Sekme 1

KEREM ENGÜR

WEB TEMELLERİ

İÇİNDEKİLER

WEB NEDİR

Türkçe karşılığı örümcek ağı anlamına gelmektedir.Internet ağının karmaşık yapısından dolayı web ismi verilmiştir. Web teknolojisi internetin bir alt kümesidir. İnternet ile web birbirine çok karıştırılmaktadır fakat ikisi birbirinden farklı terimlerdir. İnternet dünya üzerinde bulunan cihazların birbirlerine bağlanması sonucu oluşan çok büyük bir ağıdır. Fakat web internetin üzerine kurulmuş bir teknoloji anlamına gelmektedir. Teknolojisi sayesinde internet üzerinden ses video dosya aktarımı gibi işlemler yapılabilmektedir.

İnternet üzerinde yayınlanan birbirleriyle hipermetin dökümanlarından oluşan bilgi sistemine web ismi verilmiştir. Bu dökümanlara web sayfası adı verilmektedir ve web sayfaların birleşmesiyle web sitesi oluşmaktadır. Web sayfalarını veya web sitelerine erişim sağlayabilmek için web tarayıcıları adı verilen bilgisayar programları bulunmaktadır. Web sayfaları başka web sayfalarıyla bağlantı kurulabilmektedir.Web sayesinde internetin sunduğu mekanizmalar kullanılabilmektedir. www yani world wide web sayesinde internet üzerinde bulunan web'ler tek bir ağa toplanmaktadır. Web tarayıcıları bir web sitesi açıldığı zaman web sunucusuna istemci sunucu modeli ile iletişim kurmasına olanak sağlar.Web sunucuları içlerinde hipermetin dokümanlarının bulunduğu sunuculardır. Bu iletişimi belli başlı protokoller çerçevesinde gerçekleştirmektedir.

Özetlemek gerekirse web internet üzerine kurulmuş bir teknolojidir ve internetin sağladığı mekanizmaların kullanılmasına olanak sağlamaktadır. İnsanların bilgi paylaşımı dosya transferi gibi işlemleri yapmasını sağlayan web siteleri web teknolojisi sayesinde yapılmaktadır. Web teknolojisinin altında belli başlı ana başlıklar bulunmaktadır bunlar sırasıyla aşağıda verilmiştir.

Web sayfası

Web sayfaları web tarayıcısı kullanılarak görüntülenen dökümanlardır. Web sayfaların kendine ait etiketleme dili bulunmaktadır. Genel olarak web sayfaları hiper bağlantıların bulunduğu hiper metinlerden oluşmaktadır fakat farklı teknolojiler ile web sayfaları kurulabilmektedir. Örnek vermek gerekirse geçmişte bulunan flash eski web sayfalarını örnek verilebilir. Web sayfaları bir ağ üzerinden web sunucuları tarafından yayınlanmaktadır. Web sayfaları ve sunucuları üzerinde tutulmaktadır. Web sayfaları üzerinde ses dosya gibi dökümantasyonlar bulunmaktadır. İki tür web sayfası bulunmaktadır. Bunlar sırasıyla statik sayfalar ve dinamik sayfalar olarak ayrılmaktadır.

Statik web sayfası

Bu tür web sayfaları sadece bilgilendirme amaçlı kullanılmaktadır ve kullanıcı etkileşimine açık değildir. Örnek web sayfaları olarak insanların çevrimiçi kartvizitlerini yazması gibi web sayfaları örnek verilebilmektedir.

Dinamik web sayfası

Dinamik web sayfaları kullanıcıların web sayfası ile etkileşime geçebildiği sayfalardır. Dinamik web sayfaları kullanıcı tarafından talep eden verileri almaktadır ve veri tabanı işlemektedir.

Web sayfaların kurulması asıl amacı insanlarla iletişim kurabilmektir. Web sayfaları kurarak zamanlar ve paradan tasarruf sağlanmaktadır. Aynı zamanda tüm insanlar tarafından eleştirebilir olduğundan bir ürünün pazarlanması gibi alanlarında fayda sağlamaktadır.

Web sitesi

Web siteleri bir dizi web sayfasından oluşan web kavramıdır. Web sayfaları ile web siteleri birbirine karıştırılmamalıdır ikisi arasındaki en büyük fark web sayfaları tek bir şey ifade ederken web siteleri birden fazla sayfanın birleşiminden oluşmaktadır. Web sitelerine web tarayıcıları sayesinde erişilebilmektedir.

Web sitelerinin tarayıcı üzerinde görünebilmesini sağlayan alan adı (domain) bulunmaktadır. Her web sitesi bir web sunucusuna bağlıdır web sunucuları üzerine web sitelerinin verileri tutulmaktadır. Web siteleri içinde web sayfalarının birbirlerine bağlanmasını sağlayan bağlantılar bulunmaktadır. Web sitelerinin tarayıcıda arama yapıldıktan sonra üst sıralarda çıkması arama motoru optimizasyonu sayesinde gerçekleşmektedir. Birden fazla web sitesi türü bulunmaktadır. Kişisel web siteleri bloklar portföyler veya bireysel ilgi alanları için oluşturulmuş web siteleridir. Kurumsal web siteleri devlet kurumları gibi kurumların oluşturduğu web siteleridir. Bunlar haricinde e-ticaret siteleri, haber siteleri ve eğitim siteleri de bulunmaktadır.

Web tarayıcısı

Web tarayıcıları www internet sunucuları ağına girmeye yarayan yazılımlara verilen genel addır. İlk web tarayıcıları 1990 yılında Tim Berners Lee tarafından icat edilmiştir. Web tarayıcıları ve internet zaman içinde birlikte düşünülen iki kavram haline gelmiştir.

Web tarayıcıları hem bilgisayarda hemde mobil cihazlarda kullanılmaktadır, internet sitelerine girmeyi sağlayan bir yazılım programıdır.

Web tarayıcılarının bazı özellikleri bulunmaktadır

Adres çubuğu: Ziyaret edilmek istenilen Web sitesinin adresinin girildiği arama kısmıdır.

Açılış sayfası: Tarayıcı açıldığında ilk görünen sayfa bu sayfadır kullanıcının ilgilerine göre bazı siteler önerilmektedir.

Yer imleri: Sık ziyaret edilen siteleri kaydetmek için kullanılır. Bu sayede bu sitelere daha rahat ulaşılabilir.

Tarayıcı geçmişi: Kullanıcının tarayıcıda önceden aradığı web sitelerini kaydetmek için kullanılmaktadır.

Gizli sekme: Gizli sekme ile yapılan aramalar tarayıcı geçmişine kaydedilmemektedir.

Eklentiler uzantılar: Web tarayıcısına ekstradan özellik kazandırmak için kullanılan ufak yazılım programlarıdır.

Temalar: Tarayıcının görünümünü değiştirmek için kullanılmaktadır.

Her web tarayıcısı temel anlamda aynı işlevi görmekte olsa bile aralarında bazı noktalarda farklılıklar bulunmaktadır. Bazı web tarayıcıları işletim sistemleri ile uyumlu olmayabilir. Tarayıcılar arasında yazılımsal farklılıklar da bulunabilmektedir.

Web sunucusu

Web sunucuları protokoller dahilinde web sitelerinden gelen talepleri kabul eden bir bilgisayar yazılımı ve altyapı donanımını ifade etmektedir. Web sunucularının temel amaçları web sitelerinin içeriklerini ve diğer kaynakları sunmaktır. Web sunucusundan gönderilen bir kaynak var olan bir dosya olabileceği gibi aynı zamanda o an oluşturulabilmektedir. Sunucu içerisinde halihazırda duran veri statik veri olarak adlandırılırken program sayesinde anlık olarak üretilen veri dinamik veri olarak adlandırılmaktadır. Statik içerikler tekrarlanan istekler için daha hızlı dönüt sağlamak tayken dinamik içerikler tekrarlayan isteklerde daha yavaş çalışmaktadır. Dinamik veri aynı zamanda daha geniş bir alanda bilgi sunabilmektedir.

Özetlemek gerekirse web sunucuları web siteleri üzerinden gelen verilere dönüt sağlamaktadır.

Web kavramını özetlemek gerekirse internet üzerine kurulmuş bir teknolojidir. Web teknolojisi sayesinde insanlar birbirleriyle iletişim kurabilmekte, devlet kurumları duyurular gibi işlemler yapabilmekte, insanlar internet üzerinden alışveriş yapabilmekte, ve benzeri işlemleri gerçekleştirebilmektedirler.

WEB TARİHÇESİ

WEB 1.0

WEB 1.0, basit statik web sayfalarının oluşturulduğu ilk dönemi ifade eder. WWW'deki gelişimin ilk aşamasını anlatan bir terimdir. WEB 1.0 terimi, 1999'da Darci DiNucci tarafından ortaya atılmıştır. O dönemde internet, büyük bir dönüşüm geçirmekteydi. 1990'ların başlarında çoğu web sitesi, başlangıçta statik sayfalar ve birkaç basit dil kullanılarak oluşturulmuştu. WEB 1.0'dan sonra gelen web teknolojisi, web sitelerinin neler başarabileceğini göstermektedir.

WEB 1.0'ın öne çıkan bazı temel özellikleri aşağıda sırasıyla verilmiştir:

1. **Statik Sayfalar**
   Statik sayfalar, web sitesini ziyaretçilerin etkileşime giremediği sayfalardır. O dönemlerde ve genel anlamda, bilgilendirici içeriklerin bulunduğu bir sanal ansiklopediyi andıran bir yapıdaydı.

2. **Dosyalarda Saklanan Web Sitesi İçeriği**
   Günümüzde çoğu web sitesi, içeriklerini veri tabanlarında saklarken, WEB 1.0 döneminde bu içerik doğrudan web sitesinin içeriğinde bulunan dosyalarda saklanıyordu.

3. **İçerik ve Düzenin Birleşimi**
   Günümüzde iyi bir web tasarım uygulaması, web sayfası işaretlemeleri ve stilin ayarlanmasını gerektirir. Hemen hemen tüm modern web siteleri, sayfa görünümünü düzenlemek için harici stil şablonlarından yararlanır. Ancak, WEB 1.0 teknolojisinde, içerik ve düzen, tablolar gibi unsurlarla birleştirilir ve bu, günümüzdeki web sitelerinden çok daha farklıydı.

4. **Tescilli HTML Etiketleri**
   WEB 1.0 teknolojisinde tarayıcılar, tescilli etiketleri destekleyerek ortaya çıkmıştır. Bu durum, etiketleri kullanan web siteleri ile desteklemeyen tarayıcıları kullanan ziyaretçiler arasında uyumsuzluk sorunlarına yol açmıştır.

5. **Ziyaretçi Defterleri**
   WEB 1.0 teknolojisinde yorumlar, genellikle web sitesinin içeriğine değil, "ziyaretçi defteri" adı verilen bir sayfaya eklenirdi.

6. **Formların E-posta ile Gönderilmesi**
   Ziyaretçilerin formları genellikle e-posta yoluyla gönderirdi. Genellikle, forma "gönder" tuşuna basıldığında web sitesi, bilgisayarın e-posta istemcisini çalıştırır ve kullanıcılar, form verilerini e-posta olarak web sitesine gönderirdi.

WEB 1.0 Teknolojisinden WEB 2.0’a Geçiş

Web 1.0'dan WEB 2.0'a geçiş, sunucuların yükselmesi, ortalama bağlantı hızlarının artması ve geliştiricilerin yeni beceriler ve teknikler öğrenmesiyle zamanla gerçekleşmiştir. Bu yeni teknolojiye geçiş, 1990'ların sonlarında başlamış ve WEB 2.0 özellikleri 2006'ya kadar güçlü bir şekilde gelişmiştir. Günümüzde hala bazı web siteleri, WEB 1.0 teknolojisinde kalmıştır.

WEB 1.0 SIFIR KISITLAMALARI

Web siteleri ile etkileşime geçilememektedir. Yorum yapma, kullanıcı geri bildirimi alma gibi işlemler yapılamamaktadır.

İçerik güncellemeleri manuel olarak yapılmaktadır; bu işlem zaman alıcı ve zahmetlidir. Her kullanıcı için aynı web siteleri bulunmaktadır. Kişiselleştirilmiş ve özelleştirilmiş özellikler bulunmamaktadır.

WEB 2.0

Son kullanıcılar için, kullanıcı tarafından oluşturulan içerikten yararlanan web sitelerinin sahip olduğu teknolojidir. WEB 2.0 teknolojisi, daha fazla kullanıcı etkileşimi ve işbirliği, daha yaygın ağ bağlantısı ve gelişmiş iletişim kanalları ile karakterize edilmektedir.
İlk olarak, WEB 2.0 terimi 1999 yılında Darcy DiNucci tarafından ortaya atılmıştır. Popülerleşmesi ise 2004 yılında WEB 2.0 konferansında O'Reilly Media tarafından gerçekleştirilmiştir.
Bu internet çağı, bulut bilişim, daha yüksek yatırım seviyeleri ve internet kontrolü arasında bilgi paylaşımını daha fazla vurgulamaktadır. Genel anlamda teknik bir yükselme anlamına gelse de, bu teknoloji internetin tüketilme biçiminde bir değişim yansıtmaktadır. Sosyal medya ve uygulamalar, Facebook gibi kendi kendine yayılan platformlar, bu değişim sırasında popülerlik kazanmıştır.

WEB 1.0 ile WEB 2.0 Arasındaki Farklar

WEB 1.0 ile karşılaştırıldığında, WEB 2.0 yeni internet kullanıcılarına daha fazla işbirliği imkânı sunmaktadır. WEB 2.0, asıl amacın son kullanıcının ön planda olduğu bir sistemdir. WEB 1.0 başlangıçta veriler web sitesine gönderilmekteydi ve kullanıcılar yalnızca içerikleri görüntüleyebiliyordu. Bu açıdan bakıldığında, aslında bu teknoloji çok sabit bir teknolojidir. Ancak WEB 2.0, bilgileri erişmenin dışında bu bilgilerle etkileşime girmenin de mümkün olduğunu göstermektedir.
WEB 2.0, topluluk tabanlı bir yapı sunarak etkileşim, içerik paylaşımı ve işbirliğini mümkün kılmaktadır. Kullanıcılar, birbirleriyle paylaşımlar yapabilmektedir.
WEB 2.0, bilgileri doğrusal olmayan bir formatta sunmaktadır.
WEB 1.0, statik sayfalardan oluşurken, WEB 2.0 daha çok kullanıcılar tarafından üretilen dinamik sayfalardan oluşmaktadır.
WEB 2.0 teknolojisi, hipermetin aktarım protokolü (HTTP) tabanlı programlama arayüzüne sahip olup, işlevselliği ve kullanılabilirliği arttırmıştır.
WEB 2.0 teknolojisinde istemci sonucu modeli kullanılmaktadır. Bu sayede çevrimiçi belgeler, reklamlar ve benzeri uygulamalar sunulabilmektedir.
Bloglar, video barındırma siteleri, birleşik iletişim, kullanıcı tarafına ulaşan içerikler ve mobil bilişim gibi web siteleri, WEB 2.0 örneklerindendir.

WEB 2.0 Avantajları ve Dezavantajları

Avantajlar

- **Dinamik İçerik**
  WEB 2.0, WEB 1.0'ın kısıtlı salt okunur formatına kıyasla dinamik web sayfaları sunmaktadır.
- **Artan Sosyal Ağlar**
  WEB 2.0 teknolojisi, insanların tartışmalara katılmalarını, arkadaşlarıyla ve aileleriyle

bilgi paylaşmalarını, konum fark etmeksizin insanlarla iletişim kurmalarını sağlamaktadır. Sosyal ağlar olarak adlandırılabilir.

- **Kullanım Kolaylığı ve Bilgi Paylaşımı**
  WEB 2.0 teknolojisinde kullanıcılar, birkaç tıklama ile istedikleri bilgiye erişebilmektedirler. Aynı zamanda kullanıcılar, basit işlemlerle güncelleme, paylaşım yapma ve düzenlemeleri izleyebilme imkânına sahiptirler.
- **Geliştirilmiş Pazarlanabilirlik**
  WEB 2.0 teknolojisi ile duyarlı web siteleri oluşturularak kullanıcı deneyimi iyileştirilmektedir. Ayrıca ürünler çevrimiçi olarak tanıtılabilir ve etkileşimli reklam kampanyaları aracılığıyla pazarlanabilir.
- **Eğitim Kalitesinin Artması**
  Bu teknoloji, etkileşimi öğrenme ve sınavlara katılma imkânı sunmaktadır.

Dezavantajlar

- **Siber Güvenlik Riskleri**
  Yeni teknoloji ile gelen artan çevrimiçi işbirliği, kullanıcıların kötü amaçlı yazılımların ve virüslerin indirilmesi gibi siber saldırılara maruz kalma riskini artırmaktadır.
- **Bilgi Aşırı Yükü**
  WEB 2.0, bilgi kirliliğine sebep olabilmektedir. Sürekli gelişen bu teknolojide insanlar sürekli bilgi paylaşımı yapmaktadır. Bu paylaşımların doğruluğu, büyüme oranından dolayı kontrol altında tutulamayabilmektedir.
- **Etik ve Güvenilirlik**
  Kullanıcıların web sitelerinin içerikleri ile etkileşime girebilmesinden ve içeriklerin değiştirilebilmesinden dolayı, bazı kesimler web sitesinin güvenilirliğini ve hatta yasalığını etkileyebileceğini savunmaktadır.

WEB 3.0

Web 3.0 terimi ilk olarak 2006'da Zeldman'ın Web 2.0'u eleştiren makalesinde görülmüştür. Bu web türü 2010'dan beri çalışmaktadır. Bu teknoloji, ağ kullanıcıları için önemli sonuçları olan teknolojik bir ileri atılımdır.

Web 3.0, birbirlerine ağlarla bağlı olan kullanıcıların ağ deneyimini zenginleştirmek ve bunun için konuma özgü bilgi sağlayan tarayıcının görece özerk olduğu ve semantik web'in inşa edildiği bir teknolojidir.

