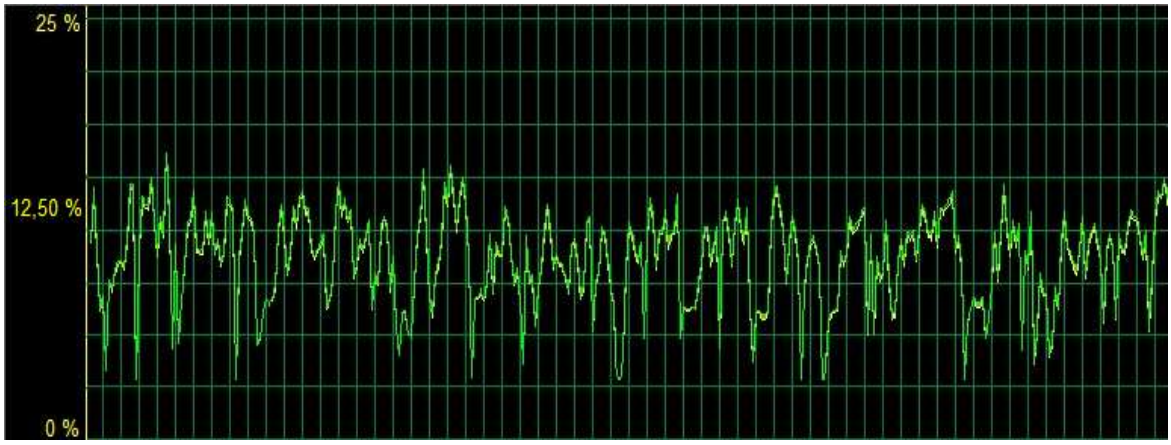
4.5. Performans Testleri

IPTV koşullu erişimi için VPN kullanımının servis kalitesi üzerindeki etkileri bu bölümde detaylarıyla sunulmuştur. IPTV hizmetinin servis kalitesi, gönderilen içeriğin yüksek bant genişliği ve düşük ağ gecikmesi ile doğru orantılıdır. Bu kapsamda, yönetim merkezi ve IPTV hizmeti verilen son kullanıcı arasındaki bant genişliği kullanım oranı ile ağ gecikmesi, VPN bağlantısının aktif olduğu ve VPN yerine genel internet şebekesi kullanımı durumlarında ölçülerek karşılaştırma yapılmıştır. Testlerde eş zamanlı olarak IPTV yönetim merkezine bağlanan farklı PC istemci programları kullanılmıştır.

Test kapsamında ilk olarak yönetim merkezi içerisinden örnek son kullanıcıya iletilen stream için VPN bağlantısı açık ve VPN bağlantısı kapalı olarak veri aktarım hızındaki değişim ölçülmüştür. Yönetim merkezi içerisinden gönderilen akış verisi, 8 Mbps indirme hızına sahip örnek son kullanıcı tarafından VPN bağlantılı ve VPN bağlantısız ortamlarda test edilerek indirme hızları Çizelge 4.4'te verilmiştir. Şekil 4.21 ve Şekil 4.22'de sırasıyla genel internet şebekesi ve VPN bağlantısı üzerinden alınan akış veri grafikleri verilmektedir.



Şekil 4.21 VPN Bağlantısı Kapalı Durum Akış Grafiği.



Şekil 4.22 VPN Bağlantısı Açık Durum Akış Grafiği.

Çizelge 4.4 VPN Kapalı ve Açık Durum için Veri İndirme Hızları.

	Ortalama Veri İndirme Hızı
VPN Kapalı Durum	7,16 Mbps
VPN Açık Durum	5,32 Mbps

Yukarıdaki grafiklerde toplam 54 Mbps bağlantı kapasitesi üzerinden gösterilen ve 8 Mbps indirme hızına sahip son kullanıcı için VPN açık ve kapalı durum için veri akış hızları verilmiştir. Yukarıda ölçüm sonuçlarında görüldüğü üzere bağlantı için genel internet şebekesi yerine VPN erişimi kullanılması durumunda yaklaşık %25 veri hızı kaybı olmaktadır. VPN bağlantısında güvenli tünel yönetiminin oluşturulması bant genişliğinde azaltıcı etkiye sebep olmaktadır.

IPTV sisteminde kaliteli servis hizmetini etkileyen bir diğer unsur ise ağ gecikmesidir. Gönderici tarafından iletilen veri paketlerinin son kullanıcı tarafında

teslim alınana kadar geçen süre ağ gecikmesi olarak adlandırılır. Aşağıda 8 Mbps veri indirme hızına sahip 3 farklı PC istemci için VPN bağlantısı aktif ve kapalı olarak ağ gecikmeleri hesaplanarak Çizelge 4.5'te verilmiştir. Test süresince farklı boyutlardaki veri paketleri, yönetim merkezinden son kullanıcılara iletilirken ortaya çıkan ağ gecikme süreleri hesaplanmıştır. Test süresince her bir farklı boyuttaki veri 100'er kez son kullanıcıya gönderilerek ağ gecikme sürelerinin ortalaması alınmıştır.

Çizelge 4.5 VPN Kapalı ve Açık Durum Ağ Gecikmeleri.

