


## Makale

# Otomatik Araçlara Saldırılar: Siber Güvenlik için Bir Derin Öğrenme Algoritması

Theyazn H. H. Aldhyani <sup>1,\*</sup>  ve Hasan Alkahtani <sup>2</sup><sup>1</sup> Applied College in Abqaiq, King Faisal University, P.O. Box 400, Al-Ahsa 31982, Suudi Arabistan<sup>2</sup> Bilgisayar Bilimleri ve Bilgi Teknolojileri Fakültesi, King Faisal Üniversitesi, P.O. Box 400, Al-Ahsa 31982, Suudi Arabistan; [hsalkahtani@kfu.edu.sa](mailto:hsalkahtani@kfu.edu.sa)\* Yazışma adresi: [taldhyani@kfu.edu.sa](mailto:taldhyani@kfu.edu.sa); Tel: +966-504937279

**Özet:** Hızlı teknolojik gelişme otomotiv endüstrisini büyük ölçüde değiştirmiştir. Ağ iletişimi gelişerek araçların tamamen makine kontrolünden yazılım kontrollü teknolojilere geçişine yardımcı olmuştur. Otonom araç ağı, kontrolör alan ağı (CAN) veri yolu protokolü tarafından kontrol edilmektedir. Bununla birlikte, otonom araç ağı, bir CAN veri yoluna yetkisiz izinsiz giriş ve çeşitli saldırı türlerine fayda sağlayan veri ve trafik davranışlarının karmaşıklığı nedeniyle siber güvenlikle ilgili sorunlara ve zayıflıklara sahiptir. Bu nedenle, CAN'daki mesaj saldırılarını hızlı bir şekilde tespit etmek için sistemler geliştirmek en büyük zorluklardan biridir. Bu çalışma, araç ağını siber tehditlerden koruyan yapay zeka yaklaşımına sahip yüksek performanslı bir sistem sunmaktadır. Sistem, derin öğrenme yaklaşımlarını kullanarak otonom aracı izinsiz girişlerden korur. Önerilen güvenlik sistemi, sahtekarlık, sel, tekrarlama saldırıları ve iyi huylu paketler dahil olmak üzere gerçek bir otomatik araç ağı veri kümesi kullanılarak doğrulanmıştır. Kategorik verileri sayısal hale dönüştürmek için ön işleme uygulanmıştır. Bu veri kümesi, saldırı mesajlarını tanımlamak için konvolüsyon sinir ağı (CNN) ve CNN ile uzun kısa süreli bellek (CNN-LSTM) modellerini birleştiren hibrit bir ağ kullanılarak işlenmiştir. Sonuçlar, modelin hassasiyet, geri çağırma, F1 puanı ve doğruluk ölçütlerine göre değerlendirildiğinde yüksek performans elde ettiğini ortaya koymuştur. Önerilen sistem yüksek doğruluk oranına (%97,30) ulaşmıştır. Ampirik gösterimle birlikte, önerilen sistem mevcut sistemlere kıyasla tespit ve sınıflandırma doğruluğunu artırmış ve gerçek zamanlı CAN veri yolu güvenliği için üstün performansa sahip olduğu kanıtlanmıştır.

**Anahtar Kelimeler:** araç içi ağ; CAN; siber güvenlik; izinsiz giriş tespiti; derin öğrenme; yapay zeka

**Atıf:** Aldhyani, T.H.H.; Alkahtani, H. Otomatik Araçlara Saldırılar: Siber Güvenlik için Bir Derin Öğrenme Algoritması. *Sensors* **2022**, *22*, 360. <https://doi.org/10.3390/s22010360>

Akademik Editörler: Bhisham Sharma, Deepika Koundal, Rabie A. Ramadan ve Juan M. Corchado

Alındı: 6 Aralık 2021

Kabul edildi: 30 Aralık 2021

Yayınlanma tarihi: 4 Ocak 2022

**Yayıncının Notu:** MDPI, yayınlanan haritalardaki yetki iddiaları ve kurumsal ilişkiler konusunda tarafsız kalmaktadır.