İnterneti veri sahipliği ve kontrolü merkezi olmaktan çıkaran blok zinciri gibi teknolojilerin kullanıldığı görülmektedir. Çoğu internet sitesi ve uygulaması, son kullanıcının verilerinin nasıl kaydedileceğini ve kullanılacağını belirleyen merkezler tarafından kontrol edilmektedir. Fakat Web 3.0 teknolojileri, merkezi yapıların yerine topluluk odaklı projelere olanak tanımaktadır. Kullanıcılar verilerinin merkezi merkezler tarafından değil, kullanıcılar tarafından yönetilmesini sağlar. Bu teknoloji, kullanıcıların birbirleriyle nasıl etkileşimde bulunduğunu otomatik olarak düzenleyen mekanizmalar içermektedir. Bu sayede merkezi etkileşimlerin kullanıcıları yönetmesine gerek kalmamaktadır.

Web 3.0 Temel Fikirler

Web 3.0 teknolojisinin dört ana temel fikri bulunmaktadır:

1. **Merkeziyetsizlik**
   Merkezî olmayan web uygulamaları, bu teknolojinin önemli bir özelliği olarak nitelendirilmektedir. Bu özelliğin amacı, verilerin merkezi olmayan ağlarda dağıtımı ve depolanmasını sağlamaktır. Bu ağlarda farklı kuruluşlar temel altyapıya sahiptir ve kullanıcılar bu alana erişebilmek için doğrudan depolama sağlayıcılarına ödeme yapmaktadır.
   Aynı zamanda bu özellik, bilgi kopyalarının birden fazla yer tarafından depolanmasını ve veri tutarlılığının sağlanmasını olanak tanımaktadır. Kullanıcılar verilerinin merkezi bir yapıda değil, nerede bulunduğunu kontrol edebilmektedir. Merkezi olmayan internet, kullanıcıların isterlerse kendi verilerini satabilmesine olanak tanır.

2. **Güven Gerekliliğinin Olmaması**
   Merkezi olan web teknolojilerinde, uygulamalar hizmetlerinde kullanıcıların verilerine işlemlerini ve etkileşimlerini yönetmek gibi bazı işlemler için genellikle merkezi bir otoriteye güvenmek zorundadır. Bu otoriteler, kullanıcıya verileri üzerinde kontrole sahiptir ve sistemin kurallarını manipüle edebilmektedir. Bu durum, kullanıcıların güvenlik riskine veya kötü yönetime tabi olmasına, dolayısıyla potansiyel olarak kullanıcı bilgilerinin kaybolmasına, kötüye kullanılmasına gibi durumlara neden olabilmektedir.

3. **Semantik Web**
   Bu teknoloji, Web 3.0'ın en önemli teknolojilerinden biridir. Semantik web, siteler ve uygulamalarının bağlamını anlayarak karmaşık görevleri gerçekleştirmeye olanak sağlar. Kullanıcılar tarafından oluşturulan verilere anlam kazandırmak için yapay zeka teknolojileri kullanılmaktadır.

   Semantik, içeriğe bir müşterinin ihtiyacına uygun en yararlı biçimlerde kendini anlama ve sunma yeteneği vererek daha akıllı ve daha zahmetsiz müşteri deneyimlerine yol açmaktadır. Bu teknoloji, çevrimiçi olarak yayınlanmış içeriğin makineler tarafından anlaşılması, bağlanabilmesi ve yeniden karşılaştırma yapabilmesi ardından sunum işlemini gerçekleştirmesi gibi özellikleri barındırmaktadır.

   Bu teknoloji, web sitelerinin kişiye özel bir hale gelmesini sağlar. Örnekle açıklamak gerekirse, iki farklı kullanıcı internet üzerinden aynı şeyi arasalar bile geçmişte yaptıkları aramalar doğrultusunda, ziyaret ettikleri web sitelerinin içeriği doğrultusunda karşılarına farklı sonuçlar çıkabilmektedir. Geçmişte ziyaret edilen web siteleri, yapay zeka ile anlamlandırılır ve kullanıcının nelere ilgi duyduğu gibi bilgiler çıkarılmaktadır.

4. **Birlikte Çalışabilirlik**
   Web 3.0, farklı teknolojiler arasında daha fazla ara bağlantı oluşturmayı amaçlamaktadır. Bu sayede, veriler farklı platformlar arasında aracılar olmadan aktarılabilmektedir. Birlikte çalışabilirlik, verilerin taşınabilir hale gelmesi anlamına gelmektedir. Bu sayede, kullanıcılar tercihlerini, profillerini ve ayarlarını korumanın yanında, hizmetler arasında sorunsuz bir şekilde geçiş yapabilmektedir.
   Aynı zamanda, nesnelerin interneti bağlamında kullanılan cihazları birbirine entegre eden protokoller, webin erişimine geleneksel sınırların ötesine genişletmektedir.

Web 3.0 Neden Önemlidir

Web ilk zamanlarında sadece salt okunur deneyimlerden oluşmaktaydı. Son kullanıcılar, sadece statik web sayfalarını barındıran altyapıyı satın alan ve sürdüren şirketler tarafından yayınlanan içerikleri okuyabilmekteydi.

Gelişen web teknolojileri sonrası, blog sayfaları, sosyal medya platformları gibi teknolojilerin ortaya çıkması sonucu uygulamalar daha etkileşimli hale gelmiştir. Kullanıcılar içerik oluşturup yayınlayabilmekte veya başkalarıyla hizmet alışverişinde bulunabilmektedir. Fakat tüm etkileşimler, hizmet alışverişinden ticari fayda sağlayan merkezi otoriteler tarafından

yönetilmektedir. Aynı zamanda, son kullanıcıların oluşturduğu dijital varlıklara sahiptirler ve bunları kontrol edebilmektedirler.

Web 3.0 teknolojisi ise, merkezi otoritelerin yerine her verinin her bilgisayarda tutulduğu blok zinciri teknolojisini kullanmaktadır. Bu sayede veriler, merkezi otoriteler tarafından manipüle edilemez veya kullanılamaz hale gelir. Kullanıcı, verilerinin nerede tutulmasını istiyorsa orada tutulmasını sağlayabilmektedir. Verilerini paylaşmak istemiyorsa, paylaşmaz. Bu sayede, kullanıcıların güvenliği sağlanmış olur.

Web 3.0'ın Bazı Avantajları

Web 3.0 teknolojisi, son kullanıcılarının kendi verilerine sahip olduğu ve kontrol ettiği, aynı zamanda nasıl kullanıldığı ve yönetildiği konusunda önceki teknolojilere nazaran daha fazla söz sahibi olduğu bir web teknolojisidir. Bu teknoloji, çeşitli mekanizmalar sağlayarak son kullanıcıların müşteri olarak değil de hissedar veya katılımcı olmalarını sağlamaktadır. Aşağıda bazı avantajlar yer almaktadır:

- **Geliştirilmiş Etkileşim**
  Kullanıcılar kendi aralarında çözüm sağlayıcı ile daha anlamlı bir şekilde etkileşime girebilmektedir. Veri değişim talepleri yerine çevrimiçi topluluklara aktif katılım için teşvik almaktadırlar.

- **Geliştirilmiş Gizlilik**
  Kullanıcı verilerinin kimler tarafından erişilebileceğini belirlemektedir. Bu verilere, verileri elinde bulunduran altyapı sahibi tarafından erişilememektedir. Çevrimiçi etkileşimler herkese açık olsa bile kimlik gizli tutulmaktadır.

- **Herkesin Katılımına Açık İletişim**
  Bu teknoloji, iletişimin önündeki coğrafi, politik veya kurumsal engelleri kaldırmayı amaçlamaktadır. Büyük teknoloji şirketlerinin sansürlerini kaldırmayı hedeflemektedir.

Web 3.0 Ana Teknolojileri

- **Blok Zinciri Teknolojisi**
  Bu web teknolojisinde, düğümler veri kayıtlarını depolamak için kullanılmaktadır. Bu sayede merkezi olmayan, dağıtılmış bir biçimde veriler tutulmaktadır. Blok zinciri teknolojisi, belirteçlerle ayırma yoluyla genişletilebilmektedir. Her belirteç, blok zinciri içinde farklı fiziksel ve dijital varlıkları temsil edebilmektedir. Sanal dünyada birden fazla belirteç türü bulunmaktadır.

- **WebAssembly**
  Merkezi olmayan uygulamaların farklı platformlarda verimli bir şekilde çalışması için kullanılmaktadır. Yayın tabanlı bir sanal makine için ikili komut biçimidir. Tarayıcı içinde korumalı bir alanda çalışmaktadır. Geliştiriciler, kodu yerel hızlarda çalıştırabilmektedir. JavaScript gibi geleneksel teknolojilere kıyasla performansta önemli bir artış sağlamaktadır.

- **Semantik Web Teknolojileri**
  Bu teknoloji, web sitelerinde ve uygulamalarda müşterilerin verilerini daha iyi anlamasına ve yorumlamasına olanak sağlar. Birden fazla veri kümesini birbirine bağlamak ve yapılandırılmış verileri yayınlamak için bağlantılı ilkeler kullanmaktadırlar. Bu ilkelerden bazıları aşağıda yer almaktadır:

    - **Resource Description Framework (RDF)**
      RDF, özne yüklem nesne biçiminde üçlü olarak ifade edilebilmektedir. Bu üçlü ifade, farklı varlıkların ilişkilerini temsil etmek için grafik tabanlı bir veri yapısı oluşturmaktadır.

    - **Web Ontoloji Dili (OWL)**
      Bilginin ve kavramlar arasındaki ilişkilerin resmi temsillerini tanımlamak için kullanılan bir dildir. Sınıf ve özellikler gibi işlemleri belirlemenin yanı sıra, aynı zamanda akıl yürütme ve çıkarım yapmayı kolaylaştırma gibi işlemler için de kullanılabilmektedir.

Bazı Web 3.0 Zorlukları

Her teknolojide olduğu gibi, bu teknolojide de uygulama aşamasında bazı zorluklar yer almaktadır.

- **Teknik Zorluklar**
  Varlık büyüklükleri arttıkça, blok zinciri ağları çok pahalı ve hesaplama açısından zorlu hale gelmektedir. Bu durumdan dolayı sürdürülebilir ve çevre dostu teknolojiler yaratma çabaları hala devam etmektedir. Aynı zamanda, blok zinciri ağları ve protokolleri arasında birlikte çalışılabilirlik de farklı bir zorluktur.

- **Kullanıcı Deneyimi ve Benimseme**
  Karmaşık arayüzler ve benzeri durumlar, genel benimsemeyi sınırlamaktadır. Blok zinciri teknolojisinin karmaşıklıklarını soyutlamak için sezgisel arayüzler tasarlamak, kullanıcı deneyimlerini iyileştirmektedir. Aynı zamanda bu teknoloji, finans ve benzeri konularda takip etmesi gereken mevzuata uygunluk konusunda da zorluk teşkil etmektedir

WEB DE KULLANILAN PROTOKOLLER VE DETAYLI AÇIKLAMALARI

HTTP

HTTP, bir kaynaktan dağıtılan ve ortak kullanıma açık olan hiper ortam bilgi sistemleri için kullanılan bir iletişim protokolüdür. HTTP, WWW (Dünya Çapında Ağ) için veri iletiminin temelini oluşturur.

HTTP, istemci-sunucu bilgi işlem modelinde bir istek-yanıt protokolü olarak işlev görmektedir. İstemci, sunucuya bir istek mesajı gönderir, hipermetin dosyaları ve diğer içerikler gibi kaynakları sağlayan veya istemciye çeviri gerçekleştirilen bir yanıt mesajı döner. Temel mantıkta, bu sistem istemci ve sunucu arasında çalışmaktadır. Dönen yanıt, isteğe göre değişiklik gösterebilir. Aynı zamanda HTTP, istemciler ile sunucular arasındaki iletişimi iyileştirme görevini de üstlenir. Yüksek trafikli web sitelerinde, bu akışı hızlandırmak için web önbellek sunucularından yararlanılmaktadır. Web tarayıcıları, önceden edinilmiş sitelere ait verileri ön belleğe alır. Bu sayede, tekrar erişilmek istenilen bir site daha hızlı açılır.

HTTP, genel olarak TCP ile çalışmaktadır; ancak başka protokollerle de kullanılabilir.

Birden fazla HTTP versiyonu bulunmaktadır. Bu versiyonların özellikleri ve isimleri aşağıda sırasıyla verilmiştir:

- **HTTP/1.0:** Her istek için sunucuyla yeniden bağlantı kurulması gerekmektedir. Bu sebeple, daha yavaş çalışır.
- **HTTP/1.1:** Temel olarak bir önceki versiyondan türetilmiştir, ancak bu versiyonda her iletişim için sunucuya yeniden bağlantı kurulmasına gerek yoktur. Bu nedenle daha hızlı çalışır.
- **HTTP/2.0:** Protokolün performansını iyileştirmek amacıyla geliştirilmiştir. Önceki versiyonda istekler sırasıyla gönderilmektedir; ancak bu versiyonda, istekler zaman uyumsuz bir şekilde gönderilebilir. Bu sayede aynı anda farklı istekler gönderilebilir.
- **HTTP/3.0:** Bu versiyon, bir önceki versiyonundan farklı olarak farklı taşıma katmanı protokolleri kullanır. Önceki versiyonda TLS kullanılırken, bu versiyonda QUIC kullanılmaktadır. Bu, daha iyi iletim hızı, daha kısa yükleme süreleri ve daha kararlı bağlantılar sağlar.

Özetlemek gerekirse, HTTP protokolü, web sitelerinin web sunucularıyla iletişim kurmalarına olanak tanıyan bir protokoldür. Bu iletişim, istekler ve yanıtlar üzerinden gerçekleşir. Web sitesine yapılan bir işlem, istek olarak sunucuya iletilir ve sunucu, bu isteğe karşılık bir yanıt döner. Böylece iletişim sağlanır.

HTTP NİN KISA TARİHİ

Hipermetin terimi, ilk kez Ted Nelson tarafından 1975'te bir projesinde ortaya atılmıştır. Tim Berners-Lee ve CERN ekibi, orijinal HTTP'yi ve HTML'i, bir web sunucusu ve metin tabanlı bir web tarayıcısı için ilgili teknolojiyi icat etmekle tanınmaktadır. Ayrıca Berners-Lee, WWW (Dünya Çapında Ağ) projesinin de mucididir. HTTP protokolünün ilk sürümünde, bir sunucudan bir sayfaya talep göndermek için "GET" adında bir istek bulunmaktadır.

HTTP'nin ilk sürümü 1991'de V 0.9 olarak yayınlanmıştır. Dave Raggett, 1995 yılında HTTP çalışma grubunu yönetmiş ve protokolü daha da geliştirmiştir. Resmi olarak HTTP V1.0, 1996 yılında tanıtılmıştır. HTTP çalışma grubu, yeni standartlar dahilinde HTTP V1.1'i 1996 yılının başlarında yapmış ve bu protokol büyük tarayıcılar tarafından hızlıca benimsenmiştir. 1997 yılının Ocak ayında ise resmi olarak yayınlanmıştır. Bundan sonra gelen versiyon, Haziran 1999'da yayınlanmıştır.

HTTP çalışma grubu, son versiyonu geçersiz kılan ve 6 bölümden oluşan bir spesifikasyon yayımlamıştır. Bundan sonra gelen versiyonlar, ileri zamanlarda geliştirilerek yayınlanmıştır.

HTTP BAĞLANTILARININ GELİŞİMİ

HTTP/0.9 ve 1.0'da, bağlantı kurulup istek-yanıt durumu gerçekleştikten sonra bağlantı kanalı otomatik olarak kapatılmaktadır. Fakat bundan sonra gelen versiyonlarda, bir bağlantının birden fazla istek göndermesini sağlamak mümkün olmuştur. Bu sayede protokol daha hızlı çalışmaktadır. Temel mantıkta, tek bağlantı üzerinden birden fazla istek yapılması, TCP'nin üçlü el sıkışma süreci sayesinde gerçekleşmektedir. Bir bağlantı kurulduktan ve istek gönderildikten sonra, istemci ile sunucu arasında bir el sıkışma işlemi gerçekleştirilir. Bundan sonra gönderilecek isteklerde el sıkışma ihtiyacı olmadığından, bağlantı üzerinden birden fazla istek gönderilebilmektedir. Aynı zamanda, yeni protokolde (yani 1.1 versiyonunda) bant genişliği optimizasyonu da yapılmıştır. HTTP 1.1 versiyonunda, istekler sırayla gerçekleşmektedir. İstemci, sunucuya bir istek gönderdikten sonra, dönüşü gelene kadar başka bir istek gönderemez. Ancak bundan sonra gelen versiyonlarda bu durum beklenmemektedir, yani istemci, bir yanıt gelmeden başka istekleri sunucuya gönderebilmektedir. Bu sayede protokol daha da hızlı çalışmaya başlamıştır.

HTTP KİMLİK DOĞRULAMA

HTTP, temel erişim kimlik doğrulaması ve özet erişim kimlik doğrulaması gibi bazı kimlik doğrulama yöntemlerine sahiptir. İstemci, sunucuyla iletişim kurmadan önce kimlik doğrulama işlemi yapılmaktadır. Bu işlem sonrasında istemcinin sunucuya erişim sağlamaktadır.. Kimlik doğrulama işlemi, istemcinin sahip olduğu URL bilgileriyle oluşturulmuş diziler üzerinden gerçekleştirilmektedir. Bu sayede kimlik doğrulama işlemi tamamlanır ve istemciye erişim izni verilmektedir.

HTTP İLETİŞİM MANTIĞI

Temel anlamda protokol mesajlar üzerinden iletişim kurmaktadır. bu mesajlar istemci ve sonucu arasında oluşturulan bir ağ üzerinden gönderilmektedir. mesajlar içlerinde birden fazla bilgİ barındırmaktadır. Mesajlar bir istek satırı başlık alanları boş satır isteğe bağlı mesaj bölümü gibi alanlarda oluşmaktadır.

istek satırı ve diğer başlık alanlara her biri bazı etiketler ile bitmektedir. HTTP 1.1 protokolünde ana bilgisayar dışındaki tüm başlık alanları İsteğe bağlıdır.

