Vize Ödevi

Siber Güvenlik için Veri Madenciliği

Harran Üniversitesi
Bilgisayar Mühendisliği

Kerem SÖYLEMEZ (200504060)
Hasan GÜRSES (180504082)

Kullanım nedenlerimiz : (Random Forest)

1. Yüksek Performans ve Hassasiyet
Random Forest, sınıflandırma ve regresyon problemlerinde diğer algoritmalara göre yüksek performans gösterir. Ensemble (topluluk) öğrenme yöntemi olarak, birden çok karar ağacını birleştirerek daha güçlü ve kararlı bir model elde edilmiş olunur.
Birden çok karar ağacının bir araya getirilmesiyle tek bir ağaç yerine birçok yapının (ağaç) birleşmesiyle daha başarılı bir genelleme yeteneği elde edilir.

2. Özellik Önem Sıralaması:
Random Forest, her ağacın oluşturulması sırasında rastgele seçilen özelliklerle eğitildiği için modelin özellik önem sıralamasını sağlama imkânı elde edinilebilir.
Bu şekilde en büyük kazanım hangi özelliklerin modelin kararlarını daha fazla etkilediğini anlaşılmasını öğrenilebilinir.

3. Aşırı Öğrenmeye Karşı Direnç:
Random Forest tekniklerinden rastgele özellik seçimi ve rastgele örnek seçimi gibi randomizasyon teknikler bu algoritmayı aşırı öğrenmeye karşı dirençli hale getiriyor.
Bu şekilde modelin eğitim verilerine aşırı özelleşip genelleme yapma yeteneğini kaybetme riskini azaltıyoruz.

4. Geniş Veri Kümeleri ile Başa Çıkma Yeteneği:
Random Forest, genellikle büyük veri setleriyle çalışmak için etkilidir. Biz de NSL – KDD ile çalıştığımızdan bizim için de etkili olmuştur. Çalışmada ise yüksek boyutlu veri kümeleri ağaçlarını rastgele alt kümelerini kullanıp ve sonradan bu ağaçlar birleştirdik. Bu şekilde modelin daha iyi bir performans sergilemesine imkân sağlamış olduk.

5. Gürültülü Veriye Karşı Dayanıklılık:
Gürültülü veri, veri madenciliği projelerinde en yaygın sorunlardandır ve bu nedenle elde edilecek sonuç yüksek sapma payları ile hatalı çıkabilmekte. Random Forest ise bu anlamda sorunları gidermek adına gürültülü veriye karşı dayanıklıdır. Çalışma mantığı olarak Random Forest yapısında birden çok ağaç kullanılıp birleştirilmekte. Bu nedenle toplam bir ağaç havuzundan tek bir ağacın hatalarının sistemin genel model performansını etkileme olasılığı azaltılmış olunur.

Sonuç Olarak Hedefimiz:

Daha Doğru Tahminler: Random Forest algoritması diğer öğrenme algoritmalarından daha doğru tahminler yapma potansiyeline sahiptir. Bunu sağlayan ise bir çok farklı yapının (ağaç) bir araya gelip bir ortak veri oluşturmasıdır. Böylelikle birçok farklı veri ile çalışmış olup tahminler daha doğru olur (veri çokluğu tahmin doğruluğunu etkiler).
Sonuç olarak Random Forest algoritması ile verilerdeki karmaşık kalıpları daha iyi yakalayabiliriz.

Daha Kararlı Tahminler: Random forest algoritması diğer öğrenme algoritmalarına göre kararlı tahminler yapabilir. Bunun nedeni ise bu algoritma bir çok ağaç yapısından oluştuğundan bir çok farklı model elde edilmiş olur. Bu şekilde ise her karar ağacının farklı verileri görür.

Bu çeşitlilik ile eğitim verilerindeki gürültülü veya eksik veriler sistemin tümüne etki etmez.