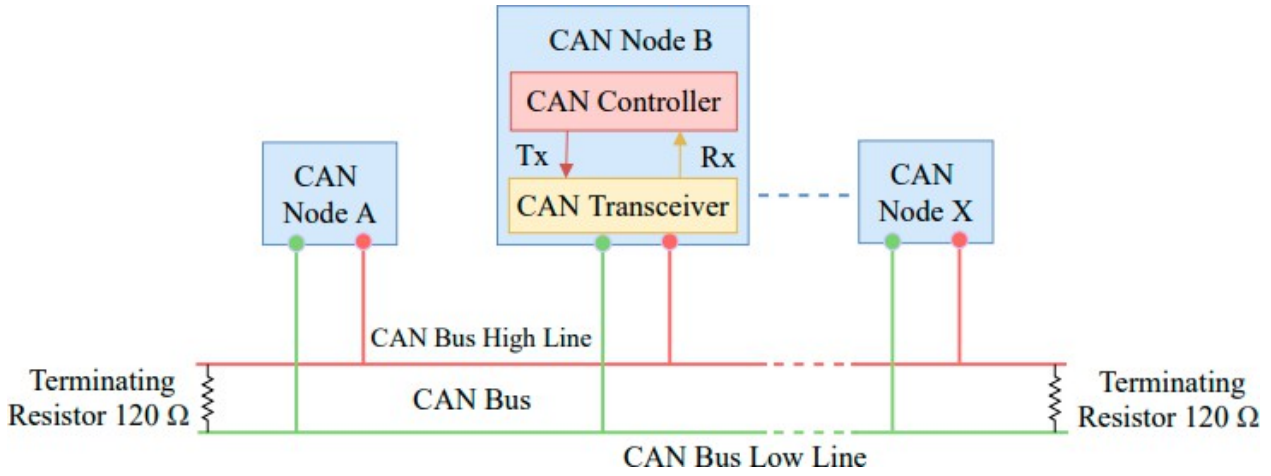
**Telif hakkı:** © 2022 yazarlar tarafından. Lisans sahibi MDPI, Basel, İsviçre. Bu makale Creative Commons Attribution (CC BY) lisansının hüküm ve koşulları altında dağıtılan açık erişimli bir makaledir (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Giriş

Sürücüsüz araçlar ve akıllı otomobiller teknolojisi son yıllarda önemli ölçüde gelişmiştir. Araç ağları terimi, trafiği yönetme, park etme ve kazalardan kaçınma gibi avantajlar sunan araç düğümlerini ifade eder [1]. Araç düğümleri bir iletişim habercisi olarak işlev görür ve farklı araştırma alanlarında incelenir, örneğin, araçsal ad hoc ağlar, araçların interneti ve araçtan her şeye iletişim. Bağımsız bir araştırma alanı olan araç içi ağlar (IVN'ler), motor kontrol ünitesi (ECU), şanzıman kontrol ünitesi, kilitlenme önleyici fren sistemi, gövde kontrol modülleri ve araç içindeki çeşitli sensörler arasındaki iletişimle ilgilenir [2].

