GEDİZ ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

TELEKOMÜNİKASYON SEKTÖRÜNDE VERİ TOPLAMA YÖNTEMLERİ, YENİ YAKLAŞIMLAR VE GÜVENLİK

YÜKSEK LİSANS TEZİ

Emine HEMŞİNLİ

Endüstri Mühendisliği Anabilim Dalı

Sistem Mühendisliği Yüksek Lisans Programı

Tez Danışmanı: Prof. Dr. Mustafa GÜNEŞ

OCAK 2015

GEDİZ ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

TELEKOMÜNİKASYON SEKTÖRÜNDE VERİ TOPLAMA YÖNTEMLERİ, YENİ YAKLAŞIMLAR VE GÜVENLİK

YÜKSEK LİSANS TEZİ

Emine HEMŞİNLİ

Endüstri Mühendisliği Anabilim Dalı

Sistem Mühendisliği Yüksek Lisans Programı

Tez Danışmanı: Prof. Dr. Mustafa GÜNEŞ

OCAK 2015

GÜ, Fen Bilimleri Enstitüsü'nün 600113008 numaralı Yüksek Lisans Öğrencisi **Emine HEMŞİNLİ** ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı **"Telekomünikasyon Sektöründe Veri Toplama Yöntemleri, Yeni Yaklaşımlar Ve Güvenlik"** başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı : **Prof. Dr. Mustafa GÜNEŞ**
Gediz Üniversitesi

Jüri Üyeleri : **Prof. Mustafa GÜNEŞ**
Gediz Üniversitesi

Yrd. Doç. Dr. Şerife DEMİROĞLU
Gediz Üniversitesi

Doç. Dr. Mehmet AKSARAYLI
Dokuz Eylül Üniversitesi

(Yedek Üye) **Yrd. Doç. Dr. Zeynep Nilhan GÜRKAN**
Gediz Üniversitesi

Teslim Tarihi : **22 Ocak 2015**
Savunma Tarihi : **27 Ocak 2015**

ÖNSÖZ

Son yıllarda teknolojinin ilerlemesi ile rekabet koşulları da değişmiştir. Bilgiye erişim, anlamlı veri üretmek ve hızlı aksiyon almak, rekabet ortamında öne çıkaran faktörlerden biri haline gelmiştir. Her ortamda veriye hızlı ve güvenli erişim bununla birlikte verinin sağlıklı bir şekilde aktarılması önem kazanmıştır.

Her sektörde olduğu gibi telekomünikasyon sektöründe de müşterileri tanımak, tanımlara göre sınıflandırmak ve satış stratejileri geliştirmek önemlidir. Müşteriyi tanımak için eldeki her türlü veri kullanılmakta ve analiz edilmektedir. Çeşitli veri toplama yöntemleri ile eldeki tüm veri kaynakları analiz edilmektedir. Hizmet sektöründe rekabet verilerin analizi üzerinden olduğu için verilerin değerlendirmesi maliyeti de etkilemektedir. Kısaca müşteri bilgileri, hizmet sektöründe birer ham madde özelliği göstermektedir ve bu hammaddeyi elde etmenin bir maliyeti vardır. Elde bulunan verilerden maksimum fayda sağlamak gerekmektedir.

Verilerin analizi ve sistemler arası aktarımda, güvenlik ve hız önemli bir sorundur. İlgili çalışmada telekomünikasyon sektöründe veri güvenliği, veri elde etme yöntemlerinde dijital arşiv sisteminin kullanılası ve aktarım teknolojileri üzerinde durulmuştur.

Veri aktarımı sırasında örnek bir sistemde kuyruk modeli geliştirilmiş ve Ankara-İzmir arası veri aktarımında bekleme süreleri ve tıkanıklık maliyetleri tespit edilmiştir. Sistemde sağlıklı veri iletimi için mevcut TCP algoritması incelenmiş ve daha hızlı veri aktarımı için geçilmesi gereken yeni sistem önerilmiştir.

Tez çalışması boyunca değerli desteklerini esirgemeyen çok değerli hocam ve tez danışmanım Prof. Dr. Mustafa GÜNEŞ' e teşekkürü bir borç bilirim.

Bu çalışmada bana ilham olan, ilk iş hayatıma başladığım ve büyük bir mutlulukla devam ettiğim firmama, yöneticilerime ve çalışma arkadaşlarıma gösterdikleri destek için sonsuz teşekkürler.

Son olarak benden desteklerini ve sevgilerini esirgemeyen canım aileme sonsuz teşekkürlerimi sunarım.

Ocak 2015 Emine HEMŞİNLİ

İÇİNDEKİLER

Sayfa

TABLO LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

AB	: Avrupa Birliği
ACK	: Acknowledgement
ADSL	: Asymmetric Digital Subscriber Line
ARPANet	: Advanced Research Projects Agency Network
ASCII	: Character Encoding Scheme
BGYS	: Bilgi GüvenliğiYönetim Standartları
CDR	: Arama Detay Bilgileri (Call Detail Record)
CRM	: Müşteri İlişkileri Yönetimi(Customer Relationship Management)
DNS	: Domain Name System
ERP	: Kurumsal Kaynak Planlama (Enterprise Resource Planning)
FBI	: Federal Bureau of Investigation
FIFO	: First in First Out
FTP	: File Transfer Protocol
HTTP	: Hiper Metin Transfer Protokolü (Hyper-Text Transfer Protocol)
HTTPS	: Secure http
ICR	: Akıllı Karakter Tanıma (Intelligent Character Recognition)
ID	: Identify
IP	: IP adresi (Internet Protocol Address)
ISDN	: Bütünleştirilmiş sayısal ağ hizmetleri (Integrated Services Digital Network)
ISDN	: Integrated Services Digital Network
ISO	: International Organization for Standardization
LAN	: Local Area Network
MRP	: Malzeme İhtiyaç Planlaması (Manufacturing Resource Planning)
OCR	: Optik Karakter Tanıma (Optical Character Recognition)

OECD	: Ekonomik Kalkınma ve İşbirliği Örgütü (Organisation for Economic Co-operation and Development)
OSI	: Open Systems Interconnection
PSTN	: Public Switched Telephone Network
QoS	: Quality of Service
RFID	: Radio Frequency Identification
SFTP veya FTPS	: Secure FTP
SGML	: Standard Generalized Markup Language
SOX	: Sarbanes Oxley Kanunu
SSLVPN	: Secure Sockets Layer Virtual Private Network
TCKN	: Türkiye Cumhuriyet Kimlik numarası
TCP	: Transmission Control Protocol
TIFF	: Tagged Image File Format
TÜİK	: Türkiye İstatistik Kurumu
VKN	: Vergi numarası
VPN	: Sanal Özel Ağ (Virtual Private Network)
WAN	: Wide Area Network
XDSL	: Digital Subscriber Line (ADSL, ADSL2, ADSL2+, SDSL, IDSL, HDSL, VDSL, VDSL2)
XML	: Extensible Markup Language

TELEKOMÜNİKASYON SEKTÖRÜNDE VERİ TOPLAMA YÖNTEMLERİ, YENİ YAKLAŞIMLAR VE GÜVENLİK

ÖZET

Günümüzde artan teknolojik imkânlarla birlikte rekabet ortamı da gelişmektedir. Bilgiye erişmek için en önemli faktörlerden biri de hız olmaktadır. Bilgiye en hızlı şekilde erişmek için firmalar tüm sistemlerini elektronik ortama aktarmak zorundadırlar. Müşterilerin doküman üzerine kaydettiği bilgiler çeşitli teknolojiler ile dijitalleştirilip elektronik ortama aktarılmaktadır. Elektronik ortamda bu bilgiler değerlendirilip incelenmektedir.

Telekomünikasyon sektöründe Dijital arşiv sistemi, müşteri evraklarının dijital ortama aktarılması ve bu ortamda saklanması sürecini kapsamaktadır. Kanallardan toplanan müşteri evrakları, operasyon merkezlerinde işlenmekte ve fiziki olarak arşiv standartlarına uygun alarak saklanan dokümanların aynı zamanda taranarak elektronik ortamda da bu evraklar üzerinde yer alan müşteri bilgilerin toplanarak sonuçlar üretilmesini kapsamaktadır. Bununla birlikte fiziki arşivleme maliyetleri minimuma indirilmekte, alan ve işgücü kaybı azaltılmaktadır.

Kanallarda müşterilerden toplanan dokümanlar üzerinde yer alan bilgiler sayısallaştırıldığında, burada karşımıza en önemli faktör veri kalitesinin ve doğruluğunun en kısa zamanda tespiti çıkmaktadır. Sayısallaşan evrak üzerindeki bilgiler ile sistemler üzerindeki müşteri bilgileri kontrol edildiğinde ortaya çıkan sonuçlar analiz için kullanıcıya zaman kazandırmaktadır. Evraklar üzerinde yer alan bilgiler OCR (Optik Karakter Tanıma) teknolojisi yada manuel kullanıcı girişleri ile sisteme kaydedilmekte ve sistemdeki veriler ile karşılaştırılmaktadır.

Dijital ortama aktarılan verilerin farklı sistemlere gönderilmesi ile veri iletiminde güvenlik, hız ve verimlilik kavramları öne çıkmaktadır. Veri güvenliği sağlanırken, veri aktarımı sırasında tıkanıklıkların önüne geçmek için çeşitli algoritmalar tasarlanmaktadır. İlgili çalışmada veri aktarımı sırasında yaşanan tıkanıklık analiz edilerek model parametreleri oluşturulmuştur ve iyileştirme önerileri sunulmuştur.

Sahadan sürekli olarak veri toplamak, anketler düzenlemek, pazar araştırmaları yapmak firmalar için ayrı bir maliyet kalemini oluşturmaktadır. Müşteri talebini, segmentini belirlemek için etkili veri toplama yöntemleri belirlemek gerekmektedir.

Tez çalışmasında telekomünikasyon sektöründe, veri kavramı, toplanma yöntemleri ve sistemler arası aktarımda yaşanan tıkanıklıklar ele alınmıştır.

İkinci bölümde telekomünikasyon sektöründe veri toplama yöntemleri incelenmiştir. Veri, enformasyon ve bilgi kavramları arasındaki ilişkilere değinilmiştir. Telekomünikasyon sektöründe veri kavramının anlamı ve önemi tanımlanmıştır. Burada sektörde çok çeşitli veri kavramları ele alınmıştır. Abone sayıları, trafik göstergeleri, finansal göstergeler, kişisel veriler, konum verileri belirtilmiştir. Veri toplama sürecinde verilerin kalitesi güvenliği ve doğrulama süreci önemlidir.

Üçüncü bölümde veri toplama sürecinde yeni yaklaşımlar ve dijital arşiv süreci incelenmiştir. Günümüzde rekabette en önemli avantaj müşteri bilgilerine en hızlı şekilde erişilmesi ve bu bilgileri değerlendirip optimum sonuca ulaşılması ile elde edilmektedir. Bununla birlikte eldeki verilerin en iyi şekilde değerlendirilmesi gerekmektedir.

Son yıllarda tüm sektörlerde kâğıt ortamda saklanan verilerin dijital ortama geçirilmesi ve burada yer alan verilerin de değerlendirilmesi önem kazanmıştır. Telekomünikasyon sektöründe de müşterilerden elde edilen kağıt dokümanların saklanması ve dijital ortama aktarılması sağlanmaktadır. Tarama, indeksleme, validasyon, OCR (Optik Karakter Tanıma) teknolojileri ile bu bilgiler değerlendirilmekte ve sonuçlar elde edilmektedir. Çalışmada dijital arşivlemenin sektöre kazandırdıklarına değinilmiştir.

Dördüncü bölümde telekomünikasyon sektöründe güvenlik kriterleri ele alınmıştır. Bilgi güvenliği süreci, standartları ve tehditlere karşı korunma yolları belirtilmiştir. Telekomünikasyon sektöründeki yasal düzenlemeler, standartlar ve yasalar anlatılmıştır. Bilgi güvenliği ile birlikte sistemlerin korunması, donanımsal ve yazılımsal önlemlerden bahsedilmiştir. Kimlik denetimi, İnkar edememe, Veri iletiminde süreklilik, veri iletiminde güvenilirlik, veri iletiminin izlenebilirliği incelenmiştir. Bu noktada bilgisayarlar arası güvenliği bağlantı yollarına değinilmiştir. Özellikle bilgisayarlar arası iletişimin sağlanabilmesi için, nasıl ve ne zaman iletişim kurulacağına dair aynı dilin kullanılması kararlaştırılması için gerekli protokoller incelenmiştir.

Veri aktarımında güvenliğin sağlıklı olması için veri iletiminin de sağlıklı olması gerekmektedir. Burada veri aktarımında veri tipleri tanımlanmıştır. Veri gönderim sürecinde temel veri transferleri, güvenilirlik incelenmiştir. TCP performansının veri transferi uygulamaları için geliştirilmesi sağlanmıştır.

Beşinci bölümde veri aktarımında yaşanan tıkanıklıkları önleme için sistem geliştirme yöntemleri incelenmiştir. TCP protokolünde, ftp veri transferi anlatılmıştır. FTP üzerinden veri transferi sırasında kuyruk ağ analizi, gecikmeler tanımlanmıştır. Kuyruk modeli oluşturulmuş ve sistem parametreli belirtilmiştir.

Altıncı bölümde, örnek bir firmada tıkanıklık algoritmaları incelenmiştir. Veri aktarımında kuyrukta bekleme süreleri analiz edilmiştir ve yeni bir sistem önerisinde bulunulmuştur.

Anahtar Kelimeler: Veri, Veri Toplama Yöntemleri, Bilgi Güvenliği, Dijital Arşiv Sistemi, Veri Aktarım Problemleri.

DATA COLLECTION METHODS IN THE TELECOMMUNICATION SECTOR, NEW APPROACHES AND SAFETY

SUMMARY

Competitive conditions are increasing with increasing technological facilitiec in today. One of the most important factors is the speed to access information. Firms are obliged to transfer to electronic media for the fastest way to access all information systems. Customer information is transmitted to save the document on digitization electronically with various technologies. This information is analyzed and evaluated on electronically.

Digital archive system in the telecommunications sector, the digitized documents of customers and covers the storage process in this environment. Customer documents collected from the channel being processed in operations centers and physically archive documents stored electronically scanned at the same time taking appropriate standards of customer information contained in the documents collected on these results include the production. However, physical archiving costs are minimized, loss of space and labor are reduced.

The information contained on the documents are recorded in the system or manually by user input with OCR technology and compared with the data in the system.

In the transmission data to be sent to different systems of data digitized safety, speed and efficiency concepts stand out. Data security is provided, various algorithms are designed to avoid the bottleneck during data transfer. By congestion experienced during data transfer analysis model parameters related work has created and presented suggestions for improvement.

Continuously from the field to collect data, organize surveys, constitute a separate cost item for companies to do market research. Customer demand, it is necessary to determine effective methods of data collection to determine the segment.

Related work in the telecommunications sector, the concept of data, collection methods and congestion experienced in the transfer between systems is discussed.

Data collection methods of the telecommunications sector was investigated in the second section. Data, information and knowledge are referred to the relationship between concepts. The meaning of the data in the telecommunications sector and the importance of the concept is defined. Sector is discussed here in a wide variety of data concepts. Number of subscribers, traffic indicators, financial indicators, personal data, location data is specified. The quality of the data security of the data collection process and the datafication process is important.

New approaches and digital archive process the data collection process has been examined in the third section. Today, the fastest way to access to the most important competitive advantage and customer information to achieve optimal results are

obtained by evaluating this information. However, it is necessary to assess the best way of extrapolation.

Be put into digital data stored in paper media in recent years in all sectors and to evaluate the data contained here has been important. Storing paper documents obtained from customers in the telecommunications industry and digitized are provided. Scanning, indexing, validation, OCR technology with this information is evaluated and the results are obtained. Work has also been mentioned that they provide digital archiving sector.

Safety criteria of the telecommunications sector are discussed in the fourth section Information security processes, standards and protection against threats path is specified. Regulations in the telecommunications industry, standards and legislation has been introduced. Protection of information systems with the security, hardware and software measures are mentioned. Authentication, nonrepudiation, continuity of data transmission, data transmission reliability, traceability of data transmission were investigated. At this point, we focused on the security of the connection path between computers. In particular, in order to ensure communication between computers, and protocols necessary to decide how to use the same language on when to communicate were examined.

Data transfer security of data transmission to be healthy also need to be healthy. Data types of data transfer are defined herein. Data transmission basic data transfer process, the reliability was evaluated. Improving TCP performance for data transfer applications is provided.

System development methods to prevent data transfer bottlenecks experienced in the fifth section was examined. In the TCP protocol, FTP data transfer are described. Queuing network analysis during data transfer via FTP, delays have been identified. Tail model was created and the system parameter is specified.

In the sixth chapter, samples were examined congestion algorithms in a company. Were analyzed in the queue waiting time and the data transfer has been made to suggest a new system.

Keywords: Data, Data Collection Methods, Information Security, Digital Archive System, Data Transfer Problems.

1. GİRİŞ

Telekomünikasyon sektöründe en önemli sorun müşteri kaybıdır. Müşteriler doğru tanımlandığında kuruluşlar hangi müşterilerini kaybedebileceklerini önceden belirleyebilir ve böylece bu müşterilerini elde tutma amaçlı stratejiler geliştirebilir, düşük maliyetli ve etkili kampanyalar düzenleyebilirler. Kaybetme olasılığı olmayan bir müşteri için sürekli mail yada mesajlarla bu müşteriyi bilgilendirmek maliyet kaybına sebep olabilmektedir. Doğru analiz ile bu maliyetlerden elimine edilebilmektedir.

Firmalar ellerinde bulunan kayıtları kullanarak, benzer özellikler gösteren müşterileri bölümlendirip (müşteri segmentasyonu), fiyatlandırma ve promosyon stratejileri geliştirebilirler (Rygielski, Wang ve Yen, 2002, s.488). Ellerinde müşterilere ait yeterli kayıt bulunmayan firmalar ise bu rekabet ortamında zor durumda kalmaktadır. Bu yüzden müşterilerden doğru veri toplamak yada eldeki verileri en iyi şekilde çözümleyip analiz etmek gerekmektedir.

Günümüz teknolojilerinde, telekomünikasyon sektöründe müşteriden toplanan verilerin korunması, saklanması önem arz etmektedir. Müşterilerden, evrak üzerinden yada doğrudan alınan verilerin sistemlere kayıtları ve bu sistemler üzerinde incelenmeleri gerekmektedir. Son yıllarda; fiziki olarak müşterilerden alınan dokümanlar da dijital ortama aktarılarak verileri işlenmekte ve analizleri yapılmaktadır. Bundan sonraki süreç ise müşterilerden alınan verilerdeki yeterlilikler, tekrarlar ve güvenlik kapsamında gerekli olan ve olmayan verilerin analizidir. Müşterilerden alınan ham verinin anlamlı ve güvenli hale getirilmesi telekomünikasyon sektöründe önemli bir yer tutmaktadır.

Rekabetin arttığı ve bilgiye en hızlı şekilde erişmenin önem kazandığı günümüzde, müşterilerden minimum maliyet ile veri toplamanın yollarının araştırılması gerekmektedir. Bilgi toplamak için, her an müşteri ile iletişime geçmek her zaman mümkün olmamaktadır. Çoğu zaman müşteri ile iletişime geçilerek toplanan veriler maliyetlidir. Müşteriden, telefon, mesaj, internet yada kanallar yoluyla sürekli veri toplamak zaman ve işgücü gerektiren bir süreçtir.Bu yüzden eldeki verilerin en iyi şekilde değerlendirilmesi gerekmektedir. Geçmişte elde edilen veriler incelenmeli bunlar güncel süreçlere dâhil edilmelidir.

Tüm sektörlerin olduğu gibi telekomünikasyon sektöründe de müşterilere ait dokümanlar belirli arşivlerde depolanmaktadır. Bu dokümanlarda müşterilere ait çeşitli tarife bilgileri, yaş, eğitim vb. müşteri tiplerini belirleyen özellikler yer almaktadır. Bu bilgiler dijital ortama aktarıldığında, tekrar aynı bilgiler için müşterinin karşısına çıkma maliyeti engellenir. Sisteme bilgiler aktarıldığında arşivlerden bilgiye erişim hızlanmaktadır.

2. TELEKOMÜNİKASYON SEKTÖRÜNDE VERİ TOPLAMA YÖNTEMLERİ

2.1. Veri, Enformasyon, Bilgi, Üst Bilgi Kavramları ve Aralarındaki İlişki

Günümüzde veri, enformasyon, bilgi, üst bilgi kavramlarına farklı farklı alanlarda ve kullanımlarda rastlanılmaktadır. Bu kavramların yerine, genelde Türkçede sadece bilgi kelimesi kullanılırken İngilizcede her kavram için farklı kelimeler kullanılır. Veri- veri, Enformasyon- Information, Bilgi-Knowledge, Üst Bilgi-Wisdom olarak tanımlanır (Çelik ve Akgemici,2010).

2.1.1 Veri

Veri; enformasyon, bilgi, üst bilgi hiyerarşisinin en alt basamağında yer alır. Veri tek başına bir şey ifade etmez. Veri bir organizasyonda olayları temsil eden ham gerçeklerdir (Çelik ve Akgemici,2010).

Veri, tanım itibariyle, herhangi bir işletmeye tabi tutulmadan, gözlem veya ölçüm yöntemleri ile ortamdan elde edilen her türlü değerdir. Örneğin saatin kaç olduğu, ortamın anlık basıncı, bir firmadaki bir çalışanın ismi, maaşı veya yaşı gibi değerlere veri denir (Şeker, 2013).

Veri; olgu, kavram yada komutların iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimidir.

2.1.2 Enformasyon

Önemi ve amacı olan veri demektir (Çelik ve Akgemici,2010). Kısaca anlam kazandırılmış ve bir amaca hizmet eden veridir. Enformasyonun amacı, alıcının bir konudaki düşüncelerini değiştirmek, değerlendirmesi yada davranışı üzerinde bir etki yaratmaktır (Özveren, Gürsu-2004). Buradan anlaşılabileceği gibi enformasyon, anlamlandırılmış veridir.

2.1.3 Bilgi

Bilgi, sistemli bir şekilde herhangi bir iletişim aracı ile başkalarına aktarılan, mantıklı bir hükme veya tecrübeye dayanan, sonucu gösteren gerçekler veya fikirlerle ilgili düzenli ve sistemli ifadelerdir. Bilgi belli bir düzen içindeki tecrübelerin, değerlerin, amaca yönelik bir araya gelen enformasyon bütünüdür (Çelik ve Akgemici,2010).

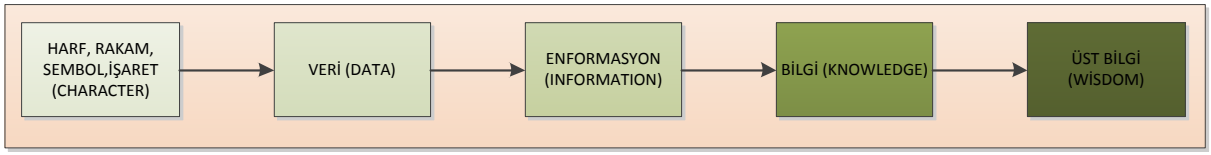
2.1.4 Üst Bilgi

Özel bir amaca yönelik olarak bilgilerin çeşitli analiz, sınıflama ve gruplama işlemlerinden geçirilmesiyle ileriye yönelik yol gösterici kullanıma hazır bilgidir. Karar verme yetisine sahip bilgidir(Çelik ve Akgemici,2010). Kısaca üst bilgi kullanılabilecek özelleşmiş bilgidir. Örneğin %45 veridir, Türkiye'de işletmelerin %45'nin düşük verimlilik arz ettiği bir bilgidir. Eğer yetkili bir kamusal kurum, bu

işletmelerin %10' nu için özendirici tedbirler öngörmekte ise, bu artık kullanılabilecek ve özel hale gelmiş bir üst bilgidir (Öğüt, 2003).

2.1.5 Veri, Enformasyon, Bilgi ve Üst Bilgi Arasındaki İlişki

Bu kavramlar birbirlerini tamamlayan, birbirlerinin devamı olan kısaca birbirleriyle ilişkili olan kavramlardır. Fakat bu kavramlar anlamları itibariyle birbirilerinden farklıdırlar. Türkçeye sonradan giren kavramlar olduğu için kelime anlamı olan tüm kavramların yerine sadece bilgi kavramına anlam yüklenmekte ve diğer kavramlar yerine de bilgi kelimesi kullanılmaktadır. Oysa İngilizcede tüm bu kavramlara ayrı kelimeler kullanılmaktadır.



Şekil 2.1 : Veri, Enformasyon, Bilgi ve Üst Bilgi Arasındaki İlişki (Çelik ve Akgemici,2010)

Toffler, veri, enformasyon ve bilgi kavramları arasındaki ilişkiyi şu şekilde tanımlamıştır: Veri genellikle farklı maddeleri tek bir bağlantıda toplamak için kullanılır; örneğin, 'X eczacılık firmasına ait 300 hisse senedimiz var' gibi. Enformasyon daha geniş, daha yüksek kalıplara yayılıp başka kalıplarla bağlantılı hale getirildiğinde bilgi dediğimiz şeyi elde ederiz; örneğin, pazarda iki puan yükselen X eczacılık firmasına ait 300 hisse senedimiz var ama volüm düşük ve muhtemelen devlet faiz oranlarını yükseltecek" gibi (Toffler, 2006).

2.2. Telekomünikasyon Sektöründe Veri Kavramı

Piyasada rekabet ortamı seviyesi yükseldikçe ve piyasa yapıları karmaşık hale geldikçe, gerçekçi ve ekonominin gelişen haline uygun politikalar oluşturabilmek için daha detaylı veriye ve daha kapsamlı veri analizine ihtiyaç duyulmaktadır.

Veri (İng. ve Lat. datum; çoğul veri) bir ham (işlenmemiş) gerçek ya da enformasyon parçacığına verilen addır (Bosij,2003).

Veriler ölçüm, sayım, deney, gözlem ya da araştırma yolu ile elde edilmektedir. Ölçüm ya da sayım yolu ile toplanan ve sayısal bir değer bildiren veriler nicel veriler, sayısal bir değer bildirmeyen veriler de nitel veriler olarak adlandırılmaktadır.

Her sembolik gösterim gibi, veri de belirli bir nesne, birey ya da olguya ilişkin bir soyutlamadır. Ancak enformasyon ve bilginin soyutluk düzeyleri ile karşılaştırıldığında, verilerin soyutluk düzeyi daha düşüktür. Bir verinin tek başına bir anlamı ve işlevi bulunmamaktadır. Veriler toplandıktan sonra gruplanarak, sıralanarak ve özetlenerek, elle ya da bilgisayarla işlenip enformasyona dönüştürüldüklerinde anlam kazanmakta; ait oldukları bağlamı açıklama gücüne

kavuşmaktadır. Problem çözme ya da karar verme gibi bir amaca hizmet edebilecek duruma gelmektedir (Peterson, 2007).

Telekomünikasyonda veri kavramı; uygulamaları için veri, anlam ve bağlamdan bağımsız, bütünlüğü ve yapısı bozulmamış ve ekonomik olarak bir noktadan diğerine iletilmesi istenen metinler, sesler, görseller ve videoları ifade eder (Peterson, 2007).

Kısaca telekomünikasyon sektöründe veri abone yada kullanıcıyı tanımlamak için gerekli olan trafik verisi, konum verisi, abone başvuru bilgilerini içerir. Her aboneye özel kullanıcı kimlikleri geliştirilmiştir. Pazar tanımlamaları ve analizleri sonucu elde edilen; Abone Sayıları, Trafik göstergeleri, tarife göstergeleri, finansal göstergeler de önemli veri türleridir (Şahin, 2011).

Tüm sektörlerde olduğu gibi telekomünikasyon sektöründe de müşteri ile herhangi bir ilişki başlamadan önce, iki tarafın birbirinin kimliklerini bilmesi ve karşısındakine dair bir görüş oluşturması gerekir. Bu noktada elde edilen veriler ile müşteriler tanımlanmaktadır. Müşterileri tanılamanın hedefi, hangi tip müşterileri istediğimizi bulmak değil (bu daha sonra gelir), her müşteriyi, kurulan her temasta o müşteri olarak tanımak ve bu farklı veri noktalarını birbiriyle birleştirerek her müşteriye dair eksiksiz bir resim çizmektir (Peppers, 2013).

Müşterileriyle ilişki kurmak isteyen firmalar bu müşterilerinin kimliklerini bilmek zorundadır. Bu yüzden de öncelikle bireysel ve kurumsal müşterilerini tanımlamak zorundadır. Burada önemli bir konu müşterilerden verileriler elde etme yöntemleridir. Firmalar ellerinde bulunan tüm veriler ile müşterileri değerlendirecek sonuçlar üretmesi gerekmektedir. Öncelikli olarak:

- Her türlü elektronik formatta mevcut müşteri verilerinin tümünün envanterinin çıkarılması gerekmektedir. Burada müşteriyi tanımlayan veriler, internet sunucusu ya da temas merkezi veri tabanı gibi birçok elektronik ortamda depolanabilir.

- Dosyalanmış ama elektronik ortamda derlenmemiş, fakat müşteriyi tanımlayan bilgiler bulunabilir. Bu bilgiler sonuç üretmek için öncelikle bilgisayar veri tabanlarına aktarılır ve buradan anlamlı sonuçlar üretilir (Peppers, 2013).

2.3. Telekomünikasyon Sektöründe Veri Çeşitleri

Çok çeşitli alanlardan veriler toplanabilmektedir. Daha önce de belirtildiği gibi sektörde veri toplarken maliyeti minimum tutmak önemlidir. Bu yüzden eldeki verilerin en iyi şekilde değerlendirilmesi gerekmektedir. Telekomünikasyon sektöründe veriler, girdi verileri ve çıktı verileri olarak iki ana gruba ayrılmaktadır.

Girdi verileri ile kastedilen, pazar segmentini belirlerken, yeni bir ürün paketi oluştururken tanımlanması gereken tüketiciye yönelik girdilerdir. Bunlar genelde,

müşteri ad/soyad, TCKN, VKN, yaş, eğitim, iş, yaşam koşulları vb bilgilerdir. Bu bilgilere göre müşteriler analiz edilir ve pazarda ürün/hizmet grupları oluşturulur.

Çıktı verileri ise ürün ve hizmeti alan müşterilerin aldıkları ürün/hizmet miktarlarını, kullanılan alanlar, elde edilen gelir vb bilgilerdir.

Her iki bilgi grubu da hem telekomünikasyon sektöründe hem de denetleyici kurumlar tarafından izlenmekte ve değerlendirilmektedir.

Elektronik haberleşme sektöründe verinin kullanılma amaçlarını üç ana başlıkta toplamak mümkündür (Güngör,2014).

1. Tekel veya Etkin Piyasa Gücüne (EPG) Sahip işletmecinin düzenlenmesi,
2. Rekabetin teşvik edilmesi ve pazarın geliştirilmesi,
3. Rekabetçi işletmecilere ve tüketicilere bilgi verilmesi.

2.3.1 Abone Sayıları

Abone sayıları, hizmetlerin erişebilirlik derecesini belirleyen en önemli göstergelerden biridir. Sektörün durumu, firmanın sektör içindeki durumu en kolay bu göstergelerden anlaşılır. Bu göstergeler çıktı göstergeleridir. Sistemler üzerinden çeşitli raporlamalar ile bu verilere erişilmektedir.

2.3.2 Trafik Göstergeleri

Trafik göstergeleri, özellikle günümüzde büyük önem kazanmıştır. Trafik verilerini en uygun düzeyde ve en uygun maliyetletlendirme ile tüketiciye sunmak önemlidir. Bu veriler sektörde yaşanan rekabeti de gözler önüne sermektedir. Trafik göstergelerinde tarife paketlerinin belirlenmesi ve piyasa sunulması sağlanmaktadır. AB mevzuatında trafik verisi ilk olarak ISDN (Bütünleştirilmiş sayısal ağ hizmetleri, Integrated Services Digital Network) direktifinde çağrıların kurulumu için işlenen veriler olarak kullanılmış ancak cep telefonları ve internetin hızlı gelişimiyle birlikte anılan direktifin yenilenme ihtiyacı ortaya çıkmıştır. Bu çerçevede, ISDN Direktifini yürürlükten kaldıran E-Gizlilik Direktifi trafik verisi için sadece telefona bağımlı olmayan bir tanım getirmiştir (Fischer, 2010). Buna göre trafik verisi, "Bir elektronik haberleşme şebekesinde haberleşmenin iletimi veya bu haberleşmenin faturalandırılması amacıyla işlenen veri' olarak tanımlanmaktadır (E-Gizlilik Direktifi, md. 2lb).

Trafik verisi, bir haberleşmenin zamanı, süresi, boyutu, yönlendirilmesi; kullanılan protokol; gönderici ve alıcının terminal cihazının konumu; haberleşmenin başladığı ve sonlandığı şebeke; bir bağlantının başlangıcı, bitişi, süresi ve ayrıca bir şebeke tarafından haberleşmenin iletildiği format hakkında bilgiler içerebilmektedir (E-Gizlilik Direktifi, md.15).

Abone ve kullanıcılara ilişkin trafik verileri bir haberleşmenin iletimi için gerekli olmadıkları takdirde silinmeli ya da anonim hale getirilmelidir (E-gizlilik Direktifi, md. 6/1). Haberleşme iletiminin tamamlandığı ve trafik verisinin - işlenmesine izin verildiği haller dışında- silinmesi gereken zaman dilimi, sağlanan hizmet türüne bağlı olmaktadır. Örneğin bir telefon görüşmesi için iletim, kullanıcılardan birinin bağlantıyı sonlandırmasıyla tamamlanırken e- posta için iletim, alıcı kişilerin hizmet sağlayıcının sunucusundan mesajları almasıyla sonlanmaktadır (E-Gizlilik Direktifi, md. 27).

2.3.3 Finansal Göstergeler

Sektörde yapılan altyapı maliyetleri, ulusal ve uluslararası piyasalardaki durum karşılaştırmaları önemli verilerdir. Firmalar bu çıktı verilerine göre durum analizi yapmaktadırlar.

2.3.4 Kişisel Veriler

Bir aboneye ait kimlik bilgileri, iletişim bilgileri, ekonomik, sosyokültürel bilgilerini içermektedir. Kişisel veriler her türlü bilgileri içerebilmektedir. Burada bir kişinin adıyla doğrudan telefon numarasına, araç plaka numarası, kimlik numarası, adres vb. bilgilere erişilebilmektedir.

Tüm bu bilgilerin korunmasında kişisel verilerin işlenmesi ve elde edilme yöntemleri önem kazanmaktadır.

Bilgi toplamada en önemli problemlerden biri de amaca uygunluk ve yeterliliktir. İnternet sitelerinden, satış noktalarından birçok bilgi toplanmakta ve bilgilerin hangi amaçla kullanılacağı belirtilmemektedir. Ölçüsüz bilgi talepleri zorunlu hale getirilmektedir.

Telekomünikasyon sektöründe önemli bir yere sahip olan örnek bir işletmede yapılan çalışmalarda müşteri bilgilerinin yer aldığı müşteri evrakları dijital sistemlere aktarılarak bu evraklar üzerinden de müşteri bilgisi elde edilmesi sağlanmaktadır. Sistem üzerindeki verilerle, evraklar üzerindeki veriler karşılaştırılarak, verilerin tutarlılığı da değerlendirilmektedir.