Daha Dayanıklı Tahminler: Kullandığımız Random Forest algoritması diğer öğrenme algoritmalarına göre daha dayanıklıdır ve daha kapsamlı tahminler yapma potansiyeline sahiptir. Bunun nedeni ise önceki nedenlerle aynıdır ve bu 3 ana başlığı bu özellik ile elde ettik.

Spesifik Sıralama: Random Forest, her ağacın oluşturulması sırasında rastgele seçilen özelliklerle eğitildiği için modelin özellik önem sıralamasını sağlayabiliyoruz.
Sonuç olarak hangi özelliklerin modelin kararlarını daha fazla etkilediğini anlayabildik.

Tespit ve seçtiğimiz güvenlik tehditleri ise şunlardır:

- DoS
- U2R
- Probe
- R2L

DOS siber güvenlik için etkileri:

Sistem Zararı:

- **Hizmet Kesintisi (Service Disruption):** DoS saldırıları, hedef sistem veya ağın normal işleyişini engeller. Sonuç olarak ise hizmetleri kullanılamaz hale getirebilir. Bu durumda kullanıcılar normalde erişebildikleri hizmetlere erişimini zorlaşabilir veya engellenebilir.

- **Veri Kaybı ve Bozulma**: DoS saldırıları sırasında sistem ve ağ kaynakları yoğun bir şekilde meşgul edildiğinden mevcut işlemler sırasında veri kaybına veya bozulmasına neden olabilir. Bu ise kritik verilerin güvenliği açısından ciddi bir tehdit oluşturur.

- **İş Sürekliliği Sorunları:** DoS saldırıları hedef organizasyonun iş sürekliliğini etkileyebilir. Özellikle kritik iş süreçlerine ve hizmetlere yönelik saldırılar sistemin normal işleyişini engeller ve maddi zarara yol açar.

Maddi Zarar:

- **Finansal Kayıplar:** Bu saldırılar hedef organizasyona finansal kayıplara yol açabilir. İş sürekliliği sorunları gibi nedenlerin finansal sonuçları olumsuz etkiler.

- **Müşteri Memnuniyetsizliği:** Hedeflenen hizmette kesintiler ve erişim zorlukları, müşteri memnuniyetsizliğine yol açabilir. Bu ise uzun solukta müşterilerin güvenini zedeler ve rekabet avantajını kaybettirir.

- **Marka İtibarı Kaybı:** DoS saldırıları hedeflenen organizasyonun marka itibarına zarar verebilir. Bu da uzun vadeli müşteri kaybına neden olabilir.

Önlemler:
DoS saldırılarına karşı alınan önlemler; güvenlik duvarları, saldırı tespit ve önleme sistemleri, trafik filtreleme çözümleri, yedekleme sistemleri ve acil durum planları.

U2R siber güvenlik için etkileri:

U2R (User to Root) saldırıları, saldırganın normal kullanıcı yetkilerinden (user), sistem yönetici (root) yetkilerine yükselmesidir.

Etkileri:

Geniş Kontrol Yetkisi: Bu saldırılar sonucunda kişi sistem yönetici yetkilerine sahip oluğundan (ele geçirdiğinden); sistemi kontrol etme, konfigürasyonları değiştirme ve diğer süreçlerin üzerinde geniş bir yetkiye sahip olma hakkını elde etmiştir ve dilediğini yapabilir.

Veri Güvenliği ve Manipülasyon: Saldırgan root (yönetici) yetkilerine sahip olduğundan sistemin tüm verilerine erişim sağlayabilir ve bu verileri manipüle edebilir (bilgilerin çalınması veya değiştirilmesi).

Hizmet Kesintisi ve Bozulması: U2R saldırıları sistem hizmetlerin normal çalışmasını engelleyebilir. Bu durum iş sürekliliği sorunlarına ve hizmet kesintilerine neden olabilir.

