Journal of the Faculty of Engineering and Architecture of Gazi University 31:3 (2016) 645-653

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Web tabanlı saldırı önleme sistemi tasarımı ve gerçekleştirilmesi: yeni bir hibrit model

Adem Tekerek[1*], Cemal Gemci[2], Ömer Faruk Bay[3]

[1]Gazi Üniversitesi, Bilgi İşlem Dairesi Başkanlığı, Ankara, 06500, Türkiye
[2]CymSoft Bilişim Teknolojileri, Ankara, 06800, Türkiye
[3]Gazi Üniversitesi, Elektronik ve Bilgisayar Eğitimi Bölümü, Ankara, , 06500, Türkiye

ÖNEÇIKANLAR

- Web tabanlı saldırı önleme amaçlı web uygulama güvenlik duvarı
- Anormal tabanlı ve imza tabanlı denetim türlerinin beraber kullanıldığı hibrit model
- Bayes sınıflandırma kullanılarak anormal tabanlı denetim

Makale Bilgileri
Geliş: 01.07.2015
Kabul: 15.02.2016

DOI:
10.17341/gummfd.63355

Anahtar Kelimeler:
Web güvenliği,
imza tabanlı denetim,
anormal tabanlı denetim,
web uygulama güvenlik duvarı

ÖZET

Web uygulama güvenliğini sağlamak için ağ ortamından yapılan saldırılara karşı güvenlik duvarları, saldırı tespit ve engelleme sistemleri kullanılmaktadır. Web uygulamalarına HTTP kullanılarak da saldırılar gerçekleştirilmektedir. Bu saldırıları önlemek için HTTP istek denetimi yapılmaktadır. Bu çalışmada, imza tabanlı denetim ve anormal tabanlı denetim kullanılarak web tabanlı saldırıları önlemek için yeni bir hibrit model önerilmiştir. Bilinen bazı web tabanlı saldırı türlerinin denetimi imza tabanlı denetimle yapılmaktadır. Alfanümerik Karakter, Harf Frekans ve İstek Uzunluğu öznitelikleri kullanılarak veri madenciliği yöntemlerinden bayes sınıflandırma algoritması ile anormal tabanlı denetim yapılmaktadır. İmza tabanlı denetim anormal tabanlı denetimden daha hızlı olduğu için, imza tabanlı denetim veri tabanı anormal tabanlı denetim sonucu tespit edilen anormal HTTP istekleri ile güncellenmektedir. Önerilen model CSIC 2010, ECML-PKDD 2007 ve çalışma kapsamında geliştirilen WUGD 2015 veri kümeleri kullanılarak test edilmiştir. Test sonuçlarına göre ortalama olarak %95,1 oranında başarılı anormal tabanlı denetim yapılmıştır. Test sonuçları benzer bazı çalışmalar ile karşılaştırılmıştır. Karşılaştırma sonucuna göre önerilen modelin mevcut çalışmalara göre daha yüksek denetim performansı gösterdiği ve düşük yanlış pozitif oranına sahip olduğu görülmüştür.

Design and implementation of a web-based intrusion prevention system: a new hybrid model

HIGHLIGHTS

- Web application firewall algorithm for web-based intrusion prevention
- Hybrid model that used anomaly-based detection and signature-based deteciton
- Anormaly-based detection by using bayesian classification

Article Info
Received: 01.07.2015
Accepted: 15.02.2016

DOI
10.17341/gummfd.63355

Keywords:
Web security,
signature-based detection,
anomaly-based detection,
web application firewall

ABSTRACT

Firewalls, intrusion detection and prevention systems are used to protect web applications against network attacks. HTTP is also used to attack to web applications. HTTP request detections are performed in order to prevent these attacks. In this study, a new hybrid model is proposed which uses signature-based detection and anomaly based detection to prevent web-based attacks. Some types of web-based known attacks detection were implemented by signature-based detection. Anomaly based detection were implemented by bayes classification, which is a data mining technique, using features of Alfanumeric Character, Letter Frequency and Request Length. Because signature based detection is faster than anomaly based detection, signature based detection database is updated with detected anomaly HTTP requests obtained by anomaly based detection. Proposed model was tested by using CSIC 2010, ECML-PKDD 2007 and WUGD 2015 dataset which is generated during this study. According to the test results; anomaly based detection was conducted with a high mean achievement percentage (95,1%). The test results were compared with some similar studies. According to the comparison results, proposed model provided high performance and low false positive rate compared to the other studies.

1. GİRİŞ (INTRODUCTION)

İnternetin kullanımının artmasıyla, web uygulamalarının ve web servislerinin de sayısı gün geçtikçe artmaktadır. İnternetten verilen hizmetler arttıkça web uygulamalarına yönelik saldırılar ve çeşitleri de her geçen gün artmaktadır. İnternetin yaygınlaşması ile beraber güvenlik riskleri de aynı ölçüde artmıştır. Son derece güvensiz olan internet ortamında

* Sorumlu Yazar/Corresponding author: atekerek@gazi.edu.tr / Tel: 0 312 202 2246

bilgi kaybının ve zafiyetinin önlenmesi için web uygulamalarının güvenlik ihtiyaçlarının karşılanması gerekmektedir. Bu durum, web uygulamaları geliştirilirken güvenli yazılım geliştirme yöntemleri kullanılarak veya web uygulamaları güvenlik duvarı araçları kullanılarak karşılanabilmektedir [1-2]. Web uygulamalarının çok geniş kullanım alanlarına sahip olması ve kolay erişilebilir olmaları, web uygulamalarını saldırganlar için çok cazip hale getirmektedir. Bu özelliği onlara karşı yapılan saldırı çeşidini ve sayısını da artırmaktadır. Siteler Arası Kod Yazma (XSS), SQL enjeksiyonu gibi saldırı türleri; taklit etme, veri tabanında bulunan bilgileri açığa çıkarma veya web sayfasında modifikasyon yapma gibi çok dramatik sonuçlar doğuran saldırılardır [3]. Uygulama geliştiriciler uygulamanın fonksiyonelliğini uygulamanın güvenlik ihtiyaçlarından daha ön planda tuttukları için ve web uygulamalarının güvenlik ihtiyaçları bakımından yeterli bilgiye sahip olmadıkları için web uygulamaları güvenlik zafiyetleri açısından oldukça yüksek riskler taşımaktadırlar [4]. Geleneksel güvenlik duvarları ağ katmanından gelen paketleri başarılı bir şekilde engellerken, web uygulamalarına karşı yapılan saldırılarda etkili değillerdir [5]. Web uygulamaları (Hyper Text Transfer Protocol) HTTP kullanmaktadır, dolayısıyla saldırılar da bu protokol üzerinden gerçekleştirilmektedir. HTTP istek denetimi yapılarak web uygulamalarına yapılan saldırıları engellemek mümkündür.