Kişisel veriler Veri Koruma Direktifinde, "Doğrudan veya dolaylı olarak; kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğin bir ya da birden fazla unsuruna dayanılarak kimliği belirlenebilen veya belirli gerçek kişilere ilişkin bütün bilgiler' olarak tanımlanmaktadır (Şahin, 2011).

- Kişisel veri kavramı herhangi türde bir bilgiyi barındırabilir. Hassas veriler, kişinin iş ilişkileri, sosyal ve ekonomik davranışları bu kapsamdadır.
- Bilgilerin yer aldığı araç ya da bilginin formatına ilişkin olarak kişisel veri kavramı akustik, foto grafik, sayısal ve alfabetik formatta bilgileri içerdiği

gibi videokaset veya kâğıt üzerinde saklanan bilgiler ile ikili kod (binary kod) şeklinde bilgisayar hafızasında depolanan bilgileri de kapsamaktadır.

- Bir kişinin belirlenebilir olması Veri Koruma Direktifinin tanım kısmında da belirtildiği üzere kişinin adı, boyu, saç rengi, mesleği gibi tanımlayıcılar aracılığıyla gerçekleşebilir.

- Bir kişi adıyla doğrudan; telefon numarası, araç plaka numarası, sosyal güvenlik numarası, pasaport numarası veya kişinin tanınmasına imkân verecek yaş, meslek, oturduğu yer gibi bilgilerin kombinasyonu aracılığıyla dolaylı olarak belirlenebilir.

- Ad ve adres gibi tanımlayıcılar çoğu zaman kişileri belirlemede yeterli olsa da kişisel verilerin tutulduğu elektronik dosyalar kişilere, özgün tanımlayıcılar (unique identifiers) atayabilmekte, dolayısıyla kişiyi belirlemek için ad ve adres bilgilerine gerek olmayabilmektedir.

- Internet erişim sağlayıcıları dinamik IP adresi, tarih, zaman ve süre bilgilerini sistematik olarak bir dosyada tuttukları için, IP adresi verilen internet kullanıcılarını belirleyebilmektedir. Aynı durum HTTP' sunucu üzerinde bir kayıt defteri (logbook) tutan internet servis sağlayıcıları için de geçerlidir. Bu nedenle, IP adresleri belirlenebilir bir kişiye ilişkin veriler olarak değerlendirilmektedir.

2.3.4 Konum Verileri

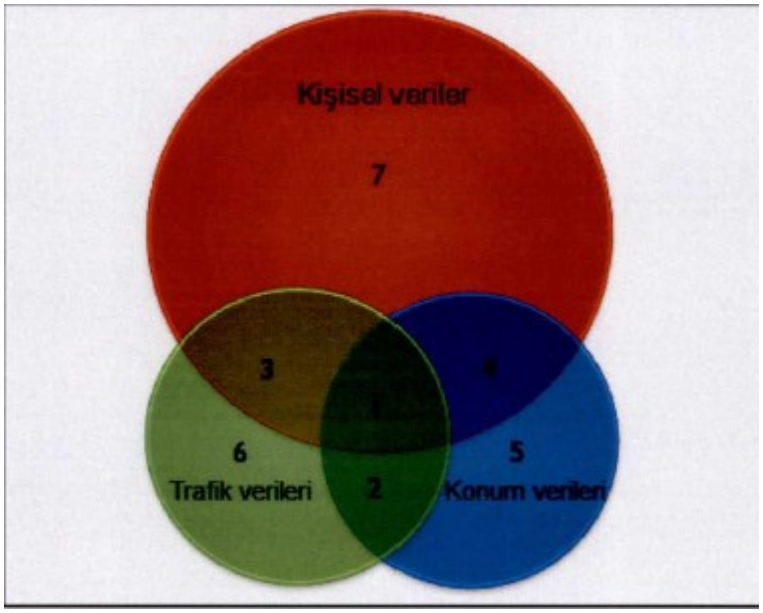
Konum verileri E-Gizlilik Direktifinde, “Kamuya açık bir elektronik haberleşme hizmeti kullanıcısına ait bir terminal cihazının coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde “işlenen her türlü veri” olarak tanımlanmış, Vatandaş Hakları Direktifinde ise tanım, “elektronik haberleşme hizmeti aracılığıyla" işlenen verileri de kapsayacak şekilde genişletilmiştir. Kullanıcı terminal cihazının enlem, boylam ve yükseklik değeri, konum bilgisinin hassasiyet düzeyi, kullanıcının hareket yönü, belirli bir zamanda terminal cihazının konumlandırıldığı şebeke hücresinin kimliği, konum bilgisinin kaydedildiği zaman gibi bilgiler konum verileri olarak değerlendirilebilmektedir (E-Gizlilik Direktifi, md.14).

Mobil şebekelerde haberleşmenin iletiminin sağlanması amacıyla işlenen ve mobil kullanıcının terminal cihazının coğrafi konumunu gösteren veriler, trafik verisi kapsamına dâhil edilirken haberleşmenin iletimi için gerekli olandan daha fazla hassasiyet sağlayan veriler konum verisi olarak değerlendirilmektedir (E-Gizlilik Direklifi. Md.35).

Örneğin mobil haberleşmenin faturalandırmasında kullanılan çağrı detay kayıtlarında (CDR) hücre kimliği (cell lD) bilgisi yer almaktadır. Burada hücre kimliği bilgisi, çağrının kurulması ve dolayısıyla haberleşmenin sağlanması için gerekli bir veri olduğundan trafik verisi niteliğindedir.

2.3.5 Veri Türleri Arasındaki İlişki

AB mevzuatında kişisel veri tanımının yer aldığı Veri Koruma Direktifi yanında elektronik haberleşme sektörüne özel Direktif hazırlanması ve trafik/konum verileri gibi veri türlerinin tanımlanmasının altında bu verilerin gizlilik karşısında belirli bir risk barındırmaları yatmaktadır. Bu nedenle, anonim hale getirme ve rıza alma gibi önlemleri teşvik etmek ve gizliliğin korunmasını sağlamak için trafik ve konum verilerinde ekstra koruma gerekli görülmektedir (Rannenberg, 2009). Veri türleri arasındaki ilişki aşağıdaki grafikte belirtilmiştir:



Şekil 2.2: Veri Türleri Arasındaki İlişkiler (Fidis,2007)

1) Kişisel veri ve trafik verisi olarak değerlendirilen konum verisi (bir cep telefonu çağrısının başlatıldığı veya sonlandırıldığı hücrenin kimlik numarası),

2) Kişisel veri olmayan trafik ve konum verisi (çağrı yapılabilen bir telefon kulübesinin konum bilgisi),

3) Konum verisi olmayan kişisel veri ve trafik verisi (bir cep telefonu abonesi tarafından yapılan çağrının tarih ve saati),

4) Trafik verisi olmayan kişisel veri ve konum verisi (bir kişinin sabit telefon adresi),

5) Trafik verisi veya kişisel veri olmayan konum verisi (gerçek sürücü adı kaydedilmeyen bir şirket arabasının GPS konumu),

6) Konum verisi veya kişisel veri olmayan trafik verisi (bir internet kullanıcısının anonim internet servisleri kullanarak bir şirketin internet sayfasına eriştiği tarih ve saat),

7) Trafik veya konum verisi olmayan kişisel veri (bir kişinin sosyal güvenlik numarası).

2.4 Veri Toplama Süreci

Telekomünikasyon sektöründe elde edilen, kullanılan ve sunulan veriler büyük önem arz etmektedir. Özellikle ulusal ekonomilerde hizmet sektörünün gelişimi telekomünikasyon sektörünün de ön plana çıkmasına neden olmuştur. Diğer hizmet sektörlerinin gelişiminde kritik bir destek unsuru olan telekomünikasyon sektörünün geliştirilmesi, günümüzde her ülkenin öncelikli politikaları arasında yer almaktadır. Telekomünikasyon operatörlerinin özelleştirilmesi, pazarların rekabete açılması gibi pek çok etken nedeniyle telekomünikasyon; mühendislerden devlet görevlilerine, ekonomistlerden bankacılara kadar pek çok farklı grubun odak noktası haline gelmiştir (ITU,2005).

Veri toplama yöntemleri planlı bir süreç gerektirir. Sektörde aboneye ait farklı alanlardan veriler toplanmaktadır. Veri toplanacak alanlar sınıflandırılmakta ve bu sınıflandırmalar üzerinden hareket edilmektedir. Toplanan verilerin analizi ve değerlendirme süreci de büyük önem kazanmaktadır. Özellikle, veri ambarlarında tutulan verilerin değerlendirilmesi ve gerektiği zaman istenen raporların ortaya çıkması ile veri madenciliği de burada önem kazanmaktadır. Veri toplama noktaları (ITU,2005):

- Yüz yüze Görüşme
- Bilgisayar Destekli Telefon Anket Sistemi
- Bilgisayar Destekli Anket Sistemi
- İnternet Üzerinden Araştırma
- Tarife Bilgileri,
- Başvuru Süreleri
- Dijital Arşiv Sistemi- Veri Doğrulama
- Veri Madenciliği (Otomatik Raporlama Platformları) Çıktı sonuçlarını incelemek için

Telekomünikasyon sektöründe; üzerinde kesin bir yargıya varılmış, anlam kazanmış her türlü ses, görüntü ve yazılar veri analizi ve anlamlı sonuç üretmek için kullanılmaktadır.

Bundan sonraki süreçte toplanan verilerin kaliteli olması; verilerin kullanıcıların ihtiyaçlarını karşılaması ve amaca uygun olması önem kazanmaktadır. Burada toplanan verilerin;

- Doğruluk: Değerler güvenilir mi?
- İlgililik: Veri kullanıcısının beklediği veriler mi?

- Zamanındalılık
- Tamlık
- Erişebilirlik olması gerekmektedir.

Veri toplama sürecinde öncelikle müşteriden alınacak verinin türü ve alınma ortamının **tanımlanması** gerekmektedir. Hangi verinin müşterinin gerçek kimliğini oluşturacağına karar verilmesi gerekmektedir. Ad, adres, ev telefonu, hesap numarası vb.Daha sonra müşteri kimliklerinin **toplanması** için gerekli düzenlemeler yapılır. Toplama mekanizmaları arasında en sık müşteri barkodları, kredi kartı verileri, kağıt uygulamaları, OCR teknolojisi, internet sitesi üzerinden internet tabanlı etkileşimler, blog yorumları, Facebook yada Twitter, Radyo frekans tanımlayıcı (RFID) gibi çok çeşitli toplama araçları sayılabilir.Bir müşteri kimliği tespit edildikten sonra, o müşteriyle tüm temas noktalarında ve işletmenin tüm farklı işletme birimleri ile bölümleri kapsamında gerçekleşen tüm işlemlerin **ilişkilendirilmesi** gerekmektedir. Müşterinin kimliğinin sadece tüm etkileşimleri ile ilişkilendirilmesiyle yetinilmemeli, diğer işlerin yürütülmesi için kullanılan bilgi sistemlerine de entegre edilerek **bütünleştirilmesi** gerekmektedir.Örgütün farklı bir bölümüne geri dönen müşteri, farklı bir müşteri olarak değil, aynı müşteri olarak **tanınmalıdır.** Tüm sistemlerde müşteri birleştirilmelidir. Burada özellikle TCKN ve VKN ile kurumsal ve bireysel müşteriler ortak bir ıd altında birleştirilmesi gerekmektedir (Deloitte, 2011). Müşteriden elde veriler üç ana gruba ayrılmaktadır. Bunlar:

- Davranışsal Veri: Satın alma alışkanlıkları, müşterinin şirketle olan etkileşimleri, seçilen iletişim kanalları, kullanılan dil, trafik verileri, hizmet/ürün tüketimi,
- Tutumsal Veri: Memnuniyet düzeyleri, algılanan rekabet konumlaması, arzu edilen özellikler ve karşılanmamış ihtiyaçların yanı sıra yaşam tarzları, marka tercihleri, sosyal ve kişisel değerler, görüşler, vs.
- Demografik (Tanımlayıcı) Veri: Yaş, gelir, eğitim düzeyi, medeni hal, hane oluşumu, cinsiyet, ev sahipliği, vs. şeklinde ayrılır.

Bir müşteri veri tabanında bulunan verilerin sınıflandırılmasında, bazı verilerin (doğum tarihi yada cinsiyet gibi sabit verilerin) sadece bir kez toplanması gerekeceğini bilmek önemlidir. Doğrulukları onaylandıktan sonra, bu veriler bir veri tabanında uzun süreler ve birçok programda varlıklarını sürdürebilir. Bunun dışında sürekli güncelleme gerektiren veriler vardır. Örneğin; bir kişinin planlanan alımları, tarife tercihleri, hatta toplumsal görüşleri değişebilir (Deloitte, 2011).

2.5 Veri Toplam Sürecinde Veri Kalitesi ve Bütünlüğü

Verilerin kalitesi kullanıcıların kararlarını etkiler. Bu yüzden verilerin analizinde farklı verilerin farklı sonuçlar ortaya çıkaracağı unutulmamalıdır. Standart olmayan veriler yüzünden, verilerin işlenmesi ve analizi sonrası kalitede farklılaşmalar oluşabilmektedir.

Sektörde müşterilerden toplanan verilerin incelenmesi ve analiz edilmesi sonucu elde edilen verilerin saklanması, uygun ortamlarda aktarılması ve uygun sonuçlar üretilmesi önem kazanmaktadır. Burada veri tanımından yola çıkarak verinin nesneler ve nesnelerin niteliklerinden oluşan bir küme olduğunu varsayarsak kümeyi oluşturan elemanlar; kayıt (record), varlık (entity), örnek (sample, instance), nesne için kullanılabilir. Nitelik (attribute) bir nesnenin bir özelliğidir. Örnek olarak boyut (dimension), özellik (feature, characteristic) olarak da kullanılır. Nitelikler ve niteliklere ait değerler bir nesneyi oluşturur. Uygulamalarda toplanan veri yetersiz, tutarsız ya da gürültülü olabilir (Deloitte, 2011).

Günümüzde Veri Kalitesi ve Bütünlüğü hizmetleri aslında beş ana baslık çerçevesinde toplanmaktadır. Bunlar; Veri Doğrulama (Veri Validation), Veri Madenciliği (Veri Mining), Veri Temizleme (Veri Cleansing), Veri Optimizasyonu (Veri Optimization) ve Kontrollerin İzlenmesi/Takibi (Monitoring Controls).

2.5.1 Veri Doğrulama (Veri Validation)

Şirketler yeniden yapılanma ya da var olan sistemlerinde değişiklik yaratıp daha yeni ve kolay kullanılabilen sistemler ya da veriler yaratabilmek için inanılmaz çok zaman ve para harcamaktadır. Fakat bu noktada her yeni sistem uygulamasında ya da veri geçişinde verinin bozulma ihtimali olduğunu unutmamak gerekiyor. Kısaca, her yeni sistem değişikliği aslında bir risk doğurmakta ve veri doğrulama işlemine gereksinimi artırmaktadır. Dolayısı ile kurumların da bu yeni sistemlerin doğruluğunu ve verinin bütünlüğünü teyit etmeleri gerekmektedir.

Bununla birlikte son yıllarda telekomünikasyon sektöründe artan taleplerle beraber, müşterilerden alınan verilerin de doğruluğunu kontrol etmek önem kazanmıştır. Müşterilerden alınan verilerin sistemlere doğru girilmesi ve buradan sonuca gidilmesi gerekmektedir. Veri giriş hataları ve veri toplama, modelleme, sunma standartlarının olmaması karar verme sırasında kullanılan bilgilerin %25 oranında hatalı olmasına neden olmaktadır (Gartner, 2009) .Kurumlar ve kuruluşlar stratejik kararlarını ve günlük işlerini doğru olmayan ve tamamlanmamış veriler üzerinde gerçekleştirmektedir. Veri kalitesinden kaynaklı kayıplar artmakta, olası problemlere dikkat çeken araştırmaların sayısı hızla artmaktadır (DWI, 2009; Devillers vd., 2007; Goodchild, 2007). Veri kalitesi verinin kendisi kadar eski bir konu olmasına rağmen, karar verme aşamasında paydaşların katılımı arttıkça önemi hızla artmaktadır (Demirel,2009).

2.5.2 Veri Madenciliği (Veri Mining)

Veri madenciliği, büyük ölçekli veriler arasından bilgiye ulaşma isi ya da bir anlamda büyük veri yığınları içerisinden gelecek ile ilgili tahminde bulunabilmemizi sağlayabilecek bağıntıların bilgisayar programı kullanarak aranmasıdır. Veri madenciliği, büyük hacimli veri yığınları içerisinden karar alabilmek için potansiyel olarak faydalı olabilecek, uygulanabilir ve anlamlı bilgilerin çıkarılmasına verilen addır. Veri madenciliği aşamaları:

- Veri Temizleme (gürültülü ve tutarsız verileri çıkarmak)
- Veri Bütünleştirme (birçok veri kaynağını birleştirebilmek)
- Veri Seçme (Yapılacak olan analiz ile ilgili olan verileri belirlemek)
- Veri Dönüşümü (Verinin veri madenciliği tekniğinden kullanılabilecek hale dönüşümünü gerçekleştirmek)
- Veri Madenciliği (Veri örüntülerini yakalayabilmek için akıllı metotları uygulamak)
- Örüntü Değerlendirme (Bazı ölçümlere göre elde edilmiş bilgiyi temsil eden ilginç örüntüleri tanımlamak)
- Bilgi Sunumu (Madenciliği yapılmış olan elde edilmiş bilginin kullanıcıya sunumunu gerçekleştirmek)

Veri madenciliği, özel ve kamu sektörü kuruluşlarında birçok şekilde kullanılabilmektedir. Bunlardan bazıları aşağıdaki gibi sıralanabilir:

- Bir süpermarket müşterilerinin satın alım eğilimlerini irdeleyerek, promosyonlarını belli müşterilere yönlendir yönlendirmesi, aynı kaynakla daha çok satış gerçekleştirmesine yardımcı olabilir.
- Bankalar kredi kararlarında kredi isteyenlerin özelliklerini ve davranışlarını irdeleyerek batık kredi oranını azaltabilir.
- Havayolları sürekli müşterilerinin davranış biçimlerini irdeleyerek daha etkin fiyatlandırma ile kârlılıklarını artırabilirler.
- Bir telefon şirketi müşteri davranışlarından öğrendikleri ile yeni hizmetler geliştirerek, müşteri bağlılığını ve kârlılığını artırabilir.
- Maliye Bakanlığı Gelir İdaresi, şirketler için risk modelleri kurarak vergi incelemelerini daha etkin yönlendirip, vergi kaçaklarını azaltabilir.
- Hastaların teşhis ve tedavi maliyetleri irdelenerek hastalık riskinin ilk aşamada tespiti, kontrolü ve kaynak planlama açısından faydalı olur.

3. VERİ TOPLAMA SÜRECİNDE YENİ YAKLAŞIMLARDA DİJİTAL ARŞİVLEME SİSTEMİ

Günümüzde artan teknolojik imkânlarla birlikte rekabet ortamı da gelişmektedir. Bilgiye erişmek için en önemli faktörlerden biri de hız olmaktadır. Bilgiye en hızlı şekilde erişmek için firmalar tüm sistemlerini elektronik ortama aktarmak zorundadırlar. Müşterilerin doküman üzerine kaydettiği bilgiler çeşitli teknolojiler ile dijitalleştirilip elektronik ortama aktarılmaktadır. Elektronik ortamda bu bilgiler değerlendirilip incelenmektedir.

Dijital arşivlerde belgelerin özellik ve nitelik açısından da donatılabilirliği sağlanmaktadır. Etiketleme, tasnif etme, sınıflandırma, karşılaştırılabilme özellikleri ile donatılmış belgeler bilgi hiyerarşisi açısından belgeyi anlamlı bilgiye dönüştürebilmeyi de mümkün kılmaktadır. Ham veri arşive alınmış belgenin ilk hali olarak düşünülebilir. İçerisindeki veriler arşive eklendiğinde sınıfı ya da tarihi hakkında da bir veri mevcuttur fakat belgenin içeriği işlenmediği ya da başka bir kavramla ilişkilendirilmediği için ham veri şeklindedir (Gümüş, 2012).

Birleşmiş Milletler Arşivler ve Belge Yönetimi Birimi (ARMS) tarafından 2006 yılında yayımlanan Belge Dijitalleştirme Rehberi'ne göre dijitalleştirme, kâğıt belge, fotoğraf, grafik malzemeler gibi fiziksel/analog materyallerin elektronik ortama ya da elektronik ortamda depolanan imajlara dönüştürtmesi işlemi olarak tanımlanmaktadır (United Nations Archives and Records Management Section, 2006). Dijitalleştirme uygulamalarının temel olarak üç nedenden ötürü yapıldığı dile getirilmektedir (Gümüş, 2012):

- Kâğıt belge ve depolama maliyetinin azaltılması: Seçilmiş dijital belgelerin dijital ortamda depolanması kâğıt ve depolama alanı maliyetinde azaltma yarattığı gibi hayati belgelerin (vital records) korunması açısından önemlidir.

- Kurumsal İçerik Yönetimi (Enterprise Content Management) Çözümlerinin Uygulanması: Belgelerin dijitalleştirilmesi ve elektronik belgelerin kullanımının artması, kurumsal süreçlerde farklı bilgi kaynaklarının paylaşımını kolaylaştıracağı için kurumsal içerik yönetimi faaliyetleri etkin biçimde gerçekleştirilebilmektedir.

- Arşivsel Koruma: Dijitalleştirme orijinal kopyaların kullanımını azaltacağı için arşiv belgelerinin uzun süre korunmasında önemli avantajlar sağlayacağı gibi çoklu kullanım olanakları da yaratabilmektedir (United Nations Archives and Records Management Section, 2006).

Dijitalleştirme kurumsal bilgi ve belge yönetimi programlarının bir parçası olarak uygulanmak durumundadır. Kurumların hâlihazırda dosyalama, bilgi güvenliği ve belge saklama vb. planlarının olması ilgili alanda dijitalleştirme uygulamalarını kolaylaştıracaktır. Bilgi ve belge kaynaklarının kanıt niteliğinin sürdürülebilmesi için elektronik kopyaların özgün (authentic), bütün (complete) ve erişilebilir (accessible)

olması gerekir. Öte yandan hassas ya da gizlilik değeri olan belgelerin dijitalleştirilmesi dikkatli gerçekleştirilmelidir. Bu tür belgeler için uygun meta veri, güvenlik ve erişim unsurları mutlaka tanımlanmalıdır. Bu tür belgelere sadece gerekli yetkilere sahip personelin tanımlanmış sınırlamalarla erişimi sağlanmalıdır. Gizlilik değeri taşıyan belgelerin dijitalleştirilmesi ve tanımlanması işlemleri diğer belgelerden ayrı tutulmalıdır (Gümüş, 2012).

3.1 Dijital Arşiv Sistemi

Kâğıt ortamda üretilen belgelerin dijitalleştirilmesinde teknik alt yapının planlanması gerekmektedir. Görüntüleme teknolojileri, kâğıt belgelerin taramasını ve dijital ortama aktarılmasını sağlayarak elektronik doküman haline getirilmesini sağlayan sistemlerdir (Megill ve Schantz, 1999:41). Böylece diğer elektronik belgelerle birlikte bir bütünlük içinde yönetilmesi sağlanmış olur. Dijital görüntüleme işlemleri esas olarak, donanım ve yazılım bileşenlerini kullanarak görüntü yakalama, saklama, görüntüleme, işleme ve kayıtları elektronik olarak paylaşma olarak tanımlanabilir. Bir başka ifade ile dijital görüntüleme, belgelerin tarayıcılar aracılığıyla bilgisayar ortamına aktarılması ve analog formattan bilgisayar tarafından okunabilecek formata dönüştürülmesidir. Tarama işleminden sonra, belge görüntüsü farklı elektronik depolama ortamlarına aktarılabilir. Dijital Görüntüleme sistem bileşenlerini oluşturan yazılım ve donanımda teknolojiye bağımlı yaşanacak değişimler mutlaka göz önünde bulundurulmalıdır. Bu açıdan sistemde yazılımsal güncellemelerin ve donanımsal eklemelerin kolaylıkla yapılabilmesine imkân vermelidir. Sistem, verilerin taşınabilirliğini sağlamalı ve farklı yazılım ve donanım yapılarına belgelerin kolaylıkla aktarılmasını desteklemelidir. Dijital ortama aktarılan belgelerin yasal açıdan geçerliliğini sağlamak için, belgelerin güvenli bir ortamda dijital ortama aktarılmasının sağlanması gereklidir. Sistemin bunu sağladığının ve herhangi bir değişikliğe müsaade etmediğini ortaya koyması önemlidir (Aydın, 2010).

Dijital arşiv sistemlerinde evrakların elektronik ortama aktarılmasında çeşitli işlemler yapılmaktadır. Bunlar sırasıyla:

- Evrak Ayrıştırma
- Tarama
- Görüntü İyileştirme
- İndeksleme
- Kalite Kontrol
- Aktarma süreçlerini içermektedir.

3.1.1 Evrak Ayrıştırma

Servis büro hizmetine tabi dosyalardaki evraklar tarama öncesi hazırlanırlar. Bu aşamada evraklardaki zımba, ataş gibi tarayıcılarda sorun çıkarabilecek malzemeler çıkarılır, dosya içindeki farklı evraklar arasına ayraçlar yerleştirilir, taranmaya gerek olmayan sayfalar bir kenara ayrılır ve taranacak evraklar tarayıcıdan rahatlıkla geçecek şekilde düzeltilir.

3.1.2 Tarama

Düzenlenen evraklar profesyonel doküman tarayıcıları ile taranarak bilgisayar ortamına aktarılırlar. A3 ebatına kadar olan evraklar genellikle otomatik kâğıt beslemeli doküman tarayıcılar ile taranır. Burada kullanılan tarayıcılar dakikada 40 ila 100 sayfa arasında tarama yapabilmektedirler. Bu tarayıcılarda çift kâğıt geçişini engelleme/algılama, çift yüzlü tarama, otomatik görüntü iyileştirme gibi özellikler bulunur.

3.1.3 Görüntü İyileştirme

Bu aşamada taranmış görüntülerin kalitesini arttırıcı algoritmalar uygulanır. Bu işlemler yazılımsal olarak veya görüntü işleme kartları ile gerçekleştirilebilir. Sanal yeniden tarama denilen yöntemler ile her bir sayfa için ideal görüntü parametreleri otomatik olarak yeniden taramaya gerek kalmadan uygulanabilir.

3.1.4 İndeksleme

Bu adımda evraklar için arama/tasnifleme kriterleri girilir. Bu kriterler dosya numarası, müşteri adı, numarası, evrak tipi, evrak sayısı, tarih gibi bilgileri içerebilir. Bu aşamada sayfaların birleştirilmesi, evrakların birbirinden ayrıştırılması işlemleri de yapılabilir.

3.1.5 Kalite Kontrol

Kalite kontrol servis büro hizmetlerinin en önemli bileşenidir. Kısa sürede çok fazla sayıda evrakın işlenmesi hizmeti hataya meydan verebilmektedir. Bu durumda verileri hatalı girilen, taranmayan evraklar bilgisayar ortamından erişilemeyecektir. Evraklara bilgisayar ortamından erişime geçilmesinin temel dayanağı bu ortamdaki verilerin ve belgelerin hatasız olarak aktarılmasıdır. Bu durum kalite kontrol adımını ön plana çıkarmaktadır. Tarama adımı sonrası ve indeksleme adımı sonrası ayrı ayrı kalite kontrol işlemleri ile işlem doğruluğu sağlanır.

3.1.6 Aktarma

Taranmış, görüntü işleme tabi tutulmuş, verileri girilmiş evrakların verileri ile birlikte doküman arşiv sistemlerine kaydedilmesi ile işlem tamamlanmış olur. Kitap, Doküman, Belge veya formların dijital ortama aktarılması amacı ile OCR ve ICR teknolojileri kullanılmaktadır fakat OCR ve ICR teknolojileri düzensiz olarak doldurulmuş formlarda işe yaramamaktadır. Bu tarz bilgi kaynakları ve ses

kayıtlarının dijital veriye dönüştürülmesi ancak tecrübeli veri giriş operatörlerinin klavye aracılığı ile bilgisayar girilmesi ile sağlanmaktadır.

3.2 Dijital Arşiv Sisteminin Kazandırdıkları

Dijital arşivleme işlemi sonucunda fiziksel arşivlerdeki dokümanlar sunuculara kaydedilerek firma veya kuruluşlara aşağıdaki konularda zamandan ve finansal açılardan tasarruf sağlamaktadır. Burada:

- Aranılan bilgi, evrak veya dokümana doğru ve anlık erişim sağlanarak tarama ihtiyacı olmadan anlık olarak kullanılabilmesi veya iletilebilmesi.
- Ofis içi ve ofis dışından dijital arşivdeki dokümanlara VPN (Sanal Özel Ağ) veya Web Tabanlı Doküman Yönetim sistemleri sayesinde erişim imkanı.
- Dijital dokümanlara gruplandırma ve yetkilendirme yapılarak evrakların yetkisiz çalışanlara ve yetkisiz diğer kişilerin ellerine geçmesine karşı güvenliğinin sağlanması ve yanlışlıkla silinmesinin önüne geçilebilmesi.
- Dijital arşivleme yapılan ve saklama zorunluluğu olmayan evrakların imha edilerek yer tasarrufu sağlanması.
- Fiziksel ofis taşınma durumlarında doküman arşivinin taşınma giderinin olmaması.
- Dijital arşivin yeniden kullanma planına dahil edilerek ister bulut ortamında isterse başka bir lokasyonda yedeklenerek yangın, sel, deprem gibi doğal afet veya meydana gelebilecek diğer olaylarda veri kaybının önlenebilmesi.
- Aynı anda birden fazla çalışanın aynı evraklara ulaşabilmesi sayesinde ekip çalışmasına uygun olması gibi avantajlar sağlanmaktadır.

Dijital arşivleme işlemi yukarıda listelenmiş avantajları sayesinde kısa sürede yatırım maliyetinin amortismanını sağlamaktadır ve dolaylı yollardan üretim ve verimliliğe olumlu yönde etki etmektedir.

3.2.1 Dokümanlara Erişim Zamanından Tasarruf

Taranarak sayısallaştırılmış dokümanlar, resmi evraklar, belgeler ve diğer bilgi kaynakları veri tabanı veya dosya sunucularına sayısal dosyalar olarak aktarıldıktan sonra dosyalara ister index alanlarına göre isterse dosyalarda kelime veya kelime grupları bazında aramalar yapılarak hızlı erişim imkanı sağlamaktadır. Bu dosyalar saniyeler içerisinde mail eki olarak eklenerek iletilebilmekte veya içerisinden kopyalama yapıştırma yöntemiyle alıntılar yapılabilmektedir. Dokümanlara erişim hızının artması sayesinde kullanıcılar zamanlarını daha etkin kullanarak verimliliğin artmasına yardımcı olmaktadırlar.

3.2.2 Doküman Depolama Alanından Tasarruf

Saklanma zorunluluğu olan veya firmaların geçmişini barındıran tüm evrakların muhafaza edilmesi için evrak arşivi gibi fiziksel bir alan gerekmektedir. Bu alanlar seneler geçtikçe ve evraklar çoğaldıkça sorun haline gelmektedir. Kemirgenler, nem, su basmaları gibi ortam koşulları da evrak arşivlerini tehdit eden bazı etkenlerdir. Dijital arşive geçen firmalar hem bu tehditlerden kurtularak ortaya çıkan bu alanları ofis, rekreasyon vb. amaçlarla kullanarak tasarruf veya çalışanlarına motivasyon sağlamaktadırlar.

3.2.3 İnternetten Ofisinizdeki Dokümanlara Erişim İmkânı

Dijital dosyalara internet üzerinden VPN, uzak masaüstü bağlantılarla veya web tabanlı programlarla ya da doküman yönetim programlarıyla güvenli bir şekilde erişilebilmektedir. Gelişen dosya sıkıştırma teknolojileri ve internet hızları ile birlikte binlerce sayfa tek bir dosya olarak saniyeler içerisinde dünyanın her tarafından açılabilir hale gelmiştir.

3.2.4 Doküman Arşivindeki Dosyaların Ticari Programlarla Entegrasyonu

Doküman arşivlerindeki dosyalar ERP, MRP, CRM gibi ticari programlara kayıt bazında eklenerek kayıtlar üzerinden bu dosyalara erişim imkanı sağlanabilmektedir.

3.2.5 Dokümanlardaki Verilerin Güvenliği

Fiziksel olarak depolanan dokümanlar, resmi evraklar ve diğer basılı bilgi kaynakları ne kadar iyi korunursa korunsun belli bir zaman sonra yetkisiz kişilerin eline geçebilmekte kaybolabilmekte veya zamana yenik düşerek okunamaz veya kullanılamaz hale gelebilmektedir. Faks kâğıtları gibi termal kâğıtlara basılmış dokümanlar ise 1 - 2 sene sonunda tamamen yok olmaktadır. Dijital dokümanlar ise gerekli önlemler alındığı takdirde gerekli olduğu sürece saklanabilmektedir. İşletim sistemleri veya Doküman Yönetim Programları sayesinde gruplandırma ve yetkilendirme yapılarak yetkisiz kişilerin eline geçmesi de önlenebilmektedir.

3.2.6 Sınırsız Doküman Muhafaza İmkânı

Gelişen sayısal depolama ve dosya sıkıştırma teknolojileri sayesinde şirketlerin yüzlerce metrekarelik alanlarda sakladıkları tüm dokümanları gömlek cebine sığan taşınabilir disklere dahi sığabilmektedir. Dijital arşiv depolama alanının arttırılması veya başka bir ortama taşınması da oldukça kolay ve düşük maliyetlidir. Bu verilerin saklandığı ortamlar için gerekli önlemler alındığı taktirde sınırsız olarak saklanmaları mümkündür.

3.2.7 Sel ve Yangın gibi Felaketlerden Kurtarma

Firmalar veya kurumlar Disaster Recovery (Felaketten Kurtarma) planlarına dijital arşivlerini de dahil ederek. Çalışma ortamlarında meydana gelebilecek deprem, su basması, yangın, hırsızlık, patlama gibi felaket durumları, fiziksel doküman

arşivlerinin çok büyük zararlar görmesine veya tamamen yok olmasına neden olabilmektedir. Dijital arşivlerde, veriler periyodik olarak farklı ortamlara aktarılarak veya yedeklenerek çalışma ortamında oluşabilecek bu tarz felaketlerden korunabilmektedir.

3.2.8 Doküman Arşivlerinin Geri Dönüşümü

Dijital arşive geçen firmalar saklanma zorunluluğu olmayan dokümanlarını geri dönüşüme aktararak çevre koruma misyonuna katkıda bulunabilmektedirler.

3.3 Dijital Arşivlemede Belge Tanımlama Sistemleri

Tanıma teknolojilerinde önemli nokta belgeyi tanıma ve karakter tanımadaki güvenirlilik düzeyidir. Hayati belgeler için güvenlik düzeyi yüksek tutulmalıdır. Başarı oranının düşük olması, düzeltme maliyeti ve teknolojik maliyeti arttırır. Kâğıt ortamda üretilen belgelerin dijital ortama aktarıldıktan sonra ihtiyaca göre tanıma süreçlerinden geçirilebilirler. Dijitalleştirilen kâğıt belgeler için literatürde geçen birçok karakter tanıma sistemleri vardır.

