**GİRİŞ**

Günümüzde internet teknolojilerinin gelişmesi ile birlikte, özellikle e-posta yaygın olarak kullanılmaktadır. Bununla birlikte e-posta sistemini art niyetli olarak kullananların sayısı da son yıllarda oldukça artmıştır. Özellikle reklam, dolandırıcılık ve propaganda amaçları başta olmak üzere pek çok sebeplerden ötürü e-postalar, internet üzerindeki e-posta trafiğinin büyük kısmını oluşturmaya başlamıştır. Bu durum, başta bant genişliğinin gereksiz kullanımı olmak üzere pek çok açıdan zararlar oluşturmaktadır.

Bir e-postanın önemsiz/spam e-posta olduğunu düşünmek için öncelikle o e-postanın istenmeyen bir ileti olması ve e-postanın çok fazla alıcıya gönderilmiş olması gerekmektedir.

Bireysel içeriği olan ve gönderici bilgileri olan mesajların ilk etapta çöp e-posta olarak düşünülmemesi gerekmektedir. Gelen e-postanın gönderici ile ilgili bilgileri barındırmaması yani kişisel özellikler taşımaması durumunda bu e-postanın istenmeyen bir mesaj olabileceğini gösterebilmektedir.

**ÇALIŞMALAR**

1. **Pyzor ve Bayes Yaklaşımı**

Pyzor gelen e-postaların belirli sunucular üzerinden kontrol edilip çöp e-posta olup olmadığını sorgulayan bir sistemdir.

Bayes ise bizim sunucumuzun gelen maillerin önemsiz e-posta olup olmadığını otomatik olarak öğrenmesini sağlayan bir sistemdir. Temeli Thomas Bayesian adlı matematikçi tarafından geliştirilen bu yöntem, eğer önemsiz e-posta olan bir ileti içerisindeki karakterler ve işaretler bir başka ileti içerisinde de geçiyorsa muhtemelen o ileti de önemsiz e-postadır, ilkesine göre çalışır. Bu yöntem daha önce gelen iletileri esas alarak, olasılık hesaplarıyla, bir sonraki iletinin önemsiz e-posta olup olmadığını tahmin ederek işler.

1. **DCC (Distributed Checksum Clearinghouse)**

DCC sunucu-istemci mantığıyla çalışan bir yapıdır. E-posta sunucu üzerine kurulan bu yapı sayesinde, gelen e-postalar DCC sunucuları üzerinden kontrol edilmektedir. Bu e-posta aynı şekilde pek çok kişi tarafından alınmışsa ve önemsiz e-posta olarak tespit edilmişse, bizim sunucumuza gelen e-posta da önemsiz e-posta olarak sınıflandırılmaktadır. Bu yöntem aynı zamanda bant genişliği kullanımına da sebep olmaktadır.

1. **Spamassassin**

Perl programlama dili ile yazılmış bu çöp eposta engelleyici, elle dikkatlice yazılmış kuralları kullanır ve "strong buy", "you received this mail because", "viagra", "limited time offer" gibi tipik önemsiz e-posta ifadelerini inceler. Aynı şekilde e-posta üzerinde başlık, içerik ve ek kısımlarını inceleyerek bulduğu her bir önemsiz eposta belirtisi için e-postaya puanlar ekler. Eğer bu tip ifadeler belirli bir seviyenin üzerindeyse, e-postayı önemsiz e-posta olarak algılar. Bu seviye genellikle sistemi oluşturan kişi tarafından belirlenir. Bu değerin çok yüksek olması önemsiz eposta olan bazı e-postaların tespitini güçleştirir (False-Negative). Tam aksine bu değerin küçük olması ise, önemsiz e-posta olmaya bazı e-postaları önemsiz e-posta olarak tespit edip engelleyebilir (False Positive). Bu iki durumda istenmeyen durumlar olduğundan ortalama bir değer çeşitli denemeler sonucunda elde edilen deneyimlerle tespit edilebilir. Yine bu yazılım üzerinde önemsiz epostaların ne yapılacağı veya dikkate alınacak eposta boyutu gibi pek çok ayarlama yapılabilmektedir.

**KIYASLAMA**

1. DCC (Distributed Checksum Clearinghouse) sistemi yoran bir yapısı vardır.
2. Kişi tarafından sürekli kontrol edilmesi gerekmektedir. Hata payı olan bir yapısı mevcuttur.
3. Bayes sistemi bir yapay zeka sistemleri gibi bir yapısı mevcuttur. Önemsiz e-postaları otomatik olarak öğrenebilen bir yapısı vardır. Bu yüzden dolayı bayes sistemi en doğru sistem olacağı düşüncesindeyim.

**Blok Listelerin Kullanılması**

Önemsiz/Spam e-posta engelleme sistemlerinde en çok kullanılan yöntemlerden biri de blok listelerinin kullanılmasıdır. Daha önce spam e-posta yayan sunucular bir şekilde blok listelerini tutan sunucululara bildirilerek, bu sunucuların etki alanı bilgilerini ve IP adresi kayıtlarını tutması sağlanır. Daha sonra herhangi bir e-posta sunucudan e-posta alacak olan diğer bir e-posta sunucu, SMTP bağlantısını kabul etmeden önce istekte bulunan e-posta sunucunun bilgilerini blok listelerinden kontrol edip, bağlantıyı kabul edip etmeyeceğine karar verir.

Aynı şekilde üçüncü şahıslar tarafından spam e-posta yollamak amacıyla kullanılan güvensiz sunucular da bu listelerde kaydedilir. Bu yöntemin en büyük avantajı, e-posta gönderilmeden önce sorgulama yapılıp engellendiği için, e-postanın gereksiz yere bant genişliği kullanımının engellenmiş olmasıdır. Dezavantajı ise bu listelere giren herhangi bir sunucu, bu listeleri kullanan hiçbir e-posta sunucuya e-posta gönderemez. Hemen hemen tüm spam e-posta bloklama sistemleri bu yöntemi kullanmaktadır. Günümüzde genel amaçlı olarak en çok kullanılan blok listelerine örnek olarak bl.spamcop.net, safe.dnsbl.sorbs.net, blackholes.njabl.org, sbl-xbl.spamhaus.org sunucuları verilebilir.

**Qmail E-posta sunucu yazılımı**

Qmail, UNIX ve UNIX benzeri(\*BSD, Linux) işletim sistemleri için bir MTA'dir (Mail Transfer Agent - Posta Aktarım Aracısı).

**QSheff Yazılımı**

QSheff, Qmail e-posta kuyruğuna girecek epostaların virüs ve çöp e-posta filtreleme programları tarafından kontrol edilebilmesi için bir ara programdır. Problemsiz olarak kontrollerden geçen e-postalar Qmail kuyruğuna verilecektir. Basit ve güçlü algoritması ile yüksek performans sağlamaktadır. Kolay kurulum, karantina, anlaşılabilir loglama, konu filtreleme, kara delik, ve kara liste özellikleri vardır.

**Ripmime**

QSheff, e-postaların parçalanması için ripmime yazılımına ihtiyaç duyar. Ripmime, epostaları başlık, gövde ve ekler şeklinde ayrı ayrı dosyalara böler. Bu sayede spam e-posta kontrolü yapılırken başlık, gövde ve eklerdeki bilgiler ayrıştırılarak kontrol edilebilmektedir.