	Ağ Gecikmesi (VPN Kapalı)			**Ağ Gecikmesi (VPN Açık)**		
Veri Boyutu	**PC 1**	**PC 2**	**PC 3**	**PC 1**	**PC 2**	**PC 3**
3024 Bytes	6.23 ms	9.16 ms	8.78 ms	12.34 ms	18.27 ms	14.54 ms
4608 Bytes	8.32 ms	6.94 ms	9.35 ms	13.78 ms	16.75 ms	15.63 ms
5120 Bytes	7.34 ms	9.68 ms	8.12 ms	13.57 ms	17.85 ms	18.44 ms
6144 Bytes	10.83 ms	7.39 ms	8.45 ms	15.63 ms	21.45 ms	16.94 ms
10240 Bytes	12.47 ms	9.83 ms	11.04 ms	22.68 ms	16.33 ms	24.19ms
65500 Bytes	12.69 ms	13.78 ms	10.27 ms	17.37 ms	24.50 ms	22.13 ms

Yapılan analizlerde VPN bağlantısı açık olduğu durumda, kapalı duruma göre ağ gecikme değerlerinin daha büyük olduğu gözlemlenmektedir. VPN açık olduğu durumda veri paketleri şifrelenerek gönderildiği için şifreleme ve şifre çözme süreleri alıcı tarafta hesaplanan ağ gecikmesi süresini artırmaktadır.

Bu çalışma kapsamında IPTV hizmetinin son kullanıcıya ulaştırılmasında 128 bit anahtar uzunluğuna sahip AES şifreleme metodu kullanılmıştır. VPN şifreleme yöntemi ile yönetim merkezinden gönderilen akış verisi kapsüller halinde şifrelenmektedir. Her bir kapsülün şifrelenmesinde kullanılan şifreleme yöntemi ve anahtar uzunluğuna göre işlem yapılmaktadır. Şifreleme yöntemi ve anahtar uzunluğunun son kullanıcıya iletilen içerik üzerindeki oluşturduğu ağ gecikmesi hizmet kalitesini etkileyen bir diğer faktördür. Test kapsamında ilk önce 128 bit anahtar uzunluğuna sahip AES şifrelemesi kullanılarak ağ gecikmesi ölçülmüştür. Daha sonra yönetim merkezinde yapılan konfigürasyon değişikliği ile VPN sunucu şifreleme işlemi için 168 bit anahtar uzunluğuna sahip 3DES şifreleme algoritması kullanılmış ve ağ gecikmesi ölçülmüştür. Test için yönetim merkezinden farklı

boyutlarda veri paketleri son kullanıcıya iletilerek ortaya çıkan ağ gecikmeleri hesaplanmıştır. Her iki durumda da son kullanıcı indirme hızı 8 Mbps olarak seçilmiştir. Çizelge 4.6'da AES ve 3DES şifreleme algoritmaları için ağ gecikme süreleri verilmiştir.

Çizelge 4.6 AES ve 3DES Şifreleme Algoritmaları için Ağ Gecikmeleri.

	Ağ Gecikmesi	
Veri Boyutu	**AES-128 Bit Şifreleme**	**3DES-168 Bit Şifreleme**
3024 Bytes	19.27 ms	28.77 ms
4608 Bytes	17.63 ms	32.72 ms
5120 Bytes	18.91 ms	26.64 ms
6144 Bytes	21.38 ms	34.07 ms
10240 Bytes	20.25 ms	38.14 ms
65500 Bytes	24.86 ms	41.52 ms

Test kapsamında her iki durum için hesaplanan değerlerde 3DES şifreleme algoritması için ağ gecikmesinin daha büyük olduğu gözlemlenmiştir. AES şifreleme algoritması ile veri şifreleme ve şifre çözme işleminin 3DES şifrelemesine göre daha hızlı olduğu değerlendirilmektedir.

IPTV hizmetinin servis kalitesinin ölçülmesi amacıyla uygulanan testlerde VPN bağlantısı açık ve kapalı olarak son kullanıcıya içerik dağıtımı gerçekleştirilmiştir. VPN açık durumda yapılan testlerde, genel ağ üzerinden iletim yapılmasına göre %25'e kadar bant genişliğinde azalma olabilmektedir. Ayrıca VPN şifreleme algoritmasına ve anahtar uzunluğuna bağlı olarak ağ gecikmesinin değişebildiği görülmektedir. Sonuç olarak son kullanıcıya kaliteli bir IPTV hizmetinin verilebilmesi için geniş bant internet erişimi ihtiyacı olduğu değerlendirilmektedir.

5. SONUÇ VE ÖNERİLER

Bu bölümde, tez çalışmasının sonuçları değerlendirilmiştir. Ayrıca, gelecekte tez konusu ile ilgili olarak yapılabilecek çalışmalara yönelik öneriler de sunulmuştur.

5.1. Sonuçlar

Giriş bölümünde de bahsedildiği gibi, bu tez çalışmasında yüksek güvenlik gereksinimi olan IPTV uygulamaları için VPN şifreleme tekniği ile yazılım tabanlı koşullu erişim sisteminin oluşturulması amaçlanmıştır. Bu amaç doğrultusunda yapılan çalışmada konu detaylı olarak incelenmiş ve bu alandaki kaynaklardan faydalanılmıştır. Pek çok farklı ayağı bulunan bu çalışmada hem IPTV kavramına yönelik hem de programlama ve tasarım detaylarına yönelik tecrübe ve kazanımlar elde edilmiştir.

Tez çalışmasında, IPTV platformunu oluşturan yönetim ve son kullanıcı programı üretilmiştir. IPTV yönetim merkezi, kullanıcı programı ve veri tabanından oluşan programın ilk versiyonunda toplam 6 farklı dosyaya yayılmış olarak yaklaşık 1800 satır kod bulunmaktadır. Toplam satır sayısının yaklaşık yüzde 38'lik kısmı geliştirme ortamı tarafından otomatik olarak üretilen kodlardan oluşmaktadır.