3.3.1 Optik Karakter Tanıma (OCR)

Optik karakter tanımada taranan belgenin görüntü analizi ve karakter görüntüleri, elektronik belge yönetim sisteminde kullanılan ASCII karakter kodlarına dönüştürülebilir. Esasında OCR farklı formatlardaki herhangi bir dosya içindeki yazıyı tanıyarak, sonradan tekrar düzenlenebilecek metin biçimine dönüştürmektedir. Bu noktada, belge üzerindeki karakterlerin baskı kalitesi, font, nokta büyüklüğü, tip ağırlığı gibi parametrelerle desteklenerek belirli bir oranda başarı ile elde edilebilir. Örneğin, JPG formatında bulunan bir belge OCR programı ile word ya da pdf dokümanı şekline dönüştürüp kaydedilebilmektedir (Aydın,2010).

Optik Karakter Tanıma (Optical Character Recognition), bilgisayar ortamında bulunmayan yazılı dokümanların özel tarayıcılar arayıcılığıyla veya normal olarak taranmış resimlerinin FineReader, OmniPage gibi bazı özel programlar yardımıyla bilgisayar ortamına düzenlenebilecek sayısal halde ("Word", "txt") aktarılmasıdır. Bu teknoloji tipi kullanılarak masaüstü tarayıcı ile taranan bir kitabın tümü text dokümana çevrilebilmektedir. Benzer şekilde perakendeci uygulamalarda kontrol zamanında fiyat etiketleri okunabilir ve elde edilen bilgiler oluşturulan text dosyalar ile kredi kartı hesaplarında bilgi fişi yazımında da kullanılabilir(Aydın,2010).

3.3.2 Akıllı Karakter Tanıma (ICR)

Akıllı karakter tanıma, zayıf kalitedeki makine yazıları ile belli kurallar çerçevesindeki el yazılarının tanınmasında kullanılan bir yöntemdir. Orijinal el yazısı olan belgelerin dijital ortama aktarılmasında kullanılan bir sistemdir. İşleyiş açısından, optik karakter tanıma işlemiyle benzerlik gösterir. Ayrıca, OCR ve ICR birlikte kullanılabilmektedir. ICR teknolojisi fontları ve farklı el yazısı stillerini öğrenebilmektedir. Bu ya belgeler üzerinde örnek olabilecek karakterlerin

öğretilmesiyle ya da süreç içinde yeni karakter yapılarının girilerek sistemin gelişerek ilerlemesi şeklinde olabilir (Aydın,2010).

Karakter tanıma sistemlerinin yanında doküman tanıma sistemleri de bulunmaktadır. Optik doküman tanıma sistemleri, şablon tabanlı form işleme olarak bilinir ve formların tanınması ve belirli alanlarından verilerin okunarak bunların ilgili uygulamalara aktarılmasıdır. Özellikle nüfus sayım formları, Maliye Bakanlığının doldurulmasını istediği bildirgeler bu tür formlara örnek olarak verilebilir. Aklı doküman tanıma ise, temelinde formun yerleşimi ve yapısına bakarak tanınması ve bağlı olarak doküman künyesinin çıkarılmasına dayanır (TBD, 2009).

Elektronik belgelerin bütünlüğü ve gerçekliği bağlamında belge tanıma sistemlerini değerlendirdiğimizde kullanımları farklılık göstermektedir. Zira belge tanıma sistemine tabi tutulmuş bir belgenin gerçekliği ve bütünlüğünden söz edilemez. Dijital ortama aktarılan bir belgeyi bütünüyle tanımlayan bir sistemde mevcut değildir. Bu açıdan belge tanıma sistemlerini daha çok belgeye erişim açısından değerlendirmek gerekmektedir. Belge tanıma sistemlerinden geçmiş belgeleri, erişim amaçlı kullanmak gerekmektedir. Yasal geçerlilik açısından her ne kadar dijital ortama aktarılmış belgenin zaman damgası olmaması durumunda geçerliliği olmasa da, arşivsel erişim amaçlı olarak belge tanıma sistemlerinden geçmemiş dijitalleşmiş belgeleri kullanmak gereklidir. Bu çerçevede dijital ortama aktarılan belgeler için gerekli ayrımın ve sınıflandırmanın yapılması gerekmektedir. Erişim amaçlı ve arşivsel amaçlı kullanılacak belgeler olarak ayırmak faydalı olacaktır. Belge tanıma sistemlerinden geçmemiş belgeler de yasal açıdan geçerli olmasa da en azından orijinal belgenin kayıpsız görüntüsü görülebilecektir. Bu görüntülerin renkli çıktıları alınmak suretiyle yasal süreçlere belli oranda da olsa katkı sağlanabileceği düşünülmektedir(Sitts, 2000).

3.4 Dijital Arşivlemede Dosya Türleri

Genel olarak seçilen dosyanın türü arşivleme işleminin nasıl gerçekleştirileceğini belirleme açısından önemlidir. Bununla birlikte erişimin etkin ve hızlı gerçekleşmesini de doğrudan etkilemektedir. İçerdikleri bilgi türü bakımında dört ana elektronik dosya türü bulunmaktadır. Bunlar;

- Metin dosyaları,
- Görüntü dosyaları,
- Veri dosyaları
- Çoklu ortam dosyalarıdır.

Her bir dosya türü ile belge özel ya da özel olmayan formatlarda kaydedilebilir. Metin dosyaları için başlıca özel olmayan format ASCII dır. Bir ASCII metin doyası, klasör olarak da tanımlanır, zira metin özelliği ya da formatları içermez (Records Management Institute, 2000). Kelime işleme programları dokümana temel olarak

ASCII metin dosyası kullanır ve kendi özel formatlarını metine uygularlar. Dosya uzantısı belirli bir uygulamanın özel formatını tanımlar. Başlıca kelime işleme yazılımları, dokümanların başka bir kelime işleme uygulamalarınca üretildiğini göstermek için özel bir filtre ile birlikte gelir.

Arşivleme açısından farklı formatlar kullanılır. Arşivlemede kullanılan TIFF formatı, çoğu görüntüleme sistemi tarafından desteklenen oldukça yaygın ve bozulmaz bir formattır. Genellikle veri tabanı formatında depolanan belgeler, klasörler ve dosyalarla ilgi bütün üst bilgiler, erişilebilir şekilde muhafaza edebilmek için ASCII dosya formatında gönderilmelidir. Günümüzde, bu format, dijital muhafaza açısından en iyi standartları sunuyor görünmektedir. TIFF formatı yerine, uluslararası ISO8879 standart SGLM ve XML formatı gibi farklı alternatifler gözden geçirilmektedir. Ancak, TIFF dönüştürme işleminde standardı oluşmuş bir formattır. Ancak SGML ya da XML dönüştürme işlemi için hala özel gereklilikler sağlanmasına ihtiyaç vardır (Aydın,2010).

Uzun dönem dosya arşivleme için özel olmayan formatlar en ideal formatlar olmasına rağmen, az sayıda olmaları ve birtakım kısıtlayıcı unsurlar içermeleri dolayısıyla pek tercih edilmemektedir. ASCII ya da düz metin, veriyi yaygınlığı düşük formatta, yapıda ve fonksiyonda kayıplarla kaydedecektir. Metin dosyası olarak adlandırılan Word ve zengin metin formatı (RTF) bir Microsoft formatıdır. Bununla beraber birçok satıcı ve yazılım uygulamalarınca da desteklenmektedir. Adobe'nin ürünü PDF formatı, dosya paylaşımı ve depolanması için yaygın olarak kullanılmaktadır. Çünkü Adobe PDF özelliklerini herkesin kullanabileceği şekilde tasarlamış ve açık bir standart olarak kullanıma sunmuştur. Aslında şirketin gelecekte bu uygulamayı devam ettirme konusunda yasal bir zorunluluğu yoktur. Bunun yanında, PDF formatının geriye uyumluluk ile ilgili sorunları bulunmaktadır. Yeni sürüm genellikle eski sürümle üretilmiş dosyaları doğru bir şekilde okuyamamaktadır. Bu sorunun çözümüne yönelik olarak PDF/A olarak hâlihazırda belirlenmiş arşivsel bir sürüm geliştirilmiştir (Minnesota Historical Society, 2004).

Zaman içinde teknolojide yaşanacak tahmin edilen değişmelere rağmen, gelecekte, arşivleme için büyük zorluklar yaratacak birçok veri ve alt veri türü olacaktır. Bütün bu veri türlerini aynı düzeyde destekleyen bir sistem oluşturmak ve sürdürmek oldukça zordur. Ancak önemli belgeler XML gibi formatlarda üretilebilir (Sproull ve Eisenberg, 2005:21). Bu bağlamda, uzun dönem arşivleme ve kullanım açısından, XML şu anda en uygun format seçeneği olarak görülmektedir. 1998 yılından buyana ulusları bir standart olarak, XML hem dosya formatı ve metin tabanlı, hem de kendini tanımlayabilen, donanım ve uygulama sistemlerinden bağımsız insanın okuyabileceği işaretleme dilindedir (Minnesota Historical Society, 2004:5). Çünkü altyapından bağımsızdır. XML belgenin içeriğini yeniden tasarlama ve/veya diğerleriyle paylaşma bakımından en iyi çözümdür. XML in doğru kullanımı, belli oranda gerekli planlamanın yapılması, bunun paralelinde para ve zaman gerektirir. Ancak, yapısal niteliği dolayısıyla, gelecekte muhtemel oluşabilecek açık formatlara ilişkin takip yapabilmeye imkân tanımaktadır.

Bütün bu hususlar çerçevesinde farklı dosya türlerinin olduğu değerlendirildiğinde, dosya türünün seçiminde göz önünde bulundurulması gereken hususların mutlaka değerlendirilmesi gerekmektedir. Bunlar, aşağıdaki gibidir;

- Erişilebilirlik: Belgelerin erişilebilir ve görüntülenebilir formatta olması gereklidir.
- Uzun Ömürlülük: Dosya formatını üretenlerin uzun süre destek vermeyi sağlamları gereklidir. Eğer bu sağlanamıyorsa uzun vadede elektronik belgelerin kullanılabilirliği söz konusu değildir.
- Esneklik: Seçilen dosya formatı elektronik belgelerin paylaşımı ve kullanımıyla ilgili kurumsal amaçları mutlaka karşılamalıdır. Eğer seçilen dosya türü sadece belli bir yazılım ve donanım profiliyle okunabiliyorsa veya yaygın kullanımda olan bir format değilse, elektronik belgenin kullanımı ve paylaşımının sınırlı olduğu değerlendirilir.

3.5 Dijital Arşivlemede Dünyada Durum

- 2011 yılında dijital dünyada var olan bilginin büyüklüğü 2006 yılına oranla 10 kat daha büyük olmuştur.
- Dünyanın en zengin kütüphanesinde (Kongre Kütüphanesi) 170 milyon belge var. İnternet ortamında 550 milyar belge var. Dünya üzerinde her bir kişiye 90 belge düşmektedir.
- Her yıl Kongre Kütüphanesi‘ni 37 000 kez dolduracak kadar bilgi üretilmektedir. Bu bilginin %92‘si manyetik ortama kayıtlıdır.
- Dünyada her yıl 2 Exabyte (100 katrilyon byte) bilgi üretiliyor (20 milyar adet The Economist dergisi).
- ABD‘de yılda 80 milyar fotoğraf, 2 milyar röntgen filmi çekiliyor. Günde 610 milyar elektronik posta gönderiliyor. Dünya‘da her yıl üretilen bilgi için 1,5 milyar gigabyte‘lık saklama ortamı gerekiyor (Gümüş, 2012).

3.6 Dijital Arşivlemede Türkiye’de Durum

TÜİK‘in 2010 yılı araştırmasına göre (TUİK, 2010)

- Hanelerin %34‘ünde masaüstü ve %17‘sinde dizüstü bilgisayar var. Toplam %51. 2 evden birinde bilgisayar var.
- İnternet abonesi 2003 yılında 19 000, 2006‘da 2,8 milyon ve 2010 Haziran‘ında 7,7 milyon. İnternette yıllık büyüme oranı %25.
- Hanelerin %42‘si İnternete ulaşabiliyor. Bu oran kentlerde %49.

- İnterneti dergi gazete okuma amacıyla kullanım oranı %59. Ailelerin yarısı İnterneti radyo dinleme ve TV izleme amacıyla kullanıyor.
- Cep telefonu üzerinden hizmet alanların sayısı şimdilik 1 milyon.
- 2010 yılı ortasında cep telefonu abone sayısı 61,5 milyon. 3G abone sayısı 11,4 milyon.
- Kuruluşlarda bilgisayar kullanım ve internet erişimine sahiplik oranları 2009 yılı itibariyle %90,7 ve %88,8.
- İnternet erişimine sahip girişimlerin internet sayfasına sahiplik oranı 2009 yılı Ocak ayında %58,7'dir.
- Milli Kütüphane koleksiyonunda bulunan 26 700 cilt yazma eserden yaklaşık 25.200 cildinin dijital ortama aktarılması tamamlanmıştır. Bu yazmalara ait dijital ortama aktarılan sayfa sayısı da yaklaşık 3 525 000 poza ulaşmıştır. 1100 adet sesli kaset kitaptan 387 adeti dijital ortama aktarılmıştır.
- Devlet Arşivleri Genel Müdürlüğü Cumhuriyet Arşivi'nde 9 386 457 dijital materyal bulunmaktadır.

3.7 Telekomünikasyon Sektöründe Dijital Arşiv Sisteminin Veri Toplamada Etkisi

Telekomünikasyon sektöründe Dijital arşiv sistemi, müşteri evraklarının dijital ortama aktarılması ve bu ortamda saklanması sürecini kapsamaktadır. Kanallardan toplanan müşteri evrakları, operasyon merkezlerinde işlenmekte ve fiziki olarak arşiv standartlarına uygun alarak saklanan dokümanların aynı zamanda taranarak elektronik ortamda da bu evraklar üzerinde yer alan müşteri bilgilerin toplanarak sonuçlar üretilmesini kapsamaktadır. Bununla birlikte fiziki arşivleme maliyetleri minimuma indirilmekte, alan ve işgücü kaybı azaltılmaktadır.

Kanallarda müşterilerden toplanan dokümanlar üzerinde yer alan bilgiler sayısallaştırıldığında, burada karşımıza en önemli faktör veri kalitesinin ve doğruluğunun en kısa zamanda tespiti çıkmaktadır. Sayısallaşan evrak üzerindeki bilgiler ile sistemler üzerindeki müşteri bilgileri kontrol edildiğinde ortaya çıkan sonuçlar analiz için kullanıcıya zaman kazandırmaktadır. Evraklar üzerinde yer alan bilgiler OCR teknolojisi ile yada manuel kullanıcı girişleri ile sisteme kaydedilmekte ve sistemdeki veriler ile karşılaştırılmaktadır.

4. GÜVENLİK

4.1 Genel Olarak Bilgi Güvenliği

Bilgi sistemlerinin gelişme göstermesi ve elektronik ticaret uygulamalarının yaygınlaşarak firmaların yazılımlara bağımlılığının artması, beraberinde güvenlik sorunlarının da dikkatle ele alınmasını gerekli kılmıştır. Bilgi Güvenliği, bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özelliklerini de kapsar (TS ISO/IEC 27001, 2006).

Firmalar için kaybedilen bilginin maliyetinin mega byte başına 2000-8000$ arasında değiştiği öngörülmektedir. FBI'ın 2004-2005 yılları arasında firmaların kayıpları ve sınıflandırılmasına yönelik yaptığı çalışmada bilgi hırsızlığında ortaya çıkan durumları aşağıdaki şekilde belirtmiştir. (Çelik, 2010):

Tablo 4.1 : FBI Anket Sonuçları

	Firmaların Kayıpları		
Suç Kategorisi	**2004 n=269**	**2005 n=639**	**2004'den 2005'e değişim**
Bilgiye Yetkisiz Erişim	51.545$	303.234$	%488
Kişisel Bilgi Hırsızlığı	168.2594$	355.552$	%111
Tüm Suçlardan Toplam Kayıplar	526.010$	203.606$	-%61
	141.496.560$/269	130.104.542$/639	

4.1.1 Gizlilik

Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliğidir (ISO/IEC 27000:2009).

Gizlilik, bilgiye, varlığa sadece yetkili insan ve organizasyonların ulaşılabilmesidir. Bugün şifreleme altyapılarının olmasının sebebi temel olarak gizlilik ve bütünlüktür. Bilgi güvenliğinin her kavramı her kurum için eşit önemde olmayabilir. Gizlilik özellikle kamu kurumları ve bankalar gibi kuruluşlar için önemlidir (Zobi, 2008).

Gizlilik Uluslararası Standartlar Örgütü (ISO) tarafımdan "Bilgiye sadece yetkilendirilmiş kişilerce ulaşılabilmesi" olarak nitelenir. Günümüzde birçok Bilişim ve Telekomünikasyon firmasında şifreleme alt yapılarının kullanılmasının sebebi temel olarak bilginin gizliğinin sağlanılmasının gerekliliğidir. Gizlilik genel olarak; Bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir (Önel ve Dinçkan, 2007).

Gizlilik, özellikle bir yasa, kanun veya standart dolayısıyla kurum için bir zorunluluk ise önemlidir. Örneğin avukat - müvekkil ilişkisi ya da doktor hasta ilişkisi gibi

mesleki bilgiler kanun ile koruma altına alınmıştır. Bazı durumlarda ise taraflar birtakım bilgileri sözleşme ile birbirlerine verirlerken gizlilik anlaşmaları yaparlar. Her iki durumda da gizlilik büyük önem taşımaktadır (Henkoğlu, 2012).

Telekomünikasyon sektörü içinde gizlilik; bilgi güvenliği kavramları arasında en önemli kavram olarak nitelenmektedir. Bu nedenle Bilgi Teknolojileri ve İletişim Kurumu tarafından 2004 yılında 25365 Sayılı Resmi Gazete ile ―Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik‖ yayınlanmıştır. Bu yönetmelikte Telekomünikasyon Sektöründe Gizliliğin önemi Madde 8 ile açıkça belirtilmiştir. Madde 1 ile de ilgili yönetmeliğin kapsamı belirlenmiştir.

Madde 1 — Bu Yönetmeliğin amacı, Telekomünikasyon sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunmasının güvence altına alınmasına ilişkin usul ve esasları düzenlemektir. Bu Yönetmelik, Telekomünikasyon sektöründe hizmet veren ve alan gerçek ve tüzel kişileri kapsar.

Madde 8 — Yasaların ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının izni olmaksızın, telekomünikasyonun üçüncü şahıs tarafından dinlenmesi, kaydedilmesi, saklanması, kesilmesi veya gözetimi yasaktır. İlgili trafik verilerinin ise işletmeci tarafından hizmet amaçları dışında kaydedilmesi, saklanması ve gözetimi yasaktır.

Bu yönetmelik sonrası birçok Telekomünikasyon Kurumu için Erişim Politikaları hazırlayarak yönetmeliğe uyum sağlamışlardır. Erişim Politikaları; şifre üretim ve dağıtım, yetkilendirme, uzaktan erişim, bilgi paylaşım prosedürlerini içermektedir (Alasulu,2012).

4.1.2 Bütünlük

Varlıkların doğruluğunu ve tamlığını koruma özelliği olarak bilinmektedir (ISO/IEC 27000:2009, 2009). Bütünlük özetle verinin yahut bilginin yetkisiz kişilerce değiştirilmesine, tahrip edilmesine veya yok edilmesine karşı korunmasıdır (Zobi, 2008).

Bilgi varlığının bozulması kasten yahut kaza ile olabilir bu durum bütünlük özelliğinin bozulmuş olduğu gerçeğini değiştirmez. Güvenlik önlemi alanların iki tür riske karşı da tedbir almaları gerekmektedir. Bilginin bütünlüğü; kesinlik, doğruluk ve geçerlilik kıstaslarını sağlaması gerekmektedir (Zobi, 2008).

National Information Assurance'nin tanımına göre veri bütünlüğü güvenlik anlamında verinin yahut bilginin yetkisiz kişilerce değiştirilmesine veya yok edilmesine karşı korunmasıdır Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması diyebiliriz (Yıldız, 2007).

Verinin bozulması kasten yahut kaza ile olabilir ve bu bütünlüğün bozulmuş olduğu gerçeğini değiştirmez. Güvenlik önlemi alanların iki tür riske karşı da tedbir almaları gerekmektedir. Bilginin bütünlüğü için; Kesinlik, Doğruluk ve Geçerlilik kıstasları sağlamalıdır (Yıldız, 2007).

4.1.3 Kullanılabilirlik

Varlığın kullanılabilirlik özelliği birçok kaynakta "Erişilebilirlik" olarak geçmekte ise de TS ISO/IEC 27001:2005 Standardında "Kullanılabilirlik" olarak ifade edildiğinden tezde kullanılabilirlik olarak tanımlayacağız. Kullanılabilirlik, bilginin (varlığın) yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğidir. Varlığın ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. Başka bir ifadeyle, sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır (Koç, 2008).

Matematiksel olarak ifade edilirse, kullanılabilirlik herhangi bir sistemin yapılış amaçlarına göre işlev gördüğü zaman, işlev gördüğü ve görmediği toplam zamana oranıdır. Daha yalın bir anlatımla, doğru yetkilendirilmiş bir kişinin ihtiyacı olduğu anda ihtiyacı olan hizmetin orada olma oranına kullanılabilirlik, diğer bir deyişle ise erişilebilirlik denir. Verilen hizmetin ne kadar güvenilir olduğunun bir ölçütüdür. Kurumlar hizmetin ne kadar önemli olduğunun ölçümünü yapıp sistemleri ve verileri bu ihtiyaca göre yedekli hale getirirler (Yıldız, 2007).

Kullanılabilirliği anlatan bir diğer tanım ise bilginin her ihtiyaç duyulduğunda kullanıma hazır olmasıdır. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır (Dinçkan, 2007). Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir. Bu nedenle özellikle kurumun güvenlik kurallarının verinin erişilebilirliğini engellemesi gerektiği unutulmamalıdır.

Şekil 4.1 : Bilgi Güvenliği Kavramları(Yıldız, 2007).

4.2 Bilgi Güvenliği Yönetim Sistemi

Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı bir yönetim sistemidir (TS ISO/IEC 27001, 2006).

Bilgi Güvenliği Yönetim Sistemi kurumun iç verimliğinin artmasında da önemli paya sahiptir (Calder, 2009). Bu sebeple BGYS, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içermelidir.

Bilgi Güvenliği Yönetim Sistemi'ni kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek isteyen kuruluşlar TS ISO/IEC 27001:2005 Standardı gereklerini yerine getirmelidirler. Bu standartta ISO tarafından hazırlanmış ve TSE tarafından Türkçe 'ye tercümesi yapılarak Türk Standardı olarak kabul edilmiştir (TS ISO/IEC 27001, 2006).

Bilgi Güvenliği Yönetim Sistemi'ni kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır. BGYS'nin benimsenmesi kuruluşun stratejik bir kararı olmalıdır. BGYS tasarımı ve gerçekleştirmesi, ihtiyaçları ve amaçları, güvenlik gereksinimleri, kullanılan prosesler ve kuruluşun büyüklüğü ve yapısına birebirinden farklılıklar gösterecektir (TS ISO/IEC 27001, 2006).

TS ISO/IEC 27001:2005 Standardı, kuruşun kurmuş olduğu BGYS'nin akredite belgelendirme kuruluşları tarafından uygunluk değerlendirmesine esas teşkil eder.

Kuruluş Bilgi Güvenliği Yönetim Sistemi'nin etkin şekilde işlev görmesi sağlamak için, birçok faaliyetini tanımlaması ve yönetmesi gerekir (TS ISO/IEC 27001, 2006). Bu standarda diğer tüm ISO standartları gibi "Proses Yaklaşımını" benimsemiştir. Kaynakları kullanan ve girdilerin çıktılara dönüştürülebilmesi için yönetilen her faaliyet, bir proses olarak düşünülebilir. Çoğunlukla, bir prosesin çıktısı doğrudan bunu izleyen diğer prosesin girdisini oluşturur. Kuruluş içerisinde, tanımları ve bunların etkileşimi ve yönetimleriyle birlikte proseslerin oluşturduğu bir sistem uygulaması "proses yaklaşımı" olarak tanımlanabilir (Alasulu, 2012).

Bu standarda sunulan bilgi güvenliği yönetimi proses yaklaşımı, kullanıcılarını aşağıdakilerin öneminin vurgulanmasına özendirir (Buluç,2009: Kılıç, 2010):

- İş bilgi güvenliği gereksinimlerini ve bilgi güvenliği için politika ve amaçların belirlenmesi ihtiyacını anlamak,
- Kuruluşun tüm iş risklerini yönetmek bağlamında kuruluşun bilgi güvenliği risklerini yönetmek için kontrolleri gerçekleştirmek ve işletmek,
- BGYS'nin performansı ve etkinliğini izlemek ve gözden geçirmek,
- Nesnel ölçmeye dayalı olarak sürekli iyileştirmek.

Bu standart, tüm BGYS proseslerini yapılandırmaya uygulanan "Planla-Uygula-Kontrol Et-Önlem al" (PUKÖ) modelini benimser (TS EN ISO 9000, 2007). BGYS'nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve prosesler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını nasıl ürettiğini gösterir.

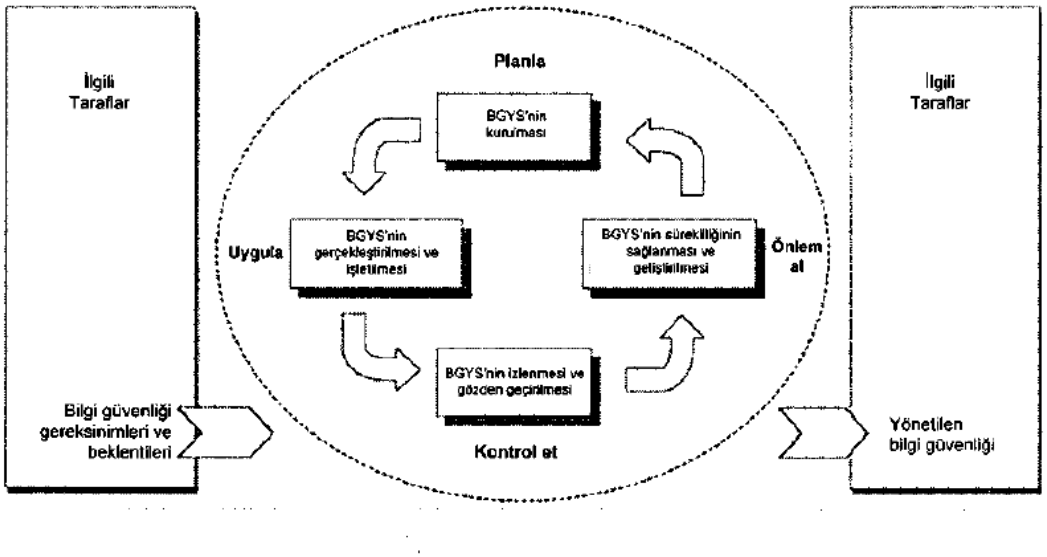
Bilgi Güvenliği Yönetim Sistemi proses tabanlı bir sistemdir. "Plânla - Uygula - Kontrol et - Önlem al" olarak bilinen (PUKO) metodolojisi, bütün proseslere uygulanabilir. PUKO kısaca şöyle açıklanabilir (TS ISO/IEC 27001, 2006).

Planla (BGYS'nin Kurulması): Sonuçları kuruluşun genel politikaları ve amaçlarına göre dağıtmak için, risklerin yönetimi ve bilgi güvenliğinin geliştirilmesiyle ilgili BGYS politikası, amaçlar, hedefler, prosesler ve prosedürlerin oluşturulması

Uygula (BGYS'nin Gerçekleştirilmesi ve İşletilmesi): BGYS politikası, kontroller, prosesler ve prosedürlerin gerçekleştirilip işletilmesi.

Kontrol Et (BGYS'nin İzlenmesi ve Gözden Geçirilmesi): BGYS politikası, amaçlar ve kullanım deneyimlerine göre proses performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesi.

Önlem Al (BGYS'nin Sürekliliğinin Sağlanması ve İyileştirilmesi): BGYS' nin sürekli iyileştirilmesini sağlamak için, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi.



Şekil 4.2 : BGYS Şeması (Yıldız, 2007).

Bilgi güvenliği, bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen

kişiler tarafından elde edilmesini önleme olarak tanımlanır. Bilgisayar teknolojilerinde güvenliğin amacı ise kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır (Canberk G. ve Sağıroğlu Ş., 2006).

Güvenlik açıklarını kurum içinde en aza indirmek ve yetkisiz kişilerin kurum için bilgilere erişimlerini engelleyebilmek amacıyla bazı altyapılar kullanılmakta ve bu alt yapılar belirli politikalar, prosedürler, planlar ve standartlar yardımıyla yönetilmektedirler (Yıldız, 2009).

Standartlar; bilgi güvenliği kurallarının kurum içinde uygulanmasını sağlarlar. Kurum içi bilgi güvenliği teknik standartları şu konuları kapsamalıdır (Carlson, 2001);

- Kişisel Güvenlik
- Çalışan Yönetimi
- Veri Sınıflandırma
- Veri Kullanma
- Veri İletimi
- Veri şifreleme
- VPNs- Sanal Özel Ağlar (Virtual Private Network)
- Veri Kurtarma
- Veri Yönlendirme (routing)
- Erişim Kontrol
- Firewall Standart
- Ağ Güvenliği
- Ağ Uygulamaları
- Log Üretimi ve Yönetimi
- Varlık Yönetimi
- Alarm Yönetimi
- Fiziksel Güvenlik

Politikalar; Bilgi güvenliğinin en iyi uygulanma biçimini resmileştirerek kurum içinde uygulanmasını sağlarlar. Kurum içi bilgi güvenliği teknik politikaları şu konuları kapsamalıdır (Carlson, 2001);

- Erişim Kontrol
- Veri Güvenliği
- Router (yönlendirici) Konfigürasyonu ve Yönetimi
- Organizasyonel Güvenlik

Prosedürler; Detaylı Bilgi güvenliği kurulumunu uygun standart ve kurallar ile kurum içinde uygulanmasını sağlarlar. Kurum içi bilgi güvenliği teknik prosedürleri şu konuları kapsamalıdır (Carlson, 2001);

- Risk Yönetimi
- Yedekleme ve Geri Yükleme (Backup/Restore)
- Sistem kullanıcı ekleme, silme ve değiştirme
- Altyapı Bakım
- Altyapı Kontrol
- Güvenlik Bakım
- Şifre Yönetimi
- Firewall Kurulumu
- Vaka Yönetimi

Plan/Programlar; Bilgi güvenliği hedeflerine uyuma teşvik ederler. Kurum içi bilgi güvenliği teknik plan ve programları şu konuları kapsamalıdır (Carlson, 2001);

- Bilgi Güvenliği Farkındalık
- Değişim Yönetimi
- Vaka Yönetimi
- Atak Tespit İş Sürekliliği

Kurumun güvenliği, organizasyonu koruyan teknolojilerden kaynaklanan ek tehditlere açık olabilir. Bu gibi durumlar, uygun teknik çözümlerin bilinmemesi ve teknoloji yönetimindeki yetersizlikler nedeniyle ortaya çıkar. Daha açık söylemek gerekirse, yanlış ve etkisiz bir konfigürasyon veya teknoloji çözümleri yönetiminin uygunsuz olması teknolojinin bilmeden ve yanlış kullanılmasına sebep olmaktadır.

Kurum içi tehditler incelendiğinde tehdidi oluşturan kişinin potansiyel olarak kurum içindeki koruyucu sistemlere giriş bilgisine ve genişletilmiş erişim kontrollerine sahip olduğu görülmüştür. Bütün bunlar saldırıyı etkiler ve tespit edilmeyi zorlaştırır (Williams, 2008). Bu nedenle Bilgi Güvenliği Ekibinin yetkinlik seviyesi teknik açıklıkların kapatılmasında ve vakaların önlenmesi açısından çok önemlidir.

4.3 Telekomünikasyon Sektöründe Bilgi Güvenliği Yönetimi ve Denetim İçin Standartlar, Yasalar ve Düzenlemeler

4.3.1 Standartlar

Bilgi güvenliği yönetimi, IT güvenliğinin tersine ancak günümüzde olgunlaşmış bir alandır. Yıllar boyu odaklanan nokta IT güvenliğiydi ve bu güvenliğin uygulanması ve kontrolü IT departmanları ve teknik uzmanlar tarafından yürütülmekteydi. 90'ların başında bu durum, güvenliğin IT kadar insana, süreçlere ve bilgiye bağlı olduğu noktasına odaklanan BS 7799 bilgi güvenliği yönetimi standardının ilk taslağıyla değişmeye başladı. 90'lardan bugüne bilgi güvenliğini bu seviyeye getiren ise taslak durumundaki bu güvenlik standartlarının birçok yenilenme ve gelişim ile ISO/IEC tarafından yayınlanan uluslararası standartlara dönüşmesidir. Bu standartlar günümüzde dünya çapında binlerce organizasyon tarafından kullanılmaktadır (Humphreys, 2008).

4.3.1.1 TS ISO/IEC 27001

Bu standart, ISO tarafından kabul edilen, ISO/IEC 27001 (2005) standardı esas alınarak, TSE Bilgi Teknolojileri ve İletişim İhtisas Grubu'nca hazırlanmış ve TSE Teknik Kurulu'nun 02 Mart 2006 tarihli toplantısında Türk Standardı olarak kabul edilerek yayımına karar verilmiştir (ISO/IEC 27001, 2006).

Bu standart, Bilgi Güvenliği Yönetim Sistemi'ni -BGYS (Information Security Management System - ISMS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır. Bir kuruluş için BGYS'nin benimsenmesi stratejik bir karar olmalıdır. Bir kuruluşun BGYS tasarımı ve gerçekleştirmesi, ihtiyaçları ve amaçları, güvenlik gereksinimleri, kullanılan prosesler ve kuruluşun büyüklüğü ve yapısından etkilenir. Bunların ve destekleyici sistemlerinin zaman içinde değişmesi beklenir. Bir BGYS gerçekleştirmesinin kuruluşun ihtiyaçlarına göre ölçeklenmesi beklenir (örneğin, basit durumlar basit BGYS çözümleri gerektirir) (ISO/IEC 27001, 2006).

ISO/IEC 27001, uyumluluğu değerlendirmek için ilgili iç ve dış taraflarca kullanılabilir. 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı, tüm kuruluş türlerini (örneğin, ticari kuruluşlar, kamu kurumları, kar amaçlı olmayan kuruluşlar) kapsar. Dokümantasyon edilmiş bir BGYS, kuruluşun tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsar. Bağımsız kuruluşların ya da tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için

gereksinimleri belirtir. BGYS, bilgi varlıklarını koruyan ve ilgili taraflara güven veren yeterli ve orantılı güvenlik kontrollerini sağlamak için tasarlanmıştır (Yıldız, 2009).

Bilgi güvenliği standardı BS 7799-2'nin revize edilip 2005'in sonlarında ISO 27001:2005 olarak değiştirilmesiyle yürürlüğe giren bu standart kurumların bilgi güvenliği yönetim sistemi kurmaları için gereklilikleri tanımlamaktadır. Bu bölümde temel olarak ISO 27001 standart oluşumu ve içeriğine değinilmiştir. Standardın içeriği ile ilgili maddeler ve diğer detaylar Bilgi Güvenliği Yönetim Sistemi kurulumu ile ilgili başlıklar altında aktarılmıştır (Yıldız, 2009).