Bu çalışmada, imza tabanlı denetim (İTD) ve anormal tabanlı denetimi (ATD) yöntemleri birlikte kullanılarak hibrit bir model önerilmektedir. İTD, izin verilemeyecek isteklerin tespit modelini oluşturmaktadır. İmza tabanlı denetimle bilinen saldırı türlerinden *SQL Enjeksiyonu*, *Siteler Arası Kod (XSS) Yazma* saldırı türlerine karşı denetim gerçekleştirilmiştir. Anormal istek denetimi için kullanılan öznitelik değerleri veri madenciliği sınıflandırma tekniklerinden bayes sınıflandırma yöntemi kullanılarak HTTP isteklerinin anormallik tespitleri gerçekleştirilmiştir. HTTP isteklerinin anormallik tespitleri, *Alfanümerik Karakter*, *Harf Frekans* ve *Cümle Uzunluğu* olmak üzere üç öznitelik kullanılarak gerçekleştirilmiştir. ATD yöntemiyle elde edilen sonuçlar bayes sınıflandırma kullanılarak İTD veri tabanı güncellenmektedir. İTD hızlı çalışırken sıfır gün saldırılarına karşı etkili değildir. ATD yöntemi ise sıfır gün saldırılarında etkilidir, fakat İTD, ATD metoduna göre daha hızlı çalışmaktadır [5]. Bundan dolayı bu çalışmada iki yapının önemli özellikleri ortak bir yapı içerisinde birleştirilmiştir.

Bu çalışma beş bölümden oluşmaktadır. İkinci bölümde literatürdeki benzer çalışmalar incelenmiş ve önerilen çalışmanın farklılıkları vurgulanmıştır. Üçüncü bölümde bir hibrit model önerilmiş ve bu modelin detayları verilmiştir. Dördüncü bölümde önerilen model farklı veri setleri ile test edilmiş ve benzer çalışmalar ile sonuçları karşılaştırılmıştır. Beşinci bölümde ise yapılan çalışmanın etkinliği vurgulanarak çalışma sonlandırılmıştır.

2. İLGİLİ ÇALIŞMALAR (RELATED WORKS)

Literatürde konu ile ilgili benzer çalışmalar bulunmaktadır. Nguyen ve diğerleri [7] yaptıkları çalışmada web saldırı denetiminde öznitelik seçimine yönelik bir çalışma gerçekleştirmişlerdir. Genel öznitelik seçimi (GeFS) için CSIC 2010 ve ECVL/PKDD 2007 veri kümeleri kullanılarak C45, CART, RamdomTree, RandomForest olmak üzere 4 farklı sınıflayıcıyla veri kümelerinde uzman görüşü ile belirlenen 30 farklı öznitelik oluşturularak denetim gerçekleştirilmiştir. Çalışmada siteler arası kod yazma (XSS), SQL enjeksiyonu, LDAP enjeksiyonu, XPATH enjeksiyonu saldırı türleri için sınıflandırma yapılmıştır. Yazarların yaptığı çalışmada HTTP isteklerini denetlemek için kullanılabilecek özniteliklerin performans değerlendirmesi yapılarak, öznitelik seçimi yapılmaktadır. Bizim önerdiğimiz çalışmada da bu çalışmada belirlenen istek uzunluk özniteliği kullanılmıştır. Palka ve diğerleri [8] yaptıkları çalışmada, web uygulamalarına gelen HTTP isteklerini doğrulayarak ve HTTP isteklerinin parametrelerini, daha önceden kaydedilmiş kullanıcı alışkanlıklarıyla karşılaştırarak, web uygulamalarını koruma altına alan web uygulama güvenlik duvarını gerçekleştirmişlerdir. Kullanıcı alışkanlıkları, web uygulamasını ziyaret eden kullanıcıların davranışları sonucunda üretilmiştir. Öğrenme tabanlı web uygulama güvenlik duvarı esnek, uygulamaya özel ve devreye alınması kolay bir çözüm sunmasının yanında HTTP isteklerinin denetimi sürecinde sınıflandırma yapılırken öğrenme sürecinde hatalar gerçekleşmektedir. Yazarlar yaptıkları bu çalışmada öğrenme tabanlı web uygulama güvenlik duvarlarının öğrenme sürecinde gerçekleşen hataları tartışmışlardır. Yazarların yaptığı bu çalışmada kullanıcı davranışlarına göre denetim gerçekleştirilmiştir. Sadece kullanıcı davranışlarının kullanılması web uygulamasına yapılan saldırıların denetiminde yeterli değildir. Çünkü web uygulamalarına yapılan saldırılar sadece kullanıcı davranışlarıyla tespit edilemeyecek kadar çok fazla çeşide ve sayıya sahiptir. Dolayısıyla bizim önerdiğimiz çalışmada web uygulamalarına yapılan bilinen saldırı türlerine karşı ve anormal HTTP isteklerine karşı denetim gerçekleştirebilmek için hibrit model önerilmiştir. Basile ve diğerleri [9] yaptıkları çalışmada web uygulama güvenlik duvarında paket filtrelemek için anormal denetim gerçekleştirmişlerdir. Önerdikleri modelde düzenli ifadeler ile belirtilen metin tabanlı içerik filtreleme yapmışlardır. Modelin etkinliği HTTP proxy olan SQUID'in erişim kontrol özelliğine karşı başarılı bir şekilde test edilmiştir. Yazarların yaptığı çalışmada metin tabanlı anormal denetim yapılmıştır. Metin tabanlı denetim web uygulamalarına yapılan saldırıların denetimi için yeterli değildir. Fakat önerdiğimiz çalışmada web uygulamalarına yapılan bilinen saldırı türlerine ve anormal HTTP isteklerine karşı denetim gerçekleştirebilmek için hibrit model önerilmiştir. Cho ve diğerleri [10] ise yaptıkları çalışmada kullanıcılar tarafından istenen web sayfalarının benzer özelliklere sahip olduğunu tespit etmişlerdir. Web erişim verilerinden web oturumlarını açığa çıkarmak için bayes parametre tahmin tekniği