IPTV içeriği, diğer IP hizmetleri gibi içeriğin çalınması, kullanıcının taklit edilmesi, spam ve diğer saldırılarla karşı karşıyadır. Bunların engellenmesi ve içeriğin güvenli bir şekilde son kullanıcıya kadar iletilebilmesi için uçtan uca bir güvenlik sistemine gereksinim vardır. Bu çalışma kapsamında oluşturulan IPTV platformunun yayın merkezi ve son kullanıcı arasındaki iletişim ve içerik güvenliği yazılım tabanlı koşullu erişim sistemi ile sağlanmıştır. Sistemdeki son kullanıcıların yayın merkezinden içerik talep edebilmeleri için emsalsiz kullanıcı ID ve şifre verilmiştir. Ayrıca kullanıcının bağlandığı fiziksel adresi (MAC) kayıt altına alınmakta başka bir PC vb. ile giriş denemeleri yapıldığında sistem erişim vermemektedir.

IPTV yönetim merkezi ve PC kullanıcı programı arasındaki güvenli erişim VPN şifreleme tekniği kullanılarak sağlanmaktadır. VPN şifreleme sistemi kullanılarak sunulan içerik şifrelenerek güvenlik düzeyi en üst seviyeye çıkartılmış bir IPTV mimarisi tasarlanmıştır. IPTV hizmeti servis kalitesinin ölçülmesi için VPN bağlantısı kullanılarak ve VPN bağlantısı olmaksızın genel internet trafiği üzerinden verilen servis hizmetleri karşılaştırılarak yorumlanmıştır. VPN bağlantısında güvenli tünel yönetiminin oluşturulması, bant genişliğinde yaklaşık olarak %25 oranında azaltıcı etkiye sebep olmaktadır. Diğer taraftan sistemin

güvenlik boyutu düşünüldüğünde, geniş bant internet erişimi kullanımı durumunda IPTV içeriği için gerekli bant genişliği sağlanabileceğinden dolayı bir problem teşkil etmemektedir. Bunun yanında IPTV içeriğinin şifrelenmesinde kullanılan şifre algoritması ve anahtar uzunluğu da IPTV şebekesinin hızını etkilemektedir. Testler kapsamında VPN tünel yönetimi Tez kapsamında AES ve 3DES şifre algoritmalarıyla şifrelenen verinin oluşturduğu ağ gecikmeleri kayıt altına alınmıştır. Yapılan analizlerde AES şifreleme algoritmasının performansının 3DES algoritmasına göre daha hızlı olduğu değerlendirilmiştir. Bu açıdan, tez kapsamında VPN bağlantısı içerisinde şifreleme işlemi için AES şifreleme algoritması kullanılmıştır.

Sistemin son kullanıcı kısmında IPTV PC kullanıcı programı üretilmiştir. Kullanıcı arayüzü sade bir şekilde tasarlanarak kolay kullanım sağlamakta ve anlaşılabilirliği artırmaktadır. Programda seyredilmek istenen TV kanalı arayüz kullanılarak seçilmektedir. Bunun yanında kullanıcının herhangi bir istek talebi bu arayüz kullanılarak gerçekleştirilmektedir. IPTV yönetim sunucusuyla entegre olarak çalışan bu program kullanıcı izleme alışkanlıklarına göre son kullanıcıya özgü hizmetin sunulabilmesi için reklam, TV kanalı vb. içerik öngörüsünde bulunmaya yardımcı olmaktadır.

Günümüzde içerik hırsızlığı daha çok internet üzerinden içerik dağıtımı veya şifre anahtarlarının paylaşımı şeklinde gerçekleşmektedir. Bu nedenle, DVB ortamında çalışan tüm koşullu erişim sistemlerinin genel güvenliği için smart kart ile DVB şifre çözücünün devreleri arasındaki bağlantı kanalının saydam olmaması son derece önemlidir. Bağlantı kanalının iyi korunmadığı durumda kontrol sözcüklerine girilme ihtimali artmaktadır. 2.3 Güvenlik bölümünde açıklanan kontrol sözcüğünün güvenlik zafiyeti ile ilgili olarak, smart kart ile STB arasındaki ara bağlantı, kontrol sözcüklerinin geçtiği kanalın bir parçasını oluşturur. Bu nedenle koşullu erişim sistemleri üreticilerinin, tüm STB'lerde çok yüksek seviyede müdahaleye dayanıklı uygulamaları tek başına yeterli olmamakla birlikte smart kart ile STB arasında yüksek güvenlikli haberleşmeyi de garantilemeleri gerekir. Diğer taraftan smart kartların sınırlı boyutları, eklenen akıllı kart yongasının yeteneklerini ve bu yüzden kullanılabilecek güvenlik teknolojilerini sınırlamaktadır.

