E-Bülten

Sayı 11 / Haziran 2021

İSTANBUL AYDIN ÜNİVERSİTESİ

İleri Araştırmalar Uygulama ve Araştırma Merkezi

İçindekiler:

Merkez Müdürü: Prof. Dr. Hasan SAYGIN
Tel: 0 (212) 444 1 428
E-mail: iauygar@aydin.edu.tr

Personel: Öğr. Gör. Sajad Einy
Tel: 0 (212) 444 1 428
E-mail: iauygar@aydin.edu.tr

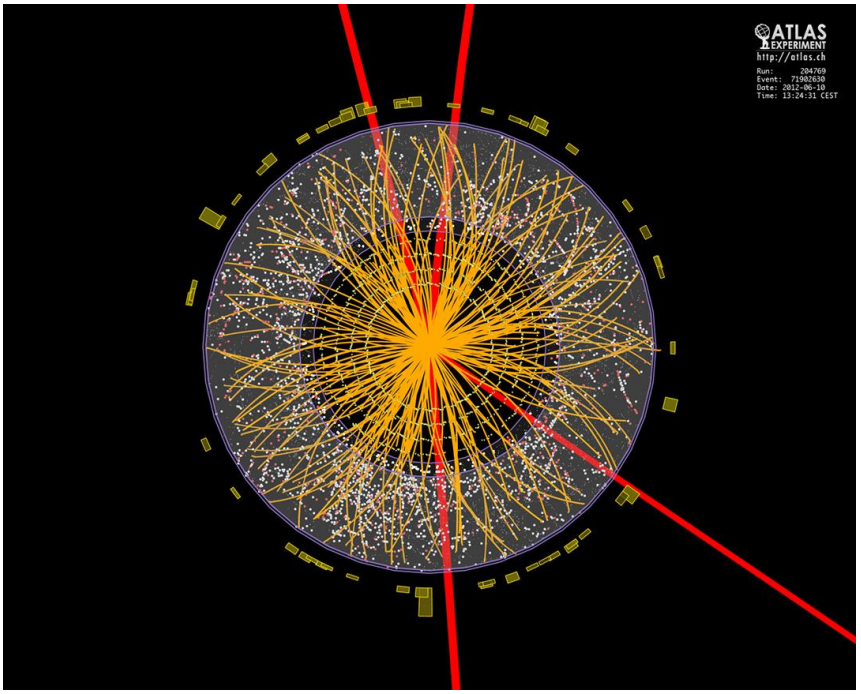
E-Bülten

Sayı 11 / Haziran 2021

İSTANBUL AYDIN ÜNİVERSİTESİ

İLERİ ARAŞTIRMALAR UYGULAMA ve ARAŞTIRMA MERKEZİ

13 Temmuz 2014 tarihinde resmi gazetede yayınlanan yönetmelikle kurulan İstanbul Aydın Üniversitesi, İleri Araştırmalar Uygulama ve Araştırma Merkezi, CERN ATLAS ve CMS deney sonuçları ile ilgili uluslararası kolaborasyonları ile ortak bilimsel araştırmalarda bulunmakta ve bilimsel makaleler üretmektedir. 2020-2021 yılları arasında İAÜ adresli ve SCI tarafından taranan dergilerde Yüksek Enerji Fiziği alanında yayınlanan makale sayısı an itibariyle 225 ve 2020-2021 yılı için alınan cite sayısı ise 960 olmuştur.



Görsel 1: ATLAS ve CMS Deneyi Sonuçları

E-Bülten

Sayı 11 / Haziran 2021

İSTANBUL AYDIN ÜNİVERSİTESİ

İLERİ ARAŞTIRMALAR UYGULAMA ve ARAŞTIRMA MERKEZİ

Ağ Saldırı Tespit Sistemi

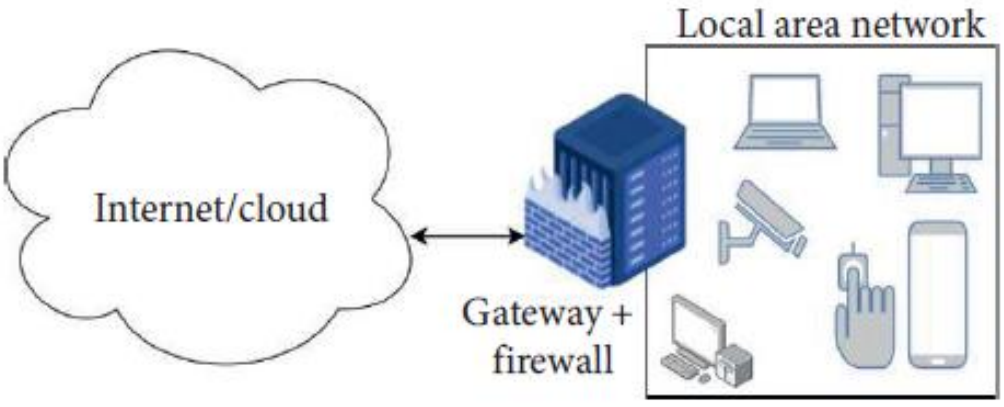
Son on yılda, birçok ağ türü (iletişim ağları, sosyal ağlar, mobil internet ağları ve ings ağlarının interneti) kullanılmaktadır. Birden fazla ağ türünün olması dünyanın her yerinden insanlar tarafından memnuniyetle karşılanmakta ve günlük hayatı kolaylaştırmaktadır. (alış-satış, tıbbi danışmanlık, iş ve eğitim)

Sistem güvenliğinin sağlanması en önemli zorluklardan birisidir. Zayıflıkları ortadan kaldırmak, izinsiz giriş ve saldırıları tespit edebilmek için farklı yöntemler kullanılmaktadır. (güvenlik duvarları, kriptografi, ağa erişimi kısıtlamak) Görülen herhangi bir anormal durum veya bilgilerin kötüye kullanımını tespit etmek amacıyla kullanılan sistem, izleri takip etmekte ve kötü amaçlı yazılımların ağ yapısına verdiği zararın engellenmesi veya azaltılmasında önemli rol oynamaktadır.