kullanılarak, oturum bilgilerinden anormallik tahmini gerçekleştirilen oturum anormallik tespiti (Session Anomaly Detection - SAD) ismi verilen bir çalışma geliştirilmiştir. Yazarların yaptığı bu çalışmada web uygulamasına yapılan saldırılar, oturum bilgileri kullanılarak bayes sınıflandırma yöntemi ile anormal denetim gerçekleştirilerek tespit edilmiştir. Sadece oturum bilgileri kullanılarak ve anormal denetim yapılarak web uygulamalarına yapılan saldırıların denetimi yetersiz kalacaktır. Bizim önerdiğimiz modelin bu çalışmadan farkı hem HTTP isteklerine karşı hibrit bir denetim modelinin önerilmesi, hem de web tabanlı saldırıların en çok yapıldığı HTTP istek satırının denetimini gerçekleştirmesidir. Razzaq ve diğerleri [11] ise yaptıkları çalışmada bayes sınıflandırma kullanılarak ontoloji tabanlı uygulama katmanı saldırı tespit sistemi önermiştir. Önerilen sistemde, HTTP istek parametreleri ontoloji değişkenleri olarak belirlenerek değişken değerlerine göre bayes sınıflandırma işlemi HTTP isteklerinin anormallik tespiti gerçekleştirilmiştir. Yazarların yaptığı anormal tabanlı denetim bizim önerdiğimiz gibi bayes sınıflandırma kullanılarak geliştirilmiş olsa da yazarlar ön işleme kısmında ontoloji tabanlı sınıflandırma kullanmışlardır. Bizim yaptığımız çalışma da ise önişleme sürecinde farklı öznitelikler kullanılmıştır. Bremler-Barr ve diğerleri [12] yaptıkları çalışmada, imza tabanlı denetim kullanan güvenlik araçlarının sıkıştırılmış trafiklere karşı etkili olmadığını belirtmişlerdir. Çalışma ile sıkıştırılmış HTTP trafiği üzerinde durulmaktadır. HTTP, GZIP sıkıştırma yöntemi kullamaktadır ve metin karşılaştırması yapabilmek için bazı farklı açma (sıkıştırılmış veriyi kullanılabilir hale getirme) yöntemlerinin kullanıldığı belirtilmiştir. Yazarlar gerçek HTTP trafiğinin ve gerçek web uygulama güvenlik duvarı imzalarının analiz edilmesiyle, verilerin % 84'ünden fazlasının taranmasının atlandığını ortaya çıkarmışlardır. Ayrıca sıkıştırılmış veriyle desen eşleştirerek denetim yapmanın sıkıştırılmamış veriyle yapmaktan daha hızlı olduğunu ortaya koymuşlardır. Bizim önerdiğimiz çalışma ise sıkıştırılmamış HTTP isteklerine karşı denetim gerçekleştiren hibrit bir çalışmadır. Singh ve diğerleri [13] yaptıkları çalışmada siber saldırı veri kümesi sınıflandırılması için iyileştirilmiş destek vektör makinesi (iSVM) algoritması kullanarak denetim modeli önermişlerdir. Sonuçlar iSVM, Normal ve Hizmet Aksatma (DOS) sınıflarına karşı %100 doğruluk vermiş ve yanlış alarm oranı, eğitim ve test süreleri karşılaştırılabilirliğini göstermişlerdir. Geleneksel SVM performansı, Gauss çekirdek ile bir konformal haritalama marjı etrafında uzaysal çözünürlüğü büyütmek için geliştirilmiştir. Böylece saldırı, sınıflar arasındaki ayrılabilirliliği artacaktır. Bu işlem çekirdek fonksiyonu tarafından uyarılan Riemann geometrik yapısına dayanmaktadır. Bizim önerdiğimiz çalışma ise yazarların önerdiği çalışmadan farklı olarak İTD ve ATD modelleri kullanılarak bayes sınıflandırma yöntemi ile geliştirilmiş hibrit bir modeldir. Torrano-Gimenez ve diğerleri [14] yaptıkları çalışmada, anormal tabanlı denetim sonucunda bilinmeyen web tabanlı saldırıları tespit edebilen bir web uygulama güvenlik duvarı geliştirmişlerdir. Geliştirilen model bir HTTP isteğinin saldırı olup olmadığına bir XML dosyasının yardımı ile karar vermektedir. XML dosyası web uygulamasını hedef alan istatistiksel olarak normal davranışlara sahip yapay zeka tabanlı olarak üretilmiş normal HTTP isteklerini barındırmaktadır. Normal davranışın dışında sapma gösteren istekler, sistem tarafından anormal olarak nitelendirilmektedir. Sürekli artan eğitim verileri sistemin eğitiminde kullanılmaktadır. Deneyler sonucunda XML dosyasında web uygulamasının karakteristiğini ortaya çıkacak yeteri kadar istek bulunması, çok başarılı denetim oranına ulaşılmasını sağlarken, yanlış alarm oranını da düşürmektedir. Bizim önerdiğimiz çalışma ise İTD ve ATD modelleri kullanılarak bayes sınıflandırma yöntem ile geliştirilmiş hibrit bir modeldir. ATD sonucu tespit edilen anormal HTTP istekleri İTD imza listesine eklenerek imza veri tabanı güncellenmektedir. Bu özellik sayesinde modelin denetim performansını artırmaktadır. Peng ve diğerleri [15] yaptıkları çalışmada, ağ tabanlı saldırıların, günümüzde büyük ölçüde birbirine bağlı bilgisayar sistemleri için temel tehdit haline geldiğinden bahsederek, yetkilendirilmemiş aktiviteler ve erişimler için ağların en büyük problemleri olduğunu belirtmişlerdir. Saldırı tespit sistemleri artan güvenlik açıklıklarına karşı kullanılması kaçınılmaz sistemlerdir. Yazarlar çalışma ile imza tabanlı ve anormal tabanlı denetim metotlarının avantajlı taraflarını güçlendiren, hibrit bir saldırı tespit ve görüntüleme sistemi önermişlerdir. Saldırı tespit edildiğinde, sisteme entegre olan bağımsız ajan kötüye kullanım davranışlarına karşı eylem gerçekleştirerek, ağı içerden veya dışarıdan yapılan saldırılara karşı korumaktadır. Yazarlar önerdikleri çalışmayla ağ tabanlı saldırılara karşı hibrit bir model gerçekleştirmişlerdir, ama bizim önerdiğimiz çalışmada web tabanlı saldırılara karşı hibrit bir model geliştirilmiştir. Locasto ve diğerleri [16] yaptıkları çalışmada, binary kod enjeksiyonu saldırısını önlemek için hibrit bir yaklaşım sunmuşlardır. Model imza tabanlı, anormal tabanlı sınıflandırıcı ve öğrenme aracı olmak üzere üç mekanizmadan oluşmaktadır. Anormal denetim sonucu elde edilen saldırılar ile imza üretimi gerçekleştirilmiştir. Geri besleme mekanizmasına bağlı olarak işleyen öğrenme aracı kod enjeksiyon saldırısını sınıflandırarak engelleyen bir yapıya sahiptir. Tespit edilen saldırı içeren zararlı kod içeren paketler, sıfır gün saldırılarını engellemek için imza üretimi gerçekleştirilmiştir. Yazarların geliştirdiği model binary kod enjeksiyonu için geliştirilmiş hibrit çalışmadır, ama bizim önerdiğimiz model ise yine öğrenme tabanlı olarak hem bilinen saldırı türlerine karşı hem de sıfır gün saldırılarına karşı geliştirilmiş hibrit modeldir. Hwang ve diğerleri [17] yaptıkları çalışmada yeni bir hibrit saldırı tespit sistemin tasarım gerçekleştirmişlerdir. Hibrit model düşük yanlış pozitif oranına sahip imza tabanlı denetim modelinin ve bilinmeyen yeni saldırıları denetleyen anormal tabanlı denetim modelinin avantajlarını birleştirmektedir. SNORT'da bulunan anormal verilerin belirlenmesini sağlayan anormal denetim modeliyle imza üretimi gerçekleştirilmiştir. Hibrit saldırı tespit sisteminin anormal denetim süreci ile tespit edilen imzalar, daha hızlı denetim gerçekleştirmek için SNORT imza veri tabanına