Tez kapsamında oluşturulan koşullu erişim sistemi, geleneksel şifreleme yöntemleri ile karşılaştırıldığında yazılımsal olarak tasarlandığı için decoder ve smart kart çözümlerine gerek duyulmamaktadır. Smart kart üretim, değişim vb. maliyetler olmadığından dolayı set-top box dizayn maliyetlerinin ucuzlamasıyla birlikte %60'a kadar daha ucuz çözümler sunulabilmektedir. VPN şifreleme algoritması herhangi bir donanıma bağımlı olmadığı için güvenlik teknolojilerinde bir sınırlama yoktur. Koşullu erişim, güncelleme veya değişim işlemlerinde herhangi bir donanım değişikliği gerektirmemektedir. Geleneksel yöntemlerden farklı olarak kullanıcının işletmeciler arasında geçiş yapması durumunda kart veya donanım birimi değişikliği ihtiyacı olmamaktadır. Çalışma kapsamında bu tür harici donanımlar kullanılmadan üst düzey güvenlik isterlerinin sağlandığı daha uygun maliyetli ve kullanımı kolay bir koşullu erişim metodu önerilmiştir.

5.2. Öneriler

Tez kapsamında hazırlanan IPTV koşullu erişim sistemi yönetim ve son kullanıcı programı tasarım ve kod yapısı olarak değişikliğe ve geliştirmeye açıktır. Bu çalışma üzerine yenilikler getirmek ya da iyileştirmeler yapmak isteyenler için uygun bir yapı mevcuttur. Programa yönelik birkaç iyileştirme önerisi de aşağıda belirtilmektedir. Yeni çalışmalarda kullanılabileceği düşüncesi ile programa ait kaynak kodu da EK 3'te sunulmuştur.

IPTV yönetim programı çok yönlü değişikliklere imkân verebilecek şekilde tasarlanmıştır. Yönetim programında kullanıcıların izleme alışkanlıkları ölçülebilmektedir. İlerleyen dönemde kullanıcı alışkanlıklarına göre içerik sunumu reklam vb. yapılması mümkündür.

Son kullanıcı arayüzü ilk versiyonu kullanıcı dostu olacak şekilde sade bir şekilde tasarlanmakla birlikte ileri düzey kullanıcılar için içerik zenginleştirilebilir. Programın ilk versiyonunda belirli yayın kategorileri sunulmakla birlikte daha fazla kategori ve favori liste oluşturulması mümkündür. Bunun haricinde son kullanıcı arayüzündeki kullanıcı talep girişi çeşitli uygulamalar için geliştirilebilir.

IPTV yönetim merkezi ile son kullanıcı arasında güvenli bağlantıya imkân tanıyan VPN bağlantı yöntemi Cisco tabanlı olmakla birlikte farklı firmaların ürünlerinden de yararlanılması mümkündür.

KAYNAKLAR

[1] İnternet'in gelişim tarihi, http://tr.wikibooks.org/wiki/%C4%B0nternet%27in_geli%C5%9Fim_tarihi, (12 Nisan 2012).

[2] Yilmaz, A., Sayısal Teknolojilerin Televizyon Yayıncılığına Sağladığı Yeni Açılımları Değerlendirmek, http://edergi.atauni.edu.tr/index.php/SBED/article/viewFile/512/505, (3 Mayıs 2012).

[3] O'Driscoll, G., 2008, Next Generation IPTV Services and Technologies, Wiley, New Jersey, 490 p.

[4] Telekomünikasyon Kurumu, 2008, IP Tabanlı Hizmetler: VoIP ve IPTV, http://www.tk.gov.tr/kutuphane_ve_veribankasi/raporlar/arastirma_raporlari/dosyalar/IP_Hizmetleri_Raporu_V5.pdf, (11 Ağustos 2012).

[5] Acar, E., Türkiye IPTV 2011 Raporu, http://iptv.org.tr/iptv/wpcontent/uploads/2011/07/IP-TV_Mart_2011Son.pdf, (27 Ağustos 2012).

[6] Hens, F. J., Caballero, J. M., 2008, Triple Play: Building The Converged Network for IP, VoIP, and IPTV, Wiley, Chippenham, 401 p.

[7] Ramirez D, 2008, IPTV Security, Wiley, West Sussex, 234 p.

[8] Paul, S., 2011, Digital Video Distribution in Broadband, Television, Mobile and Converged Networks, Wiley, West Sussex, 367 p.

[9] Çakır., Y. A., Türk Telekomünikasyon A.Ş. IPTV Projesi, http://syc2008.ee.hacettepe.edu.tr/bildiriler/TTKOM_IPTV.pdf, (17 Mayıs 2012).

[10] ITU-T, IPTV Focus Group Proceedings, IPTV-GSI, 2008.

[11] Hjelm, J., 2008, Why IPTV?: Interactivity, Technologies, and Services, Wiley, Singapore, 358 p.

[12] Simpson, W., Greenfield, H., 2007, IPTV and Internet Video, Elsevier, Burlington, 240 p.

[13] Conditional-Access Broadcasting Systems, ITU Rec. 810, 1992.

[14] Smart Cards; Card Application Toolkit (CAT), ETSI TS 102 223, Release 4.

[15] Taşkın, C., IPTV Yayın Merkezi, http://www.cebrailtaskin.com/yayin.htm, (3 Mayıs 2012).

[16] ISO/IEC 13818-1: 2000(E), "Information technology – Generic coding of moving pictures and associated audio information: Systems," 2000.

[17] ETR 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems",

European Telecommunications Standards Institute, Ekim 1996.

[18] Digital Video Broadcasting (DVB); DVB Simulcrypt; Part 1: Head-end architecture and synchronization, DVB TS 101 197-1 V1.1.1, June1997.

[19] [ETSI, TS 103 197 v1.4.1, Digital Video Broadcasting (DVB); Head-End implementation of DVB Simulcrypt, Eylül 2004.

[20] ETSI, Technical Report 289, Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems, Ekim 1996.