HTTP protokolünde birden fazla istek tipi bulunmaktadır.Bu istek tipleri sunuculara önceden tanımlanmıştır. istekler sunucu üzerinde bulunan bazı verilerin verilmesi veya başka işlemler için kullanılabilmektedir. istekler belli başlı tipler halinde yollanmadıkları zaman sunucular tarafından güvensiz ve benzeri olarak ele alınmaktadır. bu istekTürleri aşağıda sırasıyla verilmiştir.

GET

GET yöntemi, belirtilen kaynağı sunucudan istemek için kullanılmaktadır. Bu tip istekler yalnızca veri almak için kullanılmaktadır ve başka bir etkisi bulunmamaktadır. GET isteği, kaynak üzerinde herhangi bir değişiklik yapmamaktadır. Yalnızca belirtilen veriyi sunucu üzerinden getirmek için kullanılmaktadır.

HEAD

HEAD yöntemi, GET isteği ile aynı mantıkta çalışır fakat yanıt gövdesi olmayan bir yanıt istemektedir. Bu sayede, tüm içerik taşınmak zorunda kalmaz ve yalnızca yanıt başlıkları alınmış olur. HEAD yöntemi, içeriğin varlığını kontrol etmek veya başlıklar hakkında bilgi almak için kullanılmaktadır.

POST

POST yöntemi, sunucunun talepte yer alan varlığı web sunucusunda bulunan kaynaklara yeni bir alt üye olarak kabul etmesini ister. Başka bir deyişle, POST edilen veriler, web sunucusunda bulunan veritabanına veya ilgili kaynağa eklenmektedir. POST, genellikle veri oluşturma veya mevcut kaynağa veri ekleme işlemleri için kullanılmaktadır.

PUT

PUT yönteminde iletilen veri sunucu içerisinde bulunan veritabanına işlenmektedir. Eğer bu veri önceden veritabanında bulunuyorsa, veritabanındaki bilgi değiştirilir ve yeni gelen veri, veritabanındaki bilgi ile yer değiştirir. Eğer böyle bir kaynak bulunmuyorsa, yeni bir kaynak oluşturulur ve içine verilen veri yazılır.

DELETE

DELETE yöntemin ne istek üzerinde bulunan veri kaynağı veri tabanından silinmektedir.

TRACE

TRACE yönteminde alınan istek sunucu tarafından tekrar yansıtılmaktadır. Bu sayede bir istemci hangi değişikliklerin veya eklemelerin yapıldığını görebilmektedir.

OPTİONS

Sunucunun desteklediği HTTP yöntemlerini öğrenmek için kullanılmaktadr. Aynı zamanda belirli bir kaynak yerine "*" isteyerek bir web sunucusunun işlevselliğini kontrol etmek için kullanılabilmektedir.

CONNECT

CONNECT yöntemi isteğin iletileceği tünelin şifreli bir tünel haline gelmesini sağlamaktadır. Genellikle bu yöntem SSL ile yapılmaktadır. Bu sayede güvenlik düzeyi arttırılmış olmaktadır.

PATCH

PATCH yöntemi bir kaynak üzerine kısmi değişiklikler yapmaktadır. Bu sayede bir kaynağın tamamı değil de değiştirilmek istenilen kısmı değiştirilmektedir.

Bazı türler geleneksel olarak güvenli olarak tanımlanmaktadır. Bu yöntemler genellikle sadece bilgi alma amaçlıdır ve sunucunun durumunu değiştirmemektedir. Örnek vermek gerekirse, GET metodu kullanıldığında sunucu üzerinde herhangi bir değişiklik olmamaktadır, keyfi olarak bu metod kullanılabilmektedir. Fakat her ne olursa olsun, bu standartların güvenliği olduğu kesin olarak garanti edilmemektedir. Geleneksel olarak güvenli kabul edilen metodlar arasında GET, HEAD, OPTIONS, TRACE metodları yer almaktadır.

Buna karşılık, POST, PUT, DELETE, PATCH gibi metodlar, sonucu üzerinde değişiklik yapabildiğinden dolayı geleneksel güvenli metodlar arasında yer almamaktadır.

Fakat GET öngörülen güvenliğe rağmen bazı güvenlik açıklarına sebep olabilmektedir. Kullanım alanları hiçbir şekilde sınırlı değildir; dikkatsiz ve kasıtlı kullanımında sunucu üzerinde bazı önemsiz değişikliklere sebep olabilmektedir. GET isteği ile bazı kaynakların silinmesi mümkündür. Bunun bir örneği, Google Web Accelerator'ın beta sürümünde gerçekleşmiştir; bir kullanıcı, önceden gelen URL ile kaynakları silmiştir. Bu yüzden bu uygulama, ilk sürümünden birkaç hafta sonra askıya alınmıştır.

Güvenli yöntemler haricinde etkisiz yöntemler de bulunmaktadır. Etkisiz yöntemlere örnek olarak PUT ve DELETE yöntemleri verilebilmektedir. Etkisiz yöntemlerin tanımı, bilgiden çok aynı içeriğe sahip isteğin tek bir istekle aynı etkiye sahip olması demektir. Yani aynı istek birden fazla yollansa da tek sefer yollansa da aynı şeyi yapmaktadır.

Fakat POST yöntemi etkisiz bir yöntem değildir. Bu nedenle aynı POST isteğinin birden fazla yollanması bazı yan etkilere sebep olabilmektedir. Bazı durumlarda bu istenebilir fakat genel olarak bu durum istenmeyen bir durumdur. Aynı POST isteğinin birden fazla kez yollanması, kullanıcının ilk talebinin yapıldığına dair yeterli geri bildirim alamaması gibi bazı kazalardan meydana gelebilmektedir. Bazı web tarayıcıları, sayfaların yeniden yüklenmesi sonucu tekrardan POST isteği yollanabileceğine dair mesaj kutucukları göstermektedir.

Aşağı tarafta isteklerin özelliklerine göre karşılaştırıldığı bir tablo yer almaktadır.

Yöntem	RFC	İstek gövdesi	Yanıt gövdesi	Güvenli	Etkisiz	Bellekte tutulabilir
PATCH	RFC 5789	Evet	Evet	Hayır	Hayır	Hayır
POST	RFC 7231	Evet	Evet	Hayır	Hayır	Evet
PUT		Evet	Evet	Hayır	Evet	Hayır
CONNECT		Kısmen	Evet	Hayır	Hayır	Hayır
DELETE		Kısmen	Evet	Hayır	Evet	Hayır
GET		Kısmen	Evet	Evet	Evet	Evet
HEAD		Kısmen	Hayır	Evet	Evet	Evet
OPTIONS		Kısmen	Evet	Evet	Evet	Hayır
TRACE		Hayır	Evet	Evet	Evet	Hayır

İstemci üzerinden giden istekler sonucunda sunucu üzerinden bazı yanıtlar dönmektedir. Aşağıda yanıtların bazı genel yapı taşları yer almaktadır.

Durum kodunu ve neden mesajını içeren bir durum satırı yer almaktadır. Bu durum kodu istemcilerin isteğin başarılı olup olmadığı gibi konularda bilgi vermek için kullanılmaktadır. Yanıt başlığı alanı bulunmaktadır. Bunlar haricinde boş satır ve isteğe bağlı mesaj bölümüde bulunmaktadır.

HTTP DURUM KODLARI

İstekler sonucunda yanıtlar meydana gelmektedir. Bu yanıtlar durum kodları sayesinde oluşturulmaktadır. Her bir durum kodu farklı anlama gelmektedir. 60'tan fazla durum kodu bulunmaktadır. Bu kodlardan bazıları karşımıza sık sık çıkmakta bazıları az kullanılmakta bazıları ise gelecekte kullanılmak üzere şimdiden tasarlanmıştır. Durum kodları 5 başlık altında incelenmektedir.

1XX DURUM KODLARI

Bu durum kodları bilgilendirme kodları olarak tanımlanmaktadır. İstemcinin isteğinin sunucuya ulaştığı ve işlemin başlığına dair bilgilendirme amaçlı kullanılmaktadır. Sunucu tarafından cevap oluşturulduktan sonra bu kodlar kaldırılmaktadır. Sık karşılaşılan bilgilendirme kodları aşağıda yer almaktadır.

100: İstemci tarafından gönderilen isteğin başlığının alındığı gövdesinin ise alınmaya hazır olduğu anlamına gelmektedir.

101: İstemcinin sunucunun protokol değiştirmesini istediğini ve sunucunun protokol değiştirmeyi onayladığını ifade etmek için kullanılmaktadır.

2XX DURUM KODLARI

İstemcinin isteklerine sunucunun başarılı verdiğini ifade etmek için kullanılmaktadır. Web sitelerinde bu durum kodu sayfaların sorunsuz çalıştığını ifade etmek için kullanılmaktadır. Genellikle web siteleri bu durum kodlarını döndürmektedir. Birden fazla 2XX durum kodu bulunmaktadır. Bunlardan bazıları aşağıda yer almaktadır.

200: Sayfaların sorunsuz çalıştığını belirtmek için kullanılan durum kodudur.

201: Sunucunun istek oluşturuldu anlamında kullandığı durum kodudur. Sunucu gelen isteği kabul ettiğinde ve işlem sürecine başladığında bu kod döndürülür. İstek yerine getirilebilir veya getirilemez.

204: Sunucunu isteği başarılı bir şekilde aldı fakat döndürülecek bir veri bulamadığını ifade etmek için kullanılmaktadır.

205: İçeriği sıfırla yanıtı olarak tanımlanmaktadır. Sunucunun işlemi başarılı bir şekilde işleme koyduğu fakat istek gönderenden belge görünümünü değiştirmesini istediği durumlarda bu durum kodu kullanılmaktadır.

206: Kısmi içerik yanıtı olarak adlandırılmaktadır. Sunucu istemci tarafından gönderilen bir aralık bağlılığı nedeniyle kaynağın yalnızca bir kısmını gönderdiğinde bu durum kodu kullanılmaktadır.

207: Bu durum kodu birden çok durum kodunun doğru olabildiği zamanlarda kullanılmaktadır.

3XX DURUM KODLARI

Geçici veya kalıcı yönlendirme kodlarıdır.Bu durum kodları sayfaların arama motoru optimizasyonunu korumak için önemli durum kodlarıdır.

301: Bir web sayfasının kalıcı olarak başka bir Web sayfasına yönlendirildiği durumlarda kullanılan durum kodudur. Eğer ziyaret edilen web sitesi başka bir web sitesine kalıcı olarak yönlendirildi ise otomatik olarak bu işlem gerçekleşmektedir.

302:Geçici yönlendirmelerin olduğu durumlarda bu durum kodu kullanılmaktadır. 301 durum kodundan farklı olarak bu durum kodu 1 sayfanın test gibi durumlarda aktarılması durumunda kullanılmaktadır. aynı zamanda ilgili sayfanın tekrardan aktif edileceği durumlarda bu durum kodu kullanılmaktadır. kullanıcılar 301 ile 302 arasındaki farkı anlayamamaktadır Çünkü otomatik olarak yönlendirme işlemi gerçekleşmektedir.

307: geçici yeniden yönlendirme kodunu ifade etmektedir 302 gibi bir kaynağın başka bir kaynağa geçici olarak yönlendirildiğini ifade etmektedir.

308: bir kaynağın kalıcı olarak başka bir kaynağa aktarıldığı durumlarda kullanılan koddur 301'den farklı olarak HTTP yönetiminin değişmesine izin vermemektedir.

4XX DURUM KODLARI

İstemci hata durum kodları olarak ifade edilmektedir arama motoru optimizasyonu denetimleri yapılırken en çok dikkat edilen durum kodudur.

400: Sunucunun istemci kaynaklı hatadan dolayı isteği yerine getirmemesi durumunda kullanılan koddur.

403: Yasaklanmış içeriklerde kullanılan durum kodudur yapılan istek sunucu tarafından anlaşılır fakat reddedilmektedir.

404: Sayfanın bulunamadı durumlarda kullanılan durum kodudur. En çok karşılaşılan durum kodlarından biridir. İstenilen kaynağın bulunamadı fakat genellikle bulunabileceği anlamına gelmektedir. Bu hatanın çözümü için bazı 404 sayfaları ve ya 3XX yönlendirme kodları kullanılmaktadır.

5XX DURUM KODLARI

Sunucu hatalarını ifade eden durum kodlarıdır. Sunucu istemciden gelen istekleri işleyemediği durumlarda bu kodu kullanmaktadır. Bu kodun olduğu sayfalar kullanıcılar tarafından görüntülenememektedir.

500: Beklenmeyen bir durumda sunucunun karşılaştığı hatalarda kullanılan durum kodudur.

502: Sunucunun başka bir sonucu istek göndermesinden sonra geçersiz yanıt aldığı anlamına gelen durum kodudur.

504: Bir isteğin işlemi sırasında bir sunucunun başka bir sunucudan istediği dönüşün zaman aşımına uğraması sonucunda kullanılan durum kodudur.

505: Protokol sürümünü desteklenmediği durumlarda kullanılan durum kodudur.

511: İstemcinin isteği sunucu iletilmeden önce kimlik doğrulama işleminin yapılması gerektiğinde kullanılan durum kodudur.

Şifreli bir HTTP bağlantısı kurmanın en popüler yolu HTTPS'dir. Şifreli bir HTTP bağlantısı kurmak için iki başka yöntemde mevcuttur. Fakat Günümüzde en çok HTTPS kullanılmaktadır.

Özetlemek gerekirse HTTP istemci sunucu mantığında çalışan bir protokoldür. Bu protokol sayesinde web siteleri ve sunucuları ile haberleşebilmektedir. Fakat günümüzde bazı güvenlik açıklarından dolayı güvenlik hiper metin transfer protokolü anlamına gelen HTTPS daha fazla kullanılmaktadır.

HTTPS

HTTPS bir bilgisayar ağı üzerinden güvenli İletişim için internet üzerinden yaygın olarak kullanılan bir HTTP uzantısıdır. HTTPS iletişim Protokolü TLS veya SSL ile şüphelenmektedir. Bu nedenle bu protokol genel olarak TLS üzerinden HTTP veya SSL üzerinden HTTP olarak adlandırılmaktadır.

HTTPSTemel amacı erişilen Web sitesinin kimlik doğrulaması ve aktarılan verilerin iletişimi sırasında gizliliği ve bütünlüğünün korunmasıdır. genel anlamda bu protokol istemci ile sunucu arasında gerçekleşen üretim sırasında olası bir saldırıyı önlemek için kullanılmaktadır.2016 yılında Electronic Frontier Foundation web tarayıcılarının desteği ile çıkan kampanya sayesinde bu protokol yaygınlaşmıştır.

HTTPS protokolünün ilk kullanım alanları www ödeme işlemleri e-posta ve kurumsal bilgi sistemlerini hassas işlemleri gibi işlemlerdir. 2018'den itibaren HTTPS web sitelerine sık sık kullanılmaya başlamıştır.

Netscape Communications, Netscape Navigator web tarayıcısı için 1994 yılında HTTPS oluşturulmuştur. başlangıçta bu protokol SSL ile kullanılmıştır son aralarında gelişen TLS ile kullanılmaya devam etmiştir.

Şubat 2018'de Google HTTPS kullanılmayan sitelerin güvenli değil olarak işaretlemeye başlayacağını duyurduğunda web site sahiplerinin çoğu HTTPS protokolüne geçiş yapmıştır.

HTTPS HTTP ile aynı kullanım mantığına sahiptir. Fakat HTTPS trafiği korumak için Tarayıcıyı belli başlı güvenlik protokolleri kullanacak şekilde uyarmaktadır. bu protokoller HTTP ile uyumlu çalışmaktadır. iletişimin sadece bir tarafı doğrulanmış olsa bile koruma sağlayabilmektedirler. bu doğrulama genellikle yalnızca sunucu kimliğinin doğrulanması ile sağlanmaktadır.

HTTPS güvenli olmayan bir ağ üzerinden güvenli bir kanal oluşturmak için kullanılmaktadır.

HTTPS sayesinde HTTP protokolünün tamamı şifrelenebilmektedir. bu şifreleme istek URL'sini, sorgu parametrelerini, üst bilgileri ve çerezleri şifrelemek için kullanılmaktadır. fakat makine adresleri ve port numaraları TCP/IP protokollerini bir parçası olduğundan HTTPS tarafından şifrelenememektedir. temel anlamda doğru şekilde yapılandırılmış olsa bile Bir web sitesini dinleyiciler tarafından web sunucusunun IP adresini ve Port numarasını çıkartabileceği anlamına gelmektedir. iletişim içeriği olmasa bile iletişim süresi gibi bazı bilgilere ulaşılabilmesini sağlamaktadır.

web tarayıcıları yazılımlarını önceden yüklenmiş sertifikalara dayanarak HTTPS web sitelerinden size güvenebileceklerini bilmektedirler.Web tarayıcısı üreticileri ise hangi sertifika otoritelerine güvenebileceğini bilmektedir.

HTTPS özellikle güvensiz ağlarda büyük önem taşımaktadır. aynı zamanda birçok WLAN ağı web sayfalarına kendi reklamlarını verebilmek için paket iletimini dahil olmaktadır. aynı zamanda bu paket iletime dahil olmak zararlı yazılımları yüklenmesi gibi işlemlerin yapılabileceği anlamına gelmektedir.

Eser bilgileri çalan suçlular hakkında günümüzde daha fazla bilgi ortaya çıkması sonucunda kullanılan internet türüne bakılmaksızın çoğu web sitesi HTTPS protokolünü kullanmaktadır. konular üzerinde ziyaret ettiği web sitelerdeki üst bilgiler tek tek bir anlamı ifade etmese bile birleştirildiği zaman kullanacağı hakkında çok fazla bilgi edinmeye olanak sağlamaktadır. bu durum kullanıcıların gizliliğini ihlal etmektedir.

Kasım 2017 itibariyle 1 milyon Web sitesinin yaklaşık %30'u HTTPS protokolünü kullanmaktadır. aynı zamanda internetin en popüler yaklaşık 150.000 sitesinin %50'ye yakın kısmı HTTPS protokolünü kullanmaktadır.