Güvenlik Zafiyetlerinin Sömürülmesi: U2R saldırıları güvenlik açıklarının bulunup sömürülmesi yoluyla gerçekleşir. Bu, sistemlerdeki güvenlik zafiyetlerini artırabilir ve saldırganlara daha fazla zarar verme ve erişim fırsat sunabilir. Farklı saldırılara da imkan sağlanabilir.

Veri Kaybı ve Zarar: Saldırgan yönetici (root) yetkileriyle sistemi ele geçirdiği için, veri kaybına veya zarara neden olabilir. Bu durum sistemin önemli verilerini silinmesine veya kullanılamaz hale gelmesine yol açabilir.

Önlemler:

- Bu tür etkileri önlemek için; güvenlik politikalarının sıkı bir şekilde uygulanması, güvenlik açıklarının düzenli olarak taraması ve açıkların giderilmesi(sık güncellemeler), yetki yönetimi ve erişim kontrolü uygulanması.

Probe siber güvenlik için etkileri:

Güvenlik Zafiyetlerinin Belirlenmesi: Probe saldırıları, bir sistemin veya ağın güvenlik açıklarını belirlemek amacıyla gerçekleştirilir Bu kuruluşların güvenlik önlemlerini değerlendirmelerine ve potansiyel riskleri belirlemesine yardımcı olabilir.

Sistem ve Ağ Performansının Etkilenmesi: Kapsamlı bir probe aktivitesi sistem donanım kaynaklarını tüketebilir ve ağ performansını düşürebilir. Bu durum kullanıcılara hizmet vermede zorluklara yol açar (sistemsel).

Güvenlik İhlallerinin Erken Belirlenmesi: Probe aktiviteleri sistem için güvenlik sistemleri tarafından izlenebilir ve anomalide alarm verilebilir.

Reputasyon Kaybı: Zarar vermek isteyen kişi tarafından yapılan probe saldırısı bir kuruluşun itibarına zarar verebilir. Müşteri güveni kaybı ve maddi kayıplara neden olabilir.

Güvenlik Bilinci: Bu saldırılar ile bir kuruluşun güvenlik zafiyetlerini ve risklerini ortaya çıkartılabilir. Bu şekilde güvenlik bilinci arttırılabilir ve güvenlik önlemlerini güçlendirmek için bir öngörüler sunabilir.

Önlemler:
Bu etkileri önlemek için; güvenlik testleri yapmalı, güvenlik açıklarını düzenli olarak taranmalı, güvenlik önlemlerini güncellenmeli ve güvenlik politikaları sıkı bir şekilde uygulanmalıdır.

R2L siber güvenlik için etkileri:

"R2L" (Remote-to-Local), siber güvenlikte uzaktan bir sisteme veya ağa erişim sağlanarak lokal bir hedefe (local system) yetki kazanma girişimlerini ifade eder.

Gizlilik İhlali: R2L saldırısı bir sisteme yetkisiz erişim sağlanmasıyla hassas verilere ulaşma potansiyelini sağlar. Bu durum birçok gizli, kişisel, ticari bilgilerin veya diğer özel verilerin tehlikeye girmesine neden olur.

Yetki Kötüye Kullanımı: R2L saldırıları elde edilen yetkilerin kötüye kullanılması, sistemi ele geçirme ve kontrol etme amacıyla gerçekleşir. Bu şekilde sisteme giren kişinin yetkilerini genişleterek daha fazla zarar verebilmesine imkân tanır.

Veri Bozulması: Saldırgan bu saldırı sırasında sistem verilerine müdahale edebilir veya değiştirebilir. Bu ise tüm sistemin veri bütünlüğünü tehdit eder.

Servis Kesintisi: R2L saldırıları, hedef sistemdeki kaynakları normalin dışında aşırı kullanabilir ve hizmetleri aksatabilir. Bu sistemin normal çalışmasını engelleyerek hizmet ve servis kesintisine neden olabilir.

