1-Problemin Tanımı;  
Bu projenin temel problemi, geleneksel siber saldırı tespit sistemlerinin siber tehditlere karşı yetersiz kalması ve tespit edilen saldırı verilerinin manipülasyon riskine açık olmasıdır. Geleneksel sistemler, genellikle saldırı verilerini merkezi bir veri tabanında depoladığından, kötü niyetli aktörler tarafından bu verilerin değiştirilmesi veya silinmesi mümkün hale gelmektedir. Bu durum, siber güvenlik alanında veri bütünlüğü ve güvenilirlik açısından ciddi zafiyetler yaratmaktadır. Ayrıca, saldırıların dinamik ve sürekli değişen doğası, bu sistemlerin zamanında ve doğru tespit yapabilmesini zorlaştırmaktadır. Dolayısıyla, verilerin manipüle edilemeyeceği, güvenilir bir kayıt mekanizmasına ve saldırıların zaman serisi analiziyle öngörülebilir bir şekilde tespit edilebileceği bir sisteme ihtiyaç duyulmaktadır. Bu proje, Blockchain'in güvenli kayıt yapısı ile LSTM modelinin zaman serisi analiz kabiliyetini birleştirerek, hem güvenli hem de dinamik bir siber saldırı tespit çözümü geliştirmeyi amaçlamaktadır.

2-verilerin Tanımı

**Gerçek Zamanlı Ağ Trafiği Verileri**: Bu veriler, sistemin çalıştığı ağdan gelen ve giden veri paketlerinin analiz edilmesiyle elde edilecektir. Her bir veri paketi, kaynak ve hedef IP adresleri, port numaraları, protokol türü (TCP, UDP, ICMP vb.), veri paketinin boyutu ve zaman damgası gibi bilgileri içerecektir. Bu veriler, Docker konteynırları kullanılarak toplanacak ve MongoDB veritabanında saklanacaktır. Gerçek zamanlı ağ trafiği verileri, saldırı tespit modelini sürekli olarak beslemek ve güncel tehditlere karşı duyarlı hale getirmek için kullanılacaktır.

**Siber Saldırı Veri Setleri**: Projede, geçmişte gerçekleşmiş siber saldırılara ait veri setleri kullanılacaktır. Bu veri setleri, çeşitli siber güvenlik platformlarından, akademik veri havuzlarından veya açık kaynak siber güvenlik projelerinden elde edilebilir. Veri setleri, farklı saldırı türlerine (örneğin, DDoS, SQL Injection, Phishing, Brute Force) ilişkin etiketlenmiş örnekler içerecektir. Her bir saldırı kaydı, saldırı türü, saldırı zamanı, saldırının hedefi, saldırganın IP adresi, saldırı süresi ve saldırıya ilişkin diğer teknik ayrıntıları içerebilir.

3-kaynakların Tanımı

-Siber saldırılara ilişkin veri setleri

-Akademik Veri Havuzları ve Araştırmaları

-Gerçek Zamanlı Ağ Trafiği

-Simüle Edilmiş Siber Saldırılar

4-Tüm sistemin Tanımı

**1. Veri Toplama ve Hazırlama Aşaması**

* **Siber Saldırı Veri Setleri**: Sistem, öncelikle siber saldırıların tespit ve analizi için gerekli olan geçmiş veri setleri ile çalışmaya başlar. Bu veri setleri, farklı kaynaklardan (açık kaynak projeler, akademik veri havuzları) elde edilir. Veri setlerinde, DDoS, SQL Injection, Phishing gibi farklı saldırı türleri yer alır ve bu saldırılar zaman damgaları ile etiketlenmiştir.
* **Gerçek Zamanlı Ağ Trafiği Verisi**: Docker konteynırları kullanılarak, sistemin kurulu olduğu ağ ortamından gerçek zamanlı veri toplanır. Bu veri, ağ trafiğindeki paketlerin kaynak IP adresleri, hedef IP adresleri, kullanılan protokoller, zaman damgaları ve veri paketlerinin boyutlarını içerir. Toplanan bu veriler, MongoDB veritabanında saklanır ve yapay zeka modeli için kullanıma hazır hale getirilir.

**2. Yapay Zeka Modelinin Eğitimi**

* **LSTM (Long Short-Term Memory) Modeli**: Zaman serisi analizine dayalı olarak çalışan LSTM modeli, geçmişe yönelik saldırı verilerini kullanarak eğitilir. LSTM modeli, zaman damgasına dayalı olarak ağ trafiği içindeki anormal davranışları ve saldırı paternlerini öğrenir. Bu süreçte, modelin eğitimi için veri setleri temizlenir, normalleştirilir ve zaman serileri haline getirilir.
* **Model Optimizasyonu**: Modelin saldırı tespit performansını artırmak için hiperparametre ayarları, katman sayısı, öğrenme hızı ve pencere boyutu (window size) gibi parametreler optimize edilir. Eğitim sürecinde, modelin doğru saldırı tespiti yapabilmesi için doğruluk, hassasiyet ve F1 skoru gibi performans metrikleri izlenir.