Adres çubuğunda kullanılan web sitesinin HTTPS kullanıp kullanmadığına dair bazı ibareler bulunmaktadır. Bu ibare kilit sembolü Yuvarlak içinde i sembolü Üçgen içinde ünlem işareti sembolü gibi semboller olabilmektedir.

HTTPS ŞİFRELEME İŞLEMİ

HTTPS iletişimleri şifrelemek için bir şifreleme protokolü kullanmaktadır. Protokol temel mantıkta 2 adet anahtar bulunmaktadır.

Özel anahtar: Bu anahtar bir web sitesinin sahibi tarafından kontrol edilir ve gizli tutulmaktadır genel anahtar tarafından şifrelenen verileri çözmek için kullanılmaktadır.

Genel Anahtar: Bu anahtar sunucuyla güvenli bir şekilde iletişim kurmak isteyen tüm herkes tarafından kullanılabilmektedir genel anahtarın şifrelediği verileri sadece özel anahtar çözümleyebilmektedir.

HTTP VE HTTPS ARASINDAKİ FARKLAR

HTTPS URL’leri https ile başlamaktadır fakat HTTP URL’leri http ile başlamaktadır.

HTTP olası Siber saldırılara açık bir iletişim protokolüdür. saldırganlar web sitesi hesaplarına erişim elde edip web sitesini değiştirebilir ya da kötü amaçlı yazılım enjekte edebilirler. Fakat HTTPS bu saldırılara dayanacak şekilde tasarlanmıştır.

HTTP iletimden önce mesajı şifreleyen ve varışta mesajın çözülmesini sağlayan TLS güvenlik protokolünü kullanmaktadır. HTTPS farklı bir protokol değildir şifreli bir bağlantı üzerinden normal HTTP kullanımını ifade etmektedir.HTTP mesajındaki her şey şifrelenerek iletilmektedir.

WEBSOCKET

WebSocket, istemci ile sunucu arasındaki iletişimi sağlamak için kullanılan protokollerden biridir. WebSocket, durum bilgisi olan bir protokoldür; istemci ve sunucu arasındaki bağlantı, taraflardan biri bağlantıyı sonlandırıncaya kadar canlı kalmaktadır. Her iki taraftan biri bağlantıyı kapattığında, bağlantı her iki noktada da sonlandırılmaktadır.

WebSocket fikri, tek yönlü olan HTTP protokolünün kısıtlamalarından dolayı oluşturulmuştur. HTTP protokolünde tek yönlü iletişim söz konusudur. İstemci, sunucudan istekler doğrultusunda bazı bilgileri istemektedir; sunucular da bu bilgiler doğrultusunda bazı dönükler döndürmektedir. İstemci üzerine bir değişiklik olduğunda bu, sunucuya bildirilebilir, fakat sunucu üzerinde bir değişiklik olduğunda bu istemciye bildirilmemektedir. Sunucu üzerinde gerçekleşen değişiklikleri öğrenebilmek için WebSocket ortaya çıkmıştır. WebSocket protokolü sayesinde, sunucuda meydana gelen değişiklikler istemciye, bir istek olmadan, bildirilebilmektedir.

WebSocket, ilk olarak TCP tabanlı soket API'sinin yerine TCPConnection olarak düşünülmüştür. Haziran 2008'de, WebSocket olarak bilinen protokolün ilk versiyonu, Michael Carter tarafından bir takım çalışmalarla gerçekleştirilmiştir.

Bunun üzerine kısa bir süre sonra IRC chat odası ile işbirliği sonucunda "WebSocket" ismi verilmiştir; duyurusu ise Michael Carter tarafından bir blog üzerinden yapılmıştır. Aralık 2009'da, WebSocket protokolünün standartlarını tam anlamıyla uygulayan ilk tarayıcı Google Chrome olmuştur. Sonrasında protokol gelişmiş ve birden çok tarayıcı tarafından standart olarak kabul edilmiştir.

WebSocket, ilk olarak sunucu ile işlemci arasında bir bağlantı oluşturmaktadır. Bağlantı kurulum aşamasında, istemci ile sunucu arasında bazı bilgiler değiş tokuş edilmektedir. Bu değiş tokuş işlemi HTTP üzerinden gerçekleşmektedir. İstemci veya sunucu, mesajları kurulan bağlantı üzerinden göndermektedir. WebSocket, verilerin şifrelenerek iletilmesini sağlamaktadır; aynı zamanda WebSocket kullanımı için sunucuların SSL sertifikalarına sahip olmaları gerekmektedir.

Anlık sohbet uygulamalarında, WebSocket sayesinde kullanıcıların anlık mesajları gerçek zamanlı olarak iletilebilmektedir.

Çok oyunculu oyunlarda, oyuncuların birbirleriyle girdikleri etkileşimlerin gerçek zamanlı olarak birbirlerine aktarılmasını sağlamak için WebSocket kullanılmaktadır.

Anlık fiyat takiplerinin ihtiyaç olduğu durumlarda, WebSocket kullanılmaktadır.

Uzaktan kontrol veya izleme uygulamaları gibi uygulamalarda, gerçek zamanlı olarak görüntü aktarımı sağlanabilmesi için WebSocket kullanılmaktadır.

FTP

Türkçe karşılığı "Dosya Aktarım Protokolü" anlamına gelmektedir. Bilgisayar alanında bulunan bir istemci, belirlenen dosyaların aktarılması sırasında kullanılan iletişim protokolüdür. Bu protokol, istemci-sunucu mimarisine dayanmaktadır. Genellikle bu protokolle kullanıcılar, kullanıcı adı ve parola biçiminde kendilerini doğrulayabilmektedirler; fakat sunucu bu şekilde yapılandırılmadıysa anonim olarak da bağlanabilmektedirler. Bu protokol genellikle daha güvenli olan FTPS veya SFTP ile değiştirilmektedir.

Dosya Aktarım Protokolü için ilk spesifikasyon Abhay Bhushan tarafından yazılmıştır ve 16 Nisan 1971'de yayınlanmıştır. İlk olarak FTP protokolü, TCP/IP'nin öncülü olan NCP üzerinde çalışmıştır.

Protokol, veri bağlantısının nasıl kurulacağını belirleyen iki farklı modda çalışabilmektedir. Bu modlar sırasıyla aktif ve pasif mod olarak adlandırılmaktadır.

Aktif modda istemci, sunucunun 21 numaralı portundan kontrol bağlantısı ile FTP sunucusuna bağlanmaktadır. Tüm veri aktarımı bu 20 numaralı port üzerinden gerçekleşmektedir.

Pasif mod ise, değişik sebeplerden dolayı meydana gelen problemlere sunucu tarafından çözüm bulmak amacıyla çıkarılmıştır. İstemci, ilk başta port üzerinden kontrol bağlantısı kurarak sunucuya bağlanmaktadır. Aktif bağlantıda olduğu gibi, istenildiği zaman veri aktarımı gerçekleştirmek isterse istemeden yeni bir port açılmaktadır. Bu sayede veri aktarımı, istemcinin ve sunucunun en son açtığı portlar arasında gerçekleşmektedir. Zaten bağlantı filtreleme, güvenlik duvarı gibi problemleri ortadan kaldırmaya yönelik geliştirilmiş bir yöntemdir.

FTP, ilk başlarda güvenli bir protokol olarak tasarlanmamıştır. Günümüz standartlarından bakıldığında, bu protokolde birçok güvenlik açığı bulunmaktadır. Mayıs 1999'da bir grup insan, bu protokolün zaaflarını listelemiştir.

SFTP, FTP'nin aksine verileri şifreleyen bir dosya aktarım protokolüdür. Bu nedenle veri aktarımı sırasında üçüncü şahısların müdahale etmesi, verilerin ele geçirilmesi, manipüle edilmesi gibi işlemler, FTP protokolüne göre çok daha zordur. SFTP protokolü, SSH protokolü kullanarak çalışmaktadır ve birçok FTP istemcisi tarafından desteklenmektedir.

SCP, SSH protokolü kullanarak dosya kopyalamak için kullanılan bir protokoldür. Bu protokol, tıpkı SFTP gibi verilerin şifrelenmesini ve güvenli bir şekilde aktarılmasını sağlamaktadır.

WebDAV, HTTP protokolü üzerinden dosya aktarımı yapmak için kullanılan bir protokoldür. Aynı diğer kategoriler gibi şifreleme ve güvenlik özellikleri sağlamaktadır.

SMTP

SMTP Nedir?

SMTP açılımı "Simple Mail Transfer Protocol" anlamına gelmektedir. E-postaları internet üzerinden iletmek amacıyla hizmet veren bir protokoldür. Dijital ortamda e-posta iletimini sorunsuz bir şekilde kolaylaştırmak için kullanılmaktadır. Birincil amacı, soruları arasında iletişim sağlamak için bir çerçeve oluşturmaktır.

Bu protokol, bir mesaj aktarım aracı kullanarak e-postaların aktarımını sağlar. Bu sebepten dolayı e-posta göndermek için sistemde bir istemci mesaj aktarım aracı içermelidir. Aynı şekilde, posta almak için ise bir sunucu mesaj aktarım aracısının varlığı zorunludur.

E-posta Aktarım Süreci

SMTP protokolü ile e-posta aktarım süreci, SMTP sunucusuna bir TCP bağlantısının başlatılması ile başlar. Daha sonra istemci, e-postayı kurulan TCP bağlantı üzerinden göndermektedir. İstemcilerden gelen bağlantılar, genellikle 25 numaralı port üzerinden kurulur. Bu hızlı bağlantı kurulumuyla, istemcilerin e-postaları hızlı bir şekilde işlenir.

SMTP Protokolü Bileşenleri

SMTP protokolü belli başlı bileşenlerden oluşmaktadır. Aşağıda bu bileşenler sırasıyla verilmiştir:

1. **Posta Kullanıcı Aracısı:** E-postaların hem gönderilmesine hem de alınmasına yardımcı olan bir bilgisayar programıdır. Posta aktarım aracısı ile e-posta mesajlarının iletilmesini sağlar.
2. **Posta Gönderme Aracısı:** Posta kullanıcı aracısından aldığı e-postaların aktarımını kolaylaştırmak için posta aktarım aracı ile işbirliği yapar.
3. **Posta Aktarım Aracısı:** SMTP protokolünün yeteneklerini kullanarak e-postaları bir sistemden diğerine verimli bir şekilde aktaran yazılımdır.
4. **Posta Teslim Analizi:** E-postaların yerel sisteme teslim edilmesini sağlar.

SMTP Protokolleri

İki türlü SMTP modeli bulunmaktadır. Bunlar "uçtan uca yöntemi" ve "sakla ve ilet yöntemi" olarak adlandırılmaktadır.

- **Uçtan uca yöntemi:** Farklı işletmeler arasındaki iletişim için kullanılır.
- **Sakla ve ilet yöntemi:** Bir işletme içinde kullanılır.

Gönderici ve Alıcı Arasındaki İletişim

1. **Posta Gönderme:** Posta göndermek, temel olarak istemci ve sunucu arasında bir dizi istek ve yanıt mesajının gönderilmesidir. Gönderilen mesaj, bir başlık ve bir gövdeden

oluşur. Boş bir satırla sonlandırılır ve bu boş satırdan sonraki her şey mesaj gövdesi olarak kabul edilir.
2. **Posta Alma:** Sunucu, kullanıcı aracısının posta kutularını belirli aralıklarla kontrol etmesini sağlar. Herhangi bir bilgi alındığında, kullanıcı bilgilendirilir. Kullanıcı, e-postalarını okumak için her birini, kısa bir açıklamasıyla birlikte görüntüleyebilir.

SMTP'nin Amacı

Birincil amacı, e-posta mesajları göndermek için güvenilir ve verimli bir yöntem sağlamaktır. E-posta göndericilerinden alınan e-postaların alıcının e-posta sunucusuna doğru şekilde yönlendirilmesini sağlar. Aynı zamanda, bir e-posta başarılı bir şekilde teslim edilemediğinde, göndericiye geri gönderilen hata bildirimlerini de sağlar.

SMTP Nasıl Çalışır

1. **Gönderici ve Alıcı Arasındaki Etkileşim:** Gönderici istemcisi, iletiyi oluşturarak süreci başlatır. Bu ileti, posta aktarım aracısına gönderilir. Posta aktarım aracı, e-postayı ağ üzerinden alıcının posta aktarım aracısına taşır. Bir sistemde posta göndermek için bir istemci posta aktarım aracına ve bir sunucu posta aktarım aracına ihtiyaç vardır.
2. **E-posta İletişiminin Başlaması:** E-postaların iletimi, istemci ve sunucu arasında bir dizi alışveriş ile gerçekleşir. E-posta mesajı, bir başlık ve bir gövde içerir. İçeriği bulunmayan boş bir satır, baştan sonuna kadar ifade eder. Sonrasındaki tüm veriler e-postanın gövdesi olarak adlandırılır.
3. **Gelen E-postaların Alınması:** Son kullanıcı aracı, posta kutularını belirli aralıklarla kontrol eder. Yeni bilgiler geldiğinde kullanıcı anlık olarak bilgilendirilir. Posta kutusuna gidildiğinde, her bir e-posta başlıkları ve kısa içerikleriyle bir liste halinde gösterilir. Kullanıcı, seçtikleri e-postayı terminalde doğrudan görüntüleyebilir.

SMTP Komutları

Komut	Açıklama
HELO	Bu komut e-posta gönderme işlemini başlatmak için kullanılır ve kullanıcıyı ve tam alan adını tanımlamak için kullanılır. Bu, sunucunun alan adıyla birlikte bir HELO komutu gönderdiği görüşmenin başlangıcıdır.
MAIL	Bu komut mesaj aktarımını başlatmak için kullanılır ve postanın kaynağını tanımlar. Bu komuttan sonra sunucu her şeyi sıfırlar ve e-posta adresini kabul etmeye hazır olur ve kabul ettikten sonra 250 OK koduyla yanıt verir.
RCPT	Bu komut postanın alıcısını tanımlar ve SMTP sunucusu yine aynı kodla yanıt verir.
DATA	Bu komut, istemci ile sunucu arasında veri aktarımını tetikler.
QUIT	E-posta gönderildikten sonra, istemci sunucudan çıkmak için bu komutu gönderir ve başarılı bir şekilde kapatılırsa, sunucu bir 221 kodu ile yanıt verir.
RSET	Posta işlemini durdurmak veya iptal etmek için bu komut kullanılır. Bu, bağlantıyı kapatmaz ancak her şeyi sıfırlar ve posta ve e-posta adresleriyle ilgili önceki tüm verileri kaldırır.

SMTP Protokolünün Avantajları

Güvenilir E-posta Teslimatı: E-posta sunucuları arasında mesajların aktarılması için standartlaştırılmış bir yöntem sayesinde e-postaların güvenilir bir şekilde teslim edilmesine olanak sağlar.

Yaygın Uyumluluk: SMTP, bilinen e-posta istemcileri ve sunucuları tarafından yaygın olarak desteklenmektedir ve farklı sistemler arasında sorunsuz iletişim sağlar.

Köklüdür: SMTP, çok uzun süredir kullanılmaktadır. Bu durum, protokolün olgunlaşmış ve iyi test edilmiş bir sistem olmasını sağlar.

Esnek Yapılandırma: SMTP, değişen koşullara uyum sağlayabilir ve yapılandırma ayarlarına izin verir, böylece optimum e-posta dağıtım performansı sağlanır.

Mesaj Kuyruğu Yönetimi: SMTP sunucuları, mesaj gruplarını yöneterek büyük veri e-postalarının verimli bir şekilde işlenmesini sağlar. Ayrıca, başarısız teslimat denemeleri durumunda yeniden deneme imkanı sunar.

SMTP Protokolünün Dezavantajları

Güvenlik Endişeleri: SMTP, doğal güvenlik özelliklerinden yoksundur. Bu durum, e-posta sahteciliği, kimlik hırsızlığı ve mesajların yetkisiz erişime açık olmasına neden olabilir.

E-posta Spaması: Spam, istenmeyen e-postaların tekrar tekrar gönderilmesine yol açar ve aşırı yüklenmeye, potansiyel sistem kaynağı israfına neden olabilir.

Sınırlı Başlık Bilgisi: Başlık, posta hakkında sınırlı bilgi sağlar, bu da bazen e-postaların yönetilmesinde zorluklar çıkarabilir.

Yerleşik Şifreleme Olmaması: Güvenli e-posta iletimi için ek protokoller kullanılması gerekmektedir.

SMTP Protokolünün Tarihçesi

SMTP e-posta iletimi için kullanılan en yaygın protokoldür. 1980'li yılların başında geliştirilen SMTP, özellikle internetin genişlemesiyle birlikte e-posta sistemlerinin birbirleriyle uyumlu bir şekilde çalışmasını sağlayan önemli bir araç haline gelmiştir.

SMTP'nin ilk temelleri, 1970'lerin sonlarına dayanmaktadır. E-posta iletişiminin temelleri, Ray Tomlinson'un 1971 yılında geliştirilen ve bugünkü e-posta sistemlerine çok benzeyen "send" komutuyla atılmıştır. Tomlinson, bilgisayarlar arasında e-posta göndermek için bir iletişim protokolü geliştirmişti. Ancak bu ilk sistemdeki iletişim, yalnızca tek bir bilgisayar ağındaki cihazlarla sınırlıydır ve her ağ için özel çözümler gerektirmektedir. E-posta iletimi için standart bir yöntem bulunmamaktadır.

1982 yılında, Jon Postel ve diğer İnternet mühendisleri, e-posta iletiminin daha verimli ve evrensel bir şekilde yapılabilmesi için yeni bir protokol geliştirmek üzere çalışmaya başlamışlardır. Bu çalışmaların sonucunda, 1983 yılında SMTP protokolü RFC 821 olarak tanımlanmış ve ilk kez tanıtılmıştır. SMTP, temelde, e-posta mesajlarının bir sunucudan diğerine gönderilmesini sağlayan bir protokoldür.