Güvenlik Duvarlarını Aşma: R2L saldırıları, güvenlik duvarlarını aşarak iç ağlara sızma girişiminde bulunabilir. Bu ise iç ağlardaki diğer sistemlere veya verilere erişim sağlama potansiyeline sahiptir ve daha büyük zararlara yol açma hakkı elde edilebilir.

İş Sürekliliği Sorunları: Sistemin ele geçirilmesi veya kontrol altına alınması, iş sürekliliği sorunlarına yol açabilir. Hizmetlerin ve süreçlerin aksamaması için önemli olan sistemlerin tehlikeye girmesi operasyonlarını ciddi şekilde etkileyebilir.

Önlemler: Bu etkileri önlemek için; güvenlik önlemleri almak, sistemlerde güvenlik açıklarını düzenli olarak taramak, güçlü yetki ve parola politikalarını uygulamak, güvenlik duvarları ve güvenlik yazılımları kullanmak.

Analiz Özeti ve Doğruluğu

Uyguladığımız veri madenciliği teknikleri:

Seçilen özellikler DoS: ['src_bytes', 'dst_bytes', 'wrong_fragment', 'num_compromised', 'count', 'srv_count', 'same_srv_rate', 'diff_srv_rate', 'dst_host_serror_rate', 'dst_host_rerror_rate', 'Protocol_type_icmp', 'service_ecr_i', 'flag_S0']
Seçilen özellikler Probe: ['src_bytes', 'dst_bytes', 'count', 'dst_host_srv_count', 'dst_host_same_srv_rate', 'dst_host_diff_srv_rate', 'dst_host_same_src_port_rate', 'dst_host_srv_diff_host_rate', 'dst_host_rerror_rate', 'dst_host_srv_rerror_rate', 'Protocol_type_icmp', 'service_eco_i', 'service_private']
Seçilen özellikler R2L: ['duration', 'src_bytes', 'dst_bytes', 'hot', 'num_failed_logins', 'dst_host_count', 'dst_host_srv_count', 'dst_host_same_srv_rate', 'dst_host_diff_srv_rate', 'dst_host_same_src_port_rate', 'dst_host_srv_diff_host_rate', 'service_ftp', 'service_ftp_data']
Seçilen özellikler U2R: ['duration', 'src_bytes', 'dst_bytes', 'hot', 'num_compromised', 'root_shell', 'num_root', 'num_file_creations', 'count', 'dst_host_count', 'dst_host_srv_count', 'dst_host_srv_diff_host_rate', 'service_ftp_data']
(113270, 13)
(78999, 13)
(68338, 13)
(67395, 13)

İlk 10 gözlemin tahmin edilen olasılıklar:
array([[0.5, 0.5],
[0.5, 0.5],
[0.9, 0.1],
[1. , 0.],
[0.8, 0.2],
[0.9, 0.1],
[0.8, 0.2],
[0.5, 0.5],
[0.6, 0.4],
[1. , 0.]])
çapraz doğrulama : doğruluk, hassasiyet, geri çağırma, f-ölçü

Dos
Accuracy: 0.99790 (+/- 0.00245)
Precision: 0.99892 (+/- 0.00162)
Recall: 0.99692 (+/- 0.00295)
F-measure: 0.99765 (+/- 0.00183)

Probe
Accuracy: 0.99646 (+/- 0.00305)
Precision: 0.99690 (+/- 0.00332)
Recall: 0.99406 (+/- 0.00703)
F-measure: 0.99508 (+/- 0.00463)

U2R
Accuracy: 0.99714 (+/- 0.00153)
Precision: 0.97236 (+/- 0.08204)

Recall: 0.85927 (+/- 0.13695)
F-measure: 0.88105 (+/- 0.10944)

R2L
Accuracy: 0.97999 (+/- 0.00767)
Precision: 0.97417 (+/- 0.01297)
Recall: 0.96830 (+/- 0.01340)
F-measure: 0.97314 (+/- 0.00739)

Seçilen Özellikler:
Her sınıf (DoS, Probe, U2R, R2L) için farklı özellikler seçilmiş. Bu özellikler, belirli bir saldırı türünü tanımlamak veya sınıflandırmak için kullanılan girdi özelliklerini temsil eder.