4.3.1.2 TS ISO/IEC 27002

ISO 17799:2002 numaralı standart ISO 17799:2005, bilgi teknolojileri güvenlik teknikleri en iyi uygulamalar rehberi, olarak revize edilip yayınlanmıştır ve ISO 27001'e göre kurulacak bir BGYS'nin nasıl gerçekleştirilebileceğine dair açıklamaları içerir. ISO 17799:2005 ismi daha sonra ISO/IEC 27002:2005 olarak değiştirilmiştir (Yıldız, 2009).

4.3.2 Telekomünikasyon Sektörü için Yasalar ve Düzenlemeler

Kurumlara bilgi güvenliği yönetim altyapısını oluşturma zorunluluğu getirmenin en önemli ve kaçınılmaz yolu gerekli bilgi güvenliği yasalarını çıkarmaktan geçmektedir. BGYS kurulmasında itici güç olarak ülkedeki tüm kamu kurumlarının ve özel sektörün uyması gereken bilgi güvenliği kurallarının yer aldığı, teknoloji bağımsız bir bilgi güvenliği kanunu olması gerekmektedir. Türkiye'de gerek kamu kurumlarında gerekse özel sektörde bilgi güvenliği yönetimi tüm kuruluşların uymakla yükümlü olduğu bir yasa olmadığı için tam manasıyla algılanıp uygulanamamaktadır. Örneğin ABD'de kurumsal yönetişim ile ilgili ilkeleri ortaya koyan SOX (Sarbanes-Oxley kanunu) ve bilgi güvenliği yönetişimi ile ilgili FISMA kanunları çıkartılmış ve uygulamaya konulmuştur. Türkiye'de ise bu konuda yasal bir düzenleme bulunmamaktadır (Karabacak, 2008). Bu durumda, kurumlar için ISO/IEC 27001:2005 standardı çerçevesinde kurumsal çapta bir Bilgi Güvenliği Yönetim Sistemi oluşturmak ve işletmek oldukça zor olmaktadır.

Türkiye' de Telekomünikasyon sektöründe etkinliğini gösteren Yasa ve Düzenlemeler olarak 5651 yasası ve SOX kanunu gösterilebilir. Sarbanes-Oxley kanunu (SOX), Enron, Arthur-Anderson, Worldcom gibi uluslararası firmalarda çıkan kurumsal ve muhasebe skandallarıyla yitirilmiş olan yatırımcı güvenini arttırmak ve firmalardaki kurumsal yönetimi güçlendirmek amacıyla 2002 yılında Amerikalı Senatör Paul Serbanes ve Amerikalı Temsilci Michael Oxley tarafından çıkarılmıştır. Yasa, ABD Sermaye Piyasası Kurulu'na (Securities and Exchange Commission-SEC) kayıtlı şirketlerin, finansal raporlama üzerindeki iç kontrollerin etkinliğini değerlendirecek bir iç kontrol sistemi oluşturmalarını öngörmektedir. Dolayısıyla Türkiye'de SOX, Amerikan Serbest Piyasa Kurulu'na (SEC) kayıtlı olan şirketler üzerinde yaptırımlar içermektedir. SOX Yasası, Amerika Birleşik Devletleri

borsasında kurumların alınıp satılmasının yasalaştırılmasını etkileyen en önemli parçalardan biridir.

SOX'un Telekomünikasyon sektöründeki kuruluşlara etkileri şu şekilde sıralanabilir (Gordon, 2006);

- SEC'e kayıtlı şirketlerin her yıl bağımsız denetim firmaları tarafından SOX denetimi geçirmesi zorunlu hale gelmiştir. Denetlenen firmaların diğer ülkelerde bulunan bağlı ortaklıklarının %90' ı da bu denetlemelerden geçmek zorundadır.

- Birçok firma iç denetim sistemlerini SOX ile uyumlu hale getirebilmek için iç denetim hizmeti veren danışmanlık firmaları ile çalışmaktadır. Bu firmalar PriceWaterHouseCoopers, KPMG ve Ernst&Young gibi dünyaca kabul görmüş danışmanlık firmalarıdır. Danışmanlık firmaları şirketlerin iç denetim departmanları ile ortak çalışarak firma genelinde danışmanlık hizmeti verir.

- Şirketlerde SOX sayesinde hemen hemen her iş prosedürlere bağlanmış, özellikle manuel işler minimum seviyeye indirilmiş ve kontroller için yeni raporlar hazırlanmıştır.

4.3.3 Telekomünikasyon Sektöründe Denetim Kurumları ve Kapsamları

Kurumlar genellikle yılda bir kez danışman firmalara sistemlerinin güvenlik denetimlerini yaptırmaktadır. Fakat Danışman firmalar yanında, sistemler muhakkak kurumda çalışan bilişim teknolojileri müfettişleri tarafından denetlenmelidir. Buda kurumlarda İç Denetim ekiplerinin oluşturulması ile sağlanabilir.

Denetlemeler iç veya dış denetçiler tarafından gerçekleştirilebilir. ISO/IEC 27001 standardı bu konuda BGYS süreçleri dahilinde kurum içinde iç denetim fonksiyonu bulunmasını ve organizasyonun bunu normal denetim fonksiyonu gibi gerçekleştirmesini beklemektedir. BGYS iç denetimine ek olarak organizasyon ISO/IEC 27001 uygunluğu konusunda dış sertifikasyon denetimi almaya karar verebilir ya da şirket hisse senetlerinin SEC de değerlendirilmeye başlaması ile mecburi olarak SOX denetimlerine tabi tutulmaya başlanabilir (Humphreys, 2008).

Dışarıdan sağlanacak bir denetim seçme kararı tamamen organizasyona bağlıdır, iç denetim ise yönetim, risk yönetimi ve etkin bilgi güvenliğinin sağlanması, uygulanması, kontrolü ve yönetimi ve güncellenmesinin zorunlu bir parçasıdır. Humphreys'nin 2008 yılında yaptığı çalışmaya göre 4600 şirketin ISO/IEC 27001 sertifikasına sahip olduğu gözükmektedir (Yıldız, 2009).

Elektronik haberleşme sektöründe verilerin toplanması ve yayımlanması yetkisi sektörü düzenlemekle görevli Bilgi Teknolojileri ve İletişim Kurumuna (BTK) Kanunla verilmiştir. 5.11.2008 tarih ve 5809 sayılı Elektronik Haberleşme Kanun"unun "Kurumun Görev ve Yetkileri" başlıklı 6ncı maddesinin (h) bendinde " İşletmecilerin ticari sırları ile kamuoyuna açıklanabilecek bilgilerinin kapsamını

belirlemek, işletmecilerin ticari sırları ile yatırım ve iş planlarının gizliliğini korumak ve bunları adli makamların talepleri dışında muhafaza etmek." ifadesine yer verilerek, Kurumun verilere ilişkin yetkisi açıkça ortaya konmuştur (Güngör, 2014).

Bu Kanuna dayanılarak çıkarılan "İşletmecilere ait Ticari Sırların Korunması ile Kamuoyuna Açıklanabilecek Bilgilerin Yayımlanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik"in amacı, BTK tarafından yetkilendirilmiş elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin ticarî sırlarının korunması ile kamuoyuna açıklanabilecek bilgilerinin kapsamını belirlemektir. Yönetmelik İrlanda örneğinde olduğu gibi bilgilerin yayımlanmasında şeffaflığın artırılması, tüketicinin azami seviyede bilgilendirilmesi ve bilinçlendirilmesi ile rekabetin korunması ve geliştirilmesi ilkelerini benimsemektedir (Güngör, 2014).

4.4. Veri İletişimi ve Güvenliği

Elektronik haberleşme sektöründe düzenleme çalışmaları genellikle pazarın arz tarafıyla ilgilenmektedir. Başka bir deyişle, düzenlemelerle pazara giriş ve yetkilendirme koşulları belirlenmekte, erişim ve ara bağlantı şartları oluşturulmakta ve toptan ve/veya perakende tarifeler kontrol edilmektedir. Evrensel hizmet düzenlemelerinde dahi pazarın arz tarafına odaklanılmakta, şebeke yayılımı, erişim hizmetlerinin makul fiyatlarla sunumu, sabit hatlar için coğrafi ortalama fiyatların kullanımı ve tüketicinin hizmet alımını kolaylaştırmak için teknik gereksinimlerin getirilmesi gibi düzenlemeler getirilmektedir (Güngör,2014).

Arz tarafına yapılan bu odaklanma aslında bir gereklilik olup, düzenleyici kurumun buradaki temel görevi önceleri tekel konumunda olan pazarlarda birbiriyle rekabet içinde olan alternatif işletmecilerin var olmasını sağlamaktır. Rekabet geliştikçe ve sabit ve mobil pazarlardaki alternatif işletmeci sayısı arttıkça düzenleyici kurumların tüketici talebine olan dikkatleri artmaktadır. Örneğin, talep yönlü bir düzenleme olarak birçok ülkede kullanıcıların sabit ve mobil pazarlarda işletmecilerini değiştirmesine olanak veren numara taşınabilirliği hizmeti uygulamaya geçmiştir (Güngör,2014).

Hem arz yönlü hem de talep yönlü düzenlemeler için doğru bilgi büyük önem taşımaktadır. Bu husus düzenleme alanında özellikle telekomünikasyon düzenlemelerinde daha da ön plana çıkmaktadır. Sürekli gelişen teknoloji ve düzenlemelerin karmaşıklığı nedeniyle düzenleyici kurumun faaliyetlerini etkin bir şekilde yerine getirebilmesi için detaylı bir bilgiye ihtiyaç duyulmaktadır. Düzenleyici kurum birçok tarafı etkileyen kararlarını gerekçelendirmek, hakim konumda olan işletmeci ve alternatif işletmeciler için teşvik unsurları oluşturmak, rekabetin gelişiminin sekteye uğramamasını sağlamak, alternatifler arasından tüketicilerin makul seçimleri yapmasına olanak sağlayacak yeterli miktarda bilgiye erişimlerini sağlamak ve toplumun tüm taraflarınca anlaşılır olmak ve desteklenmek için veriye ihtiyaç duymaktadır. Bu nedenlerle düzenleyici kurumun hangi amaçlarla veriye ihtiyaç duyduğu, hangi tür verilere ihtiyacı olduğu, bu verileri en iyi hangi yollarla elde edeceği ve var olan bilgiyi nasıl kullanacağı hususundaki görüşleri net

olmalıdır. Düzenleyici kurumun etkin bir şekilde faaliyet göstermesi ancak bu şekilde mümkün olacaktır (OECD, 2008).

Bilgi çağı, hem sosyal yapı olarak hem de bir değerler bütünü olarak tüm insanlığı değişime zorlayan bir süreçtir. Aslında uygarlığın tarihi, bilgi/veri iletişiminin tarihi olarak görülebilir. Veri iletişiminin olabilmesi için verinin sembolik bir şekilde tanımlanması temel ilkedir. Başlangıçta yalnızca basit tekniklerle yapılan veri iletişimi, uygarlıkların varoluşuna ve gelişmişliğine etki etmiş ve veri iletişimini hızlandıran yöntemler geliştirilmeye başlanmıştır. Bilgisayarın gelişimiyle oluşan ağ yapıları, veri iletişimini sağlamak için tüm dünyayı çepeçevre sarmış, veri tabanları ile devasa miktarda bilgi depolanabilmiş ve bunlara erişim sağlanmıştır. Veri iletişimi, en basit biçimiyle verilerin bir kaynaktan başka bir kaynağa hatasız olarak aktarılması sürecidir (Baykal, 2005).

Veri iletişimi bilgisayar ile birçok elektronik cihaz arasında olabilir. Veri aktarımında bilgiler cihazların iletimini gerçekleştirebileceği şekilde kodlanarak aktarılır. Bilgi teknolojilerine dayalı bu aktarım teknikleri sağladığı pek çok yararla birlikte gerekli güvenlik önlemleri alınmadığı takdirde kişi ve kurumları zarara uğratabilmektedir (Eminağaoğlu ve Gökşen, 2009).

Veri güvenliği, elektronik ortamlarda verilerin saklanması, taşınması veya erişilmesi esnasında bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir veri işleme platformu oluşturma çabalarının tümüdür. Bu durumun sağlanması için, uygun güvenlik politikaları belirlenmeli ve uygulanmalıdır. Bu politikalar, işlemlerin sorgulanması, erişimlerin incelenmesi, değişiklik kayıtlarının tutulup değerlendirilmesi, silme işlemlerinin yetkiler doğrultusunda sınırlandırılması gibi düşünülebilir ve geliştirilebilir. Bilgisayar ve veri güvenliğinde karşı taraf, kötü niyetli olarak nitelendirilen (korsan, saldırganlar) kişilerdir. Bu kişiler bilgisayar güvenliğini aşmak veya atlatmak, zafiyete uğratmak, doğrudan veya dolaylı olarak zarara uğratmak, sistemlere zarar vermek, sistemin işleyişini aksatmak, durdurmak veya çökertmek gibi amaçlarla sistemlere yaptıkları bu girişimler saldırı ya da atak olarak adlandırılır. Veri güvenliği kavramı ise; verinin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önlemek olarak tanımlanabilir (Canberk ve Sağıroğlu, 2006).

Elektronik sistemlerde karşılaşılan; dinleme, değiştirme, engelleme, yeniden oluşturma, tekrar gönderme gibi sürekli gelişen atak teknikleri vardır.

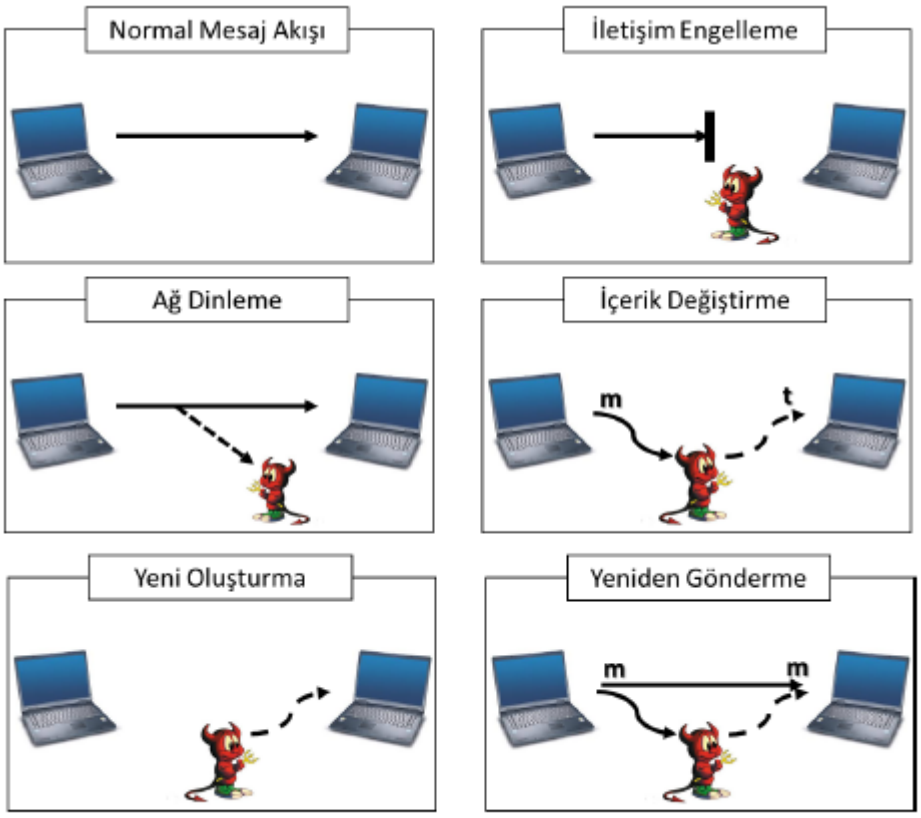
Keşif atakları; saldırı şekli olmaktan çok, arkasından yapılacak saldırılar için, hedef hakkında bilgi toplamak amacıyla geliştirilirler.

Aldatma atakları (spoofing); uç birimlerin birbirine gönderdikleri paketlerde hedef-alıcı adresi ve port bilgisinin yanı sıra gönderen uç birimin adresi ve gönderdiği port bilgisini de taşımaktadır. En çok kullanılan saldırılardan biriside “Ip Spoofing” sahte adres kullanma işlemidir. Bu basitçe bir kullanıcının kendi adresini gizlemesi olarak

düşünülebilir; fakat diğer taraftan hedefteki makine aldığı veri paketlerine karşılık yolladığı cevap paketlerini bu sahte adreslere göndereceği için bu durum masum bir adres gizleme olarak düşünülemez. Çünkü karşı tarafa gönderilen sahte adresli birçok paket, hedef uç birim kaynaklarını birçok yanlış veya ulaşamayacağı adrese cevap paketleri göndererek harcayacaktır.

Paket gözleme (sniffing); genel anlamda gidip gelen veri paketlerinin içeriğinin gözlenmesidir. Saldırgan bu şekilde ağ üzerinde aktarılan önemli bilgilere erişim sağlayabilmektedir.

Ortadaki adam saldırısı (Man in the middle); temelde ARP aldatma saldırısının kullanıldığı bu yöntemde saldırgan, bulunduğu ağdaki hedef cihaz ile hedefin iletişimde bulunduğu bir başka cihaz arasındaki trafiği kendi üzerinden geçirir. Bunu gerçekleştirebilmek için iki tarafa da gönderici ip adresi olarak birbirlerinin adreslerini fakat MAC adresi olarak kendi adresini içeren sahte ARP mesajları yollar. Uç birimler gelen bu ARP paketi sonucunda ARP geçici belleklerini güncellerler. Böylece bir uç birim diğerine bir paket gönderdiğinde bu paket aradaki saldırgana, oradan da hedef uç birime iletilir (Efe, 2006; Dwork, McSherry, Nissim, ve Smith, 2006).



Şekil 4.3: Örnek Atak Şekilleri (Hanaylı, 2014)

Elektronik ortamlarda veri güvenliğinin sağlanabilmesi için şifreleme veya gizleme teknikleri kullanılır. Bu tekniklerin dünyaca belirlenen standartlar tarafından

uygunluğu sürekli kontrol edilerek geliştirilir. Veri güvenliği üzerine NIST (Ulusal Standartlar ve Teknoloji Enstitüsü – National Institute of Standards and Technology) çağın gereklerine uygun ve güvenilir şifreleme standartları oluşturan bir kurumdur. Türkiye de ise TÜBİTAK UEKAE bünyesinde faaliyet gösteren kriptoanaliz merkezi kriptografik sistemlerin analizi ve tasarımı amacıyla kurulmuştur. Artık günümüzde veri güvenliği çok daha ön plana çıkmış ve üzerinde sürekli çalışmalar yapılan bilim haline gelmiştir.

4.4.1 Kimlik denetimi

İletimi gerçekleştirilen mesajın gerçekten karşıdaki kişi tarafından gönderildiğinden emin olunmasıdır. Bu durumda araya giren kişi mesajın içeriğini değiştirebilir ve yapılması istenilen işlemi engelleyebilir ya da kendi isteğinin yapılmasını sağlayabilir. Günümüzde kimlik denetimi birçok şekilde gerçekleştirilebiliyor ve giderek kimlik denetiminde güvenlik arttırılıyor. Bilgisayar ortamında geliştirilen matematiksel algoritmalar ya da günlük hayatta kullanılan iris, avuç içi tarama gibi güvenlik önlemleriyle kimlik denetimi güçlendirilmeye çalışılmaktadır. Bir başka deyişle kimlik denetiminde amaç verinin gerçekten karşı taraftan geldiğinin bilinmesidir. Gönderici ve alıcı birbirlerinin kimliklerini doğrulamalıdır (Hanaylı, 2014).

4.4.2 İnkâr Edememe

Ağ üzerindeki veri iletişimini sağlayan her iki taraf içinde gönderilen ve alınan verinin inkâr edilememesidir. Gönderen gönderdiğini, veriyi alan da aldığını kabul etmelidir. Bu hizmet özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde kullanım alanı bulmaktadır. Bu sistemde amaç gönderici ve alıcı arasında ortaya çıkabilecek anlaşmazlıkların en aza indirilmesini sağlamaya yardımcı olmaktadır (Ulutürk, 2010).

4.4.3 Veri İletiminde Süreklilik

Veri iletimi esnasında kullanıcı işlemlerindeki program, personel, donanım ya da kötü niyetli kişiler tarafından aksaklıklar yaşanabilir. Güvenilir bir ortamda böyle aksaklıkların hiç olmaması gerekmektedir. Veri iletiminin engellenmesi durumu online alış-veriş hizmeti sunan firmalar için düşünülebilir. Sistemlerin bir iki saat çalışmaması bile büyük zararlar oluşabilir. Bu yüzden sistem üzerindeki açıklar sürekli test edilmeli, gerekli güvenlik çalışmaları yapılmalı, personele sistem kullanımı hakkında eğitimler verilmeli, donanım ve donanımların bulunduğu ortamların bakım ve iyileştirilmesi sağlanmalıdır (Hanaylı, 2014).

4.4.4 Veri İletiminde Güvenilirlik

Sisteme verilen girdiler doğrultusunda uygun çıktıların üretilmesi ve bu durumun sürekliliğinin sağlanması veri iletiminde güvenilirliği arttırır. Amaç sistem içerisindeki tutarlılığı ve beklenen sonuçların üretilmesinin sağlanmasıdır (Hanaylı, 2014).

4.4.5 Veri İletiminin İzlenebilirliği

Ağ içerisinde işlem yapan kullanıcıların işlemlerinin kayıtlarının tutulması, incelenmesi ve sistem üzerindeki açıkların kapatılmasına ilişkin çalışmaların yapılmasıdır. Amaç yönetimin sağlanması ve gerçekleşen işlemlerin sonradan analiz edilebilmesini sağlamaktır. Uygun olamayan durumlarda oluşabilecek saldırıların önceden tespiti ve giderilmesi amaçlanmaktadır. Aynı zamanda bu yapı veri iletimindeki kavramlara destek olarak düşünülebilir (Kleidermacher ve Kleidermacher, 2012).

4.5 Bilgisayar Ağlarında İletişim Katmanları

Bilgisayar ağları veya haberleşme denildiği zaman akla ilk Telekomünikasyon kelimesi gelmektedir. Yunanca "da uzak anlamına gelen "Tele" kelimesi ve telefon, telgraf, televizyon gibi iletişim ve haberleşme cihazlarını ifade eden "Komünikasyon" kelimesinin bir araya gelmesi ile uzaktan erişimi tanımlayan bir terimdir. Günümüzde ise telekomünikasyon terimi, veri iletimi için kullanılan teknik ve terimleri tamamını kapsar hale gelmiştir (Tutkun, 2012).

Temel olarak ağ, bilgisayarları birbirine bağlayan bir dizi kablo ya da daha genel anlamda bağlantı mekanizmasından oluşur. Ağların bilgisayarları birleştirmesi, geniş bir ortamda haberleşme sağlaması sonucudur. Günümüzde sürekli hareket eden insanlar bu sayede daha rahat erişim imkânları elde etmişlerdir. Örneğin dünya çapında her gün milyonlarca kişiye hizmet veren sunucunun, hizmet alan kişiden bağımsız çalışması oldukça başarılı bir öngörü ile tasarlanmış ağ yapılarının sonucudur.

Temel bilgisayar ağlarını birbirinden ayırmak ve her birisini tanımlamak için kullanılan üç farklı kavram vardır. Bunlar LAN (Yerel Alan Ağı - Local Area Network), MAN (Şehir Alan Ağı - Metropolitan Area Network) ve WAN (Geniş Alan Ağı – Wide Area Network)"dır.

Yerel Alan Ağı – Local Area Network (LAN): Yerel ağ genellikle tek bir bina ya da birbirine yakın yerleşkeler arasındaki iletişimin sağlanması olarak tanımlanabilir. İletişimin sağlanması sırasında ağ donanımları kullanılır.

Metropolitan Alan Ağı – Metropolitan Area Network (MAN): Lan yapısına göre daha büyük bir ağ yapısıdır. Metropolitan olarak anılmasının sebebi, büyük bir şehre servis vermek için hazırlanmasıdır. Yerel alan ağları en çok iki kilometrelik alanlarda kullanılabilirken, MAN yapısında bu rakam yüz elli kilometreyi bulur.

Geniş Alan Ağı –Wide Area Network (WAN): Şehirler ve ülkeler arası iletişimi kapsayan, geniş ölçekli ağlardır. Genel olarak, farklı yapılarda yerel alan ağlarının birleştirilmesinden, geniş alan ağlarının oluşturulması mümkündür. WAN ağları sayesinde aynı şirketin, dünya üzerindeki pek çok bayi ya da satış noktasının birbirine hızlı bir ağ ile bağlanması mümkün olur. Böylece yönlendirme ayarlarının

tam olarak yapılması halinde, tek bir noktadan bütün firma çalışanları internete çıkabilecektir (Çetin ve Metin, 2005).

Bir bilgisayarda veri büyük dosyalar halinde saklanır. Veri göndermek isteyen bir bilgisayar, iletişim ortamına aynı anda çok miktarda veri gönderirse, ağ işlevselliğini yitirir, iletişim ortamı bu bilgisayarın gönderdiği büyük miktarda veri tarafından bloke edilir ve verinin tamamı gönderilene kadar diğer bilgisayarların iletişim kurması engellenir. Ayrıca, bir hata durumunda tüm verilerin bir daha gönderilmesi gerekebilir. Bu nedenle, birçok kullanıcının ortama erişimini sağlayabilmek ve veriyi hızlı bir şekilde gönderebilmek amacıyla, veri kolay kullanılabilecek küçük parçalara bölünür. Bu parçalara paket (packet) denir. Parçalar, bilgisayar haberleşmesinin temel birimleri olarak görülebilir. Bu yöntemle, ağa bağlı her kullanıcının veri gönderme ve alma şansı artar. Gönderilen paketler, alıcı tarafında hatalı olup olmadığı denetlendikten sonra, sıralı bir şekilde biriktirilir ve özgün veri yeniden oluşturulur. Bu iletişimin sağlanabilmesi için her pakete veri denetim bilgisi eklenir. Bu bilgiler, paketlerin alıcısına doğru olarak ulaşmasını sağlar. İki bilgisayar arasında paket alış-verişi sağlanması, iletişimin kurulması anlamına gelir. Fakat veri iletişimin gerçekleşebilmesi için sadece bilgisayarların birbirine bağlanması yeterli değildir. Veri iletişiminin sağlanabilmesi için iki bilgisayar sistemi arasında üst düzeyde bir işbirliği gerekmektedir. Bu işbirliği, bilgisayarlar arası iletişim (computer communication) olarak adlandırılır.

Bilgisayarlar arası iletişimin sağlanabilmesi için, nasıl ve ne zaman iletişim kurulacağına dair aynı dilin kullanılması kararlaştırılmalıdır. Bu dil protokoller aracılığıyla sağlanır. Bir başka deyişle protokoller, farklı sistemlerdeki öğeler arasındaki iletişimi sağlamak için kullanılır. Öğe, bilgi gönderme ve alma işlevini yerine getiren birim, sistem ise bir ya da birden fazla öğeden oluşan bir bütündür. Sistem bir bilgisayar, terminal ya da uzaktan algılama aygıtı olabilir. Öğe ise uygulama programları, dosya aktarım paketleri, veri tabanı yönetim sistemleri veya elektronik postalar olarak düşünülebilir. Protokoller iki öğe arasındaki veri değişiminin kurallarını belirler. Bir protokolün öncelikle belirli bir söz dizimi (syntax) olması gerekir. Ayrıca, gönderilen sinyalin düzeyi, verinin hangi biçimde gönderileceği gibi unsurların belirlenmesi gerekir. Bir protokolün, eşgüdüm ve hata saptama-düzeltme yöntemlerinin tanımlanması gerekir. Son olarak hız uyumu ve ardışık veri gönderme gibi zamanlama yöntemlerinin de belirlemesi gerekir. Veri iletişiminde farklı işlevleri yerine getirmek için farklı protokoller kullanılır. Örneğin internette, TCP/IP (Transmission Control Protocol/Internet Protocol) grubu protokoller kullanılır. İnternetin ilk yıllarında, yerel alan ağlarının, geniş alan ağlarına bağlanması kavramı ortaya çıkmış ve birbirine bağlı ağlar arası iletişim (internetwork) gündeme gelmiştir. TCP/IP de bu ağlar arası uyumsuzluk sorununun giderilmesi amacıyla geliştirilmiştir. Bir başka deyişle TCP/IP farklı topoloji ve protokollere sahip bilgisayar ağlarını birbirlerine bağlamak için kullanılan bir protokoller dizisidir (Baykal, 2005).

Bilgisayar ağlarında birçok öğe bulunur; birçok uygulama ve protokol, farklı türde uç birimler ve bunlar arasındaki iletişim türleri, yönlendiriciler ve bağlantı düzeyinde yer alan çok çeşitli ortam vardır. İnternet gibi çok büyük ağlar söz konusu olduğunda ise bu karmaşıklık daha da artar. Bir sistem birçok öğenin bulunduğu ve birçok işlevi bir anda yerine getiren karmaşık yapıya ulaştığı anda tasarımı kolaylaştırmak için soyutlama (abstraction) düzeyleri tanımlanabilir.

Soyutlama düzeyleri, ağlarda katman (layer) kavramına karşılık gelir. Büyük ve karmaşık sistemler sürekli güncellendiğinden, katmanlı yapı kullanılır. Çünkü bu yapılarda, katmanların sunduğu hizmetlerin yerine getirilme biçimini değiştirmek kolaydır. Bir katmanın işlevi değiştirildiğinde, sistemin diğer bileşenleri bundan etkilenmez. Katmanlarda da protokoller düzenlenir. Katmanlı protokol yapısında, her protokol bir katmana aittir. Bir katmana ait protokol ise, ağda bu protokolü yerine getirecek olan öğeler arasında dağıtılır. Her ağ öğesinde o katmana ait bir parça bulunur. Bu parçalar, birbirleriyle o katmana ait iletiler aracılığıyla iletişim kurar. Bu iletilere ilgili katmana ait, protokol veri birimleri (Protocol Veri Unit - PDU) denir. İki farklı ağda yer alan bilgisayarlar birbiriyle iletişime geçeceği zaman, bu bilgisayarların birbirine denk gelen eş katmanları (aynı düzey katmanlar) arasındaki iletişim, protokoller aracılığıyla sağlanır. Katmanlar ve katmanlarda uygulanan protokollerin tümüne bilgisayar ağı iletişim mimarisi ya da kısaca ağ mimarisi adı verilir. En altta veri aktarımının yapıldığı fiziksel ortam vardır. Bunun üzerinde katmanlar yer alır. Protokoller, eş düzey katmanlar arasında ortak bir dil oluşturur. Ancak veri aktarımı yalnızca fiziksel ortamdan yapılabileceği için, bu katmanlar arasında doğrudan bir iletişim yoktur.

Bunun yerine her katman, veriyi ve denetim bilgilerini bir altındaki katmana aktarır. Bitişik katmanlar arasındaki arabirimler, temel işlevleri ve hizmetleri sağlayarak bu aktarımı mümkün kılar (Baykal, 2005).

Protokollerin standartlaştırılması, farklı bilgisayar sistemlerinin birbirleri ile etkin ve doğru olarak etkileşimde bulunabilmelerine olanak sağlamaktadır. Uluslararası protokol standartlarının ilk adımı, Uluslararası Standartlar Kurumu (International Organization for Standardization - ISO) tarafından önerilmiş ve geliştirilmiştir. Bu standart Açık Sistemler Bağlantı Başvuru Modeli (Open Systems Interconnection Reference Model) ya da kısaca ISO-OSI olarak adlandırılır.

OSI başvuru modeli, yedi katmandan oluşur. Katman kavramının oluşturulması ve katman sayısının belirlenmesinde temel alınan ilkeler şunlardır:

- Yeni katman, ancak farklı düzeyde bir soyutlama gerekiyorsa oluşturulur.
- Her katman, iyi tanımlanmış bir işlevi yerine getirmelidir.
- Her katmanın yerine getireceği işlev, uluslararası protokol standartlarını tanımlamaya yönelik olarak seçilmelidir.

- Arabirimler aracılığıyla bir katmandan diğerine gönderilen bilgiler en aza indirgenmelidir.
- Katman sayısı, farklı ve çok sayıda işlevi katmanlar arasında bölüştürebilecek kadar fazla, fakat mimariyi fazla genişletmeyecek kadar az sayıda olmalıdır.

OSI bu ilkelerden yola çıkarak yedi katmanlı bir yapı önermiş ve her katmanda yapılması önerilen işlevleri tanımlamıştır.

Katman 1 (Fiziksel Katman): Verilerin fiziksel ortam üzerinden 1 ve 0 olarak aktarılmasından sorumludur. Bir başka deyişle veri ikililerinin bir iletişim kanalı boyunca doğru/hatasız gönderilmesiyle ilgilidir.

Katman 2 (Veri Bağlantı Katmanı): Gerekli eş zamanlama, hata ve akış denetimlerini sağlayarak bilginin fiziksel bağlantı üzerinden güvenli biçimde aktarılmasını sağlar. Asıl görevi gönderilen veriyi, iletişim hatalarından arındırılmış olarak fiziksel katmandan almak ve ağ katmanına göndermektir.

Katman 3 (Ağ Katmanı): Alt ağlar arasında bağlantı kurulması, sürdürülmesi ve sonlandırılmasından sorumludur. Paketlerin, ağ üzerinde yönlendirilerek gönderilmesini koordine eder. Bu katmanın temel görevi, paketlerin gönderici (kaynak) ve alıcı bilgisayara (hedef) nasıl ulaştırılacağıdır. Bu nedenle de yönlendirme protokolleri bu katman düzeyinde çalışır.

Katman 4 (Taşıma Katmanı): Oturum katmanından aldığı veriyi küçük birimlere böler ve ağ katmanına aktarır. Uçtan uca bağlantı kurulması, hata kurtarma ve akış denetimi sağlar. Gelen verinin doğruluğunu denetler ve verinin taşınması sırasında oluşan hataları ortaya çıkarır.

Katman 5 (Oturum Katmanı): Uygulamalar arasında oturum açma, sürdürme ve kapama görevlerini yerine getirerek, uygulamalar arası iletişimi ve erişim denetimini sağlar.

Katman 6 (Sunum Katmanı): Uygulamadan bağımsız olarak, verinin geçirmesi gereken sıkıştırma, kod dönüşümü, şifreleme, şifre çözme gibi işlemleri gerçekleştirir. Bu katmanda gelen paketler bilgi haline dönüştürülür. Sunum katmanı, iletilen verinin söz dizimi ve anlamıyla ilgilidir.

Katman 7 (Uygulama Katmanı): Bu katman kullanıcıya en yakın katmandır. Kullanıcıların uygulama yazılımları, veri tabanları, elektronik posta gibi programlar aracılığıyla OSI sistemine erişimini sağlar. Uygulama katmanının bir başka işlevi de dosya aktarımını sağlamaktır **(Dosya Aktarım Protokolü – File Transfer Protocol - FTP).** Farklı dosya sistemleri arasında; dosya adlandırma, metin satırı gösterimi gibi konulardaki farklılıkların yarattığı uyumsuzluklar olabilir. İki farklı sistem arasında böyle bir dosyanın aktarılmasını sağlamak, uygulama katmanının işlevleri arasındadır (Baykal, 2005).