eklenmektedir. Deneysel sonuçlara göre %60 denetim oranı elde edilmiştir. anormal denetimle üretilen imzalar SNORT performansını %33 oranında artırmıştır. Bizim yaptığımız çalışma mimari olarak yazarların yaptıkları çalışmaya benzer olsa da bizim yaptığımız çalışma web tabanlı saldırıların denetimini gerçekleştirmek için geliştirilmiş hibrit bir modeldir. Fakat yazarların yaptığı çalışma ağ tabanlı saldırıların denetimini yapmak için geliştirilmiştir. Hendry ve diğerleri [18] yaptıkları çalışmada, ağ tabanlı saldırılara karşı anormal tabanlı denetim algoritması gerçekleştirerek, imza üretimi yapmışlardır. Böylece imza tabanlı denetimin sıfır gün saldırılarına karşı etkili olmama özelliği bertaraf edilmiştir. İmza üretimi için hibrit, danışmanlı ve danışmansız sınıflandırma algoritması önerilmiştir. Gerçek zamanlı olarak oluşturulan imzalar yeni saldırıları denetlemek için gerçek zamanlı olarak devreye girmektedir. Yazarlar farklı yöntemler kullanarak önerilen çalışmaya benzer hibrit bir çalışma gerçekleştirmişlerdir, ama yazarların yaptığı çalışmada ağ tabanlı yapılan saldırılara karşı denetim gerçekleştirilirken, bizim yaptığımız çalışmada web tabanlı saldırılara karşı denetim gerçekleştirilmesi amaçlanmıştır. Yukarıda önerdiğimiz çalışmayla benzerlik gösteren çalışmalardan bahsedilmiştir. Yapılan çalışmalarda farklı yöntemler kullanılarak web tabanlı saldırılara ve ağ tabanlı saldırılara karşı farklı denetim modelleri geliştirilmeye çalışılmıştır. Kullanılan yöntemler arasında farklı yapay zeka ve veri madenciliği teknikleri bulunmaktadır. Yukarıda kısaca özetlenen çalışmalarda ATD, İTD, öğrenme tabanlı denetim ve hibrit çalışmalar gerçekleştirilmiştir. ATD modelleri yavaş çalıştıkları için gerçek zamanlı web uygulamalarında tercih edilmemektedirler ama sıfır gün saldırılarına etkili oldukları için tercih edilmektedirler. İTD modelleri ise daha hızlı çalışmaktadırlar, ama sadece imza olarak tanımlanan saldırı türlerine karşı etkilidirler. Bu çalışmada önerilen modelle, İTD yönteminin, bilinen saldırı türlerine karşı etkili olması ve hızlı çalışması özelliklerinin kullanılması ve ATD yönteminin ise sıfır gün saldırılarına karşı etkili olması ve yeni durumlara karşı kendini yenilemesi özellikleri kullanılarak, benzer çalışmalardan farklı olarak İTD ve ATD yöntemlerinin bir arada kullanıldığı hibrit bir model önerilmiştir. Literatürde [15], [17] ve [18] numaralı çalışmalar da hibrit çalışmalardır ancak ağ tabanlı saldırılara yönelik olarak yapılmışlardır. Çalışma [16] hibrit bir çalışmadır ama sadece kod enjeksiyonu saldırıları için yapılmıştır. Önerdiğimiz modelde İTD ile *SQL Enjeksiyonu*, *Siteler Arası Kod (XSS) Yazma* saldırı türlerine karşı denetim yapılmıştır. ATD ile ise şeçilen üç öznitelikle bayes sınıflandırma gerçekleştirilerek anormal HTTP isteklerinin denetimi gerçekleştirmiştir. İTD hızlı çalışırken sıfır gün saldırılarına karşı etkili değildir. ATD yöntemi ise sıfır gün saldırılarına karşı etkilidir. Dolayısıyla her iki yöntem beraber kullanılarak, mevcut yöntemlerin avantajları ön plana çıkarılmıştır. Anormal olarak tespit edilen istekler ile İTD veri tabanı güncellenerek, aynı istek web uygulamasına tekrar geldiği zaman, İTD'ye göre daha yavaş çalışan ATD sürecine dahil olmadan İTD gerçekleştirilerek anormal istekler engellenebilmektedir. Önerilen modeli benzer çalışmalardan ayıran diğer özelliği ise web uygulamasına ulaşan normal istekleri tespit ederek, aynı istek kullanıcılar tarafından tekrar talep edildiğinde, daha önceden normal olarak belirlendiği için sadece İTD gerçekleştirilip ATD gerçekleştirilmeden web uygulamasına erişim sağlanmaktadır. Bu özelliği sistemin hız performansını artırmaktadır.

3. ÖNERİLEN İMZA TABANLI VE ANORMAL TABANLI HİBRİT DENETİM MODELİ
(PROPOSED SIGNATURE-BASED AND ANOMALY-BASED HYBRIT DETECTION MODEL)

Bu çalışmada önerilen model İTD ve ATD modelleri kullanılarak geliştirilen hibrit bir sistemdir. İmza tabanlı denetimde *SQL (Structured Query Language) Enjeksiyonu*, *Siteler Arası Kod (XSS) Yazma* türleri için İTD gerçekleştirilmiştir. ATD için *Alfanümerik Karakter, Harf Frekans* ve *Cümle Uzunluğu* denetimleri yapılarak bu denetimler sonucu elde edilen verilerle veri madenciliği yöntemlerinden, bayes sınıflandırma gerçekleştirilerek anormal istekler tespit edilmektedir. Bayes sınıflandırma ile İTD veri tabanı güncellenmektedir.

3.1. İmza Tabanlı Denetim (Signature-Based Detection)

Web uygulamalarına karşı yapılan değişik türde saldırılar bulunmaktadır. Bu çalışmada, İTD gerçekleştirmek için, web tabanlı saldırılarda en yaygın olarak kullanılan *SQL (Structured Query Language) Enjeksiyonu* ve *Siteler Arası Kod (XSS) Yazma* saldırı türleri kullanılmıştır.

3.1.1. SQL Enjeksiyonu (SQL injection)

SQL enjeksiyonu, kullanıcı girdilerine göre SQL cümleleri oluşturan web uygulamalarında, kullanıcı girdilerinin doğrulanmaması veya yetersiz doğrulanmasından kaynaklanan zafiyetlerin kullanılarak, SQL cümlelerinin kötüye kullanılmasını sağlayan sızma testleridir [1]. SQL enjeksiyonu sızma yöntemiyle yapılabilecek işlemler aşağıda sıralanmıştır.

- Veri tabanları üzerinde işlemler (sorgulama, ekleme, silme, değiştirme, vb.) yapılabilir.
- Kimlik doğrulama mekanizmaları atlatılabilir.
- İşletim sistemi seviyesinde komutlar çalıştırılabilir.
- Etki alanında yeni kullanıcılar veya gruplar oluşturulabilir.

3.1.2. Siteler arası kod yazma XSS (Cross site scripting)

HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılabilmesi olarak tanımlanır. XSS genellikle HTML/JavaScript dilinde yazılmaktadır, ancak VBScript, ActiveX, Java, Flash veya web tarayıcılar tarafından desteklenen diğer dillerde de kodlama yapılabilmektedir [19]. İmza tabanlı denetim kötüye kullanım olarak

tanımlanan denetim türüdür. Ağ trafiği incelenerek saldırının karakteristiği, davranışı ve içeriği incelenerek ortaya çıkarılır [20]. İmza tabanlı sistemler genelde hızlı çalışırlar ve sadece imza veri tabanında bulunan saldırı türlerine karşı etkilidirler [21]. Yeni bir saldırı tekniği geliştirildiğinde belirtilen sistemin etkili olabilmesi için İTD veri tabanının saldırı tekniğine göre güncellenmesi gereklidir. Aksi takdirde yapılan saldırılara karşı etkisiz olacaktır.