Gözlem Sayıları:
Her bir sınıf için farklı sayılarda gözlem (örnek) bulunmaktadır. Bu, veri setinizin dengesiz olabileceği anlamına gelebilir. Bu durum, modelin her sınıftaki performansını değerlendirirken dikkate alınmalıdır.

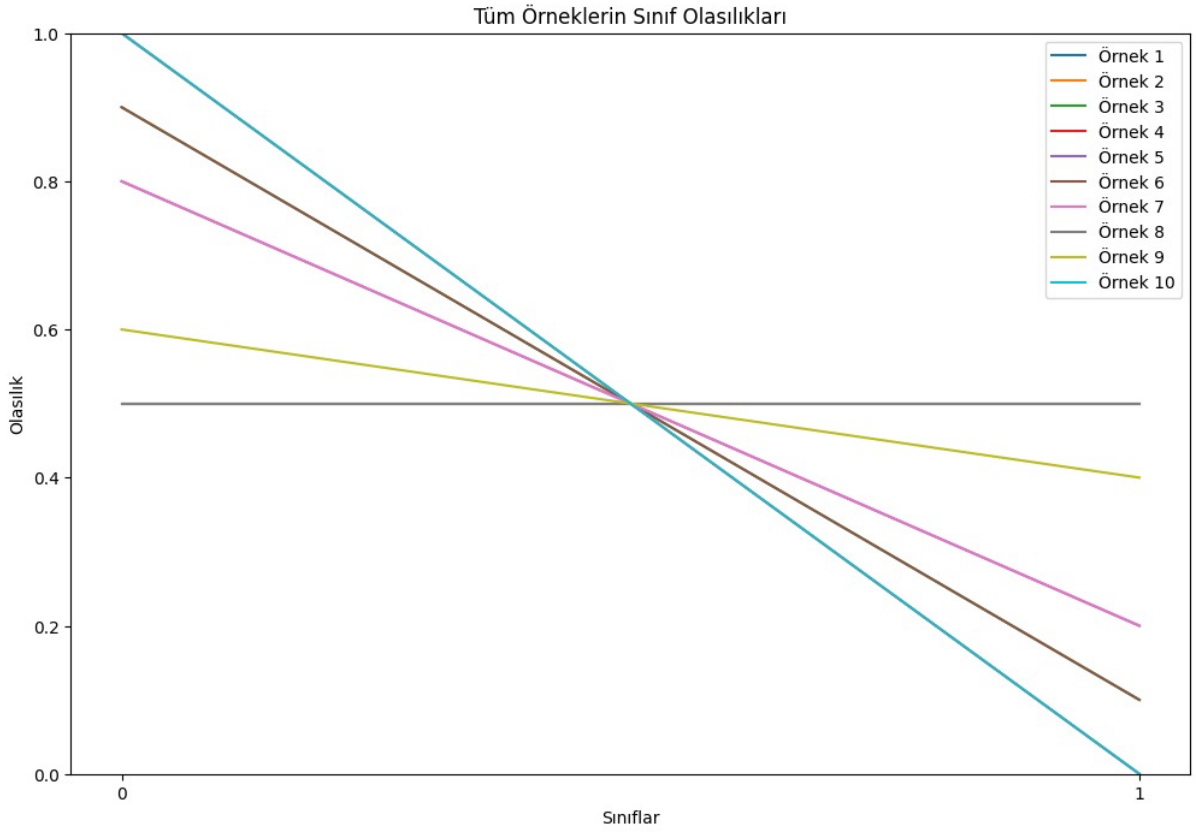
İlk 10 Gözlemin Tahmin Edilen Olasılıklar:
Her bir gözlem için iki sınıfa ait olasılık değerleri verilmiş. Bu olasılıklar genellikle bir sınıfa ait olma olasılığını ifade eder. Örneğin, bir gözlem için (0.5, 0.5) değeri, iki sınıfa eşit olasılıkla ait olduğunu gösterir.