Saldırı tespit sistemleri izinsiz girişleri iki şekilde tespit etmektedir.

1- **İmza tanıma:** Geçmişte yapılan işlemlerin verileri ve ağlardaki yetkili kullanıcı bilgisi sistem üzerinde görülmekte ve herhangi bir işlemi normal veya anormal olarak tespit edebilmektedir.

2- **Makine Öğrenimi Yöntemlerinden Kaynaklanan Anormallikler:** Sinir Ağları ve SVM, kullanıcıların davranışlarına göre (günlük ziyaret edilen ağ bilgileri, paylaşılan veya indirilen dosyaların içeriği ve ağ kullanım süresi) normal ve anormal olmak üzere iki sınıf olarak tanımlamaktadır.



E-Bülten

Sayı 11 / Haziran 2021

İSTANBUL AYDIN ÜNİVERSİTESİ

İLERİ ARAŞTIRMALAR UYGULAMA ve ARAŞTIRMA MERKEZİ

Yüz Sahtekarlığı Algılama

Yüz tanıma sistemleri olası bir saldırıya karşı savunmasızdır. Herhangi bir saldırıda kişinin verileri yasal olmayan erişim ile elde edilerek kendini farklı biri olarak gösterebilmektedir. Bu durumda görüntü kalitesini değerlendirmek, baskı artefaklarının karakterizasonları ve ışık yansımalarındaki farklılıklardan yararlanarak sistemi yanıltma sorununa doku analizi bakış açısı kullanılmasını önermekteyiz.

Yüz baskıları genellikle doku özellikleri kullanılarak tespit edilebilen baskı kalitesi kusurları içermektedir. Bu nedenle kamera karşısında canlı bir insan veya yüzünde herhangi bir iz olup olmaması gibi tespitleri yapabilmek için yüz dokularını tespit eden yeni bir yaklaşım sunmaktayız.

Bir fotoğraf, video, maske veya yetkili bir kişinin yüzünün yerini almak amacıyla yapılan saldırıların tespitinin yapılması sistemin görevidir. Bazı saldırı örnekleri:

1- **Baskı Saldırısı:** Kişinin fotoğrafı kullanılır. Görüntü, dijital bir aygıtta yazdırılır veya görüntülenir.

2- **Tekrar Oynatma/Video Saldırısı:** Genellikle kurbanın yüzünün döngüsel bir videosunu gerektiren, sistemi kandırmanın daha karmaşık bir yoludur. Bu yaklaşım, birinin fotoğrafını tutmaya kıyasla davranış ve yüz hareketlerinin daha 'doğal' görünmesini sağlamaktadır.

3- **3D Maske Saldırısı:** Bu tür bir saldırı için maske araç olarak tercih edilmektedir. Kişinin yüzünün olduğu bir videonun oynatılmasından bile daha karmaşık yapılı bir saldırıdır. Doğal yüz hareketlerine ek olarak, derinlik sensörleri bazı ekstra koruma katmanlarını aldatmanın yollarını sağlamaktadır.

Görsel 2: Yüz Tanıma Sistemi Örnek

E-Bülten

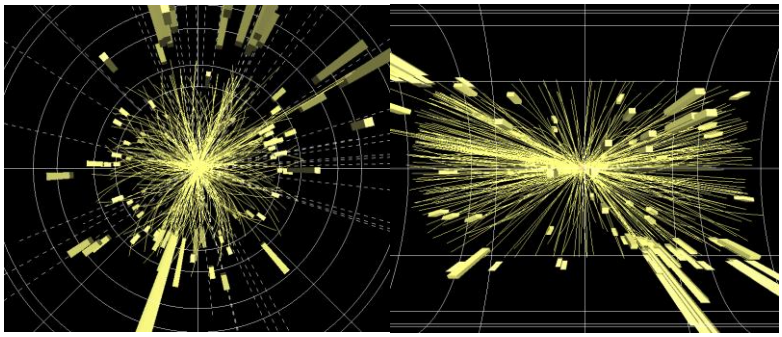
Sayı 11 / Haziran 2021

İSTANBUL AYDIN ÜNİVERSİTESİ

İLERİ ARAŞTIRMALAR UYGULAMA ve ARAŞTIRMA MERKEZİ

Nükleer Enerji Simülasyonunda Sinyal Ve Arka Plan Sınıflandırması

Bu projede, Ankara Üniversitesi işbirliği ile CERN Araştırma Merkezi'nde kullanılmak üzere yapay zeka platformları oluşturulmaktadır. Araştırmada arka plan ve sinyal görüntülerinin sınıflandırılması için derin öğrenme platformu hazırlanmıştır. Görüntüler, CERN Simülasyon Merkezi'nde üretilmektedir. Araştırmanın sonuçları makale olarak yayınlanacaktır.



Görsel 3: Sinyal ve Arka Plan Örnek