[21] EBU Technical Review, 1995: Functional Model of A Conditional Access System; European Broadcasting Union Project Group B/CA 1995.

[22] ETSI, Security Algorithms, http://portal.etsi.org/dvbandca/DVB/DVBINTRO.asp, (12 Temmuz 2012).

[23] High-Bandwidth Digital Content Protection System Revision 1.3, Aralık 2006; http://www.digital-cp.com/hdcp_technologies, (16 Ağustos 2012).

[24] GlobalComms Pay-TV, http://www.telegeography.com/researchservices/globalcommspaytv/index.html, (17 Haziran 2012).

[25] Frost & Sullivan, 2009, Analysis of the World Software-based Pay TV Conditional Access System Market, #N538-70.

[26] Simpson, W., 2008, Video Over IP, Elsevier, Burlington, 240 p.

[27] Elwood, I., IPTV Deployment: IPTV changes the way consumers watch television, http://www.dailyiptv.com/news/iptv-deployment-trends/, (26 Haziran 2012).

[28] Assuring quality of experience for IPTV, white paper, 2006, http://www.heavyreading.com, (3 Nisan 2012).

[29] B. Erman, E.P. Matthews, Analysis and Realization of IPTV Service Quality, Bell Labs, Technical Journal, 12(4), 2008.

[30] Design and Implementation of IPTV System, http://kelsayed.tripod.com/cuadi/Desig_and_Implementation_ofIPTV_System.pdf, (16 Mart 2012).

[31] Chaudhuri, R., End to End IPTV Design and Implementation, How to avoid Pitfalls, http://www.networks2008.org/data/upload/file/Tutorial/T6_Chaudhuri.pdf, (14 Nisan 2012).

[32] Information Technology Intelligence Consulting, 2011, SQL Server 2008 R2 and Windows Server 2008 R2 Deliver Industry-Leading Security, http://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CkQFjAB&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2FB%2F1%2F1%2FB115F49200EF41EA9BAFBE5D016A0FB%2FITIC

%2520Microsoft%2520SQL%2520Server%2520Windows%2520Server%2520Security%2520Paper%2520Final%2520Version.pdf&ei=EDuEUI6fN9KO4gT87YCwBg&usg=AFQjCNGh8Jn01J28vg_fy55aLUYRzRUHmg&sig2=09FsQrx7dl6MwqV0quFZzA&cad=rja, (22 Ağustos 2012).

[33] Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/MD5, (11 Haziran 2012).

[34] Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/IPTV, (5 Mayıs 2012).

[35] Wikipedia, the free encyclopedia, http://tr.wikipedia.org/wiki/AES (13 Haziran 2012).

[36] Cisco, 2006, Integrated video admission control for the delivery of a quality video experience, white paper, USA, 8 p.

[37] Cisco, Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution Design and Implementation Guide, Release 1.0, 2005, http://www.cisco.com/application/pdf/en/us/guest/products/ps6902/c2001/ccmigration_09186a0080666605.pdf, (18 Temmuz 2012).

[38] DES/3DES/AES VPN Encryption Module http://www.cisco.com/en/US/docs/ios/12_2/12_2z/12_2zj/feature/guide/gtaimvpn.pdf, (27 Ağustos 2012).

[39] VPN Nedir? http://technet.microsoft.com/trtr/library/cc731954%28v=ws.10%29.aspx, (14 Mart 2012).

[40] W. Li, H. Liu, Y. Wu, Introduction to IPTV, slides, IBC2007.

[41] J. W. Lee, Key Distribution and Management for Conditional Access System on DBS, in Proceedings of International Conference on Cryptology and Information Security, 1996, pp. 82–86.

[42] Dijital Uydu Alıcılarının Tipleri, Özellikleri, Seçim Kriterleri, Şifreli Yayınlar ve Koşullu Erişim, http://www.uydutvhaber.net/ebooks/dyteknik4.pdf, (10 Şubat 2012).

[43] VLC Player Kaynak Kodu, http://www.videolan.org/vlc/downloadsources.html, (11 Nisan 2012).

[44] J. McCombe, Protecting IPTV Infrastructure from Security Risks, http://www.convergedigest.com/bp/bp1.asp?id=378&ctgy=, (18 Ekim 2012).

EKLER

EK 1. YAPILAN BENZER TEZ ÇALIŞMALARI

- **Tez adı:** Towards multi-user personalized TV services-Introducing combined RFID Digest authentication

  Yazar adı: Ray van Brandenburg

  Yılı: 2009

  Öz: In recent years, TV has become increasingly focused on personalization and individualization. This trend is slowly diminishing the traditional use of TV as a concurrent medium; one that is shared by multiple viewers sitting on the couch next to each other. We should therefore be careful that with the increasing focus on the individual experience, the collective experience, and with it the social component of TV, is not lost. The fact that a recent IPTV architecture, IMS-based IPTV, does not even take the multi-user scenario into account, only further supports this notion. The question therefore is: Are personalization and concurrency necessarily contradictory?

  This document tries to answer this question, both from a use case perspective and from a technical point of view.

  A set of multi-user use cases is presented that show that there are in fact applications imaginable that combine the two concepts of personalization and concurrency in a way that they complement and reinforce each other; resulting in applications that provide users with personalized services while reinforcing the social and collective component of watching TV.