SMTP, başlangıçta yalnızca metin tabanlı e-posta mesajlarının iletimi için tasarlanmıştır. Ancak zamanla, internetin yaygınlaşmasıyla birlikte protokolün kullanım alanı da genişlemeye başlamıştır. 1980'lerin sonlarına doğru, İnternet'teki çoğu e-posta sistemi SMTP'yi kullanmaya başlamıştır.

SMTP, geliştirildikçe daha fazla işlevsellik kazanmış ve zamanla yeni sürümleri ortaya çıkmıştır. 1988 yılında RFC 821'in revizyonu olan RFC 822 yayınlanmıştır.

1990'larda, internetin daha geniş bir kitleye ulaşması ile birlikte SMTP, büyük bir popülerlik kazanmıştır. SMTP, internetin başlangıçtan itibaren en yaygın e-posta protokolü haline gelmeye başlamıştır. 1999'da, daha güvenli iletişim için Secure SMTP (SMTPS) tanıtılmıştır. Bu, e-posta iletimi sırasında verilerin şifrelenmesi yöntemi ile verilerin güvenliği arttırılmaktadır.

2000'lerin başında ise, e-posta spam sorunu, SMTP protokolü ile ilgili önemli bir konu haline gelmiştir. Bu nedenle, çeşitli güvenlik protokolleri ve filtreleme yöntemleri geliştirilmiştir. Bu dönemde, e-posta sağlayıcıları ve internet servis sağlayıcıları, SMTP ile ilgili güvenlik önlemleri alarak spam ve kötü amaçlı yazılım gönderen e-postaların engellenmesi için yeni teknolojiler geliştirilmiştir.

Sonuç olarak, SMTP protokolü, 1980'lerden günümüze kadar gelişerek modern internetin önemli bir parçası haline gelmiştir. E-posta iletiminin güvenli, verimli ve evrensel bir şekilde gerçekleşmesini sağlayan SMTP, dijital iletişimin temel yapı taşlarından biridir.

IMAP

İnternet Mesaj İletişim Protokolü, e-posta istemcilerinin bağlantı üzerinden bir posta sunucusundan e-posta mesajlarını almak için kullandığı bir protokoldür.

Bu protokol, bir e-posta kutusunun birden fazla e-posta istemcisi tarafından kullanılmasına olanak sağlar. Bu nedenle istemciler, kullanıcı e-postalarını silene kadar iletileri sunucuda bırakır.

E-posta alımı için kullanılan iki temel protokolden biri POP3, diğeri ise IMAP'tır. Her iki protokol aynı anda kullanılabilir.

IMAP, kullanıcıların uzak bir e-posta sunucusuna erişmesini sağlayan bir uygulama katmanı protokolüdür. E-posta mesajlarını verenden almak için yaygın olarak kullanılan bir protokoldür ve çoğu modern e-posta sunucusu tarafından desteklenmektedir.

IMAP, 1986 yılında Mark Crispin tarafından, posta kutusunun içeriğini almak için kullanılan geleneksel protokollerin aksine, uzaktan erişim sağlayan bir protokol olarak tasarlanmıştır.

Aşağıda, IMAP protokolünün farklı sürümleri sırasıyla açıklanmıştır:

- **Orijinal IMAP**: Orijinal bir kopyası bulunmamaktadır, ancak bazı komutlar açısından bir üst versiyonuyla benzer özelliklere sahip olduğu düşünülmektedir. Bu protokolde komut etiketlemesi bulunmamaktadır, bu nedenle söz dizimi hiçbir sürümle uyumlu değildir.

- **IMAP2**: Bu sürüm, halka açık ilk sürümdür. Bu sürümle birlikte komut yanıt etiketleme işlemi protokole eklenmiştir.

- **IMAP3**: 1991'de yayımlanan ve çok nadir kullanılan bu sürüm, önceki sürümüne yönelik özel öneriler sunmuştur. Ancak kabul edilmemiştir. Protokolün çalışma grubu, yeni sürüm için başlangıç noktası olarak IMAP3 değil, IMAP2'yi kullanmıştır.

- **IMAP2BIS**: IMAP2'nin bir üst versiyonu olarak geliştirilmiştir. IMAP2'de bulunmayan posta kutusu yönetim işlevlerini eklemek için genişletilmiştir. Aralık 1992'de dağıtılmıştır.

- **IMAP4**: 1990'ların başlarında bir kuruluş içinde oluşturulan IMAP çalışma grubu, IMAP2BIS tasarımını üstlenmiştir. Karışıklığı önlemek amacıyla, IMAP2BIS, IMAP4 olarak yeniden adlandırılmıştır.

Genel olarak, bir kullanıcının e-posta istemcisini kullanarak gönderdiği e-posta mesajları önce kullanıcısının oturum açtığı e-posta sunucusu tarafından kabul edilir. Ardından

genellikle SMTP kullanılarak, alıcının posta kutusunu barındıran başka bir e-posta sunucusuna iletilir. Bu aşamada, e-posta alıcısının mesajlarına ulaşabilmesi için e-posta sunucusundan e-posta istemcisi aracılığıyla veriler çekilir. Ancak, SMTP tek yönlü bir protokol olduğundan, e-posta verilerini istemci indirilemez. Bu noktada IMAP veya POP3 devreye girer ve istemcinin talep ettiği e-posta verilerini indirmek için kullanılır.

İki protokol arasındaki temel fark şudur: IMAP, e-posta sunucusuyla bağlantı kurduğunda yalnızca e-postaların başlıklarını çekerken, POP3 iletişim kurduğu e-posta sunucusundan tüm e-posta verilerini çeker. Genel olarak, e-posta kullanıcı sayısının fazla olduğu durumlarda IMAP tercih edilir.

IMAP4'ün POP3'e göre bazı avantajları vardır. POP3 ile bir e-posta sunucusuna bağlanıldığında, bütün yeni mesajlar istemciye çekilir ve bağlantı sonlandırılır. Ancak, IMAP4 teknolojisinde bağlantı sadece istemciye ihtiyaç duyulduğu sürelerde açık kalır.

POP3, aynı posta kutusunda yalnızca bir kullanıcıyı desteklerken, IMAP aynı anda birden fazla kullanıcının erişmesini destekler. Bir kullanıcının yaptığı değişiklikler, eş zamanlı olarak oturum açmış diğer kullanıcılar tarafından görülebilir.

Tüm e-postalar neredeyse her zaman MME formatında gönderilmektedir. Bu formatta e-posta parçalar halinde iletilir. IMAP, bu parçaları tek tek çekebilmektedir.

İstemci ile sunucu arasındaki bağlantıları korumak için TLS (Transport Layer Security) kullanılmaktadır.

POP3

POP3, temelde bir e-posta iletişim protokolüdür. Bu protokol sayesinde yerel e-posta alıcıları, uzak sunuculardaki bulunan e-postalarını indirebilir. Günümüzde bu işlemi yapmak için kullanılan en yaygın protokollerden biridir. Tüm güncel e-posta alıcıları ve sunucuları bu protokolü desteklemektedir. Birden fazla POP versiyonu bulunmaktadır, ancak en son kullanılan sürüm POP3'tür.

E-posta ilk başta gönderilirken **SMTP** protokolü kullanılır. E-posta sunucuları arasında aktarılırken bu protokol kullanılır; fakat alıcı e-postaya koymak istediği bilgisayarına indirmek için arka planda POP3 kullanılmaktadır. Kısacası, bu protokol yalnızca e-postayı almak için kullanılır.

POP3, posta kutularında basit indirme ve silme işlemlerini karşılamak için kullanılmaktadır. Postalar indirildikten sonra, bu postaları sunucuda bırakma seçeneği olmasına rağmen, genelde bu protokol şu işlemleri sırasıyla gerçekleştirir: Sunucuya bağlanılır, tüm e-postalar alıcının bilgisayarına indirilir, bilgisayara indirme işlemi tamamlandıktan sonra ise tüm e-postalar sunucudan silinir. Ardından bağlantı kesilir. Bu sayede sunucu üzerindeki verilerin sayısı azalır.

Güvenlik

Bu protokol güvenli bir protokol olarak kabul edilmemektedir. Çünkü kullanıcı kimlik bilgileri ve şifreler gibi veriler şifrelenmeden sunucuya gönderilmektedir. Bu sebepten dolayı, bir saldırganın kimlik bilgilerini ele geçirmesine olanak sağlayabilir. Daha güvenli bir iletişim için, bu protokol SSL veya TLS gibi protokollerle kullanılmaktadır. Bu protokoller sayesinde istemci ile sunucu arasında şifreli bir bağlantı kurulmakta ve kullanıcıların kimlik bilgileri güvence altına alınmaktadır. Böylece e-postaların güvenli bir şekilde indirilmesi sağlanır.

Ayrıca, protokolün güvenilirliği, sunucu tarafından da etkilenmektedir. E-postaların tutulduğu sunucular düzenli olarak güvenlik açıklarına karşı taranmakta ve güncellenmektedir.

Avantajlar

- Kullanımı kolaydır.
- Tüm e-postaların istemciye indirilmesi sayesinde kullanıcılar çevrimdışı olarak e-postalarına erişebilir.
- İndirilen e-postalar sunucudan silindiğinden alan tasarrufu sağlar.
- Küçük cihazlar için ideal bir protokoldür.

Dezavantajlar

- Senkronizasyon sorunları olabilir.

- Güvenlik zayıflıkları bulunabilir.
- Sınırlı özelliklere sahiptir.

POP3 ile Çalışan E-posta İstemcileri

POP3, farklı e-posta istemcileri ile çalışabilir. Bunlar arasında şunlar yer alır:

- **Microsoft Outlook**: Microsoft'un ofis paketine dahil olan popüler bir e-posta istemcisi dir.
- **Mozilla Thunderbird**: Mozilla Vakfı tarafından geliştirilen açık kaynaklı bir e-posta istemcisi dir.
- **Apple Mail**: macOS işletim sistemine varsayılan olarak dahil edilen e-posta istemcisi dir.
- **Pegasus Mail**: Windows işletim sistemi için kullanılan bir e-posta istemcisi dir.

IMAP ile POP3 Arasındaki Farklar

Her iki protokol aynı işlevi görse de yapısal olarak birbirlerinden farklıdırlar. Protokoller arasındaki farklar aşağıda ki tablo üzerinde özetlenmiştir.

POP3 Rahat, Yerleşik, Kolay	IMAP Güvenli, Hızlı, Güncel
Tüm mailler download edilmeli. Outlook, thunderbird gibi bir programa ihtiyacınız var.	Bir şey yüklemenize, outlook, thunderbird gibi bir programa ihtiyacınız yok...
Mesaj içeriği ile birlikte bilgisayarınıza otomatik olarak kayıt edilir.	Sadece talep ettiğinizde mesaj download edilir.
Sadece bir mail box yaratabilirsiniz..	Çoklu mail box yaratabilirsiniz.
Giden mailler sadece bilgisayarınızda saklanır.	Giden maillera her yerden ulaşabilirsiniz.
Mailler PC üzerinden silinebilir.	Sadece servera girip silmeniz gerekir.
Posta kutusuna erişimde aynı anda sadece tek kullanıcıyı destekler. Aksi halde karşısına hata mesajı verebilir ya da sorunlar yaşatabilir.	Çok kullanıcıyı destekler. Bir kullanıcının yaptığı değişiklik eş zamanlı olarak diğer oturum açılmış kullanıcı ya da cihazlardan da görülebilir. Dosya eklerini ise yine IMAP sayesinde ayrı bir parça olarak cihazınıza indirebilirsiniz.[4]

SSH

SSH, Türkçe karşılığıyla "güvenli kabuk" anlamına gelmektedir ve hizmetlerin güvenli olmayan bir ağ üzerinde güvenli bir şekilde iletilmesini sağlayan bir protokoldür. Bu protokol, kriptografik bir protokoldür ve istemci-sunucu mantığında çalışmaktadır. Temel mantıkta, güvenli olmayan bir ağ üzerinde güvenli bir kanal sağlayarak verilerin güvenli bir şekilde iletilmesine olanak tanır. SSH, iki farklı sürüm altında incelenebilir.

SSH, rlogin, rsh ve rexec gibi protokollerin yerini almak için tasarlanmıştır. Bu protokoller, genellikle parolalar gibi önemli verileri düz metin olarak göndermektedir. Bu sebepten dolayı üçüncü şahıslar veya saldırganlar bu verilere erişebilir. Ancak SSH, şifreleme kullanarak, güvenli olmayan ağlarda verilerin gizliliğini ve bütünlüğünü sağlamaya yardımcı olur. Bununla birlikte, ulusal güvenlik ajansları zaman zaman SSH şifresini çözerek SSH oturumlarının içeriğini okuyabilmektedir.

SSH protokolü, kimlik doğrulama gibi işlemler gerektiğinde, kullanıcının kimliğini doğrulamak için açık anahtarlı şifreleme yöntemi kullanmaktadır. İlk olarak, bir ağ bağlantısına şifre koymak için otomatik olarak oluşturulan özel ve genel anahtar çiftleri kullanılır; ardından oturumu açmak için parola kimlik doğrulaması yapılır.

Bir diğer güvenli ağ yöntemi, kimlik doğrulama işlemi gerçekleştirmek için, kullanıcıların parola veya kullanıcı adlarını belirtmeden oturum açmalarına olanak sağlayan, el ile oluşturulmuş bir ortak özel anahtar çifti kullanılmasıdır. Bu senaryoda, her birey farklı bir anahtar çifti oluşturabilir. Açık anahtarlar, eşleşen gizli anahtarın sahibine erişmesi gereken tüm bilgisayarlarla çevrilir. Özel anahtarlar ise yalnızca sahibi tarafından tutulur. Kimlik doğrulama, özel anahtarlara dayanır; kimlik doğrulama sırasında anahtarın kendisi ağ üzerinden aktarılmamaktadır. Bu protokol yalnızca ortak anahtarın sahip olup olmadığını doğrular.

SSH Kimlik Doğrulama Yöntemi

SSH, anahtarın sağladığı güvenli işlemleri simetrik şifreleme yoluyla elde eder. Bu yöntem, güvenli iletişim için bağlantıları şifresini çözmek için anahtarlar kullanır. Bu işlemde açık anahtar şifrelemesi de kullanılır.

SSH protokolü iki tip anahtar kullanır: özel anahtar ve genel anahtar. İstenen özel anahtara sahip kullanıcı, genel anahtar ile sisteme erişim sağlar. Özel anahtarları ise şifrelenmiş belgenin şifresini çözmek için kullanılır. Genel ve özel anahtarlar matematiksel olarak birbirleriyle ilişkilidir, ancak ikisi de birbirinden türetilemez.

Kimlik doğrulama işlemi sırasında, kullanıcı SSH istemcisini başlatır. SSH sunucusu, istemcilerin erişim izni talebini aldığında, belirli bir veri şifreleyerek istemciye gönderir. Eğer istemci bu veriyi doğru bir şekilde çözer ve sonuç iletirse, erişim hakkı kazanmış olur.

SSH Anahtarlarının Üretilmesi ve Avantajları

Protokol, erişim sırasında tam koruma sağlamak için anahtar çifti kullanır. Bu anahtarlar, sistem öncesi tarafından manuel veya sertifika yönetim sistemi tarafından otomatik olarak üretilebilen genel ve özel anahtarlar olarak adlandırılmaktadır.

Otomatik sertifika yönetimi, benzersiz halkayı dinlemek için matematiksel olarak ilişkili genel verici anahtar oluşturmak için kullanılmaktadır. Şifrelenmiş bu anahtar çifti, kuruluşların kritik yapılarına erişmek için kullanılmaktadır. Sistem tarafından üretilen bu anahtarlar, güvenli bir şekilde tutulur ve ağ üzerinden iletilmezler.

Üretilmesinin Kolay Olması:
SSH anahtarları, sertifika yönetim sistemi veya sistem ölçüsü tarafından üretilebilir. Üretilen bu anahtarın sistemde son kullanım tarihi yoktur ve gerektiği zaman dosyalar üzerinde saklanabilir.

Giriş ve Kimlik Bilgilerini Korumak:
Kullanıcı, uzak sisteme erişmek için oturum açma ve kimlik bilgilerini kullanır. Ancak, kullanıcı adı ve parolalar gibi veriler internet üzerinden düz metin olarak iletilmektedir. Bu sebepten dolayı güvenlik açıkları meydana gelebilir. SSH anahtarları sayesinde, internet üzerinden oturum açmak için şifrelenmiş anahtarlar kullanılır. Bu sebepten dolayı anahtarlı kimlik doğrulama, geleneksel kimlik doğrulama yöntemlerine göre daha güvenlidir.

Kullanıcılar Arasında Güvenilir İletişim:
Bu anahtarlar, kullanıcılar veya sistemler arasındaki iletişimi şifrelemek için bir şifreleme tekniği kullanır. Bu anahtarlar, gönderilen mesajı şifrelemek ve alıcıya gelen şifreli mesajı çözmek için kullanılır. Bu sayede, ağa giren mesaj şifrelenmiş olur ve üçüncü taraf kişiler tarafından erişilmesi engellenir.

Uzaktan Komutun Güvenli Yürütülmesi:
Sistem yöneticisinin, ağda bulunan başka bir cihaz üzerinde aynı komutu çalıştırması gerektiğinde, uzaktan komutlar sayesinde bu işlem gerçekleştirilebilir.

Kullanıcı Kolaylığı:
Kullanıcılar birden fazla hesaba sahip olduğunda, her hesabın kullanıcı adı ve parolasını hatırlamak zor bir durum haline gelebilir. Anahtarlar sayesinde, kullanıcılar bu bilgileri hatırlamak zorunda kalmaz ve hesaplarına daha kolay erişim sağlarlar.

Seçili Kullanıcı İçin İstenilen Fonksiyonu Seçmek:
Kullanıcı, belirli bir işlem gerçekleştirmek veya belirli bir şey yapmak için hesabını başka bir kullanıcıya devredebilir. Bu işlemde, belirli bir anahtar kullanılabilir ve yalnızca bu anahtar, belirlenen işlemi yapmak için kullanılabilir; başka işlemleri gerçekleştiremez.