4.6 Ağ Güvenlik Politikaları

Bilginin ve kaynakların paylaşılması gereksinimi sonucunda kurumlar, bilgisayarlarını çeşitli yollardan birbirine bağlayarak kendi bilgisayar ağlarını kurmuşlar ve sonra dış dünyayla iletişim kurabilmek için bilgisayar ağlarını İnternet'e uyarlamışlardır. Eskiden kilitli odalarla sağlanan güvenlik kavramı, bilgisayar ağları ve İnternet gibi ortamların gündeme gelmesiyle boyut değiştirmiştir. İnternet yasalarla denetlenemeyen bir sanal dünyadır. Bu sanal dünyada saldırganlar bilgiye ulaşmada ağların zayıf noktalarını kullanarak yasadışı yollar denemektedirler. Sadece yapılan saldırılarla değil, aynı zamanda kullanıcıların bilinçsizce yaptıkları hatalar nedeniyle birçok bilgi başka kişilerin eline geçmekte veya içeriği değiştirilmektedir. Kurumlarda oluşan kayıplar maddi olabileceği gibi güven yitirme gibi manevi zararlar da olabilmektedir. Bu tür durumlarla başa çıkabilmek için bazı kuralların belirlenmesi gerekmektedir (Karaarslan,2014).

Kurumların kendi kurmuş oldukları ve İnternet'e uyarladıkları ağlar ve bu ağlar üzerindeki kaynakların kullanılması ile ilgili kuralların genel hatlar içerisinde belirlenerek yazılı hale getirilmesi ile ağ güvenlik politikaları oluşturulur. Güvenlik politikasının en önemli özelliği yazılı olmasıdır ve kullanıcıdan yöneticiye kurum genelinde tüm çalışanların, kurumun sahip olduğu teknoloji ve bilgi değerlerini nasıl kullanacaklarını kesin hatlarıyla anlatmasıdır (Barman, 2001). Ağ güvenlik politikaları mümkünse sistem kurulmadan ve herhangi bir güvenlik sorunuyla karşılaşmadan önce oluşturulmalıdır. Bu aynı zamanda, kurulu olan bir sistemin güvenlik politikasını oluşturmaktan daha kolaydır. Güvenlik politikası olmadan güvenli bir bilgisayar ağı gerçekleştirilemez. Bu kadar öneme sahip olmasına rağmen Amerika'da güvenlik politikalarının gerçekleştirilme oranı sadece %60'larda kalmakta, Türkiye için bu oran daha da düşmektedir (Yelkenci, 2002). Ağ güvenlik politikaları, kurumların yapılarına ve gereksinimlerine göre değiştiğinden bir şablondan söz etmek mümkün değildir. Bu bildiride güvenlik politikası oluştururken dikkat edilmesi gerekenler belirtilmiştir. Bilgi ve ağ güvenlik politikalarından söz edildiğinde birçok alt politikadan söz etmek mümkündür. Bunun nedeni, politikaların konuya veya teknolojiye özgü olmasıdır (Sans,2003).Ağ güvenliğinin sağlanması için gerekli olan temel politikalar aşağıda sıralanmıştır (Karaarslan,2014):

1. Kabul edilebilir kullanım (acceptable use) politikası

2. Erişim politikası

3. Ağ güvenlik duvarı (firewall) politikası

4. İnternet politikası

5. Şifre yönetimi politikası

6. Fiziksel güvenlik politikası

7. Sosyal mühendislik politikası

4.6.1 Kabul Edilebilir Kullanım (Acceptable Use) Politikası

Ağ ve bilgisayar olanakların kullanımı konusunda kullanıcıların hakları ve sorumlulukları belirtilir. Kullanıcıların ağ ile nasıl etkileşimde oldukları çok önemlidir. Yazılacak politikada temelde aşağıdaki konular belirlenmelidir (Holbrook, 1991):

- Kaynakların kullanımına kimlerin izinli olduğu,
- Kaynakların uygun kullanımının nasıl olabileceği,
- Kimin erişim hakkını vermek ve kullanımı onaylamak için yetkili olduğu,
- Kimin yönetim önceliklerine sahip olabileceği,
- Kullanıcıların hakları ve sorumluluklarının neler olduğu,
- Sistem yöneticilerin kullanıcılar üzerindeki hakları ve sorumlulukların neler olduğu,
- Hassas bilgi ile neler yapılabileceği.

4.6.2 Erişim Politikası

Erişim politikaları kullanıcıların ağa bağlanma yetkilerini belirler. Her kullanıcının ağa bağlanma yetkisi farklı olmalıdır. Erişim politikaları kullanıcılar kategorilere ayrıldıktan sonra her kategori için ayrı ayrı belirlenmelidir. Bu kategorilere sistem yöneticileri de girmektedir. Sistem yöneticisi için erişim kuralları belirlenmediği takdirde sistemdeki bazı kurallar sistem yöneticisinin yetkisine bırakılmış olacağından, bu sistem üzerinde istenmeyen güvenlik açıkları anlamına gelebilecektir (Karaarslan,2014).

4.6.3 Ağ Güvenlik Duvarı (Firewall) Politikası

Ağ güvenlik duvarı (network firewall), kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında kurumun karşılaşabileceği sorunları çözmek üzere tasarlanan çözümlerdir. Ağın dışından ağın içine erişimin denetimi burada yapılır. Bu nedenle erişim politikaları ile paraleldir. Güvenlik duvarları salt dış saldırılara karşı sistemi korumakla kalmaz, performans arttırıcı ve izin politikası uygulayıcı amaçlar için de kullanılırlar. Bu çözümler yazılım veya donanımla yazılımın bütünleşmesi şeklinde olabilir. Güvenlik duvarlarının grafiksel arabirimleri kullanılarak kurumun politikasına uygun bir şekilde erişim kuralları tanımlanabilmektedir. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmektedir (Karaarslan,2003):

- Proxy: Proxy bir bağlantı uygulamasında araya giren ve bağlantıyı istemci (client) için kendisi gerçekleştiren bir hizmettir. Proxy'nin kullanımı, uygulama temelli (application-level) güvenlik duvarı olarak da

adlandırılabilir. Bu tür bir uygulama aynı zamanda kimlerin bu hizmetleri kullanacağını belirlemek ve performans amaçlı olarak bant genişliğinin daha etkin kullanılmasını sağlamak için de kullanılır.

- Anti-Virus Çözümleri: HTTP, FTP ve SMTP trafiğini üzerinden geçirerek virüs taramasını yapmayı ve kullanıcıya gelmeden önce virüslerden temizlemeyi hedefleyen sistemlerdir.

- İçerik Süzme (content filtering): Çeşitli yazılımlarla ulaşılmak istenen web sayfalarını, gelen e-posta'ları süzmeye yarayan sistemlerdir.

- Özel Sanal Ağlar (Virtual Private Network-VPN): Ortak kullanıma açık veri ağları (public veri network) üzerinden kurum ağına bağlantıların daha güvenilir olması için VPN kullanılmaktadır. İletilen bilgilerin şifrelenerek gönderilmesi, Genel/Özel (Public/Private) anahtar kullanımı ile sağlanır. VPN kullanan birimler arttıkça daha sıkı politika tanımları gerekli hale gelmektedir.

- Nüfuz Tespit Sistemleri (Intrusion Detection Systems-IDS): Şüpheli olayları, nüfuz ve saldırıları tespit etmeyi hedefleyen bir sistemdir. IDS, şüpheli durumlarda e-posta veya çağrı cihazı gibi yöntemlerle sistem yöneticisini uyarabilmektedir.

4.6.4 İnternet Politikası

Kurum bazında her kullanıcının dış kaynaklara örneğin İnternet'e erişmesine gerek yoktur. İnternet erişiminin yol açabileceği sorunlar aşağıdaki gibidir (10 Tips for Creating a Network Security Policy):

- Zararlı kodlar: Virüs veya truva atı (trojan) gibi zararlı yazılımların sisteme girmesine yol açabilir. Virüslerden korunmak için her kullanıcının makinasına bir antivirüs yazılımının kurulmasını sağlamak veya İnternet (http, email, ftp) trafiğini sunucu(lar)da tarayıp temizledikten sonra kullanıcıya ulaştırmak gibi önlemler alınabilir. Sistemde güvenlik açıklarına neden olacak truva atlarını engellemek için güvenlik duvarlarında kesin kurallar konulmalıdır.

- Etkin Kodlar: Programların web üzerinde dolaşmalarına olanak sağlayan Java ve ActiveX gibi etkin kodlar saldırı amaçlı olarak da kullanılabilmektedir. Java, denetim düzenekleri ile bu tür saldırıların gerçekleşmesini önleyen bazı olanaklar sunmasına karşın ActiveX için aynı şeyden söz etmek mümkün değildir. Bu nedenle bu kodların kullanıma ilişkin ayarlar İnternet tarayıcısı üzerinde yapılmalıdır.

- Amaç dışı kullanım: İnternet hattı, kurumun amacı dışında da kullanılabilmektedir. Film, müzik gibi büyük verilerin İnternet'ten çekilmesi

hat kapasitesini gereksiz yere dolduracağından kurumun dış kaynaklara erişim hızında yavaşlamalara yol açabilecektir.

- Zaman Kaybı: İnternet ortamında gereksiz web sitelerinde zaman geçirmek kurum çalışanlarının iş verimini azaltabilir. Bunu engellemek için kurum politikasında bazı kullanıcılara İnternet erişimi verilmeyebilir veya İnternet erişimi öğle molası gibi belirli saatlerle kısıtlanabilir. Farklı bir çözüm ise web erişimini denetim altına almak ve ulaşılabilecek web sitelerini belirlemektir. Bu denetimler farklı kullanıcı gruplarına farklı şekillerde uygulanabilir. Kurumda dış kullanıcılardan (çalışanlar, ortaklar, müşteriler veya diğerleri) kimlerin kurum ağındaki hizmetlere erişebilecekleri ve ne tür erişim haklarına sahip oldukları tanımlanmalıdır.

4.6.5 Şifre Yönetimi Politikası

Şifreler kullanıcıların ulaşmak istedikleri bilgilere erişim izinlerinin olup olmadığını anlamamızı sağlayan bir denetim aracıdır. Şifrelerin yanlış ve kötü amaçlı kullanımları güvenlik sorunlarına yol açabileceğinden güvenlik politikalarında önemli bir yeri vardır. Sistem yöneticileri kullanıcıların şifre seçimlerinde gerektiği yerlerde müdahale etmelidirler. Basit ve kolay tahmin edilebilir şifreler seçmelerini engellemek için kullanıcılar bilinçlendirilmeli ve programlar kullanılarak zayıf şifreler saptanıp kullanıcılar uyarılmalıdır. Her hesap için ayrı bir şifre kullanılmalı ve şifreler sık sık değiştirilmelidir (Yıldırım, 2010). Kullanıcılar şifrelerinin çalındığından kuşkulandıklarında yetkili birimlere haber vermeli, gereken önlemleri almalıdır

4.6.6 Fiziksel Güvenlik Politikası

Bilgisayar veya aktif cihazlara fiziksel olarak erişebilen saldırganın cihazın kontrolünü kolaylıkla alabileceği unutulmamalıdır. Ağ bağlantısına erişebilen saldırgan ise kabloya özel ekipmanla erişerek (tapping) hattı dinleyebilir veya hatta trafik gönderebilir. Açıkça bilinmelidir ki fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal güvenlik önlemlerinin hiç bir kıymeti bulunmamaktadır. Kurumun ağını oluşturan ana cihazlar ve hizmet sunan sunucular için alınabilecek fiziksel güvenlik politikaları kurum için belirlenmelidir.

4.6.7 Sosyal Mühendislik Politikası

Sosyal mühendislik, kişileri inandırma yoluyla istediğini yaptırma ve kullanıcıya ilişkin bilgileri elde etme eylemidir. Sistem sorumlusu olduğunu söyleyerek kullanıcının şifresini öğrenmeye çalışmak veya teknisyen kılığında kurumun içerisine fiziksel olarak sızmak veya çöp tenekelerini karıştırarak bilgi toplamak gibi değişik yollarla yapılabilir. Kurum çalışanları kimliğini kanıtlamayan kişilere kesinlikle bilgi aktarmamalı, iş hayatı ile özel hayatını birbirinden ayırmalıdır. Kurum politikasında bu tür durumlarla ilgili gerekli uyarılar yapılmalı ve önlemler alınmalıdır.

4.5 Bilgisayar Haberleşmesi Ve Ağ Teknolojileri

4.5.1 Sayısal İletişim

Sayısal iletişim ikili tabanda kodlanmış bilgi veya verinin sistemler arasında aktarılmasını kapsar. Bu amaçla birçok standart ve protokol tanımlanmıştır.

Kodlama: Bilginin her bir parçasının sayısal tabanda gösterilimi için kullanılan yöntemdir. Çok değişik kodlar kullanılmakla birlikte iletişimde, metin aktarımı için ağırlıklı olarak ASCII kodundan yararlanılır; görüntü aktarımında ise, görüntünün doğrudan bit haritası kullanılır. Aktarımda taşınacak bit sayısını azaltmak için çeşitli sıkıştırma teknikleri vardır. Bunlardan biri kullanılarak bilgi içeriği değişmeden aktarılacak bit sayısı azaltılabilir.

Seri İletim: Seri iletimde tek bir iletim yolu üzerinde n bit sıra ile aktarılır. İşaret aktarım hızı baud birimiyle ölçülür. Baud birim zamanda aktarılan ayrık işaretlerin sayısıdır.

1 baud = n bps (bit per second)

4.5.2 Birlikte Çalışabilme ve Protokol

Aynı veya farklı üreticilerin iki veya daha fazla bilgisayarı arasında veri aktarılabilmesi ve ortak süreçlerin yürütülebilmesi, karşılıklı çalışabilmenin sağlanabilmesi birlikte çalışabilme (interoperability) olarak adlandırılır. Karşılıklı çalışmanın sağlanabilmesi için alıcının, vericinin gönderdiği bilgiyi anlayabilmesi gerekir. Karşılıklı çalışma, verici ve alıcı arasında kullanılacak işaretler, veri formatları ve temel aktarım birimlerinin değerlendirme yöntemleri üzerinde anlaşma ile mümkün olur. Veri formatlarının ve bilgi alış verişinin zamanlamasını düzenleyen kurallar dizisine protokol denir. Karşılıklı çalışma için bilgisayarların aynı protokolü uygulamaları zorunludur.

4.5.3 WAN Teknolojisi

Bütünüyle bir bilgi ağı, Yerel Alan Ağlarından (LAN), uzak kullanıcılardan ve bunların bir biriyle bağlantısından (ya da merkezi bir noktaya bağlantılarından) oluşur. Ve bu bağlantılara WAN (Wide Area Network- Geniş Alan ağı) bağlantıları denir.

Farklı arayüz ve özellikte birçok WAN teknolojisi vardır. Muhakkak ki her bir teknolojinin kendine has uygulama alanı ve avantajı vardır. Büyük bir ağ'da bunların biri ya da bir kaçı kullanılabilir. WAN teknolojileri deyince hemen ilk aklımıza gelen dial-up (çevirmeli modem) bağlantısı, leased line (kiralık hat), X.25, FR, ISDN, xDSL, ATM, B-ISDN, SMDS gibi teknolojilerdir.

Daha düne kadar WAN deyince aklımıza düşük band genişliği, düşük QoS (Quality of Service) ve gecikme gelirdi. Fakat bugün itibariyle WAN teknolojilerinde büyük gelişmeler oldu. Fiber Optiğin de uygulama da geniş yer bulmasıyla artık farklı türde

hizmet gerektiren (ses, görüntü, veri) bağlantıları oluşturabilecek bir WAN teknolojisi vardır. Önceleri WAN bağlantıları için 64 Kbps, 128 Kbps hızları öngörülürken artık simdi aynı maliyete 1-2 Mbps hızları öngörülüyor. 10 km'ye kadar olan açık alandaki uzaklıklar için Wireless'in de 5-10 Mbps band genişliği sunması alternatifleri ve tabi ki hizmet kalitesini de iyice artırmıştır.

4.5.4 Veri İletim Yöntemleri

Veri iletiminde genellikle dört yöntem kullanılmaktadır.

- Atmosferde (serbest uzayda) radyo frekans dalgaları ile iletim
- Atmosferde optik iletim
- Kablo üzerinden iletim
- Fiber optik iletim hattından optik iletim

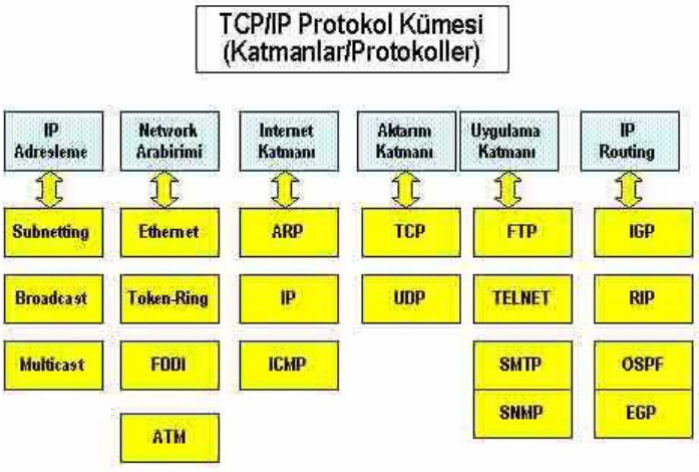
Her bir iletim yönteminin kendine has avantaj ve dezavantajları vardır (Işık, 2003). Atmosferde radyo frekans dalgaları ile iletim; ucuz ve esnek olmasına rağmen geniş band genişliklerinde (10 Gb/s (gigabit/saniye)) kullanılmaz ve uzun mesafe iletimde oldukça yüksek güç gerektirmektedir. Ayrıca iletilen sinyali bozmak oldukça kolaydır. Radyo frekans dalgaları ile iletim yaygın bir şekilde sivil ve askeri uzaktan ölçümde kullanılmakta olup, 3 Hz'den 300 GHz'e kadar olan frekanslarda gerçekleştirilir. Sinyal iletimi; görüş hattı ilerlemesi, toprak veya yüzey dalga kırınımı, iyonosfer katmanında olan yansıma veya ileri saçılma vasıtasıyla gerçekleştirilir. Koaksiyel kablo da çift burgulu kablolar gibi, kullanımı kolay ve yapay gürültü etkilerini azaltan bir kablo çeşidi olup yüksek frekanslı sinyalleri taşımak için tasarlanmıştır. Koaksiyel kabloların ortasında bulunan bakır iletken bir yalıtım katmanıyla çevrelenmiştir. Bu katmanın üzerinde ise koruyucu görev yapan örgü şeklinde bakır veya alüminyum bir kabuk kaplama vardır. Merkezdeki iletken dışarıdan karışan parazit sinyallerden örgü biçimindeki dış iletken aracılığı ile korunur. Ayrıca elektromanyetik radyasyonun bir sonucu olarak ortaya çıkan kayıplar azaldığından, çift burgulu kabloya göre daha güvenilirdir. Koaksiyel kablo üzerinden standart radyo frekans sinyal iletiminin standart elektronik devrelerle bütünleştirilmesi basittir ve oldukça kısa mesafeler ve düşük veri hızlarında idealdir. Birkaç yüz metre uzaklıktan 10 Mb/s 'lık veri rahatlıkla iletilebilir. Veriyi elektrik sinyalleri olarak iletir ve veri hızı 200 Mb/s'a çıkarılabilir. 1 Gb/s üzerindeki hızlarda ise zayıflama artmaktadır. Bu yöntem, geniş band genişliğindeki iletim için pratik değildir (Loehr, 1998).

Fiber optik kablolar veri ve ses iletimi için en ideal kablo türüdür. Yapısına göre, cam fiberler, plastik kaplı silisyum fiberler ve plastik fiberler olmak üzereüçe ayrılır. Veri iletimi açısından en iyi performansı gösteren cam fiberlerdir. Fiber optik kabloların bakıra göre birçok avantajları vardır. Fiber optik kablolar bakır koaksiyel kablolardan daha fazla iletim kapasitesine sahip olmasının yanında ağırlıkları da

düşük (daha ince) ve daha az yer kaplamaktadırlar. Ayrıca elektromanyetik etkilerden etkilenmezler ve sinyal kaçakları da meydana gelmediğinden oldukça güvenilirdir. Optik frekanslardaki taşıyıcı sinyal frekansı yüksek olduğundan fiberlerin kullanılabilir band genişliği oldukça yüksektir (25 Thz (terahertz)). Fiber optik kabloların diğer iletişim ortamlarından en önemli farkı, ses, veri ve görüntü iletişimindeki yüksek hızdır. Böylece büyük miktardaki verileri daha hızlı ve daha uzak mesafelere taşırlar (Çakır, 2000).

4.6. TCP/ IP Modeli

TCP/IP internette veri transferi için OSI'nın 3 ve 4. katmanda çalışan iki protokolü temsil eder. Bunlar Transmission Control Protokol (TCP) ve Internet Protocol (IP) şeklindedir. Bu protokoller de daha geniş olan TCP/IP protokol grubuna aittir. TCP/IP'de bulunan protokoller internette veri transferi için kullanılır ve internette kullanılan her türlü servisi sağlarlar. Bunların arasında elektronik posta transferi, dosya transferi, haber grupları, WWW erişimi gibi servisler TCP/IP sayesinde kullanıcılara sunulmaktadır. Kısaca TCP/IP internette veri transferini sağlayan protokoller grubudur. (Diğer protokoller IPX / SPX, AppleTalk, Netbeui) Protokol belli bir işi düzenleyen kurallar dizisidir. Örneğin, devlet protokolü devlet erkânının nerede duracağını, nasıl oturup kalkacağını düzenler. Ağ protokolleri de bilgisayarlar arası bağlantıyı, iletişimi düzenliyor. TCP/IP, bir protokoller kümesidir. Aslında TCP/IP protokolü diye adlandırmak çok doğru değildir. Çünkü TCP/IP çok sayıda protokol ve yardımcı programlardan oluşan bir protokol kümesidir (protocol stack) (Çakır,2000).



Şekil 4.4 : TCP/IP Protokol Kümesi (Çakır,2000)

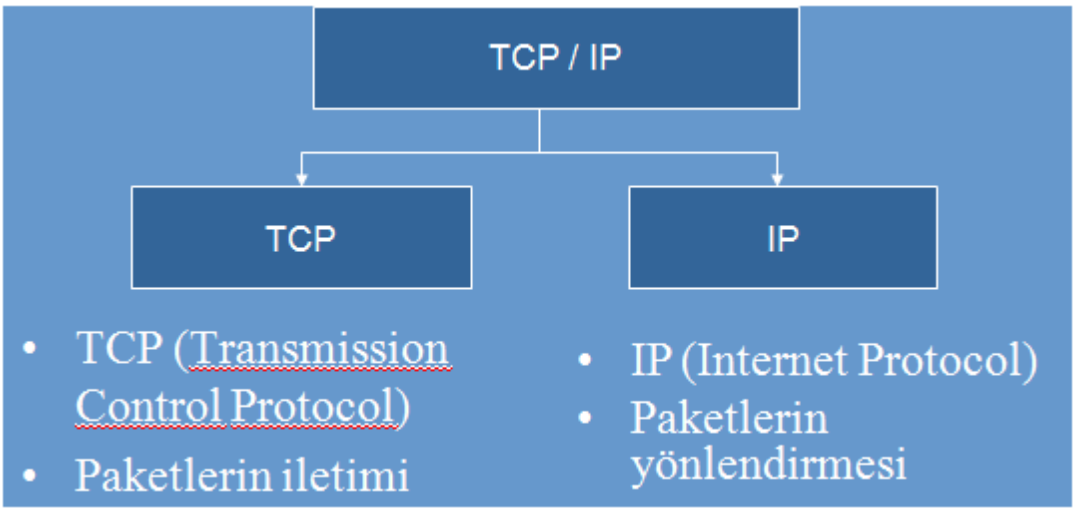
4.6.1 TCP/IP Tarihçe

TCP/IP, ilk defa ABD'de Savunma Bakanlığı tarafından ARPANet (Advanced Research Projects Agency Network) adı altında, askeri bir proje olarak geliştirildi. Önceleri askeri amaçlı düşünülen proje önce üniversiteler tarafından kullanılmaya

başlandı. İnternet'in doğuşu da bu tarihe denk gelmektedir. TCP/IP'nin ortaya çıkmasını sağlayan proje ABD'deki bilgisayarların bir felaket anında da ayakta kalabilmesini, birbirleriyle iletişimin devam etmesini amaçlıyordu. TCP/IP işletim sistemi ve bilgisayardan bağımsız olarak bilgisayarların iletişim kurmasını planlamıştı.

TCP/IP tercih edilme sebebi:

- Üreticiden bağımsız olması,
- Değişik ölçekli bilgisayarları birbirine bağlayabilmesi,
- Farklı işletim sistemleri arasında veri alışverişi için kullanılabilmesi,
- UNIX sistemleriyle tam uyumluluk,
- Birçok firma tarafından birinci protokol olarak tanınması ve kullanılması,
- Internet üzerinde kullanılması,
- Yönlendirilebilir (routable) protokol olması,
- Yaygın bir adresleme şemasına sahip olması.



Şekil 4.5 : TCP-IP İlişkisi (Çakır,2000).

4.6.2 IP Protokolü

Veri paketlerinin yönlendirilebilmesine imkân veren adres bilgisi ve bazı kontrol bilgilerini içeren protokoldür. TCP ile birlikte internet protokollerinin temeli Intenet Protocol (IP)'dir. İnternet üzerinde yönlendirme (routing) gibi temel ağ işlemlerinin gerçekleştirildiği protokol katmanıdır.

IP paketlerinin her biri kendi başlarına aradaki ağ cihazları tarafından yönlendirilen paket içinde belirtilen adrese ulaştırılır. Bu sırada fiziksel ağ farklılıklarından kaynaklanan paket parçalanmaları (fragmentation) ve bunların yeniden birleştirilmeleri aradaki ağ cihazlarının aşırı yüklenmelerini önlemek gibi görevlerde IP katmanı tarafından gerçekleştirilir.

IP adresleri bir bilgisayarı adreslemeyi amaçlayan 32 bitlik bir bilgidir. Bir sokak üzerinde yer alan evlerin adresleri gibi, İnternet'e bağlı olan her bilgisayarın da bir IP adresi vardır. Bu adres sayesinde bir bilgisayardan diğerine ulaşmak mümkün olur. IP adresi her biri onluk sistemde sayı olan 0 ila 255 arasında olan 4 sayı grubundan oluşur. Bu gruplar w, x, y, z harfleriyle temsil edilir. Örneğin: 123.45.35.122. Dörtlü gruplardan her biri 8-bitlik bir Internet adresini belirtir (Fall, 1996).

4.6.3 Yardımcı Programlar

Ping: Konfigürasyonu kontrol eder ve bağlantıyı test eder. Ping 131.140.1.1 şeklinde kullanılır.

FTP: Windows bilgisayarlar ile TCP/IP hostları arasında tek yönlü dosya transferini sağlar.

TFTP (Trivial File Transfer Protocol): Windows bilgisayarlar ile TCP/IP hostları arasında UDP kullanarak tek yönlü dosya transferini sağlar.

Telnet: Terminal etkileşimi sağlar.

RPC (Remote Copy Protocol):UNIX host bilgisayar ile Windows bilgisayar arasında dosya kopyalar.

RSH (Remote Shell):UNIX hostundaki komutları çalıştırır.

REXEC (Remote Execution): Uzak bir bilgisayardaki bir işlemi çalıştırır.

Finger: Uzak bilgisayar hakkında bilgi sağlar.

ARP: Yerel olarak düzenlenmiş IP adreslerinin ön belleğini hazırlar.

IPCONFIG: Mevcut TCP/IP konfigürasyonunu gösterir.

NBTSTAT: IP adresleriyle düzenlenmiş NetBIOS bilgisayar adlarını görüntüler.

Netstat: TCP/IP protokolünün çalışması ilgili bilgileri görüntüler.

Route: Yerel yönlendirme tablosunu gösterir ve değiştirilmesini sağlar.

Hostname: RCP, RSH ve REXEC programlarının kimlik denetimini yaparak yerel bilgisayarın adını döndürür (Fall, 1996).

4.7 Veri Gönderim Süreci

4.7.1 Temel Veri Transferi

Temel veri aktarımı TCP'nin internet ortamındaki işlevlerinden biridir. Haberleşen TCP hostlar (internet alanı) üzerinde bu katmanlar arası segment aktarımı yoluyla haberleşme sağlanır. TCP**,** veri akışını baytları sıralandırıp segment grupları halinde iletir. Eğer bir parçalama gerekliliği ortaya çıkmadıysa her segment bir IP paketine konarak iletilir (Fall, 1996).

4.7.2 Güvenilirlik

TCP, zarara uğramış, bozulmuş, ikilenmiş verinin doğru olarak iletilmesinden sorumludur. TCP, her bir bayta sıra numarası verir. Daha sonra ilettiği bu baytlara karşılık onay bekler. Eğer belirli aralıklarla beklediği onayları alamazsa onay alamadığı kısımları yeniden hedef hosta iletir. Hedef host sıra numaralarına göre segmentleri sıralarken aynı segment numarasına sahip iki segmentle karşılaşabilir. Her bir segment checksum denilen kontrol bilgilerini içerir. Bu kontrol bilgilerine göre hasara uğramış segmentler anlaşılır ve atılır. Kaynak hosta onay gönderilmezse kaynak hosttaki TCP onay alamadığı segmentleri yeniden gönderir (Fall, 1996).

4.7.3 Güvenlik Duvarı (Firewall)

Ağın içinden ve dışından ağa yönelik yetkisiz erişimleri tespit eden ve engelleyen ağ cihazlarıdır. Yazılımsal, donanımsal ve her ikisini de birlikte içeren güvenlik duvarları bulunmaktadır. Yazılımsal olarak ağ paylaşımının merkezindeki sunucu bilgisayar ve ağ içindeki tüm bilgisayarlar gerekli programların yüklenmesi ile kontrol edilebilir. Donanımsal olarak da ağın tamamını kontrol eden ve internetten gelen saldırılara koruma sağlayan cihazlar mevcuttur. Donanımsal çözümler OSI'nın 3. Katmanı olan ağ katmanında bulunurken çok daha hızlı çalışmakta ve ağ üzerindeki veri trafiğinin hızını düşürmemektedirler. Güvenlik duvarı gerçekte özel ağlar ile internet arasında her iki yönde de istenmeyen trafiği önleyecek yazılımsal ya da donanımsal sistemdir. Firewallların verimli bir şekilde kullanılabilmesi için internet ve özel arasındaki tüm trafiğin firewall üzerinden geçmesi ve gerekli izinlerin (yetkilerin) kısaca erişim listelerinin uygun bir stratejiyle hazırlanmış olması gerekir. Bir ağ üzerinde istenilen sitelere girişlerin kısıtlanması, dışarıdan gelecek saldırıların engellenmesi, port kontrolleri ile kaynakların ağ içinde daha güvenilir olarak dağıtılması güvenli duvarı kullanılarak gerçekleştirilebilir. Bugün yönlendirici, ağ geçidi ve tekrarlayıcı gibi cihazların güvenlik duvarı özelliklerine sahip modelleri üretilmektedir (Loehr, 1998).

Kullanılacak Donanımların Seçimini Etkileyen Faktörler (Loehr, 1998):

- Ağın kullanım amacı: Ağın hangi amaçlar için kullanılacağı (Evdeki iki bilgisayarı birbirine bağlamak için Switch ve Hub kullanmaya gerek yoktur, çapraz-kros (crossover) kablo ile bağlantı yapılabilir)

- Ağın büyüklüğü: Ağa bağlanacak bilgisayar sayısı (Hub'ın port sayısının belirlenmesi, bilgisayarlar arası mesafe çok uzun ise tekrarlayıcı (repeater) kullanılması)

- Ağın yapısı: Kurulacak ağın topolojisi (Farklı topolojiler varsa köprü kullanılarak ağların birbirine bağlanması) Ağın çalışma zamanı: Ağın günün belirli zaman aralıklarında mı yoksa sürekli mi çalışacağı (web sunucu hizmeti verilecekse buna göre donanım seçilmesi)

- Cihaz özellikleri: Ağ kartı ve Hub/Switch gibi cihazların hız olarak uyumlu olması.

4.8 TCP Performansının Veri Transferi Uygulamaları İçin Geliştirilmesi

Son yıllarda İnternet ağı önemli derecede büyüdüğü ve hızla büyümeye devam ettiği için TCP'nin İnternet üzerindeki performansının geliştirilmesi ile ilgili çalışmalar çok büyük önem kazanmıştır. TCP protokolü üzerinde yapılan iyileştirmeler sonucunda birçok TCP versiyonu geliştirilmiştir. Bunlardan en yaygın olanları Tahoe, Reno, Newreno ve SACK TCP'dir (Fall, 1996). Her yeni versiyonla TCP'nin sağlamış olduğu güvenilir ve sıralı veri iletimininin performansı artırılmaya çalışılmıştır.

İnternet üzerinde FTP, HTTP, TELNET gibi TCP'yi kullanarak veri iletimi yapan birçok uygulama vardır. Bu uygulamalardan bazıları veri iletimini hızlandırmak için bazı yöntemler kullanmaktadırlar. Örnek olarak bir FTP uygulaması olan FlashGet programı bir dosyayı İnternet üzerinden indirirken o dosyayı parçalara ayırır ve iki host arasında birden fazla TCP bağlantısı kurarak parçaların her birini farklı bağlantı üzerinden alır. Her bir bağlantı üzerinden yine sıralı ve güvenilir veri iletimi yapılmaktadır. Yükleme işlemi bittiğinde veri parçaları sıralı olarak birleştirilerek veri bütünlüğü sağlanmaktadır. FlashGet'de veri iletiminin hızlandırılmasına karşın birden fazla TCP bağlantısı kurulması hostlar ve ağ üzerindeki yükün artmasına sebep olmaktadır (Güneş ve Diğerleri, 2003).

TCP güvenilir olmayan IP (Internet Protocol) servisi üzerinde güvenilir ve sıralı veri iletimi sağlar. TCP güvenilir iletimi sağlarken kümülatif ACK (Acknowledge - Alındı Bilgisi) bilgisi ve bir tane tekrar gönderim zamanlayıcısı (Timer) kullanır. Aldığı veriyi onaylar ve kaybolan paketi tekrar gönderir (Güneş ve Diğerleri, 2003).

TCP kaybolan veriyi zaman aşımı süresi dolmadan önce göndermek için Hızlı Tekrar Gönderim (FastRetransmit) algoritmasını kullanır. Bu algoritma üç tane aynı ACK bilgisi alınması halinde ACK bilgisinin göstermiş olduğu paketi tekrar gönderir (Stevens, 1997).

TCP, alıcının, kaybolan paketleri veya gelen aynı paketleri belirlemesini sağlamak için sıra numarası(sequence number) kullanır. Birden fazla paketi aynı anda göndermek için ardışık düzen (Pipeline)yöntemini kullanarak veri iletim hattının verimliliğini artırır. Gönderilecek paket sayısını, TCP akış denetimi (flow control) ve

tıkanıklık denetimi (congestion control) algoritmalarını kullanarak belirler. Akış denetimi algoritması alıcının kabul edebileceği paket sayısını, tıkanıklık denetimi algoritması ise, göndericinin, ağın kullanılabilir bant genişliğine göre, iletebileceği paket sayısını belirler. Gönderilecek paket sayısı da bu iki değerin küçük olanı olarak belirlenir (Stevens, 1994). Bu gönderilecek paket sayısı pencere boyutu (window size) olarak ifade edilir.