  When trying to implement these new types of use cases, however, it becomes apparent that current IMS-based IPTV identification and authentication mechanisms are not flexible enough to support concurrent use in a way that results in a user-friendly system. To solve this problem, a new identification and authentication mechanism, called RFID Digest is

presented. This system, which is based on the use of personal RFID cards, is developed in a way so that it doesn‟t require any changes to the server side of the IPTV architecture, allowing for seamless integration in existing infrastructure.

Apart from the development details of RFID Digest, an evaluation of its properties is also presented. This evaluation consists of two parts: an assessment of RFID Digest's security level, which shows it to be comparable to other IMS authentication mechanisms, and a brief survey into the impact of RFID Digest on total TV Access times, which shows this effect to be minimal.

Finally, to show that multi-user personalized services using RFID Digest are not only possible in theory but also in practice, a proof-of-concept prototype will be presented.

- **Tez adı:** Study of Reliable Multicast for IPTV Service

  Yazar adı: Mohammad Taufiqul Islam and Azimul Hoque

  Yılı: 2008

  Öz: Internet Protocol Television (IPTV) is a service on the Internet where digital TV signal data is delivered to the participants using the Internet Protocol (IP). IPTV promises to provide many TV channels with lower price for operators, lower price for consumers and it is also distributed more efficiently than using the nowadays prevalent coaxial cable distribution. As it is assumed that broadband connection of households will grow at a brisk pace, IPTV will play more and more important role in the incoming years in our lives. The plenty of TV channels requires large bandwidth for high clear TV programs in IPTV service which is a contradictory issue to the limitation of user access line bandwidth and aggregation network bandwidth. Multicast as a mature one-to-many packet data delivery technology, the use of multicast for IPTV service is considered necessary to resolve such contradiction. But which multicast or what level multicast will be best suited

for this emerging technology is still a burning question. In this thesis we identify the appropriate multicast solution for IPTV. To accomplish our goal, we have done literature survey in gathering information to analyse different AL multicast protocol and IP multicast protocols. We have tried to find out different problems related to this protocol to deployment. Finally we have identified the best suited solution to carry multicast traffic for IPTV service.

- **Tez adı:** Fast retransmission for multicast IPTV

  Yazar adı: Martin Prins

  Yılı: 2008

  Öz: In a IPTV distribution network, broadcast television channels are distributed using multicast stream delivery. Packet loss occuring during transport will impair the displayed video signal and thus reduces the Quality of Experience. Due to the nature of video compression techniques a single lost packet can lead to visual impairments lasting for multiple seconds, so packet loss should be kept to a minimum.

  Two well known error recovery techniques are packet retransmission and Forward Error Correction (FEC). In a large multicast distribution network an end-to-end packet retransmission mechanism is not feasible as feedback implosion will occur when receivers notify the source about what packets they need retransmission of. A FEC mechanism allows the IPTV stream receivers to recover a certain amount of data, but when loss rates vary for different users there will either be some users with remaining losses or bandwidth will be wasted in large parts of the network where the loss rate is low. Another solution is to use local loss recovery for smaller parts of the multicast distribution tree. By introducing a fast-retransmission function in the access network, losses can be recovered rapidly and the video quality for the users can be maintained.

  Based on a literature study and company requirements a design of a fast retransmission mechanism is presented, intended for deployment in an

access node. For the delivery of the IPTV stream the Realtime Transport Protocol (RTP) is used. Two recent RTP protocol extensions have added functionality for time-constrained feedback and a retransmission payload format, which could be used for a retransmission mechanism mission for RTP streaming sessions. As the protocol extensions do not provide a complete retransmission mechanism, the proposed design incorporates the functionality needed to offer packet retransmissions for a time-constrained multicast IPTV service.

A prototype is implemented which is used to evaluate the effectiveness of the packet retransmission mechanism and used to determine which parameters influence the applicability of the retransmission mechanisms. For this purposes several experiments are performed, which are used to evaluate the performance in a uncongested network with different loss characteristics and a network in which packet loss occurs due to network congestion. Evaluation of the prototype shows the efficiency of the retransmission mechanism to handle losses and its performance in congested networks.

- **Tez adı:** Soft Conditional Access for Digital Television

  Yazar adı: Dominika Olczak

  Yılı: 2006

  Öz: A Conditional Access System (CAS) for digital television is a method used to restrict access to digital television broadcasts. Most conditional Access systems for digital TV are partly hardware implemented using, for example, smart cards and security modules. The purpose of this thesis work was to investigate the possibility to create a secure software-based CAS not using these hardware features.