Güvenli Port Yönlendirme:
Port yönlendirme sayesinde, uzak bilgisayarlar özel ağ üzerinden belirli cihazlara veya hizmetlere bağlanmak için bir porttan diğerine aktarılabilir. Kullanıcı, protokol üzerinden oturum açtığında güvenli şifreli özellikler kullanarak sisteme erişir.

Güvenliği Genel Anahtar ve Özel Anahtarlar Sağlar:
Protokolde kullanılan anahtarlar, özel olarak matematiksel işlemlerle üretilir ve bu anahtarları çözmek çok zordur. Genel anahtarlar mesajları şifrelemek için, özel anahtarlar ise şifreyi çözmek için kullanılır. Ancak iki anahtar da birbirinden türetilemez. Bu sayede daha güvenli bir iletişim sağlanır.

Ayrıca, birden fazla anahtar türü bulunmaktadır.

- **RSA:**
  En eski açık anahtarlı şifreleme sistemidir. Kullanım alanı genellikle verileri güvenli bir şekilde iletmektir. Büyük anahtarları çözmek için ilgili teknikler kullanılmadan dolayı yavaş çalışmaktadırlar. Genellikle toplu şifreleme ve şifre çözme işlemleri için kullanılır. Bu anahtar tipi, çok büyük asal sayılar işlenerek üretilmektedir. Gelecekte, bu asal algoritmaların kırılma olasılığı bulunmaktadır.

- **DSA:**
  Bir dijital imza algoritmasıdır. Mesajın kaynağını göndereni ve gerçek doğasını doğrulamak için kullanılır. Ayrıca spam mesajlarını tespit etmek için de kullanılır. Genel ve özel anahtarlar karmaşık bir matematiksel işlem kullanılarak oluşturulur. Özel anahtar, genel anahtar sayesinde dijital imzayı geliştirir.

- **ECDSA:**
  Şifreleme işlemlerinin daha zor olması için eliptik eğriler kullanan bir dijital imza algoritmasıdır. Bu, daha kısa anahtar uzunlugu ile daha güvenli anahtarlar sağlar. Çoğu SSH genel olarak bu anahtar tipini kullanmaktadır.

SSH Anahtarlarının Kullanımları

Anahtarlar sayesinde karmaşık şifrelerden kaçınılır ve kullanıcılar kolayca erişim sağlar. Kuruluşlar, anahtarları aşağıdaki amaçlar için kullanmaktadır:

- Yerel makinelere ve uzaktaki bilgisayarlara arasında güvenli bir iletişim sağlamak.
- Uzaktan yönetim görevlerini güvenli bir şekilde tamamlamak.
- SSH, işlemleri güvenli bir şekilde gerçekleştirmek için otomatik olarak bağlanır; işlemli eşitlikleri yüklemeleri ve benzeri işlemleri içerir.
- SSH anahtarları parola kullanmadan birden fazla hesaba kolayca giriş yapma ve tek bir yerden oturum açma sağlar.
- SSH, veritabanları için güvenli bir kimlik doğrulama süresi sağlar.

SSH Anahtar Yönetimi

Anahtarların asıl amacı güvenliği sağlamaktır. Kuruluşlar, bir kaynağa erişmek için binlerce, hatta milyonlarca anahtar kullanabilir. Bu sebepten dolayı, anahtarların düzgün bir biçimde yönetilmesi, kuruluşların işlevlerini sürdürebilmesi için çok önemlidir.

Anahtarların düzenli bakımı, kuruluşun güvenliğini sağlar. Anahtar kaybı ve yanlış yönetimi nedeniyle ortaya çıkabilecek tehlikeler, Siber saldırganlar için bir kapı açabilir. Bu durum, kuruluşun itibarını zedeleyebilir.

Güvenlik açıklarının temel nedeni, anahtarların yanlış yönetilmesinden kaynaklanmaktadır. Yanlış yönetilen anahtarlar, kuruluşu siber saldırılara açık hale getirebilir. Aşağıda anahtar yönetimine dair bazı maddeler yer almaktadır:

- Bulunan tüm anahtarlar kullanım amaçlarıyla tanımlanmalıdır.
- Anahtarlar gereksinimlere bağlı olarak üretilebilir, saklanabilir ve iptal edilebilir.
- Uygunsuz anahtar yönetimi nedeniyle ortaya çıkan sorunlar ortadan kaldırılmalıdır.
- Güvenliği sağlamak adına yenilenen veya yetkilendirilmemiş anahtarlar erken aşamalarda belirlenmeli ve silinmelidir.
- İstenmeyen anahtar kullanımı not edilerek tehditler engellenmelidir.

SSH ANAHTARI YÖNETİMİNİN ZORLUKLARI

Her SSH anahtarı farklı amaçlar için üretilmektedir. Kurumların veya kuruluşların üretkenliğini ve güvenliğini artırmak için bu anahtarları yönetmesi gerekmektedir. Ancak, anahtarların uygunsuz yönetimi sonucu çeşitli riskler ve zorluklar ortaya çıkmaktadır. Aşağıda anahtar yönetiminde karşılaşılan bazı zorluklar maddeler halinde verilmiştir:

1. **Merkezi Kontrolün Olmaması**
   Kuruluşun anahtarlarını üretme ve dağıtımı üzerinde merkezi bir kontrolün olmaması, anahtar yönetimi üzerindeki kontrolünü kaybetmesine sebep olur. Bu durum, kullanıcıların anahtarları kolayca üretebileceği veya çoğaltabileceği anlamına gelir. Üretilen bu anahtarlar sayesinde kullanıcılar, kuruluşun yetkili verilerine ve sistemlerine erişebilmektedir.
2. **Etkin Olmayan Kullanıcının Etkin Anahtarları**
   SSH anahtarları zaman içerisinde riski artıran bir şekilde sona ermemektedir. Örneğin, bir kullanıcı şirketten ayrıldığında, kullanıcı hesabı etkin kalabilir ve hesapla ilişkili anahtar ağda kalabilir. Çalışan şirketten ayrılmasına rağmen, bu anahtarlar, kaynağa erişim sağlayabilir ve verilerle zarar verebilir. Bu durum, güvenlik sorunlarına yol açabilir.
3. **Yetim Anahtarlar**
   Çalışma işlevlerine dair olmayan anahtarlara "yetim anahtar" denir. Bu anahtarlar kaybolan veya etkin olmayan kullanıcılar tarafından bırakılan anahtarlardır. Yetim

anahtarlarının amacını bilmeyen yöneticiler, bu anahtarları reddederek kritik sisteme erişimin engellenmesini sağlayabilirler.

4. **Anahtar Uzlaşması**
   Anahtar ihlali, saldırganların hem genel hem de özel anahtarları ele geçirmesi durumudur. Eğer bir saldırgan ağa girerse, kuruluş için tehdit oluşturan diğer kaynaklara da erişim sağlayabilir.
5. **Anahtar Yayılımı**
   Anahtar yayılımı, anahtarların sayısının katlanarak arttığı durumlarda meydana gelir. İstenmeyen kişilerin bu anahtarlara erişmesi, ciddi güvenlik sorunlarına yol açabilir.
6. **Yorucu Manuel İşlemler**
   Anahtarların tanımlı bir model olarak yapılması, oldukça sıkıcı ve zaman alıcı bir süreçtir. Verimli bir iş akışı elde etmek için bu aşamaların otomatikleştirilmesi gerekmektedir.

SSH ANAHTAR TEHLİKESİNİN ETKİLERİ

Kuruluşlar genellikle güvenli bir çalışma ortamı oluşturmak için SSH protokolünü kullanmaktadır. Bu protokoldeki anahtarlar, kritik kuruluş altyapısına bir ağ geçidi görevi görmektedir. Anahtarların yönetimi, güvenli bir çalışma ortamı sağlamak için zorunlu hale gelmektedir. Anahtarların kaybı veya yanlış yönetilmesi, kuruluşlar üzerinde ciddi etkilere yol açabilir. Bu gibi durumlarda gerçekleşebilecek senaryolar aşağıda sırasıyla verilmiştir:

1. **Sistem Kaynaklarına Etkisiz Erişim ve Hassas Bilgilerin İfşası**
   Anahtarların kaybı, yetkisiz kişilerin sisteme erişmesine ve hassas bilgilerin ifşasına yol açabilir.
2. **Kötü Amaçlı Yazılımlar**
   Erişim izni olmayan taraflar, kuruluşun tüm işlemlerini bozacak şekilde kötü amaçlı yazılımlar sunabilir.
3. **Anahtarın Diğer Hedef Kaynaklara Erişimi**
   Bir anahtar, başka hedef kaynaklarına erişim sağlamaya olanak tanıyabilir.
4. **E-posta Güvenliğinin İhlali**
   Anahtar kaybı, e-posta güvenliğini ihlal edebilir ve hassas verilerin sızmasına neden olabilir.
5. **Kaybedilen Veriler ve İşletme İtibarı**
   Kaybedilen veriler, işletme itibarının düşmesine sebep olabilir.
6. **Müşteri Verilerinin İfşası**
   Müşteri verilerinin ifşası, kullanıcılar arasında güven problemlerine yol açabilir.
7. **Para Cezaları**
   Kuruluşta oluşabilecek veri sızıntıları, büyük para cezaları ile sonuçlanabilir.
8. **Kritik Veri Kaynaklarına Erişimin Kısıtlanması**
   Erişim izni olan kullanıcılar, hata mesajlarıyla karşılaşarak kritik verilere erişemeyebilir.

TEMEL WEB KAVRAMLARI

URL

Açılımı Uniform Resource Locator olan URL, internette bir kaynağı tanımlamak için kullanılan karakter dizisidir. URL'ler üç ana bileşen altında incelenmektedir.

- **Protokol**: Web sitesine nasıl bağlanılacağını belirler.
- **Alan adı**: Web sitesinin adı veya adresidir; kullanıcıların siteyi bulmasını sağlar.
- **Yol**: Alan adından sonra gelen ve web sitesinin içindeki başka bir yeri ifade eden kısımdır.

URL'ler genellikle web sitelerinin www ile başlayan adresler olarak düşünülebilmektedir.

REQUEST

Türkçe karşılığı "istek" anlamına gelmektedir. Genellikle istemci tarafından sunucuya gönderilmektedir ve HTTP protokolünde kullanılmaktadır. Web sitesi sonucu olan herhangi bir bilgi istendiğinde, istemci sunucuya bir istek yollar, sunucu da buna karşılık olarak bir dönüt döndürmektedir.

Bileşenler

- **Başlık**: İstek hakkındaki temel bilgileri taşımaktadır. Örnek olarak, isteğin hangi işletim sisteminden geldiği gibi bilgiler olabilir.
- **Gövde:** Sunucudan istenilen veri hakkındaki detaylar bu bölümde yer almaktadır. Gönderilecek veri bu kısımda bulunmaktadır.

RESPONSE

HTTP protokolünden istemciden gelen istek doğrultusunda sunucunun istemciye yanıtı anlamına gelmektedir. Genellikle isteğe uygun bilgiler içermektedir.

Bileşenler

- **Başlık**: Yanıt hakkındaki meta bilgilerini taşımaktadır.
- **Durum Kodu**: Yanıtın durumunu belirtmek için kullanılmaktadır.
- **Gövde**: Sunucudan dönen asıl istenilen veri bu bölümde tutulmaktadır.

BLOCKCHAİN

Blok Zinciri Teknolojisi: Temelleri ve İşleyişi

Türkçeye blok zinciri olarak çevrilmektedir. İlk olarak 1980'ler ile 1990'larda ortaya çıkmış, özellikle dijital belgelerin tarihlerinin değiştirilmesini engellemek amacıyla geliştirilmiştir. Bu teknoloji, Haber ve Stornetta tarafından dijital belgelerin zaman damgalarını değiştirilmesini engellemek için önerilmiştir. 2008 yılında Bitcoin'in icadıyla, Nakamoto tarafından BlockChain olarak tanıtılmıştır.

Bitcoin'in ardından, blok zinciri teknolojisi kripto paralarla birlikte daha geniş bir kullanım alanına sahip olmuş ve gelişimini sürdürmüştür. Kısacası, blok zincirinin ilk çıkış sebebi, dijital belgelerin tarih değiştirmesini engellemeye yönelikken, 2008'de sanal paralarla birlikte daha yaygın bir kullanım alanı bulmuş ve günümüzde birçok sektörde kullanılmaktadır.

Blok Zincirinin Temel Yapısı

Blok zinciri, adından da anlaşılacağı gibi bloklardan oluşmaktadır.

Bloklar:

Blok zincirindeki her bir blok, belirli unsurları içerir. Bunlar sırasıyla:

- **Veri:** Blok içinde depolanan asıl bilgi anlamına gelmektedir.
- **Parmak İzi:** Her blok, kendine özgü bir hash ile şifrelenmektedir.
- **Önceki Bloğa Ait Bazı Bilgiler ve Önceki Bloğun Parmak İzi:** Bloklar, zincir halinde birbirine bağlanırken, her blok bir önceki bloğun bilgilerini ve parmak izini içermektedir.
- **Zaman Damgası:** Blokların ne zaman oluşturulduğunu gösteren zaman damgasıdır.

Her bloğun içindeki veriler şifrelenir. Bu, veriye doğrudan erişimin imkansız hale gelmesini sağlar.

Blok Zinciri:

Blok zinciri, blokların birleşmesiyle oluşur. Bloklar, kronolojik olarak sıralanır ve her biri şifreli bir biçimde birbirine bağlanmaktadır. Bu bağlantılar sayesinde blok zinciri güvenli bir yapı oluşturmaktadır.

Blok Zinciri Sistemlerinin Özellikleri:

Blok zinciri teknolojisinin en büyük özelliklerinden biri, yalnızca tek bir bilgisayar üzerinden değil, birden fazla bilgisayar üzerinden çalışmasıdır. Bu, verinin manipüle edilmesini oldukça zorlaştırmaktadır.

Blok zincirindeki her veri, ağdaki tüm bilgisayarlara gönderilir. Blok zincirine yeni bir blok eklenmek istendiğinde, bu blok, tüm düğümler tarafından onaylandıktan sonra zincire eklenir. Bu süreç, Konsensüs Mekanizması olarak adlandırılmaktadır.

Veri Değişikliği Durumu:

Bir blok zincirindeki veriyi değiştirmek isterseniz, bunun ne olacağına bakalım. Her bloğun içeriği, önceki bloğun özetini ve parmak izini içermektedir. Bu nedenle, bir bloğun verisi değiştirildiğinde, bu değişiklik hemen bir sonraki blokta ve zincirin geri kalanında fark edilecektir. Bu da, verilerin değiştirilmesini neredeyse imkansız hale getirir ve güvenliği en üst düzeye çıkarır.

Blok Zinciri Sisteminin Avantajları ve Dezavantajları

Blok zinciri teknolojisinin pek çok avantajı bulunmakla birlikte, bazı dezavantajları da vardır.

Avantajlar:

- **Güvenlik:** Blok zinciri, verilerin manipüle edilmesini engelleyen güçlü şifreleme yöntemlerine dayanır.
- **Merkeziyetsizlik:** Veriler tek bir yerde değil, ağdaki birçok bilgisayar arasında dağılmıştır. Bu da merkezi bir kontrol yapısının olmaması anlamına gelmektedir.
- **Şeffaflık:** Tüm işlem detayları halka açık olup, işlem yapanlar anonim kalmaktadır.
- **Verimlilik ve Hız:** Blok zinciri, işlem doğrulama ve veri akışı açısından yüksek verimlilik ve hız sağlar.

Dezavantajlar:

- **Yüksek Enerji Tüketimi:** Şifreleme işlemleri ve yeni blok ekleme işlemleri, blok zincirinin yüksek enerji tüketimine neden olabilmektedir.
- **Ölçeklenebilirlik Sorunları:** Çok sayıda işlem yapılması durumunda, her düğümün onay süreci nedeniyle sistem yavaşlayabilir.
- **Yasal Durumlar:** Blok zincirinin yasal statüsü, dünya genelinde henüz tam olarak bilinmemektedir.

WEB HOSTİNG

Web sitelerinin internet üzerinden erişilebilir olması için kullanılan teknik altyapıyı sağlayan hizmetlere verilen isimdir. Bu hizmet, web sitesinin dosyalarını depolamak için bir sunucu üzerinde alan tahsis eder ve bu dosyaların internet kullanıcıları tarafından erişilebilmesini sağlar.

Temel anlamda 4 ana bileşeni bulunmaktadır:

1. **Sunucu Alanı**: Web sitesine ait dosyaların depolandığı birimdir.
2. **Bant Genişliği**: Web sitesinin kullanıcılara sunabileceği veri miktarını belirtir.
3. **IP Adresi**: Web sitesinin tanımlanmasını sağlamak için kullanılır.
4. **E-posta Hesapları**: Web siteleri ile ilişkilendirilmiş profesyonel e-posta hesaplarını belirtir.

Birden fazla türde web hosting bulunmaktadır.

SEO

Türkçe karşılığı arama motoru optimizasyonu anlamına gelmektedir. Bu özellik, web sitelerinin arama motorlarında daha yüksek sıralamalarda yer almasını sağlamak amacıyla kullanılmaktadır. Teknik ve içerik odaklı çalışmaktadır. Bu özelliğin amacı, ücretsiz trafik elde etmek için arama motorlarının algoritmalarını ve kullanıcı davranışlarını anlayarak web sitelerinin optimize edilmesini sağlamaktır.

Arama motoru optimizasyonunun başlıca unsurları şu şekildedir:

- Kullanıcıların arama motorunda aradığı terimleri belirleyerek bu anahtar kelimeleri web sitesinin içeriğine entegre etmek.
- Sayfa içi ve sayfa dışı optimizasyon çalışmaları yapmak.
- Teknik açıdan web sitesinin altyapısının yerleştirilmesi, site hızının artırılması ve benzeri işlemler için düzenlemelerin yapılması.
- Kullanıcılara özgü içerikler üretmek amacıyla kullanılır.