TCP'deki Kayan Pencere Protokol'ünün iki temel görevi; veri iletiminin güvenilirliği ve akış kontrolünü sağlamaktır. Kayan Pencere Protokol'ünde, her bir pakete sıra numarası verilir ve her bir paket alıcıya ulaştığında göndericiye ACK bilgisi gönderilir. Eğer gönderici kendisine gelen ACK bilgilerine bakarak bir paketin kaybolduğunu anlarsa o paketi tekrar gönderir. TCP, bir paketin kaybolduğunu, o paket için tutulan zamanlayıcının zaman aşımına uğraması veya o paket için üç tane aynı ACK bilgisinin gelmesi sonucunda anlar. Bu iki durumda da kaybolan paket tekrar yollanarak güvenilirlik sağlanır. TCP, Kayan Pencere Protokolü ile akış kontrolü sağlayarak veri bant genişliğini daha verimli kullanır. Alıcı, gönderdiği her ACK bilgisi içinde kendi kabul edebileceği byte sayısını (window size) alıcıya iletir. Burada pencere boyutu, göndericinin, pencere içerisindeki ilk paket için ACK alınmasını beklemeden gönderilebileceği paket sayısını gösterir. Bunun sonucunda, TCP'de, göndericinin, alıcının kabul edemeyeceğinden fazla byte veya paket göndermesi engellenmiş olur (Güneş ve Diğerleri, 2003).

5. SİSTEM GELİŞTİRME

Bir bilgisayar ağlarında sistemler arasında veri aktarımında trafik arttıkça ağ performansı düşer. Bu durum tıkanıklık olarak isimlendirilir. Bu durumda gönderilen paket sayısı azalır.

Bilgisayar ağlarında tıkanıklık oluşturan sebepler; yönlendiricilerin bellek yetersizliği, yönlendiricilerin işlemci (CPU) hızları ve hatların band genişliğidir. Bu durumda yönlendiriciye gelen veri paketleri gidecekleri adreslere yönlendirilemez ve tıkanıklık oluşur (Kaptan, 2005).

Bilgisayar ağlarında kullanılan tıkanıklık kontrol algoritmaları normalde gözle takip edilemeyecek bir işlemdir. Bu algoritmaların daha iyi anlaşılabilmesi için simülatörler geliştirilmiştir.

Bilgisayar ağlarında oluşan trafik, büyük farklılıklar göstermekte ve her bir trafik tipi; bant genişliği, gecikme, gecikme sürelerindeki değişim ve bulunabilirlik faktörleri açısından kendisine özgü gereksinimlere sahip olmaktadır.

Temel olarak Servis Kalitesi, kullanıcılara belli veri akışları için daha iyi servis verebilmektedir.

Sıkışıklık, kendi içinde üçe ayrılabilir:

1. Port Düzeyinde Sıkışıklık. Giren çeşitli veri akışlarının aynı çıkış portu için mücadele verdikleri sıkışıklık tipidir. Giriş yapan veri akışlarının toplamı, çıkış portlarının kapasitelerini aşıyorsa sıkışıklık meydana gelir. Eğer sıkışıklık sıkça oluyorsa ve/veya uzun zaman sürüyorsa, uygulamanın yanıt verme süresi de etkilenecektir.

2. Aradaki Cihazlarda Meydana Gelen Sıkışıklık. Ara cihazın destekleyebildiği bant genişliği, tüm giriş yapan veri akışlarının toplamından düşükse meydana gelir. Eğer sıkışıklık sıkça oluyorsa ve/veya uzun zaman sürüyorsa, cihaz bu durumu düzeltmeye çalışırken uygulamanın yanıt verme süresi de etkilenecektir.

3. Ağdaki Sıkışıklık. Kaynak ve hedef makineler arasında görev alan bir ya da daha çok ağ aygıtında veya bağlantılarda (linklerde) meydana gelen sıkışıklık tipidir. Bu sıkışıklık, diğer iki tip sıkışıklığın birleşiminden meydana gelmekte ve uçtan uca performansı düşürmektedir.

Sıkışıklığın çözümlenmesi ve etkili bir şekilde kontrolünün sağlanması için, bütün ağda geçerli olacak şekilde sıkışıklığı belirleyebilen ve tepki verebilen bir yönetim planlaması yapılmalıdır. Bunu sağlayabilen kontrolün adı da **Trafik Kontrolüdür** (Çağrıcı, 2007).

5.1 Veri Türleri

Günümüzde, farklı hat hızlarını destekleyen, geniş bir fiyat yelpazesine sahip ürün seçeneklerinin sayısı hızla artmaktadır. Seçim, kaçınılmaz olarak kullanıcı ihtiyacı ve bu ihtiyacın karşılanması için gereken maliyete göre yapılır. Tablo 5.1' de, bazı bulunabilir iletim hız aralıkları ve bunları kullanan tipik kullanıcı uygulamaları görülmektedir. Görüldüğü gibi çok geniş bir seçenek aralığı mevcuttur, ve kbit/sn mertebelerindeki iletim oranları birçok iletim tipi için uygun olmamaktadır.

Tablo 5. 1: İletim Tipi Bit Sayısı (Çağrıcı, 2007).

İletim Tipi	Tipik Bit sayısı	9.6 kbit/sn ile iletim zamanı (sn)
Bir sayfa veya tam CRT ekranı metin (sıkıştırılmamış)	$1\text{-}4 \times 10^4$	1-4
Fotokopi resim, siyah beyaz, iki-ton (sıkıştırılmamış)	$2\text{-}6 \times 10^5$	20-60
Tam sayfa, renkli resim, yüksek kaliteli (iyice sıkıştırılmış)	$2\text{-}10 \times 10^6$	200-1000
20 cm floopy disk, tek-yönlü, double-density	5×10^6	500
720-m bilgisayar tape makarası (6250 BPI tipi) veya iki orta-büyüklükte disk ünitesi (IBM 3310)	1×10^9	100,000 (29 saat)
PCM olarak kodlanmış bir saniyelik telefon konuşması	6.4×10^4	7
PCM olarak kodlanmış bir saniyelik telefon konuşması (iyice sıkıştırılmış)	2.4×10^3	0.25
Bir saniyelik hareketli video resmi	6.3×10^6	660

Makineler arası veri iletiminde, kodları oluşturmak için bit katarları kullanılır. Veri iletiminin hızı saniye başına bit (bit/sn) ile tanımlanır. Veri iletimindeki tipik hızlar Tablo 5.2'de görülmektedir.

Tablo 5. 2: Veri İletim Hızı (Çağrıcı, 2007).

Bit/sn olarak tipik hız	Tipik kullanımları
0-600	Telgraf,eski terminaller; telemetry
600-2,400	İnsan-operatörlü terminaller; kişisel bilgisayarlar
2,400-19,200	Hızlı cevap ve/veya akış gerektiren uygulamalar; bazı batch ve dosya transfer uygulamaları
32,000-64,000	Ses; yüksek-hızlı uygulamalar; bazı videolar
64,000-1,544,000	Çoklu kullanıcılar için çok yüksek hız; bilgisayar-bilgisayar trafiği; ağlar için omurga linkleri; video
1,544,000'dan büyük	Ağlar için omurga linkleri; yüksek-kaliteli video; çoklu sayısal ses

TCP, bağlantı-yönlendirmeli bir protokoldür. TCP aynı zamanda bir ağ veya çoklu ağlar boyunca yerleşmiş bir alıcı kullanıcı uygulaması ile (veya diğer ULP) uçtan-uca veri transferi yapılmasından sorumludur.

İletilen her bir bayt için bir sıra numarası atanır. Alıcı TCP modülü bir toplamsal-hata rutini kullanarak verinin iletim boyunca bir hasara uğrayıp uğramadığını kontrol eder. Eğer veri kabul edilebilir ise, TCP gönderici-TCP modülüne bir pozitif acknowledgment gönderir. Eğer veri hasarlı ise, alıcı-TCP veriyi yok eder ve bir sıra numarası kullanarak gönderici-TCP'ye sorun hakkında bilgi gönderir. TCP zamanlayıcıları tedavi ölçümleri yapmadan önce zaman kaymasının aşırı olmadığından emin olurlar. Tedavi ölçümleri alıcı siteye acknowledgment gönderilerek veya veriyi gönderici siteye yeniden-göndererek yapılır.

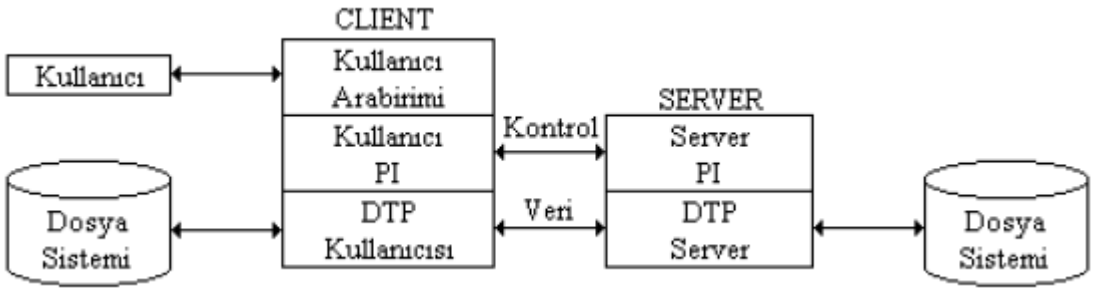
TCP, veriyi bir ULP'den nehir-yönlendirmeli biçimde alır. Nehir-yönlendirmeli protokoller ayrık karakterler (blok,çerçeve veya verigram değil) göndermek üzere tasarlanmamışlardır.Baytlar TCP katmanına varınca, TCP segmentleri olarak gruplaşırlar. Bu segmentler daha sonra diğer varışa iletilmek üzere IP'ye (veya başka bir alt-katman-protokolüne) geçirilir. Segment uzunluğuna TCP karar verir, ancak bir sistem geliştiricisi TCP'nin bu kararı nasıl vereceğine karar verebilir. TCP ayrıca ikilenmiş veri kontrolü yapar. Eğer gönderici TCP veriyi tekrar yollarsa, alıcı TCP tüm ikilenmiş gelen veriyi yok eder. Örneğin, alıcı TCP acknowledgment trafiğini belli bir zamanda gerçekleştirmezse, gönderici TCP veriyi yeniden gönderir ve veri ikilenmiş olur. TCP push fonksiyonu kavramını destekler. Bir uygulama; alt katmandaki TCP'ye geçirdiği tüm verinin iletildiğinden emin olmak istediğinde push fonksiyonunu çalıştırılır. Böylece, push fonksiyonu TCP'nin tampon yönetimini ele geçirir. ULP push'u kullanmak için, push parametresi bayrağı 1'e set edilmiş bir send komutunu TCP'ye gönderir. Bu işlem TCP'nin, tüm tamponlanmış trafiği bir veya daha fazla segment içerisinde varışa ilerletmesini gerektirir. TCP kullanıcısı bir close-bağlantı işlemi kullanarak da push fonksiyonunu sağlayabilir. TCP acknowledgment'ler için sıra numaraları kullanır. TCP bu sıra numaralarını aynı zamanda, segmentlerin son varışa sırası ile varıp varmadıklarını kontrol etmek üzere, segmentleri yeniden-sıralamada kullanır. TCP bağlantısız bir sistemin üzerinde yer aldığı için ki bu sistem internet içerisinde dinamik, çoklu rotalar kullanabilir, internette ikilenmiş verigramların oluşması muhtemeldir. Daha önce değindiğimiz gibi, TCP ikilenmiş verigramlar içerisinde taşınmış, ikilenmiş segmentleri yok eder. TCP her bir oktete sıra numarası verir. Daha sonra ilettiği bu oktetlere karşılık acknowledgment (ACK) bekler (Çağrıcı, 2007).

Eğer belirli aralıklarla beklenen ACK'leri almazsa ACK almadığı kısımları yeniden varış host'a iletir. TCP olumsuz bir geri bildirim mekanizması kullanmaz. Alıcı TCP modülü gönderici verisi üzerinde akış kontrolü yapabilir. Böylece tampon overrun ve alıcı cihazın doyması (saturation) gibi sorunlar engellenir. TCP'nin kullandığı kavramın, haberleşme protokollerinde kullanımı alışılmış değildir. Akış kontrolü göndericiye bir "pencere" değeri verilmesine dayanır. Gönderici bu pencere ile belirlenmiş sayıda bayt iletebilir, pencere kapanınca gönderici veri göndermeyi durdurmalıdır. TCP'nin bir hüneri de host cihazı üzerindeki çoklu kullanıcı oturumlarını çoğullayabilmesidir. Çoğullama; TCP ve IP modüllerindeki portlar ve soketler için basit isimlendirme anlaşmaları kullanılarak gerçekleştirilir. TCP, iki

TCP varlığı arasında tam-duplex iletim sağlar. Böylece bir dönüş işareti beklemeksizin (half-duplex'te gereklidir) eşzamanlı iki-yönlü iletim yapılır. TCP kullanıcının bağlantı için güvenlik ve öncelik seviyeleri belirleyebilmesine olanak tanır. Bu iki özellik, tüm TCP ürünlerinde bulunmayabilir ancak TCP DOD standardında tanımlanmışlardır. TCP iki kullanıcı arasında hoş close sağlar. Hoş close bağlantı koparılmadan önce tüm trafiğin ACK'larının oluşturulduğundan emin olunmasını sağlar (Çağrıcı, 2007).

5.2 File Transfer Protokolü (Ftp)

Internet standartları daha güçlü olan ve daha yaygın kullanılan bir dosya transfer protokolü olan FTP'yi (file transfer protocol) içerir. FTP iki makine arasında dosya transferi yapılabilmesi için prosedürler tanımlar. FTP, oldukça alışılmadık bir biçimde, makineler arasında iki mantıksal bağlantı sağlar. Bağlantılardan biri, makineler arasında login için kullanılır. Bu bağlantı TELNET protokolünü kullanır. Şekil 5.1'de bu kavram gösterilmiştir. Son kullanıcı bir protokol çeviricisi (PI) ile haberleşir. Bu PI kontrol bağlantısını yönetir. PI, kullanıcı ve PI'ın dosya sistemi arasında bilgiyi transfer etmelidir. Komutlar ve cevaplar kullanıcı-PI ve sunucu-PI arasında iletilir. Şekilde gösterildiği gibi, diğer makinenin (sunucunun) PI'sı, yönetim bağlantıları için de TELNET protokolünü cevaplar (Çağrıcı, 2007).

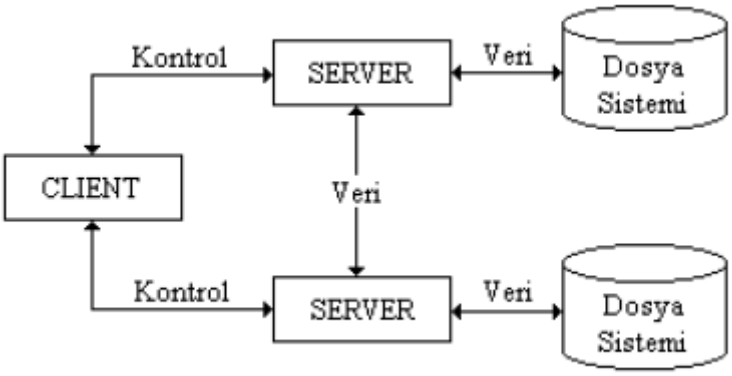


Şekil 5.1 : TELNET Protokolü(Çağrıcı, 2007).

Dosya transferi sırasında, veri yönetimi, 'veri transfer process (DTP)' denilen diğer mantıksal bağlantı ile sağlanır. Bir kere DTP fonksiyonlarını gerçekleştirince ve kullanıcının isteği sağlanınca, PI bağlantıyı kapatır. FTP aynı zamanda üçüncü-taraf transferi olarak bilinen bir işleme izin verir. Şekil 5.3'de görüldüğü gibi bir istekçi, ikisi de sunucu olarak davranan iki uzak makineyle bağlantı kurar. Böyle bir bağlantının amacı istekçinin, iki sunucunun dosya sistemi arasında dosya transfer izni almak için, istek yapmasıdır. Eğer istek onaylanırsa, bir sunucu diğer sunucuyla bir TCP bağlantısı oluşturur ve gönderici FTP modülü, veriyi TCP modülleri boyunca ilerleterek alıcı FTP modülüne transfer eder (Çağrıcı, 2007).

FTP'nin farklı tiplerdeki veri gösterilişlerini ve makineler arası bu tiplerin nasıl kullanılacağına dair müzakere yapılmasını destekleme yeteneği sınırlıdır. FTP kullanıcısı transferde kullanılacak bir tip tanımlayabilir (örneğin, ASCII, EBCDIC, vs.). ASCII default tiptir, ve FTP kurulduğu sistemde ASCII kodunun

desteklenmesini gerektirir. EBCDIC de aynı zamanda desteklenir ve mainframe host bilgisayarları arasında veri transferlerinde biraz daha yaygın olarak kullanılır. ASCII ve EBCDIC bir ikinci parametre kullanarak karakterlerin format kontrol amaçları için kullanılacağını veya kullanılamayacağını belirtirler. Örneğin carriage return (CR), line feed (LF), dikey tab (VT), ve form feed (FF) FTP oturumu boyunca kontrol karakterleri temsil etmek üzere tanımlanabilirler (Çağrıcı, 2007).



Şekil 5.2 : İki Makine Arası Bağlantı Şeması (Çağrıcı, 2007)

FTP, bit nehirlerinin transferini de destekler. Bu bit nehirlerine imaj tipleri denir. Bu işlemle, veri sürekli bit nehirleri içinde gönderilir. Gerçek transfer için veriler, 8-bit baytlara paketlenir. Çoğu işlem ikilik imajlar iletmek için imaj tiplerini kullanır. Böylece çoğu FTP uygulamaları imaj tipini destekler.

FTP yerel bir tipi de destekler. Bu tip baytlar içerisinde iletilir ve burada bayt büyüklüğüne byte size denilen bir parametre ile karar verilir. FTP'de byte size değeri ondalık bir tamsayı olarak gösterilir.

5.3 XML

XML, 1996 yılında bağımsız bir kuruluş olan W3C (World Wide Web Consortium) organizasyonu tarafından geliştirilen bir standarttır. Bilişim sistemlerinde verinin kolayca okunmasını sağlayan dokümanlar oluşturmaya yarar. Bu özelliği sayesinde farklı platformlar arasında veri alışverişini yapmaya yarar (Newcomer, 2002).

XML' in bazı temel özellikleri söyle sıralanabilir (Thangarathinam, 2006):

- XML bir işaretleme dilidir.
- XML, verinin nasıl sergileneceğini gösterir.
- XML platformdan bağımsızdır.
- XML dosyaları metin
- XML de veriyi tanımlamak için doküman tipi tanımlaması Document Type Definition (DTD) veya XML Schema kullanılması gerekmektedir.

XML dokümanları tag ve text'ler den oluşur. **Tag**; veri elementlerini tanımlar. Bu veri elementlerinde dikkat edilmesi gereken büyük küçük harf duyarlı olmasıdır (Çamalan, 2011).

XML Web servisleri, programları, nesneleri, veri tabanlarını veya karmaşık is fonksiyonlarını birbirine bağlayan XML uygulamalarıdır (Newcomer, 2002).

Web servisleri farklı kurumsal is süreçlerini gerçekleştirerek internet ve Web teknolojileri alanında bir devrimi gerçekleştirmiştir. XML Web servisleri Web ortamında veriyi http portları üzerinden platformdan bağımsız olarak sunan, farklı uygulamalar arasında iletişimin sağlanmasını sağlayan evrensel bir yapıdır. Web servisleri istemciye veriyi sunarken alt yapısını gizleyerek sadece veriyi sunan güvenli bir yapıdır. Bu yapı sayesinde istemci Web servisin hangi platform üzerinde çalıştığı, hangi dilde yazıldığı bilgisine ihtiyaç duymaz. Ayrıca Web servislerinde sunulan veriler ile ilgili yapılan işlemlerde (ekleme, silme, güncelleme vs.) bu servisleri kullanan tüm uygulamalarda eş zamanlı olarak etkilenir. Web servisleri Web ortamında yayınlanabilen, aranıp bulunabilen ve çağrılarak erişilebilen metotlar sunar (Özdemir, 2012).

5.4 Veri Aktarımında Yaşanan Gecikmelerin Yol Açtığı Kayıplar

Veri Aktarımında yaşanan gecikmeler ve iyileştirme çalışmaları aşağıdaki problemlere neden olabilmektedir (Techinside, 2014):

a) İşletim Maliyetleri: Bir kesinti halinde ücret kaybı, fazla mesai ve çalışan maliyetleri ortaya çıkar. Satışlar kaybedilebilir ve bunun sonucunda gelecekteki işlerde de bu işlerde aynı durum yaşanabilir. Diğer işletim maliyetleri arasında envanter kaybı ve işlenmede olan ürünlerin ıskartaya çıkması, hizmet düzeyi anlaşmaların yerine getirilmemesinden kaynaklanan olası hukuki cezalar ve meydana gelen kayıpların tazminini isteyen üçüncü taraflara dayalı maliyetler yer almaktadır.

b) Üretkenlik Maliyetleri: Bir kesinti halinde çalışanlar normal görevlerini yerine getiremez. Üretkenlik kaybını hesaplamada kullanılan yaygın yöntem şudur: (ortalama çalışan maaşı x üretim aksama saati) + kayıp iş zamanını kompanse etmek için çalışanların fazla mesai maliyetleri.

c) İyileştirme Maliyetleri: Bu maliyetler arasında sistemin onarılması için ödenen ücret, BT personelinin fazla mesaisi ve hizmetlerin geri kazanımı için gereken üçüncü taraf danışmanlar veya teknisyenlerin maliyetleri yer almaktadır. Göz önünde bulundurulması gereken bir diğer husus da, BT personelinin diğer kritik projeler yerine sistemin kurtarılmasına odaklanması ile harcanan zaman ve maliyettir.

d) Müşteri Kaybı: Daha önceki sadık müşteriler size olan inançlarını yitirebilir ve rakiplerinize yönelebilir. Bir şirket güvenilmez olarak görülmeye başladığında, bu algının değiştirilmesi zor olabilir.

e) İtibarın Zedelenmesi: Şirketiniz ister büyük ister küçük olsun, kötü itibar büyük bir kayba yol açabilir. Kötü bir haber başlığı ve Twitter'daki bir şikayet ya da Facebook'taki olumsuz bir gönderi de zarar verici olabilir. Sektöre yönelik web siteleri ve bloglar hedef pazarınızın dikkatini çekmektedir; bu nedenle olumsuz bir gönderi mevcut ve potansiyel müşterileriniz üzerinde etki yaratabilir.

f) Hissedar Değeri Etkisi: Kötü imaj ayrıca şirketin sermaye değerini düşürür ve pazardaki sermaye miktarını olumsuz etkiler. Özellikle sallantılı ekonomik süreçlerde, borsa bir şirket hakkındaki olumsuz haberlerden etkilenir ve bu haber önemli bir satış kaybı hakkındaysa sonuçlar daha da kötü olabilir.

2014 yılında Türkiye'de, veri kaybı ve veriye tekrardan erişebilme süresindeki aksaklıklar, işletmelere ortalama yılda 10 milyar TL'ye mal oldu. Bu zararın %60'ı veri kaybı, %40'ı ise veriye tekrardan erişebilme süresindeki kayıp olarak belirlendi. Dünya genelinde ise işletmelerin zararı, 1,7 trilyon dolar. Türkiye, veri koruma konusunda pazar olgunluğu sıralamasında 24 ülke arasında 23. sırada yer aldı; listenin başında ise Çin, Hong Kong ve Hollanda yer alıyor (Rençberler, 2014).

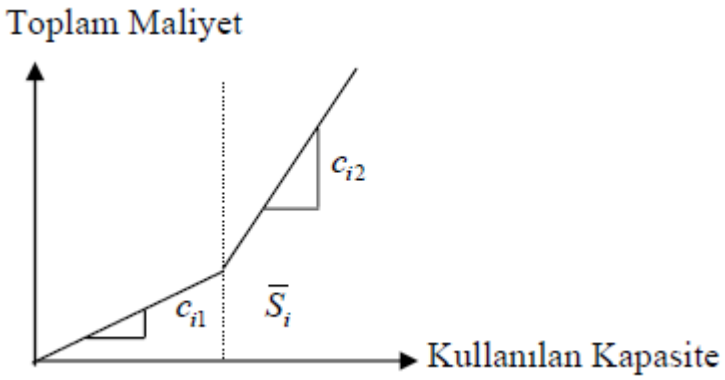
Veri şebekelerinin kullanımı sadece geleneksel veri uygulamalarını kapsamamaktadır; gerçek zamanlı sesli ve/veya görüntülü kesintisiz işlemleri, İnternet protokolü üzerinden ses aktarımlarını, eş zamanlı olmayan mesajlaşmaları ve dijital ağlar üzerindeki diğer toplu aktarımları da içermektedir. Veri ağları üzerinde gerçekleştirilen bu uygulamaların her birinin kapasite gereksinimleri ve ihtiyaç duydukları hizmet kalite düzeyleri farklıdır. Dolayısı ile her uygulama ağ güvenilirliğinden ve şebeke hızından farklı şekilde etkilenmektedir (Kasap, 2010).

Sistem üzerinde iyileştirme çalışmalarında hizmet seviyesini artırmak ve maliyeti düşürmek temel hedef olarak belirlendi. Bu amaçla bant genişliği trafik hacmi ve verimlilik hizmet kalite düzeyi (Quality of Service-QoS) analiz edildi. Tüketicilerin refah ve talepleri, birçok kaynakta QoS garantisindeki etkin bant genişliği için hesaplanmaktadır (Courcoubetis, 2000).

Etkin bant genişliğinin uygun bir şekilde tanımlanıp ölçülmesi sistem verimliliği açısından önemli bir ihtiyaçtır. Burada kullanılan kapasite ile sistem maliyeti arasında şekil 6.9'daki gibi bağlantı vardır. Bir ağ kaynağı kapasitesi (bant genişliği ve vadesi) ve QoS'i ile nitelendirilir (Kasap, 2010).

Veri şebekelerinin kullanımından doğan iki tür maliyet vardır. Bu maliyetlerden ilki kaynak kısaca bant genişliği (kapasite) elde etme maliyetidir. İkincisi ise video konferans gibi belirli işleri gerçekleştirirken sağlanan kalite düzeyinin yetersizolması sonucu uğranılan zararın doğurduğufırsat maliyetidir. Kaynak kalitesinin genel ölçümleri gecikme, seğirme ve kayıp olasılığıdır. Gecikme, verinin ağ üzerinde kaynaktan hedef noktasına gidene kadar geçen zamanı belirtir (Ragsdale, 2000). Seğirme, gecikmedeki değişimi gösterir. Ses ve video uygulamaları gecikme ve seğirmeye karşı çok hassastırlar, veri uygulamaları ise her ikisine karşı hassas değildirler. Ses uygulamalarında seğirme, kullanıcılara konuşma esnasında biçimsiz

kopukluklar olarak belirir. Paket kaybı, ağ üzerinde kaybolan (düşen) ya da tazmin edilemeyecek zarar gören veriyi gösterir. Genellikle, veri çarpışması ve arabellek taşması şeklinde gözükür. Seğirmedeki ani değişiklikler de paket kaybına sebep olabilir (Reichl, 2003).



Şekil 5.3 : Kaynak İ İçin Örnek Fiyat Eğrisi

5.5 Kuyruk Ağ Analizi

Simülasyon uygulamasında, bir paketin gecikme süresinin hesaplanması için Kleinrock'un Bağımsızlık Varsayımı kullanılmaktadır.

Uçtan Uca Gecikme= $T_{\text{Alınan Paketin Varma Süresi}} - T_{\text{Kaynaktan İstenen Varış Süresi}}$ (Royer,1990)

Kaynak, bir hedefe paket göndermek istediğinde ve paket hedefe ulaştığı andaki zaman farkı Uçtan Uca gecikme olarak tanımlanmaktadır. Bugün birçok uygulamada (örneğin IP telefon) kullanılabilir sonuçlar sunmak için küçük bir gecikme gerekmektedir. Bu gecikme uygulamalar için kullanılan protokollerin yatkınlığını göstermektedir. Bir kaynak düğüm S'den, hedef düğüm D'ye paket göndermek için beklenen tepki süresinin gecikme değeri, paketin hedefe gideceği yol boyunca ziyaret ettiği tüm linkler ve düğümlerdeki tepki sürelerinin toplamıdır (Haverkort, 1998).

$E[R(S,D)] = \sum E[R_{ij}] + \sum E[R_i]$ (McDonald, 1999).

Tüm linklerdeki beklenen gecikme süresi $E[Rij] = 1/(\mu cij - \lambda ij)$' dir. µcij = bir link ij(paket/sn.) üzerinde iletilen paketlerin sayısı, λij = bir linkin ij (paket/sn.) üzerine varış oranıdır.

$E[Si]=1/\mu i$ ve $\rho i=\lambda i / \mu i$ ile i düğümü için beklenen gecikme süresi,

$E[Ri] - (pi*E[Si])/(1- pi) + E[Si]$' dir. i =1,…, N.

Tüm bağlantılar da, bant genişliği (bit / sn) ve iletim gecikmesi (sn) karakterize bir bit olarak görülmektedir. Bu amaçla, depola ve ilet tipi her bir düğüm (anahtar

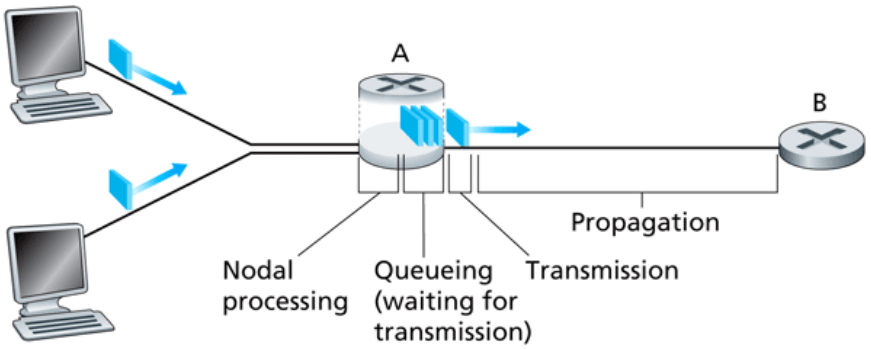
elemanının) dışarıdan gelen ve dışarıya çıkan paketlerin depolandığı tampon bir boşlukta (kuyruk) tutulmaktadır.

Bu tampon boşluk, her gelen ve giden linke bağlı tüm kuyruklar arasında paylaşılan bir kaynaktır. İletilen paketler, veri paketleri ya da yönlendirme paketleri olabilir. Paketler sıraya alınmış veya ilk giren ilk çıkar (FIFO) ilkesi temelinde iletilebilmektedir. Bir paket, yönlendirme tablosundan hedef düğüme doğru giden yolu takip etmek için kullanılacak bağlantı hakkındaki bilgileri okumaktadır. Bağlantı kaynakları kullanılabilir olduğunda, kaynaklar ayrılır ve kaynakların transferleri ayarlanır. Bir paketin bir komşu düğüme geçmek için gereken zaman, paketin büyüklüğü ve bağlantı iletiminin özelliklerine bağlı olarak değişebilmektedir. Paketi tutmak için yeterli arabellek alanı yoksa paket iletildikten sonra atılır. Ağda bulunan iki gezgin düğümden her i ve j düğümleri arasındaki bağlantılar çift yönlüdür (Üçgün, 2005).

5.6 Paket Anahtarlamalı Ağlarda Gecikme, Kayıp Ve Veri Miktarı

Bilgisayar ağlarında, saniyede aktarılan toplam veri miktarı (throughput) sınırlıdır. Ayrıca, uçtan uca gecikme ve paket kayıpları yaşanır. Bilgisayar ağlarındaki bu sınırlamaları tümüyle ortadan kaldırmak fiziksel olarak mümkün değildir. Throughput miktarını artırmak, gecikmeyi en aza indirmek ve paket kayıplarını ortadan kaldırmak için çok sayıda yöntem önerilmiş ve çok sayıda doktora tez çalışması yapılmıştır.

Bir paket bir host'tan (kaynak - source) yola çıkar, çok sayıda router (yönlendirici)'dan geçer ve en sonunda bir başka host'ta (hedef - destination) yolculuğu biter. Bir paket bir düğümden (router (yönlendirici) veya host) komşu bir düğüme (node) giderken (router (yönlendirici) veya host) yolu üzerindeki her node'da gecikmeler yaşanır. Bu gecikmeler, nodal processing delay (düğüm işlem gecikmesi), queuing delay (kuyruk gecikme), transmission delay (aktarım gecikmesi) ve propagation delay (yayılma gecikmesi) dir. Bunların tümünün toplamına toplam düğüm gecikmesi denir.



Şekil 5.4: Paket Anahtarlamalı Ağlarda Delay, Loss Ve Throughput (Üçgün, 2005).

Bir paket router (yönlendirici) A'ya geldiğinde, önce başlık bilgilerine bakılır ve ilgili çıkış bağlantısı seçilir. Eğer router (yönlendirici) A'nın ilgili çıkış bağlantısı

üzerinde bekleyen paket yoksa doğrudan gönderilir. Eğer bağlantı kullanılıyor ve kuyrukta bekleyen paketler varsa, gelen paket kuyruğa eklenir (Üçgün, 2005).

Processing delay, paketin başlık bilgisine bakılarak çıkış portunun belirlenmesi için geçen süredir. **Processing delay**, bit seviyesinde hata kontrolü için geçen süreyi de içerir. Yüksek hızlı router (yönlendirici)'larda processing delay mikrosaniye düzeyindedir. **Queuing delay**, paketin bağlantıdan gönderilebilmesi için geçen süredir. **Queuing delay** bekleyen paket sayısına bağlıdır. Bekleyen paket yoksa gecikme sıfır olur.

Bir paketin tamamı router (yönlendirici)'a geldikten sonra iletilir (store-and-forward). **Transmission delay**, bir paketin tamamının iletim ortamına verilebilmesi için geçen süredir. Bir paketin toplam boyutu L bit ve router (yönlendirici) A ile router (yönlendirici) B arasındaki bağlantının iletim oranı R bps ise, transmission delay, L/R saniye olacaktır. Transmission delay, mikrosaniye düzeyindedir.

Bir bit bağlantı üzerine gönderildiğinde diğer router (yönlendirici)'a kadar yayılım yapar. **Propagation delay,** bir bitin bağlantının bir ucundan diğer ucuna ulaşması için geçen süredir. Propagation delay, sinyalin iletim ortamındaki yayılım hızı ile mesafeye bağlıdır ve d/s (distance – m, speed - m/s) şeklinde gösterilir. Wide-area network'lerde yayılım gecikmesi milisaniye düzeyindedir.

İki router (yönlendirici) arasındaki toplam gecikme aşağıdaki gibi ifade edilir:

$d_{düğüm} = d_{süreç} + d_{kuyruk} + d_{aktarım} + d_{yayılma}$

Kuyruk Gecikmesi ve Paket Kayıpları

Bilgisayar ağlarında üzerinde en çok araştırma yapılan konu kuyruk gecikmesidir (dqueue). Diğer gecikme türlerinden farklı olarak, kuyruk gecikmesi her paket için farklı olur. Boş bir kuyruğa 10 paket gelirse, ilk paket gecikme olmadan gönderilir, ancak sonuncu pakete kadar her pakette gecikme artarak devam eder. Gecikme değerini analiz ederken ortalama bir gecikme değeri veya belirli bir değerden fazla olma olasılığı hesaplanabilir. Kuyruk gecikmesi ne zaman önemlidir ne zaman değildir?