3.2. Anormal Tabanlı Denetim (Anomaly-Based Detection)

Anormal HTTP istekleri normal HTTP isteklerinden farklı davranış gösteren sıradışı istek tipleridir. ATD ile herhangi bir saldırı türüne karşı değil, web uygulamasının HTTP istek yapısına uymayan isteklerin denetimi amaçlanmıştır. Normal HTTP istek yapısına uymayan isteklerin denetimini gerçekleştirebilmek için Harf Frekans, Cümle Uzunluğu, Alfanümerik Karakter ve İstek Sayısı olmak üzere 4 öznitelik belirlenmiştir. ATD iki aşamadan oluşmaktadır; birinci aşama bayes sınıflandırmanın işlemi giriş değerlerini oluşturmak için öznitelik seçimi, ikinci aşama ise, bayes sınıflandırma kullanılarak anormal HTTP isteklerinin tahmin edilmesidir. Belirlenen özniteliklerin denetim performansları her bir öznitelik için ayrı ayrı tespit edilerek bayes sınıflandırma işleminde kullanılıp kullanılamayacakları ortaya çıkarılmıştır. Özniteliklerin seçimi, *alfanumerik karakter* özniteliği için (1) numaralı eşitliğin, *istek uzunluk* özniteliği için (2) numaralı eşitliğin, *istek frekans* özniteliği için (3) numaralı eşitliğin ve *istek sayısı* özniteliği için (4) numaralı eşitliğin kullanılmasıyla, birbirinden bağımsız olarak herbir özniteliğin anormal HTTP isteklerini denetim performansına göre yapılmıştır. Şekil 1'de seçilen özniteliklerin, CSIC 2010, ECML-PKDD 2007 ve bu çalışma için özel olarak üretilen WUGD 2015 ismi verilen, veri kümelerine göre ATD performans değerleri yüzde (%) olarak verilmiştir. Şekil 1'e göre öznitelikler denetim performanslarına göre karşılaştırıldığında, farklı veri kümelerine göre *istek sayısı* özniteliğinin anormal HTTP isteklerini denetim performans değerleri diğer özniteliklerden daha düşük olduğu için ATD özniteliği olarak seçilmemiştir. Çünkü ATD'de anormal verinin hızlı ve doğru olarak tespit edilebilmesi için denetim özniteliklerinin sayısının düşük ve denetim performanslarının yüksek olması, yanlış pozitif değerini de düşürmektedir.

3.2.1. Alfanümerik karakter analizi (Alphanumeric character analysis)

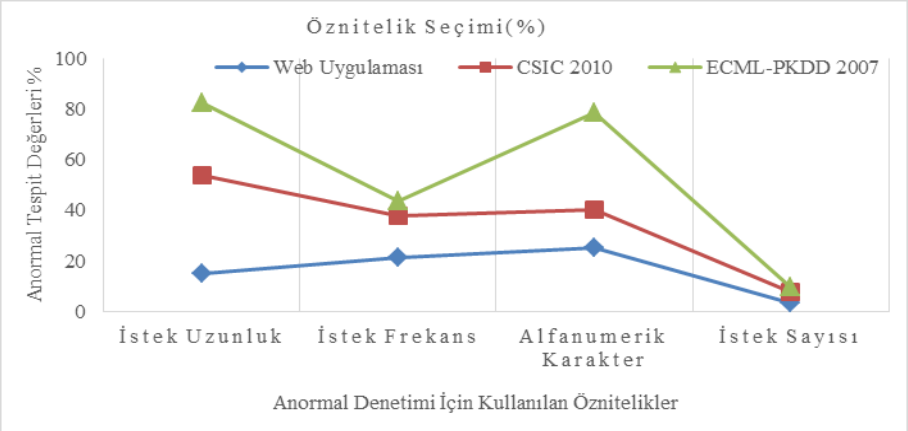
Alfanümerik, latin alfabesindeki harf ve rakam (A-Z, a-z, 0-9) kullanan karakter dizisini tanımlamak için kullanılır. Benzer şekilde bu dizinin elemanlarından her biri de alfanümerik olarak tanımlanır. Bilgisayarların veri saklama anında optimum hafıza kullanımına imkan sağlamak için oluşturulmuş bir tanım kümesidir. Byte içinde alfanümerik değerin ASCII karşılığı tutulur [22]. Web uygulamasına gelen istekler belirli karakter dizisine sahiptir. Belirlenen bu karakter dizilerinin (A-Z, a-z, 0-9) dışında bulunan ASCII karakterler içeren HTTP istekleri, bulunan karakter sayısı ölçüsünde anormal olarak belirlenmektedir. Alfanümerik karakter analiz için (1) nolu eşitlik kullanılmıştır.

$$T = \sum_{i}^{N} R_i \in E \mid (T+1) \tag{1}$$

T = Toplam Alfanümerik Karakter Değeri,
R = HTTP İsteği,
N = İsteği Oluşturan Toplam Karakter Sayısı,
E = Evrensel Küme,

3.2.2. İstek uzunluk analizi (Request length analysis)

Web uygulamasının geliştirilme yapısına göre web uygulamasına gelen isteklerin belirli bir istek yapısı vardır. Dolayısıyla bu istek yapısının özelliklerinden biri de istek uzunluğudur. Bellek taşması ve siteler arası betik yazma saldırılarının istek uzunluk değerleri normal isteklerden farklıdır. Nguyen ve diğerleri [7] tarafından yapılan çalışmaya göre isteklerin ortalama uzunluk ve varyans değerleri kullanılmıştır. İstek uzunluk analizi için (2) nolu eşitlik kullanılmıştır.



Şekil 1. Farklı Veri Kümelerine Ait Öznitelik Seçim Değerleri (Feature Selection Values of Different Datasets)

$$p = \sigma 2 /(1 - \mu)2 \quad (2)$$

P = Olasılık
μ = Ortalama (İsteklerin ortalama değerleri)
σ = Varyans (isteklerin varyans değerleri)
l = uzunluk (kontrol edilen isteğin uzunluk değerleri)

(2) Formüle göre HTTP isteğinin uzunluk değerinin sıfır (0) olması anormallik sınır değerini belirlemektedir. Her bir isteğin anormal olma olasılık değeri formüle göre hesaplanarak bulunan değer, uzunluk değeri sıfır (0) olan isteğin anormallik değerinden küçük ise, söz konusu istek anormal olarak belirlenmektedir. Dolayısıyla istek uzunluk değeri arttıkça isteğin anormal olma olasılığı artmaktadır.

3.2.3. İstek frekans analizi (Request frequency analysis)

Karakter dağılımı modeliyle isteklerin karakter (harflerin) frekans değerleri belirlenmektedir. Web uygulamasına gelen normal HTTP isteklerini oluşturan karakterlerin harf frekans değerleri normal olmayan isteklerin harf frekans değerlerine göre yüksektir. Karakter dağılımında ASCII karakterleri kullanılmaktadır. ASCII karakterleri, 0 ile 255 arasında 8 bit değer alan yazılabilen harf ve rakam karakterlerdir. İstek frekans analizi için (3) nolu eşitlik kullanılmıştır.

$$T = \sum_{i}^{N} R_i \in ASCII \mid T + F(R_i) \quad (3)$$

T = Toplam Frekans Değeri
R = HTTP İsteği
N = İsteği Oluşturan Toplam ASCII Karakter Sayısı
F = İstek Harf Frekans Toplamı

Harf frekans analizi daha çok kriptoanaliz yöntemlerinde kullanılan bir tekniktir. Bu çalışmada gelen isteklerdeki her bir karakterin toplam sayısı ve ortalama değerini tespit etmek için harf frekans analizi yapılmaktadır. Örnek olarak *index.php?secim=9&mid=50* gibi bir istek ele alındığında bu cümleyi oluşturan harflerin frekansı ve ortalama değerleri elde edilmektedir. Frekans değerleri gelen bütün isteklerdeki her bir karakterin sayısını verirken, ortalama değer ise her bir karakterin toplam değerinin gelen istek sayısına bölünmesi ile bulunmaktadır.