PORTLAR

Web'de kullanılan portlar, internet üzerinden veri iletimi ve iletişimini sağlamak için kullanılmaktadır. Bazı portlar, belirli protokollerle bağlantılıdır. Portlar sayesinde internet üzerinden veri iletimi ve iletişimi kolaylaşmaktadır. Güvenlik açısından gereksiz portların kapatılması önerilmektedir. Aşağıda bazı protokollerin kullandığı portlar verilmiştir:

- **Port 25**: SMTP protokolünün kullandığı porttur.
- **Port 80**: HTTP protokolünün kullandığı porttur.

SEMANTİK WEB

Semantik Web Nedir

Semantik Web, İnternet üzerindeki verilerin daha anlamlı, organize ve makineler tarafından anlaşılabilir bir şekilde sunulmasını amaçlayan kavrama verilen isimdir. Tim Berners-Lee'nin liderliğinde geliştirilmiştir. Semantik Web, verilerin sadece insanlar tarafından değil, aynı zamanda makineler ve yazılımlar tarafından da anlamlı bir şekilde kullanılmasını hedeflemektedir. Bu sayede, İnternet üzerindeki bilgi daha verimli bir şekilde işlenebilmektedir.

Semantik Web'in Temel Amaçları

Semantik Web'in temel amacı, web üzerinde yer alan verilerin makineler tarafından daha iyi anlaşılabilmesini sağlamaktır. Semantik Web, bilgileri makinaların da anlayabileceği bir forma dönüştürerek, arama motorlarının ve diğer uygulamaların daha hassas, doğru ve verimli sonuçlar sunmasını mümkün kılmaktadır.

Semantik Web, kullanıcının doğru bilgiyi daha hızlı ve doğru şekilde alabilmesi için verileri ilişkili hale getiren teknolojilere dayanmaktadır. İnternetteki veriler büyük veri olarak adlandırılmaktadır ve bu verilerin organize edilmesi, sorgulanması ve işlenmesi semantik web sayesinde olmaktadır.

Semantik Web'in Temel Bileşenleri

RDF: Açılımı Resource Description Framework anlamına gelmektedir, web üzerindeki verileri yapılandırmak ve ilişkilendirmek için kullanılan bir modeldir. RDF, kaynakları tanımlar ve bunları birbirleriyle ilişkilendirmek için kullanılmaktadır. Bu modelde veriler üçlü formatında sunulmaktadır.

OWL : Açılımı Web Ontology Language anlamına gelmektedir, verileri daha derinlemesine tanımlamak ve birbirleriyle ilişkilerini daha ayrıntılı bir şekilde ifade etmek için kullanılan bir dildir. RDF, genellikle veri tanımlamak için kullanılırken, OWL bu veriler arasındaki ilişkileri daha soyut ve anlamlı hale getirmeyi amaçlar.

SPARQL: SPARQL, RDF veritabanlarında sorgulama yapabilmek için kullanılan bir dil ve protokoldür. SPARQL sayesinde, makineler web üzerindeki yapılandırılmış verileri sorgulayarak, kullanıcıların ihtiyaç duyduğu bilgiyi hızlı ve doğru bir şekilde alabilmektedir.

URI : URI, bir kaynağı tanımlamak için kullanılan bir adresleme sistemidir. Semantik Web'deki her şeyin bir URI ile tanımlanması, verilerin birbirleriyle olan bağlantılarının belirlenmesini ve anlaşılmasını kolaylaştırmaktadır.

Semantik Web'in Faydaları

Semantik Web'in bazı faydaları aşağıda yer almaktadır.

Daha İyi Arama Sonuçları: Semantik Web, arama motorlarının sadece anahtar kelimelerle değil, verilerin anlamını anlayarak sonuçları daha hassas bir şekilde listelemelerine olanak tanımaktadır. Bu, özellikle kullanıcının ne istediğini daha doğru anlaşılır ve kullanıcıya daha anlamlı içerik sunulabilmektedir.

Otomatik Veri Anlamlandırma ve İşleme: Semantik Web, makinelerin veriyi sadece depolamak yerine, veriyi anlamalarına, yorumlamalarına olanak tanımaktadır. Örneğin, bir e-ticaret sitesinin ürün veritabanı, semantik web sayesinde ürün özellikleri ve ilişkili bilgileri otomatik olarak analiz edilebilmektedir.

Gelişmiş Veri Entegrasyonu: Farklı web siteleri ve uygulamalar arasında verilerin entegrasyonu semantik web ile daha kolay hale gelmektedir. Veriler, daha önce tanımlı ontolojiler ve RDF kullanılarak ilişkilendirilebilir, böylece farklı veri kaynakları arasında veri paylaşımı yapılabilmektedir.

Gelişmiş Kullanıcı Deneyimi: Semantik Web, kullanıcıların ihtiyaç duydukları bilgilere daha hızlı ve doğru bir şekilde ulaşmasını sağlamaktadır.

Semantik Web’in Uygulama Alanları

Semantik Web’in uygulama alanları aşağıda yer almaktadır.

Sağlık: Semantik Web, sağlık verilerini daha etkili bir şekilde organize ederek, hasta bilgilerinin hızlı bir şekilde paylaşılmasını ve analiz edilmesini sağlamaktadır.

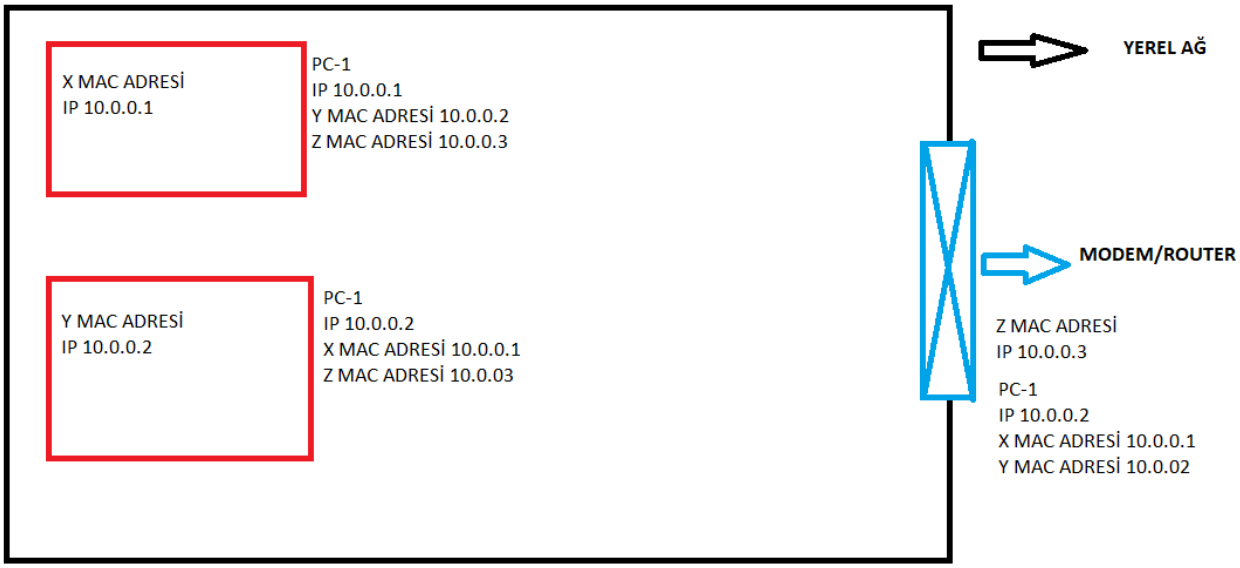
E-Ticaret: E-ticaret siteleri, semantik web teknolojilerini kullanarak ürün ve kullanıcı verilerini daha verimli bir şekilde organize edebilmektedir ve bu sayede daha uygun önermeler yapabilmektedir.

WEB NASIL ÇALIŞIR

En temel anlamda web'in çalışması HTTP istekleri üzerinden gerçekleşmektedir. Bir web sitesine girilmek istendiğinde üç farklı konumda bazı işlemler gerçekleşmektedir. İlk kısım yerel ağ kısmıdır. Ağda bulunan cihazlar, uzakta bulunan web sunucuları ile iletişime geçmek için internet ağını kullanmaktadırlar. Temel mantıkta, yerel ağda bulunan cihaz, modem üzerinden internete bağlanır. İnternet ağı ise gidilmek istenilen URL'yi DNS sayesinde IP adreslerine çevirir. IP adreslerine çevrilen web siteleri, TCP/IP protokolleri ile haberleşebilmektedir. TCP/IP protokolünün üzerine kurulmuş HTTP protokolü ile iletişim sağlanmaktadır.

İLK KISIM: YEREL AĞ

Yerel ağ, bu modelde web sitelerine erişmek isteyen bilgisayarların bulunduğu ağlara verilen isimdir. Bu ağ içinde bazı iletişim protokolleri, adresleme protokolleri ve benzeri işlemler gerçekleştirmektedir. Aşağıda yerel ağa ait bir şablon yer almaktadır.



Yerel ağ kısmında kullanıcı bilgisayarları ve modem veya router'lar bulunmaktadır. İlk olarak, DHCP protokolü ile ağ içinde bulunan bir cihaz, modeme IP adresi istediğine dair bir broadcast yayını yapmaktadır. Sonrasında modem veya router, bu çağrıya karşılık olarak IP adresi isteyen cihaza uygun olan IP adresini tanımlamaktadır. Aynı şekilde, ağda bulunan başka bir cihaz da IP adresi isteğinde bulunduğunda, modem otomatik olarak protokol ile o cihaza da bir IP adresi atamaktadır. Bu IP adresleri sayesinde iletişim sağlanmaktadır.

İletişimin Sağlanması ve ARP Protokolü

Bu iletişimin sağlanabilmesi için, ilk olarak ağda bulunan tüm cihazların birbirlerini tanımaları gerekmektedir. Bu tanıma işlemi, ARP protokolü adı verilen bir protokol ile gerçekleştirilmektedir. İlk olarak, iletişim kurmak isteyen cihaz, üzerinde tüm herkesin

bildiriyi alabileceği bir şekilde, belirlenen cihazla iletişim kurmak istediğini belirtmektedir. Sonrasında iletişim kurulmak istenilen cihaz, aldığı bildiri sonucunda kendisi ile iletişim kurmak isteyen cihazla iletişim haline geçmektedir. Bu iletişim işlemleri için ise ARP tablosu kullanılmaktadır.

ARP tablosu, daha önce iletişime geçilmiş veya ağda kendini tanıtmış cihazların bilgilerini tutan bir tablodur. Ağda bulunan her cihaz, kendi üzerinde bu IP adreslerini ve fiziksel adreslerini kaydederek bu tabloyu oluşturur. Özetlemek gerekirse, ilk başta iletişim kurulmak istenilen cihaz kendini tanıtmaktadır. Tanıtıldıktan sonra, cihazlar tarafından bu cihazın bilgileri bir tabloya kaydedilmektedir. Bu sayede, cihazlar arasında tekrar iletişim kurmak istendiğinde, cihazın kendini tekrar tanıtmasına gerek kalmaz.

Gerçek Hayat Örneği

Gerçek hayatta bu durumu şu şekilde açıklayabiliriz: Ahmet, Mehmet ve Samet'in bulunduğu bir grubu düşünelim. Bu kişiler birbirini tanımamaktadırlar. Ahmet, grup içerisinde "Ben Mehmet'le konuşmak istiyorum" şeklinde bir cümle kurar. Sonrasında, Mehmet Ahmet'in yanına gelip "Ben Mehmet'im" diyerek kendini tanıtır. Bu sayede, grup içinde Ahmet ve Samet, Mehmet'i tanımış olur. Bu tanıma sayesinde, bundan sonra Ahmet, Mehmet ile konuşmak istediğinde, "Ben Mehmet'le konuşmak istiyorum" diye bir cümle kurmak yerine doğrudan Mehmet'in yanına gidip konuşabilir. Aynı şekilde, Samet de Ahmet ve Mehmet'in birbirlerini tanıması ve aracılık etmesi sebebiyle, her ikisini de tanımaktadır. Özetle, ilk başta bir kişi, tüm grubun bildiği şekilde birileriyle konuşmak isteyebilir. Sonrasında tüm grup birbirini tanır ve bu tanıma işlemi, ağdaki cihazlar arasında da gerçekleşir.

ARP Protokolü ve ARP Tablosu

Ağda gerçekleşen bu işlem ARP protokolü olarak adlandırılmaktadır ve cihazlar, kendi üzerlerinde tanıdıkları cihazlara dair bilgileri ARP tablosu adı verilen bir tabloda tutmaktadır. Bu sayede, tekrardan iletişime geçilmek istendiğinde, tablo üzerinden iletişime geçilmek istenilen cihazın bilgileri doğrultusunda iletişim sağlanabilir. Bu protokol ile ağda bulunan cihazların birbirleriyle aynı ağda olmalarını tanımlayan alt ağ maskelerine de ihtiyaçları vardır.

Yerel Ağdan İnternete Bağlantı

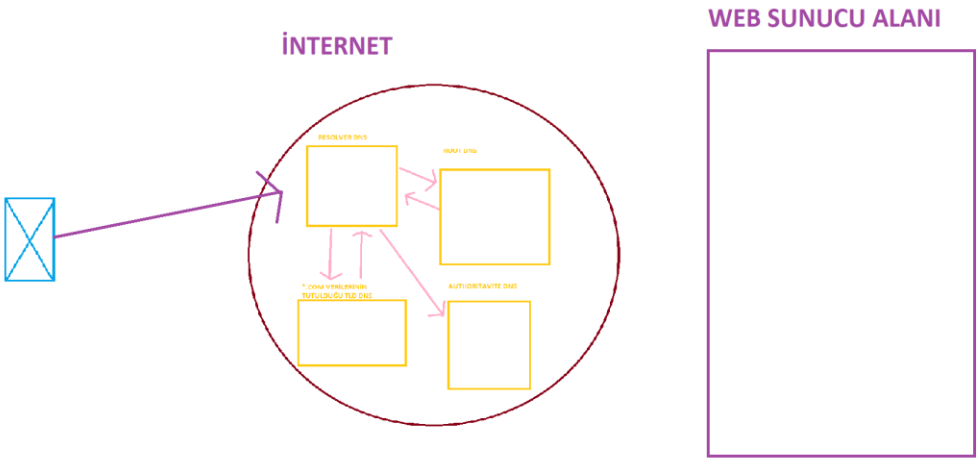
Yerel ağdan internet ağına bağlanmak isteyen her cihaz, gateway (geçit) ile internete bağlanmaktadır. NAT (Network Address Translation) adı verilen bir işlem sayesinde, internete bağlanan yerel ağ cihazları tek bir IP adresi üzerinden çalışmaktadır. Bunun sebebi, dünya üzerinde tüm cihazları karşılayacak IP adreslerinin bulunmamasıdır. NAT işlemi, yerel ağdaki cihazların, internetteki tek bir IP adresi üzerinden iletişim kurmalarını sağlar ve bu sayede IP adreslerinin verimli kullanılması sağlanır.

İKİNCİ KISIM: İNTERNET AĞI

İnternet ağları, iletişim kurulmak istenilen web sitesinin alan adını IP adresine çevirmek için kullanılmaktadır. Bu işlem DNS sayesinde gerçekleştirilir. Ancak bu işlemden önce, bilgisayar üzerindeki host dosyasına bakılmaktadır. Host dosyasında, daha önce ziyaret edilen web sitelerinin IP karşılıkları tutulmaktadır. Yani, bir web sitesinin IP adresi çözümlenmeden önce ilk olarak bilgisayar üzerinde bulunan host dosyasına bakılır. Eğer host dosyasında, web sitesine ait IP adresi bulunuyorsa, IP adresi çözümlenmeden doğrudan iletişim sağlanır. Eğer web sitesinin IP adresi host dosyasında bulunmuyorsa, DNS kullanılır. DNS, bilgisayar ilk açıldığı andan itibaren DHCP ile tanımlanır.

İlk olarak yerel ağda bulunan cihaz, DNS sunucusu ile iletişime geçmektedir. Bu iletişim, UDP protokolü aracılığıyla sağlanır ve 53 numaralı port üzerinden gerçekleşir. Yerel ağdaki cihaz, DNS sunucusunun bu portuna, web sitesinin IP adresini öğrenmek için bir soru gönderir. İlk sorgulanan DNS sunucusu, Resolver DNS olarak adlandırılır. Eğer bu DNS sunucusu, verilen web sitesinin IP adresini bilmiyorsa, başka bir DNS sunucusuna verilen web sitesinin IP adresinin bilinip bilinmediği sorulmaktadır. Bu ikinci DNS sunucularına Root DNS denir. Eğer bu DNS sunucusu da verilen adresi bilmiyorsa, isteği başka bir DNS sunucusuna yönlendirir. Yönlendirilen DNS sunucusunun tek amacı, "*.com" adreslerinin IP adresi karşılıklarını bilmektir. Eğer bu DNS sunucusu da verilen web sitesinin IP karşılığını bilmiyorsa, tüm kayıtların tutulduğu web sitesinin DNS sunucusuna yönlendirilir. Bu DNS sunucusuna Authoritative DNS sunucusu denir. Bu sunucunun tek görevi, verilen web sitesine ait taleplerin cevaplarını döndürmektir. Önemli bir konu ise, bu sunucunun sadece verilen web sitesine ait talepleri çözümlemesi gerektiğidir; başka bir domainin çözümlemesi yapılmamalıdır. Aynı işlemlerin tekrar edilmemesi için, çözümlenen web sitesi adresi belirli bir süre bellekte tutulur. Bu sayede, aynı işlem tekrar gerçekleşmez.

Aşağıda bu işlemlerin çalışma sırasıyla ilgili bir şema bulunmaktadır.



Bu işlemler gerçekleştirildikten sonra, verilen web sitesinin IP adresi alınmış olur. Adımlar halinde ilerlediğimizde, şu an yerel ağda bulunan bir bilgisayar çıkış kapısını kullanarak modem üzerinden internete ulaşmıştır. İnternete ulaştıktan sonra, DNS sunucuları sayesinde gitmek istenilen web sitesine ait IP adresi bulunmuştur. Bulunan IP adresinden sonra, belli başlı protokoller çerçevesinde iletişim başlamaktadır.