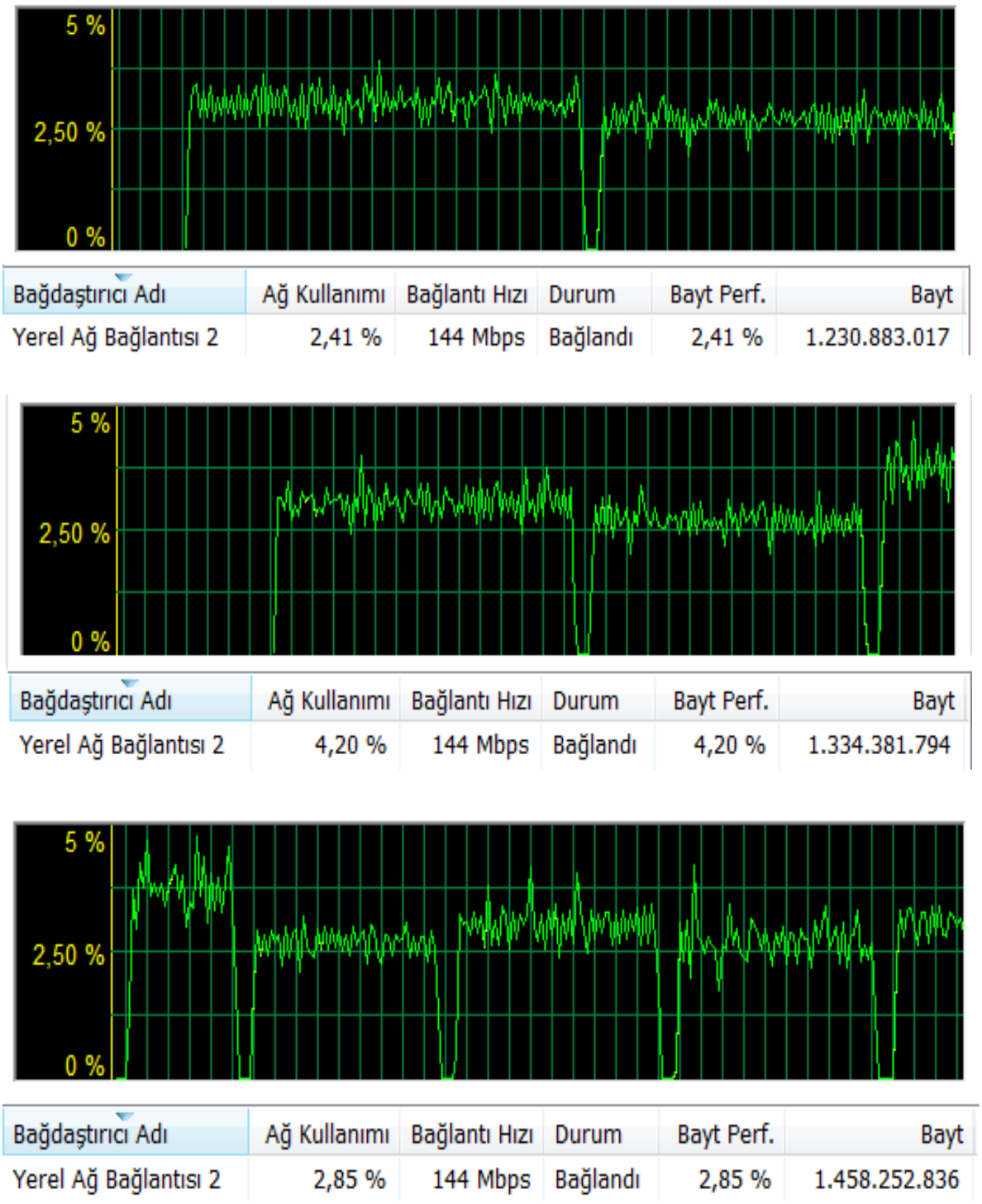
  A study was conducted to investigate the existing systems for digital TV on the market and the requirements posed on them. With this investigation as a basis, a design suggestion was created, including a model for an

organisation of system information to enhance security, and a system expansion model. Tests were conducted on a PostgreSQL database to evaluate the product's functionalities and its suitability to be used as a base in the design suggested in this report. A system communication prototype for a conditional Access protocol, adapted to the design, was also created.

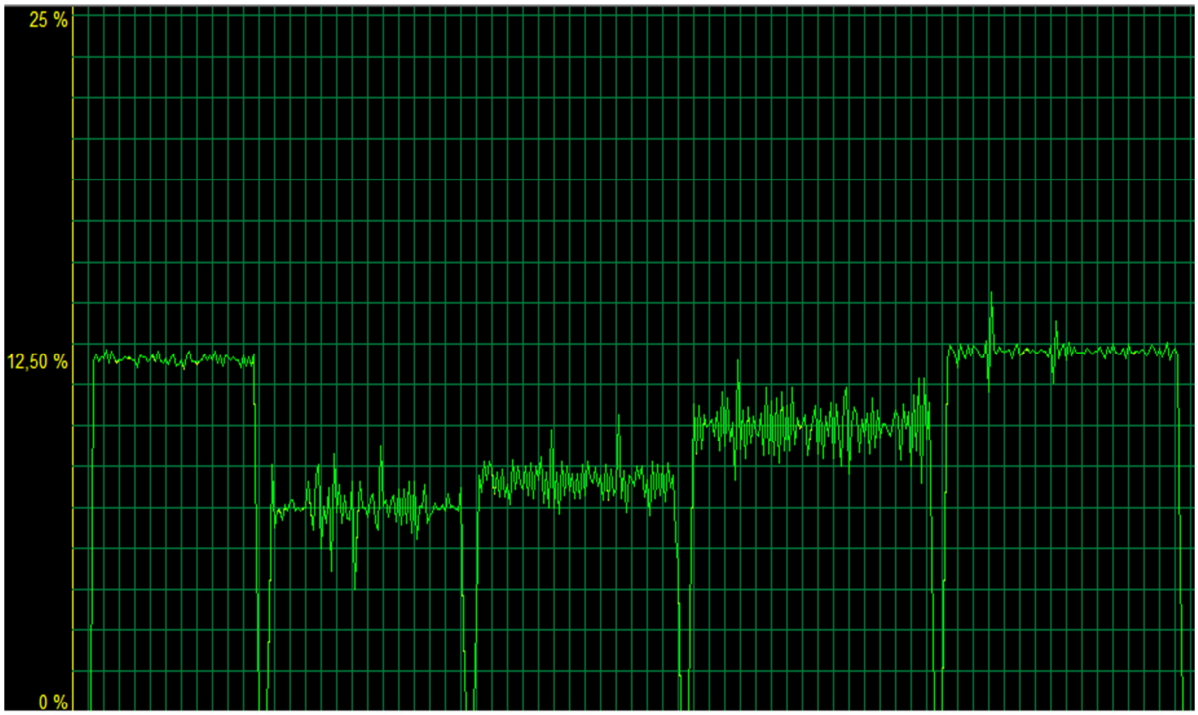
The conclusion drawn by this thesis work is that it is possible to create a software-based CAS. However, it demands a strict organisation of CAS data to maintain a high degree of security. It also requires a relatively high competence level among company personnel to maintain the system, due to its complexity.