Çapraz Doğrulama Sonuçları:
Model performansını değerlendirmek için kullanılan çapraz doğrulama sonuçları verilmiştir. Bu sonuçlar, modelin doğruluk, hassasiyet, geri çağırma ve F-ölçü (F-measure) gibi metriklerde ne kadar başarılı olduğunu gösterir.

Örnek: DoS sınıfı için doğruluk 0.99790 (+/- 0.00245) olarak verilmiş. Bu, modelin DoS saldırılarını tanımlamada yüksek bir doğruluk elde ettiğini gösterir.

U2R sınıfı için hassasiyet (precision) değeri 0.97236 (+/- 0.08204) olarak verilmiş. Bu, modelin U2R saldırılarını tanımlarken hassas olma eğiliminde olduğunu ancak bu değerin çeşitlilik gösterdiğini belirtir.

R2L sınıfı için geri çağırma (recall) değeri 0.96830 (+/- 0.01340) olarak verilmiş. Bu, modelin R2L saldırılarını yakalamada yüksek bir başarı elde ettiğini gösterir.

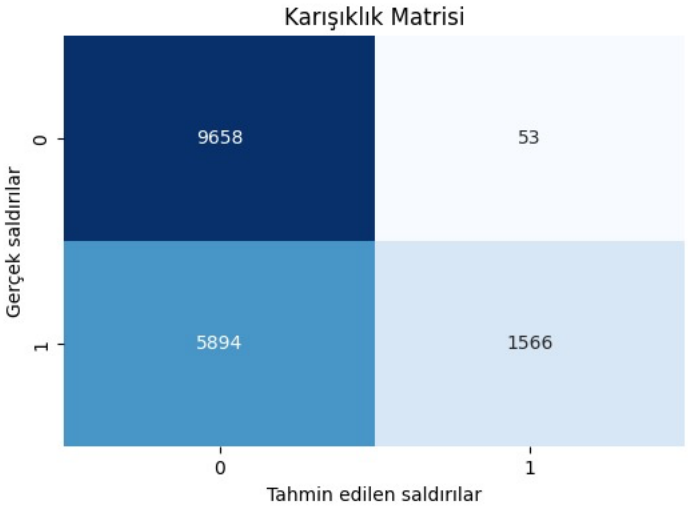


Bu grafik, her bir gözlemin farklı sınıflara ait olasılıklarını gösterir. X ekseni sınıfları, y ekseni ise olasılıkları temsil eder. Her bir çizgi, bir gözlemi temsil eder ve çizgilerin konumu, o gözlemin her sınıfa ait olasılıklarını gösterir.

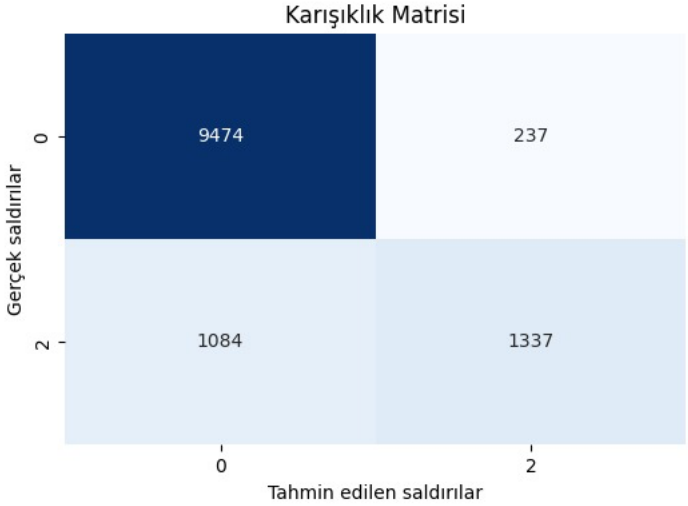
Çizgi grafiğinde, her bir çizginin zirveye ulaştığı sınıf, o gözlemin model tarafından en muhtemel sınıf olarak tahmin edildiği sınıftır. Grafik, modelin her bir gözlem için farklı sınıflar arasında ne kadar belirgin bir tercih yaptığını gösterir.