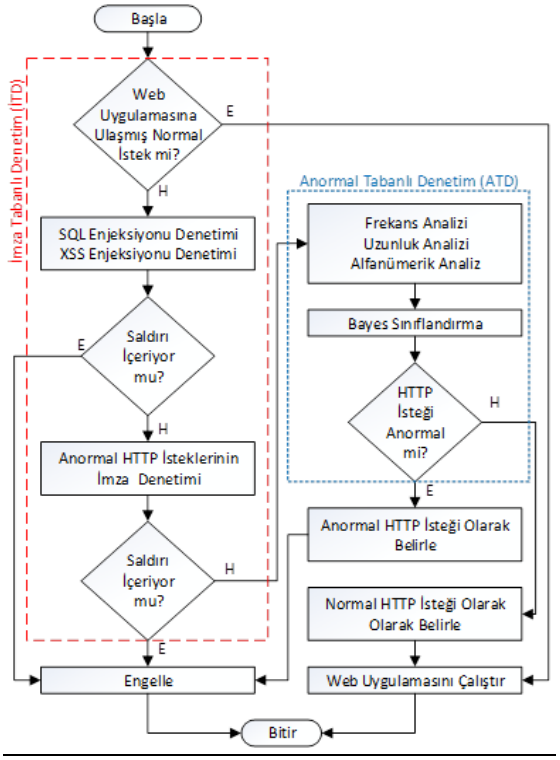
3.2.4. İstek sayısı analizi (Request count analysis)

Web uygulamasının yapısına göre gelen normal istekler kullanıcılar tarafından web sitesinin ziyaret sayısına göre sürekli olarak tekrarlanmaktadır. Çünkü farklı kullanıcılar web sitesinden farklı zamanda aynı istekte bulunmaktadırlar. Anormal olan aynı isteklerin, normal isteklere göre tekrarlanma oranları daha düşük olmaktadır. İstek frekans analizi için (4) nolu eşitlik kullanılmıştır [6].

$$T = \sum_{i}^{N} R_i \in E\ (T + 1) \quad (4)$$

T = Tekrar Eden İstek Sayısı
R = HTTP İsteği
N = Veri kümesindeki Toplam İstek Sayısı
E = Evresel Küme

Şekil 2'de önerilen modelin akış diyagramı verilmiştir. Önerilen hibrit model; İTD ve ATD olmak üzere iki aşamadan oluşmaktadır. İTD yöntemi kendi içinde üç aşamadan oluşmaktadır. Bunlar sırasıyla, web uygulamasına ulaşmış normal HTTP isteklerinin denetimidir. Web uygulamasına ulaşan normal istekler farklı bir kullanıcı tarafından da olsa, tekrar aynı web uygulamasına ulaştığı zaman sistem tarafından denetimi gerçekleştirilmeden web uygulamasına erişimi sağlanmaktadır. İTD'nin diğer aşaması bilinen web tabanlı saldırı türlerinden *SQL Enjeksiyonu* ve *XSS Enjeksiyonu* saldırı türleri için İTD yapılmaktadır. Eğer HTTP isteği *SQL Enjeksiyonu* ve *XSS Enjeksiyonu* saldırılarından birini içeriyorsa doğrudan engellenmektedir. İTD'nin bir diğer aşaması, ATD sonucu anormal HTTP istekleri tespit edilmektedir ve tespit edilen anormal HTTP istekleri, tekrar web uygulamasına geldiği zaman ATD yapılmadan İTD yapılarak engellenmektedir. Bu işlemin amacı, web uygulamasının yapısına göre imza üretimi gerçekleştirmektir ve ATD sonucunda anormal olarak tespit edilen HTTP isteklerinin denetimi ikinci kez ATD yapılmadan gerçekleştirilerek anormal HTTP istekleri engellenmektedir.



Şekil 2. Önerilen Modelin Akış Diyagramı
(Flow Chart of Proposed Model)

ATD yöntemi de kendi içinde iki aşamadan oluşmaktadır. ATD'nin birinci aşamasında, seçilen *Alfanümerik Karakter, İstek Uzunluk* ve *İstek Harf Frekans* öznitelikleri

kullanılarak HTTP istekleri sayısallaştırılmaktadır. İkinci aşamada ise, öznitelik değerlerine göre bayes sınıflandırma yapılarak anormal HTTP istekleri tahmin edilmektedir. ATD sonucu anormal HTTP istekleri tespit edilmektedir. Tespit edilen anormal HTTP istekleri, tekrar web uygulamasına geldiği zaman ATD yapılmadan denetimi yapılarak engellenmesi için anormal HTTP isteklerinin imza veri tabanına eklenerek ikinci defa web uygulamasına geldiklerinde İTD yöntemi ile doğrudan engellenmesi sağlanmaktadır. Böylece web uygulamalarının istek yapılarına göre İTD imza veri tabanı güncellenerek modelin yeni saldırı türlerine karşı kendini yenilemesi gerçekleştirilmektedir. İTD türünün yeni saldırı türlerine karşı etkili olmama özelliği bertaraf edilmiş olmaktadır ve yeni saldırılara karşı dayanıklı hale getirilmesi sağlanmıştır. Ayrıca anormal HTTP istekleri ile imza veri tabanının güncellenmesinin bir diğer amacı İTD, ATD'ye göre daha hızlı çalıştığı için gerçekleştirilen modelin hız performansının da artırılması amaçlanmıştır. ATD kullanılarak yapılan HTTP istek denetiminde veri madenciliği araçlarından, bayes sınıflandırma teoremi kullanılmıştır. Bayes teoremi (5), bir olayın meydana gelmesinde birbirinden bağımsız birden fazla etkenin olması koşulunda, olayın hangi etkenin etkinliği ile ortaya çıktığını gösterir [23].

$$P(h \mid D) = (P(D|h)P(h))/(P(D)) \quad (5)$$

P(h) = h olayının önsel (marjinal) olasılığı
P(D) = D eğitim verisinin önsel olasılığı
P(D|h) = h olayı verildiğinde D' nin koşullu olasılığı
P(h|D) = D eğitim verisi verildiğinde h'nin koşullu olasılığı

Bayes sınıflandırma, makine öğreniminde öğreticili öğrenme sınıfındadır ve sınıflandırılması gereken kümeler ve örnek verilerin hangi sınıflara ait olduğu bellidir. Sınıflandırma işleminde genel olarak elde bir örüntü vardır. Buradaki işlem de bu örüntüyü daha önceden tanımlanmış sınıflara göre sınıflandırmaktır. Her örüntü kullanılan özniteliklerle temsil edilir. Bayes sınıflandırma ile öznitelikler arasında ilişki bulunarak her bir değişkenin değerine göre isteğin anormal olup olmadığı tahmin edilmektedir. Değeri 1 (bir) olan öznitelik anormal, 0 (sıfır) olan öznitelik normal istek olarak belirlenmiştir. Her bir isteğin üç farklı özelliğe göre anormal veya normal olarak belirlenmesi uzman görüşü alınarak tespit edilmiştir.