EK 2. IPTV HD VE SD KANAL DEĞİŞİMİ VE BANT GENİŞLİKLERİ

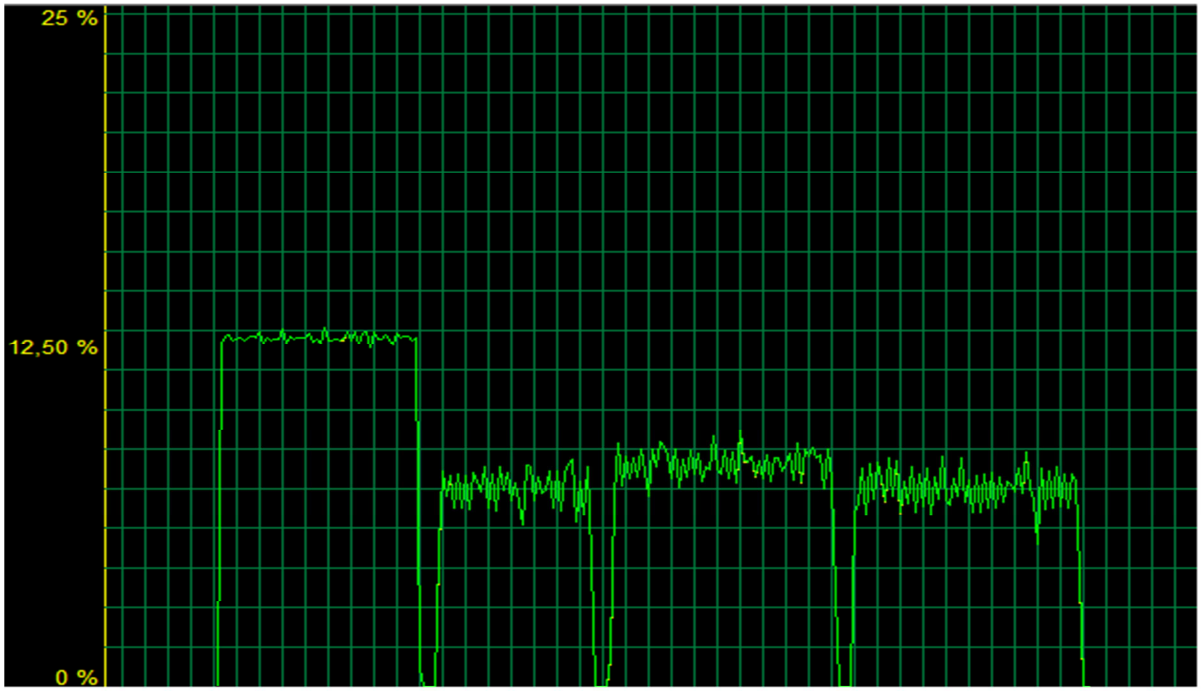
Bant Genişliği = Ağ Kullanımı Yüzdesi x Bağlantı Hızı (E2.1)



Şekil E2.1 IPTV HD VE SD Kanal Değişimi ve Bant Genişlikleri 1



Bağdaştırıcı Adı	Ağ Kullanımı	Bağlantı Hızı	Durum	Bayt Perf.	Bayt
Yerel Ağ Bağlantısı 2	13,23 %	54 Mbps	Bağlandı	13,23 %	1.620.160.995



Bağdaştırıcı Adı	Ağ Kullanımı	Bağlantı Hızı	Durum	Bayt Perf.	Bayt
Yerel Ağ Bağlantısı 2	5,75 %	54 Mbps	Bağlandı	5,75 %	729.981.069

Şekil E2.2 IPTV HD VE SD Kanal Değişimi ve Bant Genişlikleri 2

EK 3. IPTV YÖNETİM MERKEZİ VE SON KULLANICI PROGRAMI KAYNAK KODU

IPTV yönetim merkezi ve son kullanıcı programı kaynak kodu Visual Studio .NET projesi olarak aşağıdaki CD’de bulunmaktadır.

ÖZGEÇMİŞ

Adı Soyadı : Faik ÖZTÜRK

Dogum Yeri : Ankara

Dogum Yılı : 1987

Medeni Hali : Bekar

Eğitim ve Akademik Durumu

İlköğretim : 1993 – 2001 Ankara Gölbaşı Tek İlköğretim Okulu

Lise : 2001 – 2004 Ankara Dr. Şerafettin Tombuloğlu Lisesi

Lisans : 2004 – 2009 Erciyes Üniversitesi

Elektrik-Elektronik Mühendisliği Bölümü

Yabancı Dil : İngilizce

İş Tecrübesi

2011 – … Türksat Uydu Haberleşme ve Kablo TV İşletme A.Ş.

Uydu Frekans Gözlem Direktörlüğü