İletişim, TCP Protokolü ile gerçekleşmektedir. Bir TCP paketinin başlığı 4'e bölündüğünde; gideceği konumun IP adresi, gideceği konumun port numarası, kendine ait IP adresi ve kendine ait işletim sistemi tarafından rastgele atanan bir port bulunmaktadır. Gideceği web sitesinin IP adresi ve ulaşacağı port statik değerlerdir; değişime uğramazlar. Çıkış yapılan port ise dinamik olarak verilir ve işletim sistemi tarafından değiştirilebilir. Çıkış yapan IP adresi ise, daha önce bahsedilen NAT kavramı sayesinde tek bir IP adresidir. Modem, bu IP adresini rastgele bir şekilde atar ve o ağda bulunan tüm cihazlar bu IP adresi üzerinden ağla iletişim kurar.

İlk olarak, internet kısmında DNS sunucuları ile bulunan IP adresleri ve ağda bulunan IP adresleri arasında TCP Protokolü'nün üç aşamalı el sıkışma işlemi gerçekleşir. İlk olarak istemci, sunucuya SYN adı verilen bir paket gönderir. Sunucu, SYN paketini aldıktan sonra SYN+ACK paketini tekrar istemciye geri yollar. İstemci, alınan bu paket sonrasında ACK ismi verilen bir paketle sunucuya geri dönüş yapar ve el sıkışma işlemi tamamlanmış olur. Bu sürecin yapılmasının asıl amacı, istemci ve sunucunun birbirini tanımasını sağlamaktır. Aynı zamanda bu yöntem sayesinde bazı siber saldırılar engellenebilir.

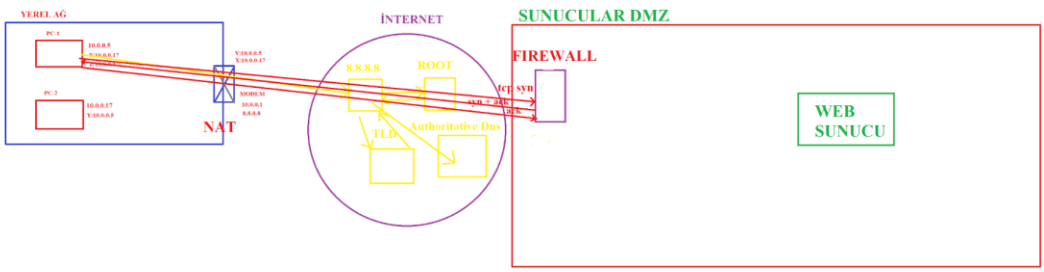
Üçlü el sıkışmanın gerçek hayattan bir örneği şu şekilde işler: Kerem, Mert'e "Seninle konuşmak istiyorum" başlığında bir söz söyler. Bu, TCP protokolünün ilk aşaması olan SYN paketinin gerçek hayattaki karşılığıdır. Sonrasında Mert, Kerem'e "Benimle konuşmak istediğini duydum ve ben de konuşmak için müsaitim" başlığında bir cümle kurar. Bu durum, TCP protokolünde SYN+ACK paketi olarak adlandırılır. Son olarak, Kerem, Mert'e "Ben seninle konuşmak istediğimi iletmiştim, sen de benimle konuşmak için müsait olduğunu ilettin. Artık konuşabiliriz" başlığında bir cümle kurar. Bu durum, TCP protokolünde ACK paketi olarak adlandırılır. Bu üç aşamalı el sıkışma sayesinde, istemci ve sunucu birbirini tanıyabilir.

Bu aşamalardan sonra, HTTP Protokolü devreye girer. Bu protokol, temel olarak istek ve dönüt mantığıyla çalışır. İstek ve dönüt paketleri, TCP katmanında çok sayıda paketin iletişimi sayesinde gerçekleşir. Şu ana kadar yapılan işlemler sırasıyla; yerel ağda bulunan bir cihaza DHCP Protokolü ile IP adresi atanmıştır. Sonrasında ARP Protokolü ile yerel ağdaki cihazlar birbirini tanımaktadır. Ardından çıkış kapısı sayesinde yerel ağda bulunan bir cihaz, NAT teknolojisi sayesinde internetle iletişim kurabilmektedir. İnternetle iletişim kurulduktan sonra, DNS sunucuları gidilmek istenilen web sitesinin IP adresi çözümlemesini gerçekleştirir. Bu çözümleme sonrasında, TCP Protokolü ile üç adımlı el sıkışma işlemi yapılır ve sonrasında HTTP istekleri başlar.

ÜÇÜNCÜ KISIM: WEB SUNUCU ALANI

FIREWALL

Web sunucularında her bir işlem için ayrı birimler bulunmaktadır. Firewall'lar bu cihazlar arasında yer almaktadır. Web sunucusu ile kurulan tüm iletişim, paketlerin öncelikle firewall üzerinden geçmesini sağlar. Temel anlamda görevi, istemciden gelen paketin sunucunun belirlenen portu ile iletişim kurup kuramayacağını belirlemektir. Firewall'ların asıl amacı, sunucuyu olası siber saldırılara karşı korumaktır. Örnek olarak, rastgele bir IP adresi ile sunucu arasında iletişim kurulmaya çalışıldığında, sunucu olmayan bir IP adresiyle sürekli iletişim kurulmaya çalışılacağından dolayı kaynaklar tükenebilir. Bu sayede, firewall sayesinde sunucunun kaynakları korunmuş olur. Üç aşamalı el sıkışma protokolü, firewall'lar ile gerçekleştirilmektedir.

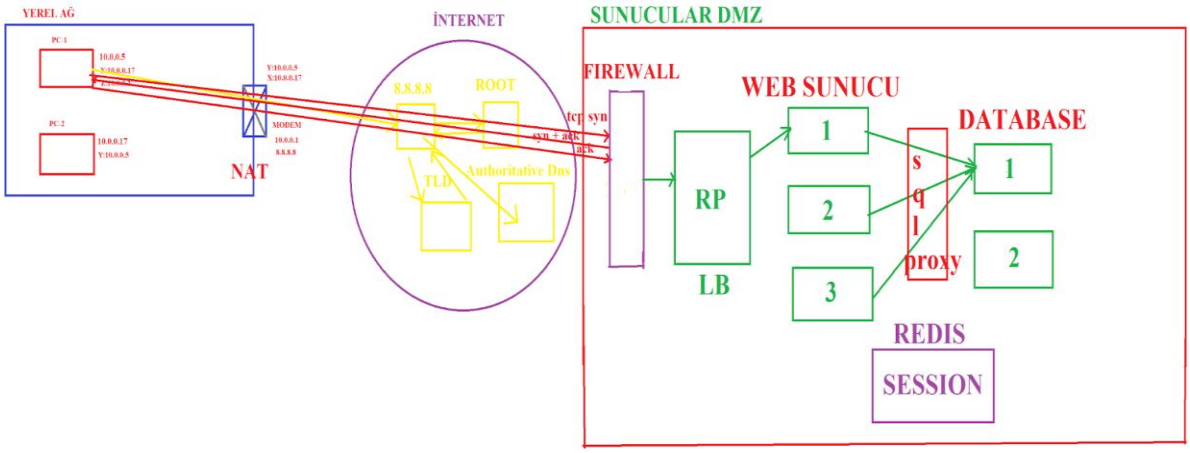


Firewall Harici Sunucu Yapısı

Firewall harici, yeni sunucu üzerinde birden fazla cihaz bulunmaktadır. Web sunucuları da, tıpkı NAT teknolojisi gibi bir teknoloji kullanmaktadır. Bunun nedeni, IP adresleri ile domainlerin sayısının birbirlerinden çok farklı olmasıdır. Bu temel mantık şu şekilde açıklanabilir: Bir IP adresine sahip sunucu, birden fazla sanal sunucuya bölünebilir. Bu işleme virtual hosting denir. Bu teknoloji sayesinde, tek bir IP adresi üzerinden birden fazla domainin hosting işlemi gerçekleştirilebilmektedir.

Bunlar haricinde, günümüzde ve sunucularda bazı sorunlar doğrultusunda değişiklikler yapılmıştır. Örneğin, e-ticaret sitelerinin indirim kampanyaları yaptığı zamanlarda, çok fazla kullanıcı tarafından ziyaret edilmesinden dolayı sunucu yetersiz kalabilmektedir. Eskiden bu problemin çözümü için sunuculara ek donanımsal cihazlar eklenirdi, ancak günümüzde bu durum, birden fazla web sunucusunun aynı anda ortak bir veri üzerinde birlikte çalışması şeklinde çözülmektedir. Aynı zamanda, reverse proxy kullanılarak, gelen isteklerin sunuculara iletilmesi sağlanır. Bu cihazın görevi, gelen istekleri müsait olan web sunucularına iletmektir.

Fakat bu durumlarda, bazen oturumun diske yazılması gibi sebeplerden dolayı, bir işlem sadece bir web sunucusu üzerinde yapılmak zorunda kalmaktadır. Eğer tüm istekler aynı web sunucusu üzerinde çalışmazsa, kullanıcı otomatik olarak sistemden atılabilir. Bu durumu çözmek için çerezler kullanılır. Çerezler sayesinde, bu isteklerin ilk hangi sunucuya gönderildiği kaydedilir. Yani, ilk olarak sunucunun numarası belirli bir çerezle kaydedilir ve yeniden gelen istek, çerezler sayesinde o numaralı web sunucusuna yönlendirilir.

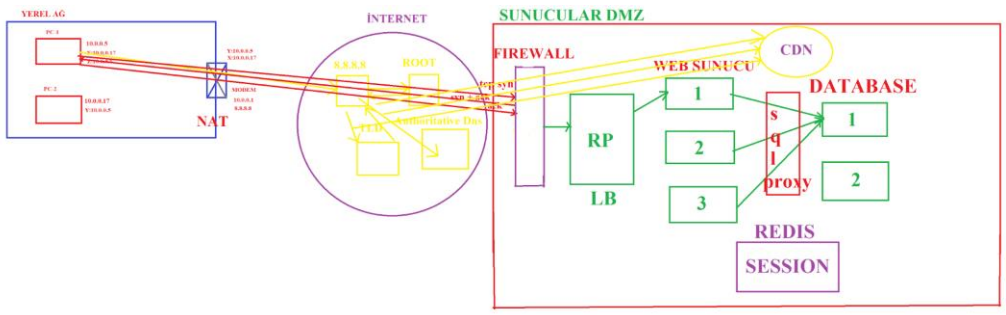


Web Sunucularında Ortaya Çıkan Problemler ve Çözümleri

Bu tür yapıların kullanılması sonucunda bazı problemler ortaya çıkabilir. Örneğin, bir numaralı veritabanı işlemi durursa ne olacak veya bir numaralı ve iki numaralı veritabanlarının aynı anda aktif olması gerektiği durumlar meydana gelebilir. Bu gibi durumların ve veri yönetiminin çözülmesi için SQL proxy kullanılmaktadır. Tüm SQL sorguları ve benzeri işlemler bu proxy üzerinden yönlendirilir. Bu proxy, hangi veritabanı daha uygun ise o veritabanı ile çalışır.

Öte yandan, oturum bilgileri veri tabanına yazılmaktadır. Ancak bu, bazı problemlere yol açabilmektedir. Bu tür sorunları çözebilmek için CDN adı verilen bir sunucu cihazı devreye girmiştir. CDN sayesinde, oturum bilgileri yalnızca firewall üzerinden erişilebilir hale gelir.

Özetle, web sunucuları birden fazla cihaza dağıtılabilmektedir. Yapılacak işlemlere göre birden fazla web sunucu cihazı bulunabilir. Ayrıca, web sunucusunun bulunduğu sağlayıcının çökmesi durumunda, aynı özelliklere sahip başka bir web sunucu alanı da mevcut olabilir.Son olarak, ağın çalışmasıyla ilgili şema aşağıda gösterilmiştir.



Works Cited

Web Ne Demek? Web Sitesi Nedir?, https://www.iienstitu.com/blog/web-ne-demek.

Web Sayfası Nedir, Ne İşe Yarar? | Amaçlarını ve İşlevlerini Keşfetme, https://www.sysnettechsolutions.com/web-sayfasi-nedir/#jump-1.

Dosya Aktarım Protokolü, https://en-m-wikipedia-org.translate.goog/wiki/File_Transfer_Protocol?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=sc.

İnternetin Hikayesi. Web 1.0'dan Web 4.0'a, https://botland.store/blog/story-of-the-internet-from-web-1-0-to-web-4-0/.

SMTP Nedir?, https://bulutistan.com/blog/smtp-nedir/#SMTP_Protokolleri.

IMAP, https://tr.wikipedia.org/wiki/IMAP.

What is an SSH Key? Its Features, Types, Uses and Importance, https://www.ssl2buy.com/cybersecurity/ssh-secure-shell-key.

Web 2.0 Definition And Meaning – WebsiteBuilders Tech Terms Glossary, https://websitebuilders.com/how-to/glossary/web2/.

Semantik (Anlamsal) Web Nedir?, https://ahmetsavasgokturk.com.tr/yazarlar/semantik-anlamsal-web-nedir/.

Web3 nedir?, https://aws.amazon.com/tr/what-is/web3/.

Web Security 101 0x04 | Bir Hacker'ın Gözünden Modern Web Nasıl Çalışır ?, https://www.youtube.com/watch?v=3AgDSw0I89A.

Semantic Web (Anlamsal Ağ) Nedir?, https://ahmetmeleq.medium.com/semantic-web-anlamsal-a%C4%9F-nedir-7495c6f7316c.

Semantik Web Nedir?, https://www.mediaclick.com.tr/blog/semantik-web-nedir#:~:text=T%C3%BCrk%C3%A7e%20kar%C5%9F%C4%B1l%C4%B1%C4%9

F%C4%B1%20Anlamsal%20A%C4%9F%20olan,web%20projesi%20olma%20%C3%B6zelli%C4%9Fi%20ta%C5%9F%C4%B1yor.

“Definition of Web.” *Gartner*, https://www.gartner.com/en/information-technology/glossary/web. Accessed 19 December 2024.

“Dosya aktarım iletişim kuralı.” *Vikipedi*, https://tr.wikipedia.org/wiki/Dosya_aktar%C4%B1m_ileti%C5%9Fim_kural%C4%B1. Accessed 19 December 2024.

“Güvenli kabuk.” *Vikipedi*, https://tr.wikipedia.org/wiki/G%C3%BCvenli_kabuk. Accessed 20 December 2024.

“HTTP.” *Vikipedi*, https://tr.wikipedia.org/wiki/HTTP#G%C3%BCvenli_y%C3%B6ntemler. Accessed 19 December 2024.

“HTTPS.” *Vikipedi*, https://tr.wikipedia.org/wiki/HTTPS. Accessed 19 December 2024.

“İnternet sitesi.” *Vikipedi*, https://tr.wikipedia.org/wiki/%C4%B0nternet_sitesi. Accessed 19 December 2024.

McCahill, Mark P. “History of the World Wide Web.” *Wikipedia*, https://en.m.wikipedia.org/wiki/History_of_the_World_Wide_Web. Accessed 20 December 2024.

“mdisec-twitch-yayinlari/docs/Web_Security_101/0x04_Bir_Hackerin_Gozunden_Web.” https://github.com/mdisec/mdisec-twitch-yayinlari/blob/master/docs/Web_Security_101/0x04_Bir_Hackerin_Gozunden_Web/README.md.

“POP3.” *Vikipedi*, https://tr.wikipedia.org/wiki/POP3#cite_note-5. Accessed 20 December 2024.

“SMTP.” *Vikipedi*, https://tr.wikipedia.org/wiki/SMTP. Accessed 20 December 2024.

“URL.” *Vikipedi*, https://tr.wikipedia.org/wiki/URL. Accessed 20 December 2024.

“WEB 1.0, 2.0, 3.0 ve 4.0’ın Tarihi.” https://dergipark.org.tr/tr/download/article-file/2122736#:~:text=B%C3%B6ylece%20art%C4%B1k%20%C3%A7o%C4%9Fumuz%20t%C3%BCketicilerin%20b%C3%BCy%C3%BCk%20bir%20par%C3%A7as%C4%B1n%C4%B1%20olu%C5%9Fturuyoruz.&text=Web%203.0%20(2010'da%20aktif,ara%C5%9Ft%C4%B1.

“Web nedir?. Web, internet alt yapısı sayesinde… | by Yusuf Kocaman | Medium.” *Yusuf Kocaman*, 26 January 2018, https://ykocaman.medium.com/web-nedir-5de10b9f588c. Accessed 19 December 2024.

“Web Sitesi Güvenliği Nasıl Sağlanır? - Blog.” *Berqnet*, 11 November 2022, https://berqnet.com/blog/web-sitesi-guvenligi. Accessed 19 December 2024.

“Web Sitesi Nedir? Bilmeniz Gereken Her Şey.” *Wix.com*, 3 August 2021, https://tr.wix.com/blog/makale/web-sitesi-nedir. Accessed 19 December 2024.

“WebSocket.” *Vikipedi*, https://tr.wikipedia.org/wiki/WebSocket. Accessed 19 December 2024.

““ WebSocket Nedir? Web Uygulamalarında Gerçek Zamanlı İletişim | by Bilaliyisoy | Teknopar Akademi.” *Medium*, 15 August 2023, https://medium.com/teknopar-akademi/websocket-nedir-a0062d00333d. Accessed 19 December 2024.

“Web sunucusu.” *Vikipedi*, https://tr.wikipedia.org/wiki/Web_sunucusu. Accessed 19 December 2024.

“Web Tarayıcı (Web Browser) Nedir?” *IdeaSoft*, 12 July 2024, https://www.ideasoft.com.tr/web-tarayici-nedir/. Accessed 19 December 2024.

"World Wide Web." *Vikipedi*, https://tr.wikipedia.org/wiki/World_Wide_Web. Accessed 19 December 2024.

Yasar, Kinza. "What is Web 2.0? | Definition from TechTarget." *TechTarget*, https://www.techtarget.com/whatis/definition/Web-20-or-Web-2. Accessed 20 December 2024.