Kuyruk gecikmesinin önemli olup olmaması, paketlerin kuyruğa geliş trafiği, bağlantının iletim oranı ve trafiğin karakteristiğine (periyodik veya burst) bağlıdır.

- a (paket/s) paketlerin kuyruğa geliş oranını göstersin.
- R (bps) iletim oranı ve kuyruktan çıkan bit sayısını göstersin.
- L ise paketlerin boyutunu (bit) göstersin.
- Kuyruğa saniyede gelen bit sayısı La bps olur.
- Trafik yoğunluğu La/R şeklinde gösterilir.

Buradan:

- Eğer La/R > 1 olursa kuyruğa gelen bit sayısı kuyruktan ayrılan bit sayısından büyüktür.
- Eğer kuyruk uzunluğu sınırsız olursa paketlerdeki kuyruk gecikme süresi sonsuza doğru artarak devam eder.
- Eğer kuyruk uzunluğu sınırlı olursa bir süre sonra gelen paketler atılmaya başlar.
- Eğer La/R ≤ 1 olursa kuyruğa gelen bit sayısı kuyruktan ayrılan bit sayısından küçüktür.
- Eğer paketler periyodik olarak L/R saniye aralıklarla gelirse kuyruk gecikmesi olmaz.
- Eğer paketler periyodik ancak burst şeklinde gelirse, örneğin N paket (L/R) saniye aralıklarla gelirse, ilk pakette gecikme olmaz sonrakilerde gecikme artarak devam eder.

Gerçekte paketlerin kuyruğa gelişi rastgeledir. Bu durumda trafik yoğunluğuna göre kuyruk gecikmesi aşağıdaki şekildeki gibi gerçekleşir. Trafik yoğunluğu 1'e yaklaştıkça kuyruk gecikmesi hızla artar. Kuyruklar sınırlı kapasiteye sahiptir ve router (yönlendirici) tasarımına ve fiyatına bağlıdır. Trafik yoğunluğu 1'e yaklaşırken paket gecikmesi sonsuza doğru artmaz. Paket tamamen dolu bir kuyruğa gelirse saklamak için yer olmadığından paket atılır (loss). Trafik yoğunluğu arttıkça paket kayıp oranı artar. Bir node için performans, paket gecikmesinin yanında paket atılma olasılığıyla da değerlendirilir.

Veri ağlarındaki en önemli performans ölçütlerinden biri paketlerin ortalama gecikmesidir. Ağdaki iletişim gecikmeleri 4 farklı gecikmeden kaynaklanır:

1. İşleme Gecikmesi: Paketin doğru bir şekilde okunması ile paketin çıkışa verilmesi arasındaki süre

2. Kuyruk Gecikmesi: Paketin iletişim için bir kuyruğa eklenmesi ile iletime başlaması arasındaki süre

3. İletim Gecikmesi: Paketin ilk ve son bitlerinin iletilmesi arasındaki süre

4. Yayılma Gecikmesi: Paketin son bitinin gönderilmesi ile paketin karşı tarafta alınması arasındaki süre

Her bağlantı yolu için bir azami iletim kapasitesi mevcuttur.

5.7 Kuyruk Modelleri

Bir paketin servis süresi L/C olarak ifade edilebilir. Burada L bit uzunluğu olarak paket boyutu ve C bit/saniye cinsinden bağlantı kapasitesidir. Böyle bir bağlantı yolunda yer alan bir kuyruk sistemi için genellikle aşağıdaki niceliklerle ilgileniriz (Kula,2006):

1. Sistemde ortalama kaç adet paket vardır?

2. Herhangi bir paket için ortalama gecikme süresi ne kadardır?

Sistemde n adet paket olma olasılığı P_n ile gösterilirse sistemdeki ortalama paket sayısı $N = \sum_{i=0}^{\infty} nP_n$ şeklinde hesaplanabilir. İlk başta boş durumda olan bir sistem için, α (t) ve β(t) ifadeleri sırasıyla;

sisteme [0-t] aralığında gelen paket sayısı ile sistemde [0-t] aralığında servis verilen paket sayısını göstersin. Bu durumda t anında sistemdeki paket sayısı N(T),

N(T) = α (t)- β(t)

şeklinde hesaplanabilir. Bu ifade yardımı ile Şekil-1'deki iki bağıntı arasında kalan alan iki farklı şekilde

$$\int_0^t N(\tau)d\tau = \sum_{i=1}^{\beta(t)} T_i + \sum_{i=\beta(t)+1}^{\alpha(t)} (t - t_i)$$

olarak hesaplanabilir. Burada T_i sistemde harcanan zamanları ve t_i geliş sürelerini gösteriyor.

Aşağıda yer alan formülde λ ortalama paket gelme oranı olmak üzere, N = λT şeklinde ifade edilen **Little formülü** elde edilir.

$$\lim_{t\to\infty} \frac{1}{t} \int_0^t N(\tau)d\tau = \lim_{t\to\infty} \frac{\alpha(t)}{t} \lim_{t\to\infty} \frac{\sum_{i=1}^{\beta(t)} T_i + \sum_{i=\beta(t)+1}^{\alpha(t)} (t - t_i)}{\alpha(t)}$$

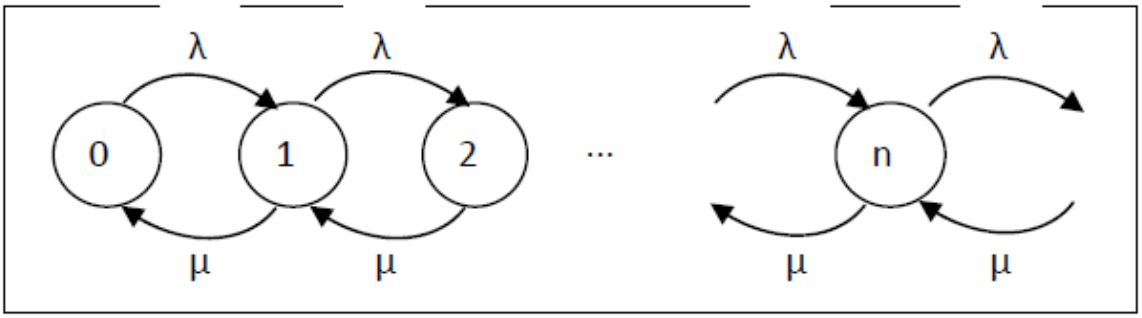
5.7.1 M/M/1 Kuyruk Sistemi

M/M/1 (Giriş Dağılımı / Hizmet Dağılımı / Sunucu Sayısı) kuyruk sistemi tek sunuculu kuyruk istasyonunu ifade etmektedir. Burada, paketler λ parametresine bağlı olarak Poisson dağılımıyla sisteme gelirler. Dolayısıyla, paketlerin geliş süreleri arasındaki fark üstel olarak dağılmaktadır (Kula,2006).

Ayrıca, ortalaması μ^{-1} olan üstel dağılıma göre kullanıcılara hizmet verilir.

M: belleksiz dağılım (Poisson - Üstel), G: genel dağılım, D: belirli dağılım olarak ifade edilmektedir.

Little teoremi ve sonuçları burada da geçerlidir (N = λT). Ayrık zamanlı Markov zincirlerini kullanarak M/M/1 kuyruk sistemini Şekil-2'deki gibi ifade edebiliriz. Bu zincirde λ sıklıkla (paket/saniye) yeni bir paket gelirken, μ sıklıkla (paket/saniye) da kuyruktaki paketlerden ilkine hizmet verilmektedir. Gelen ve hizmet verilen paketlere göre kuyruktaki paket sayısı değişmektedir. Bu durumda sonsuz uzunluklu kuyruk için aşağıdaki denklemler bulunabilir.



Şekil 5.5: M/M/1 Kuyruk Sistemi - Markov Zinciri

Sistemin kararlılığını sağlamak için, her iki yöndeki ilerleme olasılıkları eşit olmalıdır (Kula,2006).

Little teoreminden yararlanarak herhangi bir paketin sistemdeki ortalama bekleme süresi:

$$T = \frac{N}{\lambda} = \frac{1}{\mu - \lambda}$$

şeklinde hesaplanır. Bu süreden hizmet alma süresini çıkartarak kuyrukta harcanan ortalama süreyi aşağıdaki gibi hesaplayabiliriz.

$$W = T - T_{servis} = \frac{1}{\mu - \lambda} - \frac{1}{\mu} = \frac{\rho}{\mu - \lambda}$$

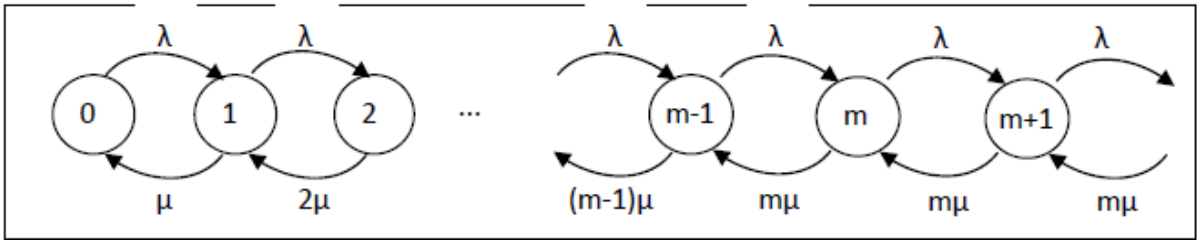
Buradan da kuyruktaki ortalama paket sayısı aşağıdaki şekilde hesaplanabilir.

$$N_k = \lambda W = \frac{\rho^2}{1-\rho}$$

Görüldüğü üzere; sistemin yalnızca faydalanılma oranı kullanılarak, kuyruktaki ortalama paket sayısı hesaplanabilmektedir.

5.7.2 M/M/m Kuyruk Sistemi

Bankadaki sistemlere benzer şekilde, kuyruğumuza toplam m adet sunucunun hizmet verdiğini düşünelim. Her bir kasiyer kuyrukta biri olduğu sürece hizmet sunsun.



Şekil 5.6: M/M/M Kuyruk Sistemi

Kuyrukta bekleyen ortalama paket sayısının, sisteme yeni gelen bir paketin boşta sunucu bulamama olasılığına göre değişimini göstermektedir. M/M/m sistemlerinin, servis hızı mμ olan M/M/1 sistemleri gibi davrandığını göstermektedir. Diğer önemli denklemleri de aşağıdaki gibi elde edilmektedir (Kula,2006).

$$W = \frac{N_k}{\lambda} = \frac{\rho P_k}{\lambda(1-\rho)}$$

$$T = \frac{1}{\mu} + W = \frac{1}{\mu} + \frac{P_k}{m\mu - \lambda} \qquad (\rho = \lambda/m\mu)$$

$$N = \lambda T = \frac{\lambda}{\mu} + \frac{\lambda P_k}{m\mu - \lambda} = m\rho + \frac{\rho P_k}{(1-\rho)}$$

5.7.3 M/M/∞ Kuyruk Sistemi

$$n\mu P_n = \lambda P_{n-1}$$

$$P_n = P_0 \left(\frac{\lambda}{\mu}\right)^n \frac{1}{n!}$$

$$P_0 = \left[1 + \sum_{i=0}^{\infty} \left(\frac{\lambda}{\mu}\right)^i \frac{1}{i!}\right]^{-1} = e^{-\lambda/\mu}$$

$$P_n = \left(\frac{\lambda}{\mu}\right)^n \frac{e^{-\lambda/\mu}}{n!}$$

Görüldüğü üzere, kararlı durumda paket sayısı λ/μ parametreli Poisson dağılımı gibi davranmaktadır. Sistemdeki ortalama paket sayısı N = λ/μ ve ortalama gecikme T=1/μ şeklindedir.

5.7.4 M/M/m/m Kuyruk Sistemi: Kayıplı m Sunucu Sistemi

Bu sistemin M/M/m sisteminden farkı, sisteme yeni bir paket geldiğinde eğer boş bir sunucu bulamıyorsa, paket düşmektedir. Bu yapı telefon sistemlerinde oldukça yoğun şekilde kullanılmaktadır.

$$n\mu P_n = \lambda P_{n-1}$$

$$P_n = P_0 \left(\frac{\lambda}{\mu}\right)^n \frac{1}{n!}$$

$$P_0 = \left[\sum_{i=0}^{m} \left(\frac{\lambda}{\mu}\right)^i \frac{1}{i!}\right]^{-1}$$

Bunlara göre, yeni gelen bir paketin tüm sunucuları dolu bulup düşme olasılığı, diğer adıyla **Erlang B** formülü aşağıdaki gibi bulunur.

$$P_m = \frac{(\lambda/\mu)^m / m!}{P_0}$$

5.7.5 Öncelikli Kuyruklar

M/G/1 sistemleri için n farklı öncelik sınıfının tanımlı olduğu durumu inceleyelim. k. öncelik sınıfı için gelme oranı ve servis süresinin ilk iki momenti sırasıyla $\lambda_k, \overline{X_k} = 1/\mu_k, \overline{X_k^2}$ şeklinde verilebilir.

5.7.6 Sırasını Bekleyen Öncelik

Düşük öncelikli servisteki paketin tamamlanmasının beklendiği durumdur. Birinci sınıftaki paketlerin kuyruktaki ortalama bekleme süreleri aşağıdaki gibi bulunur.

$$W_1 = R + \frac{1}{\mu_1} N_k^1 \quad W_1 = \frac{R}{1-\rho_1}$$

İkinci öncelikli sınıftaki paketler için de benzer bir bekleme süresi hesabı yapılabilir. İlk hesaptan farklı olarak ikinci sınıftaki kuyrukta yer alan paketler ilk sınıftaki paketleri de bekleyeceklerdir. Bu durum aşağıdaki şekilde ifade edilebilir.

$$W_2 = R + \frac{1}{\mu_1} N_k^1 + \frac{1}{\mu_2} N_k^2 + \rho_1 W_2$$

Buradan da ikinci öncelikteki paketlerin ortalama bekleme süresi aşağıdaki gibi hesaplanır.

$$W_2 = \frac{R}{(1-\rho_1)(1-\rho_1-\rho_2)}$$

Herhangi bir paket için ortalama gecikme:

$$T_k = \frac{1}{\mu_k} + W_k$$

olarak hesaplanmaktadır. Bu durumlar için $R = \frac{1}{2}\sum_{i=1}^{n} \lambda_i \overline{X_i^2}$ olarak hesaplanabilir.

Veri paketleri, kaynaktan final hedefine ulaştırılırken:

- Hesaplama (veya işleme), paketlere (veya head'leri) rehber bilgileri eklemeyi gerektirir ve paketleri doğru hedeflere iletmek için gerekli işlemi yapar.
- İletişim linkleri üzerindeki paketleri iletir

5.8 TCP'de Tıkanıklık Denetimi Ve Çözüm Yöntemleri

Paketlerin korunumunu başarısız kılacak 3 adet neden vardır:

1- Bağlantı, korunum ilkesini yerine getiremez.

2- Bir gönderici, eski bir paket alınmadan çıkmadan yeni bir tane gönderir.

3- Yol kaynaklarının yetersizliği yüzünden eşitlik ilkesi yerine getirilemez.

Birinci başarısızlık nedeni, bir paketin ilk defa iletilmesi veya yeniden iletilmesi durumunda ortaya çıkar. Bir düğüm tarafından alınan paketin başka bir düğüme

iletilmesinde sorun varsa ve bu sırada diğer düğümden paketler gelmeye devam ediyorsa bu başarısızlık meydana gelir. Bunu, paketlerin bir düğümde yığılması olarak da değerlendirebiliriz. Korunum özelliğine bir başka açıdan bakacak olursak, gönderici aldığı ACK (acknowledge) paketlerinin hızına bakarak gönderme işlemine devam ederse sistem kendini ayarlamış olur. Fakat bu durum, sistemin kendisini sınırlamasına yol açar. Yeni bir paketin iletilmesi için bir ACK gereklidir. Bir ACK almak için de bir paketin iletilmesi gereklidir. Zamanlamaya başlamak için slow-start algoritması geliştirilmiştir. Bu algoritma şu şekilde çalışır:

- Her bir bağlantı için bir tane tıkanıklık penceresi, cwnd ekle,
- Bir kayıp olduğu zaman cwnd'yi bir pakete ayarla,
- Alınan her bir ACK'den sonra cwnd'yi birer paket arttır,
- Veri gönderirken, alıcının ilan ettiği pencere ile cwnd arasından en küçük olana göre işlem yap.

İkinci başarısızlık nedeni de eşitlik ilkesinin korunmamasıdır. Bu ilkeyi korumak için iyi bir gidiş-dönüş zamanlaması'na ihtiyaç vardır. İyi bir gidiş-dönüş zamanlaması kestirimi, tekrar iletim zamanlayıcısının çekirdeğini oluşturur. Bu da, bir protokolün ağır yükler altında çökmemesi için gerekli olan en temel bileşenlerdendir. Kuyruk teorisinden şu bilinmektedir; yükle birlikte gidiş dönüş zamanı (round-trip time - RTT) ve onun değişimi hızla artmaktadır.

TCP, ortalama RTT'yi hesaplamak için bir alçak geçiren filtre tanımlamaktadır.

$SRTT = \alpha * SRTT + (1-\alpha) * RTT$

Paket kaybı genellikle ağ tıkanıklığından dolayı meydana gelir. Zaman aşımı da paket kaybından dolayı meydana gelir. Böylece, zaman aşımının ağ tıkanıklığından dolayı meydana geldiğini söyleyebiliriz. Bir ağdaki yükün ölçütü olarak, gidiş-dönüş zaman gecikmesinin neden olduğu ortalama kuyruk uzunluğunu alınırsa, tıkanmamış bir ağ bu parametrelere bağlı olarak ifade edilebilir. Bir ağdaki anlık yük L(i)=N olarak ifade edilebilir. Zamana bağlı olarak bir ağdaki yük L(i) =N+g*L(i-1) şeklinde ifade edilebilir. Bu ifade, zaman gecikmesi nedeni ile kuyrukta kalan yükün, sonraki zaman birimindeki trafiğe etkisidir. Eğer ağda tıkanıklık varsa, g değeri büyük olacaktır ve kuyruk uzunluğu üssel olarak artacaktır. Tıkanıklık durumunda pencere boyutu şu şekilde ayarlanır:

• $W(i) = d * W(i-1)$ burada $d < 1$

Tıkanıklık kaybolduğu zaman ise pencere boyutu aşağıdaki gibi ayarlanır:

• $W(i) = W(i-1) + \mu$ burada $\mu <= Wmax$

Buradaki Wmax değeri, ağın hiç yük olmaması durumundaki pencere boyutunu ifade eder. Tıkanıklıktan kaçınma algoritmasını yazan kişiler $d=0.5$, $\mu=1.0$ almışlardır.

Böylece, algoritma:

1. Herhangi bir zaman aşımında, cwnd'yi geçerli pencere boyutunun yarısına ayarla.

2. Her bir yeni veri için alınan ACK ile, cwnd'yi 1 arttır.

3. Veri gönderirken, cwnd ile alıcının duyurduğu pencere boyutundan küçük olanına göre gönder. Şeklinde ifade edilir.

5.9 Kablosuz Ağlar İçin Değiştirilmiş TCP Sürümleri

Geleneksel TCP'nin kablosuz ağlarda kullanılmasının çeşitli sakıncaları vardır. Bunlar aşağıda özetle anlatılmaktadır.

Paket Kayıplarını Yanlış Yorumlama: Geleneksel TCP, kablolu ağlar için hazırlanmıştır ve paket kayıplarını tıkanıklık belirtisi olarak değerlendirir. Bir paket kaybolduğu zaman tıkanıklık çözümü için geliştirilmiş olan algoritma işletilir. Hareketli tasarsız ağlarda, kablolu ağlara göre çok daha fazla paket kaybı yaşanmaktadır. Tasarsız ağlarda sık sık düğümlerin hareketliliğinden ötürü yol kırılmaları meydana gelmektedir, radyo sinyallerinin girişimde bulunması, tek yönlü bağlantılar gibi nedenlerden dolayı paket kayıpları yaşanmaktadır. Bu kayıpların tıkanıklık olarak değerlendirilmemesi gerekmektedir.

Sık Bağlantı Kopmaları: Hareketli tasarsız ağlarda düğümlerin hareketliliği ile ilgili olarak bir kısıtlama olmadığı için sık sık bağlantı kopmaları yaşanmaktadır. Bir bağlantı koptuktan sonra, yeni bir yolun temin edilmesi gerekmekte ve ağ üzerinde çalıştırılan yönlendirme algoritması bunu yapmaktadır. Yeni yolun kurulma süresi eğer tekrar iletim zaman aşımı aralığı (retransmit timeout interval) RTO'dan büyükse, gönderici düğüm bir tıkanıklık olduğu düşünüp, tıkanıklık algoritması çalıştıracaktır ve kaybolan paketleri yeniden gönderecektir. Bu da bant genişliğinin azalmasına ve bataryanın boş yere kullanılmasına neden olacaktır.

Yol Uzunluğunun Etkisi: Hareketli tasarsız ağlarda yol uzunluğunun büyük olması demek, hedefe daha fazla düğüm üzerinden geçilerek gidilmesi demektir. Bu da, düğümlerin hareketliliğinden dolayı daha fazla yol kırılmasına yol açar.

Tıkanıklık Penceresinin Yanlış Kullanılması: Tasarsız ağlarda bir yol kırılması meydana geldiği zaman tıkanıklık önleme algoritması işletilir ve tıkanıklık pencere boyutu azaltılır ve RTO'yu arttırır. Yeni yol kurulduğu zaman, tıkanıklık penceresi buna hemen uyum sağlayamaz. Yeni kurulmuş olan yolun kapasitesi yüksek olmasına rağmen bunun küçük bir kısmı kullanılabilir. Bundan dolayı, sık sık yol kırılmaları hattın verimliliğini düşürür.

Asimetrik Bağlantı Davranışı: Hareketli tasarsız ağda kullanılan radyo kanalı farklı özelliklere sahip olabilir. Radyo dalgalarının yayılımının çevresel etkisi, konumdan dolayı meydana gelen çekişme gibi nedenlerden ötürü hat tek yönlü olabilir. Bu da,

ACK paketlerinin iletilmesini engeller. Bu durumda, tıkanıklık algoritmasını çalıştırmak mümkün değildir.

Kablosuz bağlantılarda ile ilgili yapılan çalışmalarda, kablosuz ağlardaki paket kayıpları, çoğunlukla kablosuz kanaldaki bozulmalardan kaynaklanan bit hatalarından, ikinci olarak hareketliliğe bağlı olarak kanalı yakalayamamaktan ve son olarak da sık olmasa da tıkanıklıktan dolayı oluşmaktadır. Bit hataları ve kanalı yakalayamama gibi durumlarda TCP yeterli olamamakta ve TCP'ye bağlı çalışan uygulamalarda sıkıntılar yaşanmaktadır. Ayrıca kablosuz ağlarda yaşanan diğer bazı problemler ise, düşük sinyal nedeniyle veri iletişimini sağlayamamaktır. Bu durumlarda oluşan bir paket kaybı, TCP tarafından bir tıkanıklık olarak algılanmakta ve hemen yavaş başlangıç algoritması başlatılmaktadır. TCP'de esas problem, oluşan bir darboğaz durumunda uygulanması gereken algoritmalardır (Aygın, 2008).

TCP Tahoe'deki problem, bir paket kaybını algılamak için geçen süre tam bir zaman aşımı süresidir ve birçok gerçeklemede bu büyük bir zamanaşımı süresi gerektirir. Ayrıca acil ACK göndermediğinden, her defasında bir zamanaşımı beklenir ve hat boşaltılır. Bu durum yüksek bant genişlikli ürün bağlantılarında zaman açısından yüksek bir maliyet oluşturur. Bu maliyetin anlamı bir penceredeki kaybolan paketlerin her birisi için tekrar yeniden gönderim gerçekleşir ve çok fazla bekleme gerektirir (Aygın, 2008).

TCP Reno paket kaybı az olduğu durumlarda TCP üzerinde mükemmel çalışmaktadır. Ancak bir penceredeki paket kaybı birden fazla olursa o zaman Reno çok iyi performans gösterememektedir. Eğer birden fazla paket kaybı varsa, ilk kaybolan paket için çift ACK'lar alınır. Sonra kaybolan ikinci paket için bilgi ise ancak bir RTT sonra, yeniden iletilen ilk paketin ACK'sından sonra alınır. Bu sebeple hızlı yeniden iletim ve hızlı geri dönüş algoritmaları daha geç başlatılmış olmaktadır. Bu da tıkanıklığın giderilmesi ve iletimin tamamlanması için zaman kaybına neden olur (Aygın, 2008).

5.10 Ağ Modellemelerinde Kullanılan Benzetim Programı OPNETT

Kablosuz ağların modellenmesinde gelişmiş nesne tabanlı özellikleri ve uygulama destekleri nedeniyle OPNET programı tercih edilmiştir. OPNET programı ile sistemin davranışı ve ayrık olay benzetimi gerçekleştirilerek analiz yapılabilir. Her biri değiştirilebilir özelliklere sahip nesnelerden oluşur. Düğüm modeli ve süreç modeli oluşturma amaçlı editörler yardımıyla kullanıcı tanımlı düğümler ve protokoller oluşturulabilmektedir. Profil tanımlamaları ve uygulama tanımlamaları editörler yardımı ile değiştirilebilmektedir (Tanenbaum,2003).

OPNET benzetim programında üç seviye bulunmaktadır. Bunlar; ağ, düğüm ve süreç şeklindedir. Bu seviyeler görsel düzenleyiciler kullanılarak geliştirilebilmektedir. Her bir seviye için düzenleyici editörler bulunmaktadır. Program aynı zamanda benzetim parametrelerini düzenlemek ve veri analizi yaparak grafik oluşturmak için de araçlar içermektedir (Kirov, 2005).

Ağ yapısı, düğüm ve süreç modelleri bir proje dosyasına dâhil olan senaryolar halinde oluşturulmaktadır. Tasarım tamamlandığında benzetim aracı yardımıyla toplanacak istatistikler belirlenerek çalıştırılır. Program dâhilindeki analiz aracı sayesinde elde edilen veriler, istenen grafik türünde görüntülenebilmektedir. Birden fazla senaryoya ait verilerin aynı grafik üzerinde gösterilerek karşılaştırılması da mümkündür (Tanenbaum,2003).

6. TELEKOMÜNİKASYON SEKTÖRÜNDE DİJİTAL ARŞİV SÜRECİNDE VERİ İŞLEME VE AKTARIM TEKNOLOJİSİ ANALİZİ

Tüm sektörlerde, kurum içi yada kurum dışı yazışmalar, faturalar, sözleşmeler gibi hukuksal süreç açısından orijinalinin saklanması zorunlu olan yada olmayan belgelerin dijital ortama aktarılması önem kazanmıştır.

Bilgi ve belgeye en kısa sürede erişim sağlanması, ayrıca; kurumların iç işleyişiyle ilgili olarak üretilen ancak yasal nedenlerle saklanmasına gerek olmayan belgelerin dijital ortama aktarılması da önemli ihtiyaçlardandır.

Dijital Arşivleme Sistemi ile belgelere daha kolay erişim, birden fazla kullanıcının aynı anda bilgi edinmesi ve amaçları doğrultusunda kayıtları inceleyip kullanmasını sağlama gibi birçok avantaj sağlanmıştır.

Dijital arşiv yönetim sistemi sayesinde evrak arşivlerinizin uluslararası kalite sistemlerine göre elektronik ortama aktarılması, ilişkilendirilerek düzenlenmesi, elektronik katalog oluşturulması; yine dijital ortamda dağıtımı, saklanması, depolanması, denetimi içeren kapsamlı bir kurumsal çözüm sunar.

Telekomünikasyon sektöründe; müşteri bilgilerinin güvenli ortamda saklanması ve sistemler arası aktarılması son yıllarda büyük önem kazanmıştır. Özellikle bilgi güvenliği ve müşteri bilgilerinin saklanması, dijital arşivlemeyi telekomünikasyon sektöründe vazgeçilmez bir olgu haline getirmektedir.

Dijital Arşiv Sürecinin Amaçları:

- Arşiv belgelerinin çoklu kullanıma sunulması
- Elektronik ortamda belgeye tek noktadan hızlı bir şekilde erişimin sağlanması
- Dosya ve belgelerin yıpranmasının önüne geçilmesi
- Müşteriye ve vatandaşa kaliteli ve hızlı hizmetin sunulması
- Yetkisi olmayanların dosyaya ve bilgiye erişiminin engellenmesi ve belge mahremiyetinin korunması
- Zaman ve mekân tasarrufunun sağlanması gibi birçok amacın gerçekleşmesi sağlanacaktır

6. 1 Dijital Arşiv Sürecinde Veri Aktarım Mekanizması

Uygulamanın gerçekleştiği dijital arşivleme merkezinde, kanallardan toplanan müşteri evrakları; evrak kabul, ayrıştırma, tarama, toplama, indeksleme, kutuluma süreçlerinden sonra arşivlenmektedir. Günlük taranan evraklar, indeks aşamasından sonra tanımlanarak, bir sonraki sisteme aktarılmaktadır.

Bu süreçte uygulama gerçekleştirilen telekomünikasyon firmasında bir sonraki sisteme aktarım sırasında dokümanlar tif formatında imaj ve bu imajlara ait xml veriları ile birlikte TCP üzerinden FTP ile bir sonraki sisteme aktarılır. Aktarım İzmir ve Ankara arasında gerçekleşmektedir.

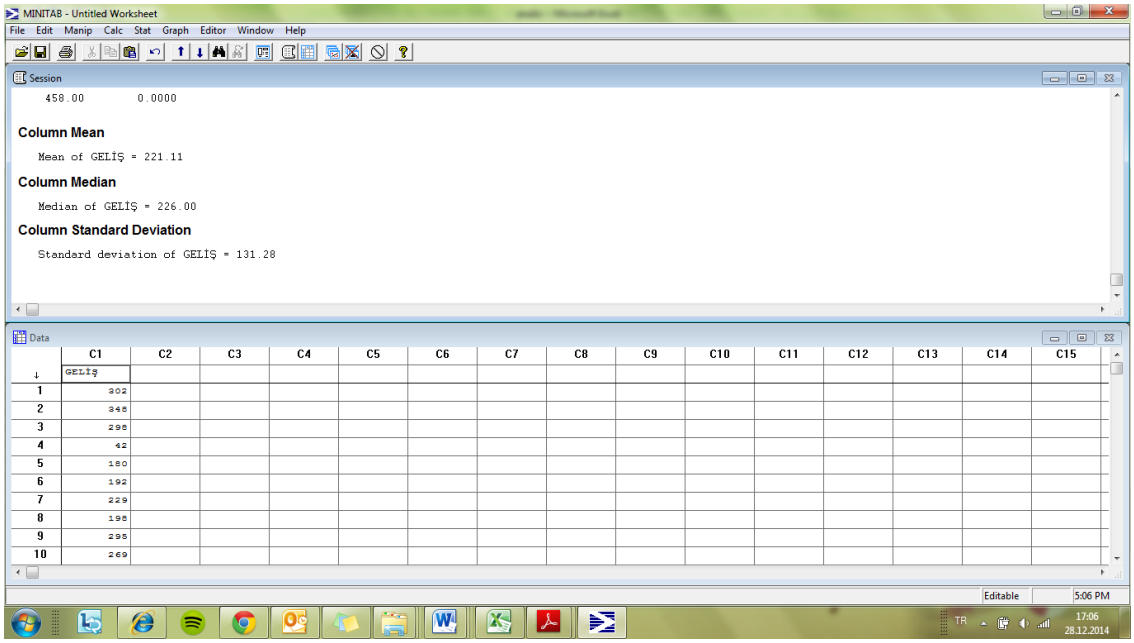
Problem konusu olan sistemde, aktarım sırasında günlük olarak kuyrukta bekleyen dosya paket sayılarında artış yaşanmaktadır. Bu artışın önüne geçmek ve yeni bir aktarım sistemi tasarlamak için OPNET benzetim ortamında, yeni oluşturulacak algoritma ile sistem davranışları ölçülmüştür.

6.2 Sistemde Oluşan Kuyrukta Bekleme Süresi Analizi ve Sistem Performansının Belirlenmesi

Uygulama gerçekleşitirilen sistemde: Mayıs-Kasım ayları arasında toplam 132 gün boyunca aktarılan paketlerin kuyrukta bekleme süreleri ölçülmüştür. Bu verilerin minitab ortamına yüklenerek dağılımları set edilmiş ve belirlenmiştir.

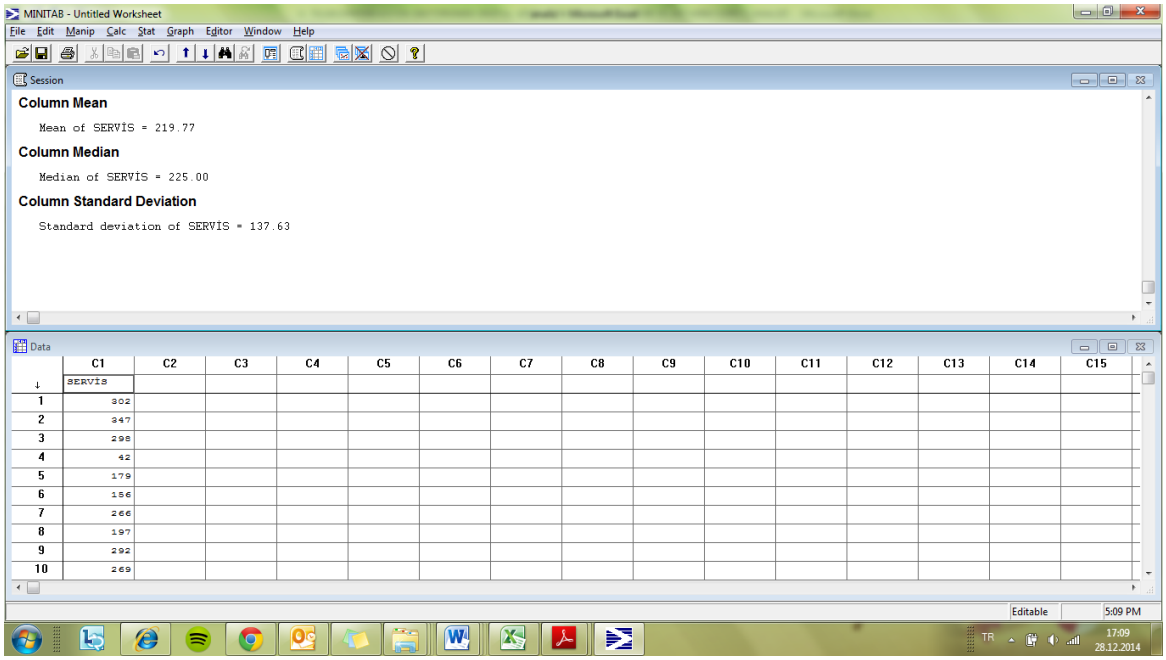
Günlük ortalama 45481 set yaklaşık 19101810 KB dosya aktarılmaktadır. TCP outbound 42532 set yaklaşık 17863348 KB dosyayı kabul etmektedir.