4. SONUÇLAR VE TARTIŞMALAR
(RESULTS AND DISCUSSION)

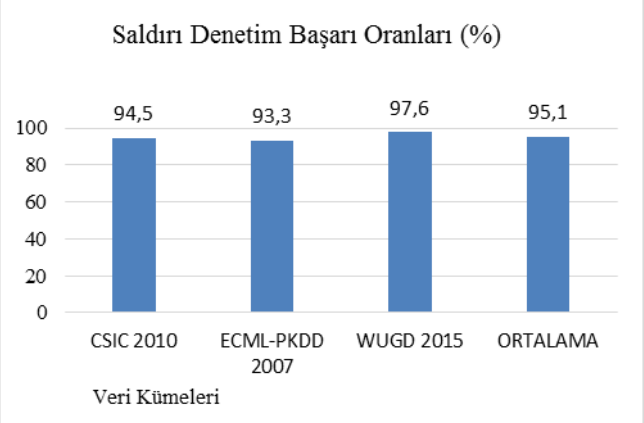
Bu bölümde önerilen modelin değerlendirilmesi, İTD ve ATD türlerinin oluşturduğu hibrit modelin denetim performansının, en uygun yapılandırma parametre tespitinin ve yanlış pozitif oranının belirlenmesi için yapılmıştır. Modelin değerlendirilmesi için benzer çalışmalarda kullanılan CSIC 2010, ECML-PKDD 2007 veri kümeleri ve gerçek zamanlı web uygulamasına gömülü olarak koşturularak elde edilen WUGD 2015 HTTP veri kümesi kullanılmıştır.

4.1. Veri Kümeleri (DataSets)

Saldırı önleme ve belirleme sistemlerini değerlendirmek için saldırıların yanı sıra normal kabul edilen verileri de içeren test veri kümeleri kullanılmaktadır. Fakat HTTP trafiği ele alındığında, yaygın olarak kullanılabilir veri kümeleri çok azdır. Çünkü var olan çoğu veri kümesi ihtiyaç duyulan HTTP istek ve cevap verilerini içermemektedirler [24]. Bu çalışmada örnek web uygulaması, CSIC 2010 ve ECML-PKDD 2007 veri kümeleri kullanılmıştır. ECML-PKDD 2007 veri kümesinin %20'si saldırı olan 50000 örnekten oluşan HTTP istekleri saldırı ve normal trafik olarak etiketlenmiştir. Kullanılan CSIC 2010 veri kümesi web tabanlı saldırı denetimi amacıyla otomatik olarak üretilen; 36000 normal ve 25000'den fazla anormal HTTP isteklerinden oluşmaktadır. Ek olarak toplam isteklerin yaklaşık % 30'u anormal olan ve SQL enjeksiyonu, bellek taşması ve XSS saldırı türlerini de içeren, gerçek zamanlı çalışan web uygulamasından üretilmiş veri kümesi de kullanılmıştır.

4.2. Değerlendirme Sonuçları (Evaluation Results)

Bayes sınıflandırmanın gerçekleştirilmesi için *Alfanümerik Karakter*, *Harf Frekans* ve *Cümle Uzunluğu* olmak üzere 3 öznitelik kullanılmıştır. Şekil 3'te İTD ve ATD sonucunda tespit edilen saldırı içeren veya anormal HTTP isteklerinin kullanılan özniteliklere göre başarı oranı verilmiştir. ATD, *WUGD 2015*, *CSIC 2010* ve *ECML-PKDD 2007* öznitelikleri kullanılarak Şekil 1'de bahsedilen veri kümeleri ile değerlendirilmiştir. Şekil 3'e göre kullanılan veri kümelerinde belirlenen anormal isteklerin denetim özniteliklerine göre denetim yüzdeleri verilmiştir. Anormallik tahmini bayes sınıflandırma yöntemi kullanılarak gerçekleştirilmiştir.



Şekil 3. Önerilen Modelin Üç Farklı HTTP Veri Kümesi Kullanıldığındaki Saldırı Denetim Başarı Oranı
(Attack Detection Performance Rate with Reference To Three HTTP Datasets for Proposed Model)

CSIC 2010 veri kümesinde bulunan anormal isteklerin % 94,5'i, ECML-PKDD 2007 veri kümesinde bulunan anormal isteklerin % 93,3'ü ve WUGD 2015 veri kümesinde bulunan anormal isteklerin ise % 97,6'sı

Tablo 1. Öznitelik, Sınıflandırma ve Veri Kümeleri Karşılaştırma (Comparison for datasets, feature, and classification)

Çalışma	İTD	ATD	Öznitelik	Sınıflandırma Yöntemi	Veri Kümesi	% ±fp*
Nguyen vd. [7]	*x*	√	√ (30 Öznitelik)	C4.5, CART, RandomTree, Randomforest	ECML-PKDD 2007 CSIC 2010	97,04 ±2,95 93,65 ±6,9
Cho vd. [10]	*x*	√	Oturum Parametre (Session Parametre)	Bayes Sınıflandırma	Web Log Verileri	90 ±6
Kirchner vd. [25]	*x*	√	*x*	K-Means	Çalışma İçin Veri Kümesi	90,9 ± 0,7
Önerilen Model	√	√	Alfanümerik Karakter, Frekans Analizi, Cümle Uzunluğu	Bayes Sınıflandırma	ECML-PKDD 2007 CSIC 2010 WUGD 2015	93,3 ± 0,6 94,5 ± 0,3 97,6 ± 0,2

fp* : false positive (yanlış pozitif)

anormal olarak tespit edilmiştir. Bütün veri kümelerinde yapılan denetim sonuçlarına göre ortalama olarak % 95,1 oranında başarılı şekilde ATD gerçekleştirilmiştir. İTD ile denetimi gerçekleştirilen SQL Enjeksiyonu ve XSS saldırı türlerinin tamamının tespiti gerçekleştirilmiştir. ATD ile İTD veri tabanı güncellenmektedir. Anormal denetimi gerçekleştirilerek anormal imza veri tabanına eklenen anormal olarak tespit edilen isteklerin %83'ü tekrar web uygulamasına gelerek İTD ile, ATD gerçekleştirilmeden engellenmiştir. Web uygulamalarının mimari yapısı uygulamaların geliştirilme sürecine göre ve kullanılan teknolojiye göre değişiklik göstermektedir. Dolayısıyla web uygulamalarının HTTP istek yapısı da uygulamanın geliştirilme teknolojisine göre ve geliştirilme yöntemine göre değişiklik göstermektedir. ATD sonucunda tespit edilen anormal istekler de her web uygulamasında farklı yapıya sahip olmaktadırlar. ATD ile tespit edilen anormal HTTP istekleriyle, İTD veri tabanının güncellenmesi, sistemin güvenliğini sağladığı web uygulamasının yapısını öğrenerek anormal HTTP isteklerinin İTD ile, ATD gerçekleştirilmeden tespit edilmesini sağlamaktadır. Böylece ATD'ye göre daha hızlı çalışan İTD sayesinde, hem sistem adaptasyonu gerçekleştirilmiştir hem de sistemin hız performansı artırılmıştır.

4.3. Karşılaştırma (Comparison)

Bu çalışmada önerilen model web tabanlı saldırıları önleme amaçlı yeni bir hibrit web uygulaması güvenlik duvarı algortirması yaklaşımıdır. Web tabanlı saldırıları engellemek için benzer çalışmalar yapılmıştır. Bu çalışmaların karşılaştırılması Tablo 1'de verilmiştir. Önerilen modeli diğer çalışmalardan ayıran en önemli özellik hibrit bir yöntem olmasıdır.