İlk 10 gözlem için sınıf olasılıkları, belirli bir örneği ele alarak modelin o örnekteki sınıf tahminini açıklar. Bu olasılıklar genellikle bir gözlemin birden fazla sınıfa ait olma olasılığını gösterir, ve modelin en muhtemel sınıf tahminini belirlemek için kullanılır.

DoS için:

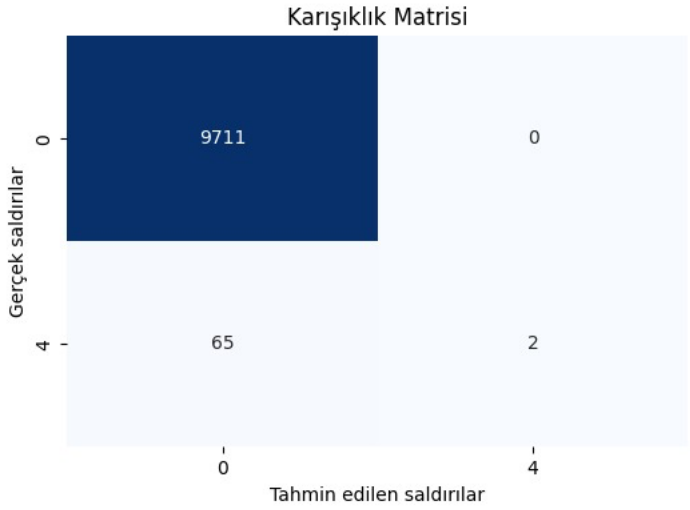


Probe için:



R2L için:

U2R için:



Bu grafikler çalışmamızın sonucu olarak matris olarak oluşturulan grafiklerin çeşitli yöntemlerde (U2R gibi) hangi oranda **tahmin** ve **gerçek saldırı** tespiti yapıldığı sonucu gösterilmektedir.

Literatür Taramımızın Raporumuz için Etkisini ve İlişkilendirilmesi

Yaptığımız teorik çalışma ile (literatür araştırması) şu ilişkilendirmeyi yapabiliriz:

Kullanılan başarılı tekniği **ön araştırmamız** sayesinde öğrenmiş ve o şekilde uygulamış olduk. Bu nedenle Random Forest tekniğini kullanmaya karar verdik.
Yukarıda da belirtilen birçok özellik nedeniyle kullandığımız tekniğin bu çalışma ile pratiğini yapmış olduk. Bu çalışma ile elde ettiğimiz veriler beklentilerimizi karşıladı.
Yüksek doğruluk ile tespitler elde ettik.

Siber güvenlik alanında gelişmeler alanına değindiğimiz literatür araştırmamızda bu araştırmamızda da yer verebildik ki, çeşitli tehditlerin etkileri ve mevcut engelleme yöntemlerini görebildik. Kullandığımız tekniğin araştırmalarımızla elde ettiğimiz özelliklerini kullanıp yararlandık. Bir teorik araştırma sonrası pratik çalışmamızla bunu pekiştirip ele alınabilir bir hale dökerek adım adım ve belirli bir yolda ilerledik. Böylelikle işin ortasından değil önce mutfağından ardından detayından çalışarak çalışmamızı başarıyla sonuçlandırabildik.