Sisteme gelişler poisson dağılmaktadır ve geliş oranı λ parametreli 221KB/saniye olarak hesaplanmıştır.



Şekil 6.1: Sisteme Geliş Oranı

Sistemde paketlerin aktarım süresi üstsel dağılmaktadır ve servis oranı μ parametreli 219KB/saniye olarak hesaplanmıştır.



Şekil 6.2: Sistemdeki Servis Oranı

Görüldüğü gibi sistemde daima kuyruk oluşmaktadır. Burada λ>μ olduğu için sistemde sürekli olarak bekleyen paketler görülmektedir.

Bu amaçla sistemde iyileştirme yapılmasına kara verilmiştir. Problem kaynağı olarak belirlenen mevcut TCP algoritma üzerinde iyileştirme yapılması planlanmıştır.

Servis sayısı iki katına çıkarıldığında burada:

ρ = λ/ 2*μ şeklinde hesaplanır. Yeni durumda:

ρ = 221/ 2*219 = %50 hesaplanır.

Buradan servis süresinde iyileşmeye gidilmesi yada yeni bir servis eklenmesi gerekmektedir.

6.3 Gecikme Verileri

Uygulamada, aktarılması ve görüntülenmesi gereken bir müşteriye ait evraklar, günlük ortalama 3 abone seti sistemde beklemektedir. 24 saat içerisinde bir sonraki sisteme aktarılmamaktadır.

Gecikme süresi günlük ortalama 326 sn'dir. Aylık Toplam gecikme süresi 12 saattir. Günde 3 abone aylık ortalama 60 abone seti, görüntüleme sistemlerine aktarılamamaktadır.

6.4. Gecikme Maliyeti

Sistem üzerinden görüntülenemeyen evrakların yol açtığı maliyetler sırasıyla:

- **Müşteri Kaybı Maliyeti:**

  Aylık Ortalama: 60*30 =1800 TL/Ay

  Yıllık Ortalama: 21600 TL/Yıl olarak hesaplanır.

  30 TL: Bir abone için ortalama fırsat maliyeti

- **İtibar Kaybı:**

  BTK ve benzeri kuruluşlara zamanında bilgi verilememesinin aylık ortalama maliyeti OECD verilerine göre belirlenmiş ceza maliyetleridir. Bu maliyetler abone başına ortlama 2500 olarak belirlenmektedir.

- **Aktarma Maliyet Kaybı:**

  Aylık Ortalama 12 saat fazla sistem çalışmasından kaynaklanan yaklaşık 500 TL sistem maliyeti bulunmaktadır.

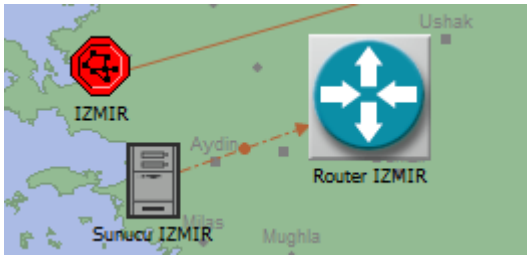
Buradan **Toplam Maliyet Aylık**: 4808 TL hesaplanmaktadır.

6.5 Sistem Üzerinde İyileştirme Önerileri

Kullanılan uygulamada Yavaş başlangıç ve tıkanıklık önleme benzetiminde, ağ üzerinde yapılan konfigürasyon ile TCP bir uçtan uca iletişim protokolü olarak çalıştırıldı. Bir sunucu İzmir'da, bir sunucu da Ankara'da yer almaktadır. Burada tıkanıklık penceresi büyüklüğü farklı mekanizmalarla incelenmiştir. Burada iki tane alt ağ oluşturuldu. Bunlar İzmir ve Ankara alt ağlarıdır. Bu iki alt ağ bir sunucu ve bir yönlendiriciden oluşmaktadır. Bu sunucuların her biri yönlendiricilere saniyede 20 megabit tabanlı bant genişliği sağlayan metro ethernet kabloyla bağlıdır. Yönlendiriciler ise internete saniyede 20 megabit tabanlı metro ethernet kabloyla bağlıdır.

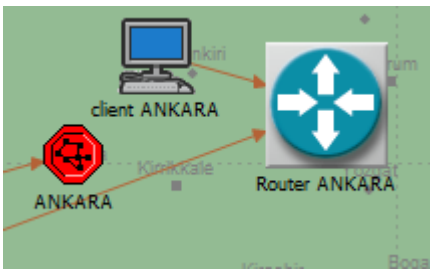
Şekil 6.3: OPNET Üzerinde Sistem Benzetimi

OPNET'te oluşturulan bu şekilde Ankara ve İzmir adlı iki tane alt ağ oluşturulmuş ve bu ağlar internet üzerinden birbirine bağlanmıştır. Uygulama olarak dosya transfer protokolü uygulaması çalıştırılmaktadır.



Şekil 6.4 : İzmir Alt Ağı

Bir sunucu ve bir yönlendiriciden oluşur.



Şekil 6.5 : Ankara Alt Ağı

Bir istemci ve bir yönlendiriciden oluşur.

Süreçte İzmir Sunucusunda oluşturulan xml va imaj yapısındaki verilar; site 2 site VPN üzerinden Ankara alıcı ftp'sine export edilir. Bu gerçeklemede yapılan bir FTP uygulaması hem İzmir alt ağında hem de Ankara alt ağında çalıştırılmış ve bu uygulama internet üzerinden veri alışverişinde bulunmuştur. Bu gerçeklemede günlük yapılan 28474143 KB paketlik veri aktarımının günlük gerçekleşme durumu incelenmiştir. Burada TCP Reno'nun, TCP Tahoe'den az bir farkla daha iyi performans gösterdiği gözlemlenmiştir.

Yeni durumda Aralık ayında toplam 19 gün boyunca aktarılan paketlerin kuyrukta bekleme süreleri ölçülmüştür. Günlük ortalama 67796 set yaklaşık 28474143 KB dosya aktarılmaktadır. TCP outbound 77738 set yaklaşık 32650071 KB dosyayı kabul etmektedir. Sisteme gelişler poisson dağılmaktadır ve geliş oranı λ parametreli 324KB/saniye olarak hesaplanmıştır. Sistemde paketlerin aktarım süresi exponantional dağılmaktadır ve servis oranı μ parametreli 353 KB/saniye olarak hesaplanmıştır. Yeni durumda sunucunun kullanım süresinin toplam zamana oranı:

$\rho = \lambda / \mu$ olarak hesaplandığında; 324/353 = 0,91 bulunur. Sunucu zamanın %91'inde kullanılmaktadır.

Son durumda;

$T_q = \lambda / \mu(\mu - \lambda)$ kuyrukta bekleme zamanı

$T_q = 324/353*(353-324)=0,0316$ sn olarak hesaplanır.

$N_q = \lambda^2 / \mu(\mu - \lambda)$ kuyrukta bekleyen paket sayısı

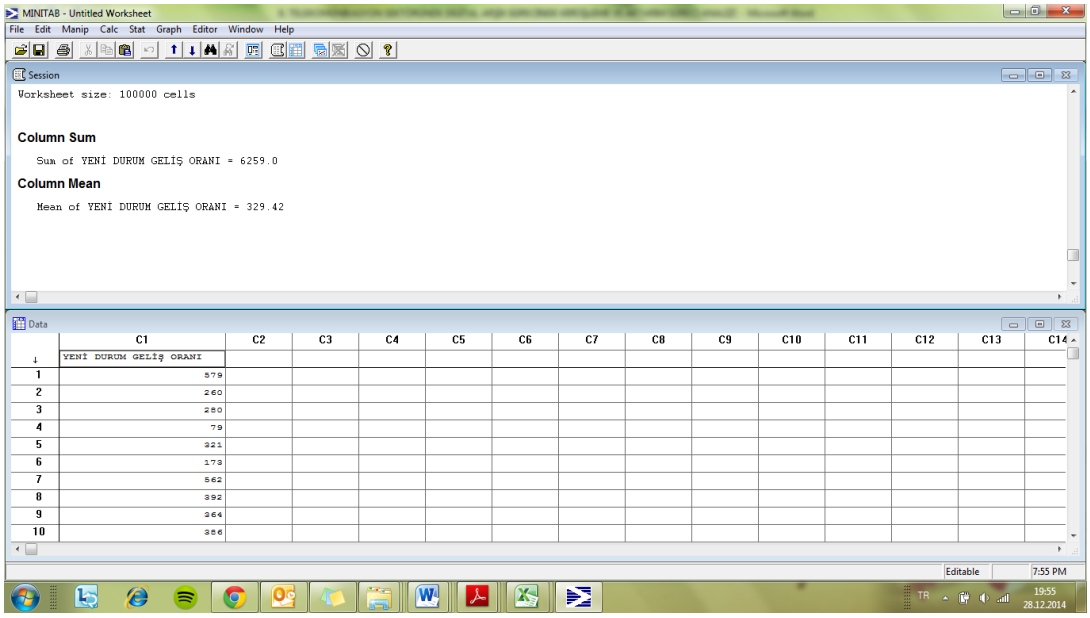
$N_q = 324^2 / 353(353 - 324) = 10,25$ KB

$T = 1 / \mu - \lambda$ Sistemde beklenen süre ise

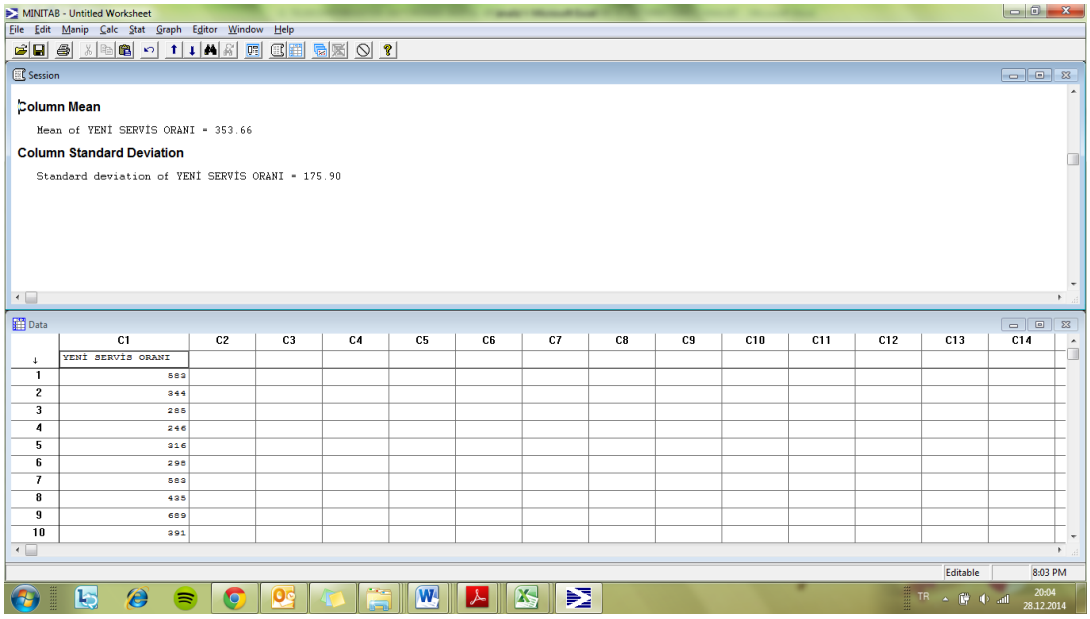
T= 1/(353-324) = 0,0344 sn şeklinde hesaplanır.

N = λ / (μ- λ) Sistemde bekleyen paket sayısı ise;

N = 324/ (353-324) =11,172 KB olarak hesaplanır.



Şekil 6.6: Yeni Durumda Sisteme Geliş Oranı



Şekil 6.7: Yeni Durumda Servis Oranı

TCP algoritmasında yapılan iyileştirme sisteme %9 oranında iyileştirme sağladı. Burada internet seviş sağlayıcısı metro eternet hizmetinde daha önce 20 Mbps (1.677,52 TL) olan internet hizmetinde, 30 Mbps'e (2.217,29 TL) çıkardığımızda maliyette %30 artış gerçekleşmektedir. Veri aktarım hızında ise %50 artış yaşanmaktadır.

Maliyette yaşanan artış, aylık gecikme maliyeti 4808 TL altındadır. Bu durumda yeni süreçte internet servis sağlayıcının hızını 30 Mbps' e çıkardığımızda servis sağlayıcı 2 katına çıkar ve sistemde boş kalma oranı %50 olarak hesaplanır. Bu durumda sistemde aktarılan veri miktarında %50 artış sağlanabilecektir.

7. SONUÇ VE ÖNERİLER

Müşteri bilgilerine hızlı erişmek ve eldeki bilgileri değerlendirebilmek için geliştirilen dijital arşiv sisteminde farklı şehirler arası veri iletiminde kuyrukta beklemek önemli bir problemdir. Kuyrukta beklemeden kaynaklı zaman kayıplarının neden olduğu maliyet yada itibar kayıplara sektörde olumsuz etkilere neden olabilmektedir.

Veri aktarımında en önemli problemlerden biri güvenlik ve sistemdeki tıkanıklıklardır. Tıkanıklıkların giderilmesi için güvenli ve sağlıklı bir veri iletimi sağlamak gerekmektedir. Bununla birlikte güvenlik seviyesi arttıkça veri iletiminde yaşanan hız düşüşleri arasında denge kurulması gerekmektedir. TCP protokolleri ile sağlanan veri iletiminde geliştirilen algoritmalar ile hız ve güvenlik dengesi analiz edilmiştir.

Sunucular arası veri akışında yapılan 132 günlük gözlem sonucu ortaya çıkan değerler minitab üzerinde set edilerek dağılımı belirlendi. Bu durumda iyileşirme öncesi sisteme gelişler poisson dağılım ve λ parametreli 221KB/saniye olarak belirlenirken aktarım süreleri exponantional dağılım μ parametreli 219KB/saniye olarak hesaplanmıştır. Bu durumda sistemde tıkanıklık sonsuz olmaktadır. Problemin giderilmesi için yeni senaryolar önerilmiştir.

İlk senaryoda; TCP algoritmalarında yapılacak değişiklerin yol açacağı iyileştirme oranları tespit edilmiştir. Burada OPNET üzerinde test edilen protokoller ile sistemede TCP algoritmasında yapılan iyileştirme sisteme %9 oranında iyileştirme sağlayacağı görüldü.

İkinci senaryoda ise aktarım hızında artış için servis sağlayıcının hızında yapılacak artışın maliyete ve verimliliğe etkisi incelendi. Burada daha önce 20 Mbps (1.677,52 TL) olan internet hizmetinde, 30 Mbps'e (2.217,29 TL) çıkartıldığında maliyette yaşanan %30'luk artışa göre veri aktarım hızında ise %50 artış yaşanmaktadır.

Bu durumda internet hızı üzerinde yükselmeye gidilmesine karar verildi. Veri aktarımında yaşanan gecikme maliyeti ile daha hızlı internete geçme maliyeti arasında optimum sonuca ulaşıldı.

Telekomünikasyon sektöründe bilgi güvenliği, sadece müşterilerin bilgilerini korumak, gereksiz bilgi almamak değil aynı zamanda sistemler arası aktarımlarda veri kayıplarını önlemek, gecikme ile yaşanan itibar kayıplarını da önlemektir. Güvenlik kriterleri arttırılırken, hız kriterleri de değerlendirilmeli ve uygun protokoller geliştirilmelidir.

KAYNAKLAR:

Alasulu, Necati (2012). Bilgi Güvenliği Ve Kalite Yönetim Sistemleri Arasındaki İlişkinin İncelenmesi Ve Bir Uygulama, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Fırat Üniversitesi, Şubat 2012.

Aydın, Cengiz (2010). Elektronik Belgelerin Arşivlenmesi Ve Erişim, Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Bilgi Ve Belge Yönetimi Anabilim Dalı, Ankara, 2010.

Aygın, Ahmet Kemal (2008). Tcp Tıkanıklık Kontrol Algoritmasının Analizi Ve İyileştirilmesi, Yüksek Lisans Tezi, Bilgisayar Mühendisliği Anabilim Dalı, Gebze Yüksek Teknoloji Enstitüsü, Mühendislik Ve Fen Bilimleri Enstitüsü, Gebze, 2008.

Barman, Scott (2001). Writing Information Security Policies, New Riders Publishing, 2001.

Baykal, N. (2005). Bilgisayar Ağları. Ankara: Sas Bilişim Yayınları.

Bosij, P., D. Chafey, A. Greasley ve S. Hickie (2003). Business Information Systems: Technology, Development and Management for the E-Business. 2. Basım. S. 4-5. Financial Times-Prentice Hall.

Buluç, S. (2009). TS EN ISO 9000:2008 Kalite Yönetim Sistemi'nin Bir Mobilya Fabrikasında Uygulama Aşamaları ve Dokümantasyon Yapısının Oluşturulması, Yüksek Lisans Tezi, Bartın Üniversitesi, Fen Bilimleri Enstitüsü, Bartın.

Calder, A. (2009). Information Security Based on ISO 27001/ISO 27002: A Management Guide, 2nd Edition, Van Haren, Amersfoort.

Canberk, G. ve Sağıroğlu, Ş., (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi, 3 : 165-174, 2006.

Carlson, T. (2001). Information Security Management: Understanding : ISO 17799, Lucent Technologies Worldwide Services, 2001.

Corral G. And Zaballos A. (2005). "Simulation Based Study Of TCP Flow Control Mechanisms Using Opnet Modeler",White paper, 2005.

Courcoubetis, C., Kelly, F., Siris, V.A. ve Weber, R., (2000). A Study Of Simple Usage-Based Charging Schemes For Broadband Networks, Telecommunication Systems, 15, 323-343.

Çağrıcı Gökhan, Ayav Tolga (2007). İzmir Yüksek Teknoloji Enstitüsü'nün Bilgisayar Ağı İçin Bir Servis Kalitesi Uygulaması, Bilgisayar Mühendisliği Bölümü İzmir Yüksek Teknoloji Enstitüsü, İzmir.

Çakır S. (2000). "Çağımızın İletişim Devrinde Fiber Optik", Bilim ve Teknik Dergisi, Ekim 2000.

Çamalan E. (2011). Internet:, "XML Nedir", http://www.yazilimgunlugu.com/XML-nedir-makalesi/328.aspx, 2011.

Çaycı, Aysel Deniz (2007).Veri Toplama Yöntemleri; Telekomünikasyon Sektörü İçin Etkin Veri Toplama ve İşleme Süreçleri Üzerine Bir İnceleme, Uzmanlık Tezi, Telekomünikasyon Kurumu (BTK), 2007, Ankara.

Çelik, Adnan ve Akgemici Tahir (2010). Yönetim Bilişim Sistemleri, Gazi Kitabevi, Ankara 2010.

Çetin, G. ve Metin, B. (2005). Linux Ağ Yönetimi. Ankara, Seçkin Yayıncılık.

Veri Şebekeleri Ve Genişbant Erişim Teknolojileri (2001). http://www.ilhanuysal.com/ders_notlari/agtemelleri/hafta_9.pdf, Ağ Temelleri Ders Notları (6&7&8), Karamanoğlu Mehmetbey Üniversitesi, Teknik Bilimler Meslek Yüksekokulu, 20.12.14

Deloitte,http://www.denetimnet.net/UserFiles/Documents/Makaleler/BT%20Denetim/Veri_Analizi_Veri_Kalitesi_ve_B%C3%BCt%C3%BCnl%C3%BC%C4%9F%C3%BC.pdf, 23.12.2014

Demirel, H. (2009). Kullanıcı Odaklı Mekansal Veri Kalitesi, TMMOB Harita ve Kadastro Mühendisleri Odası 12. Türkiye Harita Bilimsel ve Teknik Kurultayı 1115 Mayıs 2009, Ankara

Devillers, R., Bedard, Y., Jeansoulin, R., Moulin, B. (2007). Towards spatial veri quality information analysis tools for experts assessing the fitness for use of spatial veri, International Journal of Geographical Information Science, Volume 21, Issue 3, syf. 261 – 282

Dinçkan Ali ve Önel Dinçer (2007). Bilgi Güvenliği Yönetim Sistemi Kurulumu, 2007, http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0001-bilgi-guvenligi-yonetim-sistemi-kurulumu/download.html, 23.12.14

Dwork, C., McSherry, F., Nissim, K., ve Smith, A. (2006). Calibrating noise to sensitivity in private veri analysis. TCC Lecture Notes in Computer Science, 265-284.

Efe, A. (2006). Yeni Nesil İnternet Protokolü'ne (Ipv6) Geçişle Birlikte İnternet Saldırılarının Geleceğine Yönelik Beklentiler, Fen Bilimleri Enstitüsü, Beykent Üniversitesi, http://ab.org.tr/ab06/bildiri/134.doc,14.12.14

Eminağaoğlu, M., ve Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 01-15.

Fall K. (1996). Simulation-based Comparisons of Tahoe, Reno, and SACK TCP, Lawrence Berkeley National Laboratory, http://home.iitj.ac.in/~ramana/sacks.pdf, 12.12.14

Ficher, Hans (2010). Communications Network Traffic Veri – Technical and Legal Aspects, PrintService TU/e, Amsterdam, ISBN:978-90-386-2339-9.

Gartner, Inc. (2009). Gartner predicts 2009, http://www.gartner.com/, 23.12.2014

Goodchild M. (2007) Beyond metaveri: Towards usercentric description of veri quality, ISSDQ 2007, ITC, Netherlends, http://www.itc.nl/ISSDQ2007/keynote.aspx, 23.12.2014

Gordon, A. J., Loeb M. P. And Lucyshyn W. (2006). The Impact of the Sarbanes-Oxley Act on the Corporate Disclosues of Information Security Activities‖, Journal of Accounting and Public Policy, 25 : 503-530, 2006.

Gümüş, İbrahim (2012). İnsan Hesaplaması Yaklaşımı İle Türkçe Arşivlerin Sayısallaştırılması, Yüksek Lisans Tezi, TOBB Ekonomi Ve Teknoloji Üniversitesi Fen Bilimler Enstitüsü, Haziran 2012.

Güneş İhsan, Çakır Ali Yavuz, Akınlar Cüneyt (2003). Tcp Performansının Veri Transferi Uygulamaları İçin Geliştirilmesi, Bilgisayar Mühendisliği Bölümü Mühendislik-Mimarlık Fakültesi,

Güngör Müberra (2014). Bilgi Toplumunda Enformasyon Asimetrisi Kavramı ve Düzenleyici Kurumların Rolü, Türkiye İncelemesi, http://www.btk.gov.tr/kutuphane_ve_veribankasi/raporlar/AB_Gelismeler_Bulteni/gelismeler_bulteni_ekim2014.pdf

Hanaylı, Mehmet Can (2014). Linux Tabanlı Ftp Sunucularda Veri Transferinde Algoritmalar Yardımıyla Güvenli Erişim Yönetimi Uygulaması, Yüksek Lisans Tezi, Matematik Anabilim Dalı, Fen Bilimleri Enstitüsü, Dumlupınar Üniversitesi, Mayıs, 2014.

Haverkort B. (1998). Performance Of Computer Communication System, A Model Based Approach, John Wiley & Sons, Ltd., 1998.

Henkoğlu, Türkay ve Uçak, Nazan Özenç (2012). Elektronik Bilgi Güvenliğinin Sağlanması ile İlgili Hukuki ve Etik Sorumluluklar, Bilgi Dünyası, 2012, 13 (2)377-396, http://www.bby.hacettepe.edu.tr/e-bulten/dosyalar/file/aralik2012/henkoglu_ucak.pdf, 24.12.14

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management‖, Information Security Technical Report, 13 : 247- 255, 2008

ISO/IEC 13335-1: 2004 (2004). Information Technology - Security Techniques - Management of Information and Communications Technology Security,ISO Copyright Office, Switzerland.

ISO/IEC 17799:2005 (2005). Information Technology - Code of Practice Security Management,ISO Copyright Office, Switzerland.

ISO/IEC 27000:2009 (2009). Information Technology - Security Techniques- Information Security Management Systems- Overview and Vocabulary,ISO Copyright Office, Switzerland.

Işık Yasemin, Kahvecioğlu Ayşe (2003). Veri İletim Yöntemleri Ve Optik Veri İletiminin Aviyonik Sistemlerdeki Kullanımı, Havacılık Ve Uzay Teknolojileri Dergisi, Temmuz 2003 Cilt 1 Sayı 2 (91-97).

ITU, (2005). International Telecommunication Union (ITU), 2005, "Telecommunication Indicators Handbook, Cenevre, İsvçre.

J.P. Holbrook, J.K. Reynolds (1991). The Site Security Handbook, RFC 1244, Jul-01- 1991, http://rfc.net/rfc1244.html, 23.12.14

Jin C., Wei D., Low H., Bunn J., Choe D., Doyle J., Buhrmaster G., Cottrell L., Paganini F., Newmann H., Feng W. (2005). "Fast TCP:From Theory To Experiments" , IEEE Network Journal ‚January- February 2005.

Kaptan Hakan, Çamurcu Yılmaz (2005). Bilgisayar Ağlarında Tıkanıklık Kontrol Algoritmaları için Java Tabanlı Simülatör Tasarımı, Marmara Üniversitesi, Teknik Eğitim Bölümü

Karaarslan Enis, (2003). Ağ Güvenlik Duvarı Çözümü Oluşturulurken Dikkat Edilmesi Gereken Hususlar, Akademik Bilişim 2003.

Karaarslan, Enis ve Abdullah Teke (2014). http://csirt.ulakbim.gov.tr/dokumanlar/BilgisayarAglarindaGuvenlikPolitikalarininUygulanmasi.pdf, 20.12.14

Karabacak, B. (2008). ISO/IEC 27001:2005 ve Bilgi Güvenliği Yönetişimi - Türkiye Analizi, TÜBİTAK-UEKAE, 2008 https://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/iso-iec-27001-2005-ve-bilgi-guvenligi-yonetisimi-turkiye-analizi.html.

Kasap Nihat, Sivrikaya Berna Tektaş (2010). Telekom Ağlarında Kademeli Fiyatlandırmayla Kapasite Kiralanması Ve İş Dağılımı, Sabancı

Üniversitesi, Yönetim Bilimleri Fakültesi, Tuzla, 34956, İstanbul, Türkiye, İstanbul Teknik Üniversitesi, İşletme Fakültesi, Maçka, 3436, İstanbul, Türkiye, İTÜ Dergisi/ Cilt:9, Sayı:5, 3-14, Ekim 2010

Khan J, Punnam P., Zaghal R. (2007). "Event Based Extensible İnteractive Transparent Networking:Performance Study With Fast TCP Principles", 21st International Conference On Advanced Networking And Applications ,2007

Kılıç, K. (2010). ISO 9001 Kalite Yönetim Sistemi Uygulamalarının Başarısında Kurum Kültürünün Rolü; Orman Genel Müdürlüğü Örneği, Doktora Tezi, T.C. Sakarya Üniversitesi, Sosyal Bililer Enstitüsü, Sakarya.

Kirov George (2005). "A Simulation Study Analysis Of The Tcp Control Algorithms", International Conference On Computer Systems And Technologies, Compsys Tech,2005.

Kleidermacher, D., ve Kleidermacher, M. (2012). Embedded Systems Security. Elsevier Inc.

Kula Ufuk, Torkul Orhan, Taşkın Harun (2006). Endüstri ve Sistem Mühendisliğine Giriş, Değişim Yayınları

Koç, F. (2008). BGYS - Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu, Ulusal Elektronik ve Kriptoloji Araştırma Merkezi, Ankara.

Laudon, K. Laudon ve L. Laudon (2003). Essentials of Management Infirmation Systems. 5th ed., Prentice Hall, New York, sf.460)

Loehr J., Siskoninetz W., Wiemeri j., Field S. (1998). "Optical Communication Systems for Avionics", IEEE Systems Magazine, 9-12, April 1998.

McDonald AB. (1999). A Mobility-Based Framework for Adaptive Dynamic Cluster-Based Hybrid Routing in wireless Ad Hoc Netwoks. Ph.D. Dissertion Proposal, Uni. Of Pittsburgh, 1999.

Megill, K.A., Schantz, H.F. (1999). Document Management: New Technologies fort he Information Services Manager, London: Bowker-Saur.

Newcomer E. (2002). Understanding Web Services: XML, WSDL, SOAP and UDDI, Addison Wesley Professional, USA, 2002.

OECD (2008). Enhancing Competition in Telecommunications: Protecting and Empowering Consumers, , 17-18 Haziran 2008.

Öğüt, Adem (2003). Bilgi Çağında Yönetim, Nobel Yayın Dağıtım, 2. Baskı, Ankara)

Özdemir, Cüneyt (2012). XML Web Servisleri ile Oracle ve SQL Server Veri Tabanları Arasında Veri Transferi, Siirt Meslek Yüksekokulu, Siirt Üniversitesi, Siirt, Türkiye, Geliş/Received: 02.11.2011; Kabul/Accepted: 23.01.2012)

Özveren, Mina ve Gürsu, Mehmet (2004). Organizasyonlarda Bilginin Yaratılması Süreci ve Bu süreçte Liderliğin Önemli, Ulusal Bilgi Ekonomi ve Yönetim Kongre Bildiriler Kitabı, Sayı 3, Osmangazi Üniversitesi, Eskişehir, sf 646)

Paçacı Erkan (2010). http://bilgeadamlar.blogspot.com.tr/2010/06/wan-teknolojisi-butunuyle-bir-bilgi-ag.html, 21.12.14

Peppers, Don ve Rogers, Martha (2013). Müşteri İlişkileri Yönetimi, Çeviren Pınar Şengözer, Optimist Yayınları, sf 147

Perkins C.E. and Bhagwat P. (1994). "Highly Dynamic Destination – Sequenced Distance - Vector Routing (DSDV) for Mobile Computers", Comp. Comm. Rev., 234-244 (1994).

Peterson, L. L. ve B. S. Davie (2007). Computer Networks: A Systems Approach. 4. Basım. S. 542. Morgan Kaufmann Publishers.

Rannenberg Kai, Royer Denis, Deuker Andre (2009). Future of Identify in The Information Society, Springer, Almanya.

Ragsdale, G.L., Lynch, G.P. ve Raschke, M.W. (Eylül 2000), The convergence of signaling system 7 and voice-over-IP, Proje Raporu (SwRI proje no. 10.03607), Southwest Research Institute.

Records Management Institute (2000), Understanding Electronic Records: The Basics, http://www.irmt.org/documents/educ_training/term%20modules/IRMT%20TERM%20Module%201.pdf, 23.12.14

Reichl, P., Hausheer, D. ve Stiller, B. (2003). The cumulus pricing model as an adaptive framework for feasible, efficient, and user-friendly tariffing of internet services, Computer Networks, 43, 3-4.

Rençberler Fatih, (2014). http://www.teknolojigundem.com/haber/veri-kaybinin-sirketlere-maliyeti-10-milyar-tl/644951, 17.12.14

Royer EM, Toh CK. (19990). A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks. IEEE Personal Communications, Apr. 1999;10:1–2. 151

Rygielski, C., Wang, J. ve Yen, D.C. (2002). Veri Mining Techniques for Customer Relationship Management, Technology in Society, Volume 24, Issue 4, 2002

Sitts, M.K.(Ed.) (2000), Handbook for Digital Projects: A Management Tool for Preservation and Access, Northeast: Northeast Document Conservation Center.

Stallings, W. (2000). " Veri and Computer Communications" Sixth Edition; Prentice Hall International, Inc; USA, (2000)

Stevens W. R. (1994). TCP/IP Illustrated, Volume 1: The Protocols, Reading, Massachusetts: Addison-Wesley, 1994.

Stevens W. R. (1997). TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms, RFC 2001, January 1997.

Şahin, Osman (2011). Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğin Korunması, Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri İletişim Kurumu (BTK), Haziran 2011, Ankara

Şeker, Şadi Evren (2013). İş Zekası ve Veri Madenciliği sf 22)

Tanenbaum A.S. (2003). "Computer Networks", Prentice Hall Publishing, Transport Layer, Third edition, 2003.

Tanenbaum, A.S. (1996). " Computer Networks" Third Edition; Prentice Hall International, Inc; USA(1996)

TBD (2009). Elektronik Belge Yönetimi, Ankara: TBD, (2009).

TechInside (2014). http://www.techinside.com/kritik-uygulama-hatasi-maliyetleri-nasil-etkiler/, 12.12.14

Thangarathinam T. (2006). Professional ASP.NET 2.0 XML, Wiley Publication, USA, 2006.

Toffler, Alvin ve Toffler Heidi (2006). Zenginlik Devrimi, Çev. Selim Yeniçeri, Koridor Yayıncılık, İstanbul, sf.134

TS EN ISO 9000 (2007). Kalite Yönetim Sistemleri – Temel Esaslar, Terimler ve Tarifler, Türk Standartları Enstitüsü, Ankara.

TS ISO/IEC 27001 (2006). Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler, Türk Standartları Enstitüsü, Ankara.

TS ISO/IEC 27001:2006 (2006). Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler, 2006.

Tutkun, H. K. (2012). Network Sistemleri Sistem Yöneticisinin El Kitabı, Ankara, Seçkin Yayıncılık

Türkiye İstatistik Kurumu (TÜİK), (2010). Hanehalkı Bilişim Teknolojileri Kullanım Anketi (2010), http://www.tuik.gov.tr/PreTablo.do?tb_id=60&ust_id=2

Ulutürk, A. (2010). Gelişmiş Şifreleme Standardı. Ankara:Gazi Üniversitesi Fen Bilimleri Enstitüsü, 2010.

United Nations Archives and Records Management Section (2006), Guideline on records digitisation.http://archives.un.org/unarms/en/unrecordsmgmt/unrecordsresources/guideline%20on%20records%20digitisation.htm,23.12.14

Üçgün Hakan, Danacı Mustafa (2005). Ad Hoc Ağları İçin Kuyruk Ağ Analizi Ve Yapay Arı Kolonisi Algoritmalarının Birleştirilerek Routing Probleminin Simülasyonu, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bilecik Şeyh Edebali Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Erciyes Üniversitesi, Türkiye.

Williams P. A. (2008). In a _trusting' environment, everyone is responsible for information security, Information Security Technical Report, 13 : 207-215, 2008.

Yelkenci, Lütfi (2002). Güvenlik Politikasız Güvenlik Nereye Kadar? , 2002, http://www.guvenlikhaber.com/koseyazisi.asp?ID=8

Yıldırım, Burç, Dayıoğlu, Burak (2010). Kurumsal Güvenlik, http://www.yalova.edu.tr/Files/Import/ucgen3/userfiles/file/crea-world(1).pdf

Yıldız, B. (2007) ―Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması, Gebze Yüksek Teknoloji Enstitüsü - Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi.

Yıldız, Çiğdem (2009). Telekomünikasyon Sektöründe Firma İçendeki Bilgi Güvenliğini Etkileyen Faktörler Ve Bu Faktörlerin Çalışanlar Üzerine Etkileri, Yüksek Lisans Tezi, Strateji Bilimi Anabilim Dalı, Sosyal Bilimler Enstitüsü, Gebze İleri teknoloji Enstitüsü, Gebze 2009.

Yönetmelikler, (2012). http://tk.gov.tr/mevzuat/yonetmelikler/dosyalar/EHSKVIGKHak_Yon_Konsolide_Metin_2013.pdf, 17.12.14

Zobi, A., (2008). TS ISO /IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi ve KOSGEB'de Uygulaması, KOSGEB Uzmanlık Tezi, Ankara.