**Proje Başlığı: Blockchain Tabanlı Saldırı Tespit Sistemi (IDS)**

**Proje Amacı:**

Bu proje, siber saldırıları tespit etmek ve ağ güvenliğini artırmak için merkeziyetsiz bir Saldırı Tespit Sistemi (IDS) geliştirmeyi amaçlamaktadır. Bu sistemde, ağ trafiği ve sistem olayları blockchain teknolojisi ile kayıt altına alınarak, sistemin güvenliği artırılacak ve verilerin manipüle edilmesi engellenecektir. Blockchain’in merkeziyetsiz ve değiştirilemez yapısı sayesinde, saldırı tespiti daha güvenli ve şeffaf bir şekilde gerçekleştirilecektir.

**Proje Özeti:**

Geleneksel saldırı tespit sistemleri genellikle merkezi yapıya sahiptir ve bu durum onları siber saldırılara karşı savunmasız hale getirir. Özellikle merkezi bir noktaya yapılan saldırılar, sistemin bütünlüğünü ve güvenilirliğini riske atabilir. Blockchain teknolojisi ise merkeziyetsiz yapısı sayesinde veri bütünlüğünü garanti altına alır. Bu projede, blockchain kullanılarak, ağ üzerinde meydana gelen anomalileri ve saldırı girişimlerini tespit eden bir IDS tasarımı yapılacaktır.

Sistem, ağ üzerindeki her bir veri paketi veya olay kaydını blockchain üzerinde kaydederek, saldırı girişimlerine dair kanıtların değiştirilemez ve izlenebilir bir yapıda tutulmasını sağlayacaktır. Ayrıca, akıllı sözleşmeler kullanarak şüpheli aktiviteleri tespit etmek ve gerektiğinde müdahale etmek mümkün olacaktır.

**Projenin Temel Bileşenleri:**

1. **Blockchain Teknolojisi:** Blockchain, merkeziyetsiz ve dağıtık bir defter teknolojisidir. Her veri bloğu, önceki blokla bağlantılıdır ve bu da verilerin değiştirilmesini neredeyse imkansız hale getirir. Projede, blockchain ağı üzerinde ağ trafiği ve olay kayıtları saklanarak sistem güvenliği sağlanacaktır.
2. **Saldırı Tespit Sistemi (IDS):** IDS, bir ağ veya sistem üzerinde şüpheli aktiviteleri tespit eden bir güvenlik çözümüdür. Bu projede, ağ üzerindeki veri paketleri ve sistem olayları blockchain'e kaydedilecek ve saldırı tespiti blockchain'in güvenilirliği üzerinden yapılacaktır.
3. **Akıllı Sözleşmeler (Smart Contracts):** Akıllı sözleşmeler, blockchain üzerinde çalışan otomatik işlemleri yöneten kod parçalarıdır. Bu projede, şüpheli davranışları tespit etmek için akıllı sözleşmeler kullanılacak ve belirli saldırı kalıpları tespit edildiğinde otomatik alarm sistemleri devreye sokulacaktır.

**Projenin İşleyişi:**

1. **Ağ Trafiğinin İzlenmesi:** IDS, bir ağ üzerindeki tüm veri paketlerini izler ve bu verileri blockchain ağına kaydeder. Bu sayede, bir veri bloğu oluşturulur ve her bir veri paketi değiştirilemez şekilde blockchain defterine eklenir.
2. **Veri Analizi ve Anomali Tespiti:** Blockchain üzerine kaydedilen veri blokları, belirli saldırı kalıplarını arayan akıllı sözleşmeler tarafından analiz edilir. Anomaliler tespit edildiğinde, sistem bir uyarı vererek müdahale edilmesini sağlar.
3. **Saldırı Tespitinin Güçlendirilmesi:** Blockchain üzerindeki veriler merkeziyetsiz olduğundan, herhangi bir saldırganın veri kayıtlarına müdahale etmesi mümkün değildir. Böylece saldırıların tespit edilmesi ve izlenmesi daha güvenilir hale gelir.
4. **Saldırı Kayıtlarının İzlenmesi:** Herhangi bir siber saldırı girişimi tespit edildiğinde, saldırıya dair tüm kanıtlar blockchain üzerinde saklanarak gelecekteki incelemeler için güvence altına alınır.

**Teknolojik Araçlar:**

* **Blockchain Platformu:** Hyperledger, Ethereum gibi blockchain platformlarından biri kullanılabilir.
* **Akıllı Sözleşmeler:** Ethereum üzerinde Solidity dili kullanılarak akıllı sözleşmeler yazılabilir.
* **Veri Analizi:** Makine öğrenmesi algoritmaları kullanılarak anomali tespiti gerçekleştirilebilir.

**Beklenen Sonuçlar:**

* Saldırı tespit sistemlerinin merkeziyetsiz bir yapıya taşınarak daha güvenli ve manipüle edilemez hale gelmesi.
* Ağ üzerindeki saldırı girişimlerinin blockchain’in değiştirilemez yapısı sayesinde güvenli bir şekilde kayıt altına alınması.
* Blockchain üzerinde saldırılara dair şeffaf ve izlenebilir kayıtların oluşturulması.

**Projenin Katkıları:**

Bu proje, geleneksel saldırı tespit sistemlerine kıyasla daha güvenli ve izlenebilir bir çözüm sunmayı hedeflemektedir. Blockchain tabanlı bir IDS, özellikle merkezi saldırılara karşı güvenliği artırırken, şeffaf bir yapı sunarak saldırı sonrası analizlerde önemli avantajlar sağlayacaktır.