**3. Veri Yönetimi ve Depolama**

* **MongoDB Veritabanı**: Gerçek zamanlı veri akışlarını ve siber saldırı verilerini saklamak için MongoDB kullanılır. Veri tabanı, Docker konteynırları ile entegre çalışarak, sistemin her 10 saniyede bir topladığı verileri düzenli olarak kaydeder. Bu veriler, hem Blockchain’e kaydedilmek üzere hem de LSTM modeli için test verisi olarak kullanılmak üzere depolanır.
* **Blockchain Defteri**: Tespit edilen saldırı verileri ve ağ trafiğinden elde edilen kritik bilgiler, Blockchain tabanlı bir deftere kaydedilir. Blockchain, verilerin değiştirilmesini veya manipüle edilmesini engelleyen bir yapı sunar. Böylece, sistem tarafından tespit edilen her saldırı, Blockchain’e kaydedilerek güvenli ve şeffaf bir şekilde saklanır. Blockchain defteri, saldırıların kaynağının tespiti ve saldırı verilerinin izlenebilirliği için de kullanılır.

**4. Gerçek Zamanlı Saldırı Tespiti**

* **Canlı Veri Analizi**: Eğitilen LSTM modeli, gerçek zamanlı olarak toplanan ağ trafiği verilerini analiz eder. Model, normal ve anormal davranışları ayrıştırarak olası siber saldırıları tespit etmeye çalışır. Tespit edilen saldırılar, saldırı türü ve potansiyel tehlike seviyesine göre sınıflandırılır.
* **Saldırı Tespit Sonuçlarının Blockchain’e Kaydı**: Tespit edilen her bir saldırı, saldırının türü, zamanı, kaynağı ve hedefi gibi bilgilerle birlikte Blockchain’e kaydedilir. Bu sayede, saldırı verilerinin manipüle edilmesi engellenir ve geriye dönük olarak güvenilir bir kayıt sağlanır.

**5. Simüle Edilmiş Saldırılar ve Sistem Testi**

* **Kali Linux ve Metasploit Framework**: Sistemin dayanıklılığını ve doğruluğunu test etmek amacıyla Kali Linux ve Metasploit Framework kullanılarak simüle edilmiş siber saldırılar gerçekleştirilir. Bu simülasyonlar, DDoS, SQL Injection, Brute Force gibi yaygın saldırı türlerini içerir.
* **Performans Analizi**: Simülasyonlar sırasında, sistemin tespit doğruluğu, tepki süresi ve yanlış alarm oranı gibi metrikler analiz edilir. Tespit edilen saldırıların sonuçları ve Blockchain’e kaydedilen veriler, sistemin güvenilirliğini ve verimliliğini değerlendirmek için incelenir.

**6. Kullanıcı Arayüzü ve Raporlama**

* **Kullanıcı Arayüzü**: Sistem tarafından tespit edilen saldırılar ve analiz sonuçları, kullanıcıya sunulmak üzere bir arayüz üzerinden görselleştirilir. Bu arayüz, sistemin saldırılara karşı alınan aksiyonları, tespit edilen saldırıların kaynağını ve Blockchain defterinde kaydedilen verileri gösterir. Kullanıcı arayüzü, sistem yöneticilerine ve güvenlik uzmanlarına sistemin performansı ve saldırılar hakkında detaylı bilgiler sunar.
* **Raporlama ve Uyarı Mekanizmaları**: Sistem, tespit edilen yüksek riskli saldırılar için kullanıcıyı anında uyaracak bir mekanizma içerir. Ayrıca, günlük ve haftalık saldırı raporları oluşturularak yöneticilere gönderilir. Bu raporlar, sistemin genel durumu ve saldırı eğilimleri hakkında bilgi sağlar.

**7. Projenin Yaygın Etkisi ve Uygulama Alanları**

* Bu sistem, özellikle finansal kurumlar, sağlık sektörü, enerji sektörü ve kamu kurumları gibi veri güvenliğinin kritik önem taşıdığı alanlarda uygulanabilir. Blockchain tabanlı veri yönetimi sayesinde, verilerin manipülasyona uğramaması sağlanır ve saldırıların kaynağı net bir şekilde tespit edilebilir.
* Yapay zeka ve zaman serisi analizleri ile desteklenen sistem, hızlı ve dinamik saldırı tespit kabiliyeti ile, siber saldırılara karşı güçlü bir savunma mekanizması sunar. Projenin sonunda, bu sistemin sağladığı güvenlik çözümleri, siber güvenlik alanında yeni standartların oluşturulmasına katkı sağlayabilir.

5-Proje Çıktısı

Projenin çıktısı, web ortamında kullanıcıya, yapay zeka tarafından tespit edilen siber saldırılar ve bu saldırılara dair analizlerin görselleştirilmesi olacaktır. Web tabanlı arayüz üzerinden, kullanıcılar anlık olarak tespit edilen saldırı türlerini, zamanlarını, kaynağını ve tehlike seviyesini görebilecekler. Görselleştirme, grafikler ve tablolar şeklinde sunulacak ve kullanıcılar için saldırı verilerinin daha anlaşılır bir şekilde izlenmesini sağlayacaktır. Bu sayede, siber güvenlik durumları hakkında hızlıca bilgi alınabilecek ve gerekli önlemler alınabilecektir.