5. SONUÇLAR (CONCLUSIONS)

Bu çalışmada, web tabanlı saldırıları önlemek için hibrit bir sistem önerilmiş ve sistemin uygulaması gerçekleştirilmiştir. Web uygulamalarına yapılan saldırıların denetimi İTD yöntemi ve ATD yöntemi kullanılarak gerçekleştirilmiştir. ATD için *Alfanümerik Karakter*, *Harf Frekans* ve *Cümle Uzunluğu* olmak üzere üç öznitelik kullanılmıştır. Öznitelik denetimlerinden elde edilen sonuçlara göre bayes sınıflandırma gerçekleştirilerek anormal HTTP istekleri tespit edilmiştir. Bayes sınıflandırma sonucu anormal olarak belirlenen anormal istekler İTD veri tabanına eklenerek İTD veri tabanının güncellenmesi sağlanmaktadır. Bu sayede imza olarak belirlenen anormal HTTP istekleri tekrar web sitesine geldiği zaman ATD gerçekleştirilmeden İTD ile engellenmektedir ve böylece hem hız arttırılmakta hem de yeni saldırı türlerine karşı sistemin adaptasyonu gerçekleştirilmektedir. Dolayısıyla web uygulamasının istek yapısına göre İTD veri tabanı güncellenerek İTD'nin dezavantajı olan yeni saldırı türlerine karşı etkili olmama özelliği ortadan kaldırılmaya çalışılmıştır.

TEŞEKKÜR (ACKNOWLEDGEMENT)

Bu çalışma, Bilim Sanayi ve Teknoloji Bakanlığının SANTEZ projeleri kapsamında 0235.STZ.2013-1 kodlu SANTEZ projesi ile desteklenmiştir.

KAYNAKLAR (REFERENCES)

1. Lara J., Gracia G., Building Web Application Firewalls in High Availability Environments, Web Application Security, Springer Berlin Heidelberg, Berlin-Almanya, 72, 75-82, 2010.
2. Vural Y., Sağıroğlu Ş., A Review on Enterprise Information Security and Standards, Journal of the Faculty of Engineering and Architecture of Gazi University, 23 (2), 507-522, 2008.
3. Torrano-Gimenez C., Nguyen H., Alvarez G., Franke K., Combining expert knowledge with automatic feature extraction for reliable web attack detection, Security And Communication Networks, 8 (16), 2750–2767, 2015.
4. Valeur F., Mutz, D., Vigna G., A Learning-Based Approach to the Detection of SQL Attacks, in Proc. DIMVA, Cilt 3548, 123-140, 2005.

5. Gupta N., Saikia A., Sanghi D., Web Application Firewall, CS499: B. Tech Project Final Report, 2008.

6. Tekerek A., Gemci C., Bay O., F., Development of a Hybrid Web Application Firewall to Prevent Web Based Attacks, 2014 IEEE 8th International Conference on Application of Information and Communication Technologies IEEE, Astana-Kazakistan, 1-4, 15-17 Ekim, 2014.

7. Nguyen H.T., Torrano-Gimenez C., Alvarez C., Franke K., Petrovic S., "Enhancing the effectiveness of Web Application Firewalls by generic feature selection, Logic Journal of IGPL, 21 (4), 560-570, 2011.

8. Palka D. ve Zachara M., Learning Web Application Firewall - Benefits and Caveats, Availability, Reliability and Security for Business, Enterprise and Health Information Systems, Cilt 6908, Editör: Tjoa, A.M., Quirchmayr, G., You, I., Xu, L., Springer Berlin Heidelberg, 295–308, 2011.

9. Basile C., Lioy A., Analysis of Application-Layer Filtering Policies With Application to HTTP, IEEE/ACM Transactions On Networking, 23 (1), 28-41, 2015.

10. Cho S., Cha S., SAD: Web Session Anomaly Detection Based on Parameter Estimation, Computers & Security, 23 (4), 312-319, 2004.

11. Razzaq A., Ahmed H.F., Hur A., Haider N., Ontology based application level intrusion detection system by using Bayesian filter, Computer Control and Communication 2009 IC4 2009 2nd International Conference on, Karachi-Pakistan, 1 – 6, 17-19 Şubat, 2009.

12. Bremler-Barr A., Koral A., Accelerating Multipattern Matching on Compressed HTTP Traffic, IEEE/ACM Transactions On Networking, 20 (3), 2012.

13. Singh S., Agrawal,S., Rizvi M.A., Thakur R.S., Improved Support Vector Machine for Cyber Attack Detection, Proceedings of the World Congress on Engineering and Computer Science, San Francisco-USA, 19-21 Ekim, 2011.

14. Torrano-Gimenez C., Perez-Villegas A., Alvarez G., A Self-learning Anomaly-Based Web Application Firewall, Computational Intelligence in Security for Information Systems, Editörler: Herrero, A., Gastaldo, P., Zunino, R., Corchado E., Springer-Verlag Berlin Heidelberg, 85–92, 2009.

15. Peng J., Feng C., Rozenblit JW., A hybrid intrusion detection and visualization system, 13th Annual IEEE International Symposium and Workshop on Engineering of Computer Based Systems, Proceedings: Mastering The Complexity Of Computer-Based Systems, 505-506, 2006.

16. Locasto M. E., Wang K., Keromytis A. D., Stolfo S. J., FLIPS Hybrid adaptive intrusion prevention, Recent Advances In Intrusion Detection Lecture Notes in Computer Science , 3858, 82-101, 2006.

17. Hwang K., Cai M., Chen Y., Qin M., Hybrid intrusion detection with weighted signature generation over anomalous Internet episodes, IEEE Transactions On Dependable And Secure Computing, 4 (1), 41-55, 2007.

18. Hendry G., Yang S., Intrusion signature creation via clustering anomalies, Data Mining, Intrusion Detection, Information Assurance, And Data Networks Security, Proceedings of SPIE, 2008.

19. Cook S., A Web Developer's Guide to Cross-Site Scripting, SANS Institute, Los Angeles, USA, 2003.

20. Roesch M., Snort-lightweight intrusion detection for networks, 13th Systems Administration Conference-LISA'99, Seattle Washington-USA, 229–238, 7–12 Kasım, 1999.

21. Raut A.S., Singh K.R., Anomaly Based Intrusion Detection-A Review, Int. J. on Network Security, 5, 1-5, 2014.

22. Verma N., Mishra V., Singh V.P., Detection of alphanumeric shellcodes using similarity index, Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on, New Delhi-India, 1573 - 1577, 2014.

23. Ingham K., Anomaly Detection for HTTP Intrusion Detection: Algorithm Comparisons and the Effect of Generalization on Accuracy, Doktora Tezi, University of New Mexico, Albuquerque-USA, 2007.

24. Bishop C.M., Pattern Recognition and Machine Learning, M. Jordan, J. Kleinberg, B. Schölkopf, Springer, New York-USA, 2006.

25. Kirchner M., A framework for detecting anomalies in HTTP traffic using instance-based learning and k-nearest neighbor classification, Security and Communication Networks (IWSCN), 2010 2nd International Workshop on, Karlstad-İsveç, 1–8, 2010.