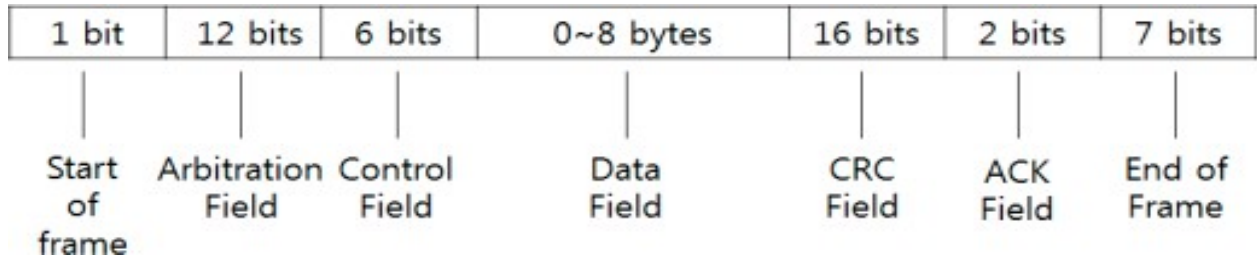
IVN'lerin işleyişini kolaylaştıran özel protokoller vardır. Bu protokoller arasında denetleyici alan ağı (CAN), FlexRay ve Ethernet bulunmaktadır [3]. CAN, otomotiv ve endüstriyel sistemi kontrol etmek için kullanılan en yaygın ağ topolojisidir. Mikrodenetleyici cihazlar arasında hızlı iletişim sunan bir iletişim ağıdır. CAN, tüm düğümlerin mesajı almasına ve ağ mesajı üzerinde işlem yapmasına izin vermek için tasarlanmış mesaj tabanlı bir protokol göndermek için birbirine bağlı düğümler kullanır [4]. Şekil 1

saldırganların iletişim ağına saldırı mesajları enjekte etmek için kullandıkları CAN standart yolu arayüzünü gösterir.



Şekil 1. CAN veri yolu arayüzü.

Şekil 2, çerçevenin başlangıcından (1 bit), tahkim alanından (12 ) oluşan CAN mesaj başlığı çerçeve formatını göstermektedir; tahkim alanı, sistem yayına başladığında CAN mesajının sahibini belirlemek için kullanılır. Döngüsel artıklık kontrolü (CRC) çerçeve başlığını kontrol etmek için kullanılmıştır ve (16 bit), Acknowledge (ACK) alanını çerçeveyi almak için ağa mesaj döndürmek için kullanır; çerçeve sonu (EOF) (7 bit) vardır.



Şekil 2. CAN veri yolu veri çerçevesi.

Sürücülere daha fazla kolaylık sunmanın yolları olarak iki önemli buluş ortaya çıkmaktadır: yüksek bağlanabilirlik ve otomotiv elektroniği [5]. Araçtan araca iletişim, sürücülerin yoldaki tehlikeli durumlar gibi önemli bilgileri paylaşmasına olanak sağlamak için akıllı cihazları ve hücresele ağı kullanır. Bir başka iletişim türü de otonom araçlara sensörler şeklinde dahil edilen araçtan altyapıya iletişimdir. Teknolojideki yeni gelişmeler, güvenlik (örn. ileri çarpışma önleme) ve konfor (örn. telematik) sunan belirli araçlarla donatılmış akıllı araçların ortaya çıkmasını sağlamıştır [6,7]. Ancak, araç bağlantısındaki bu gelişmeler dış saldırılara açıktır. Örneğin, mevcut CAN mesaj çerçevesi kimlik doğrulama mekanizmalarına sahip değildir ve bu da araç içi veriler için güvenlik eksikliğine yol açmaktadır [8]. Buna ek olarak, araç içi kontrolörlerin birbirine bağlanması, mimarinin karmaşıklığında bir artışa eşlik etmektedir. Bu nedenle, kontrolörler arasındaki karşılıklı etkiler nedeniyle istenmeyen hareketler veya arızalar meydana gelebilir ve bu da yolcuların güvenliğini veya araçların siber güvenliğini etkileyen kusurlara yol açabilir [9-11].

Araçlar gibi görev açısından kritik bir ortamın siber güvenliğini tasarlarlarken belirli prosedürler göz önünde bulundurulmalıdır. IVN'lerin korunması, yüksek doğrulukta saldırı tespit veya önleme sistemleri gerektirir [12]. Bir araç kritik bir mesajı saldırı olarak algılayabilir ve güvenlik sorunlarına neden olabilir. Sonuç olarak, saldırı önleme sistemi aşağıdaki özelliklere sahip olmalıdır

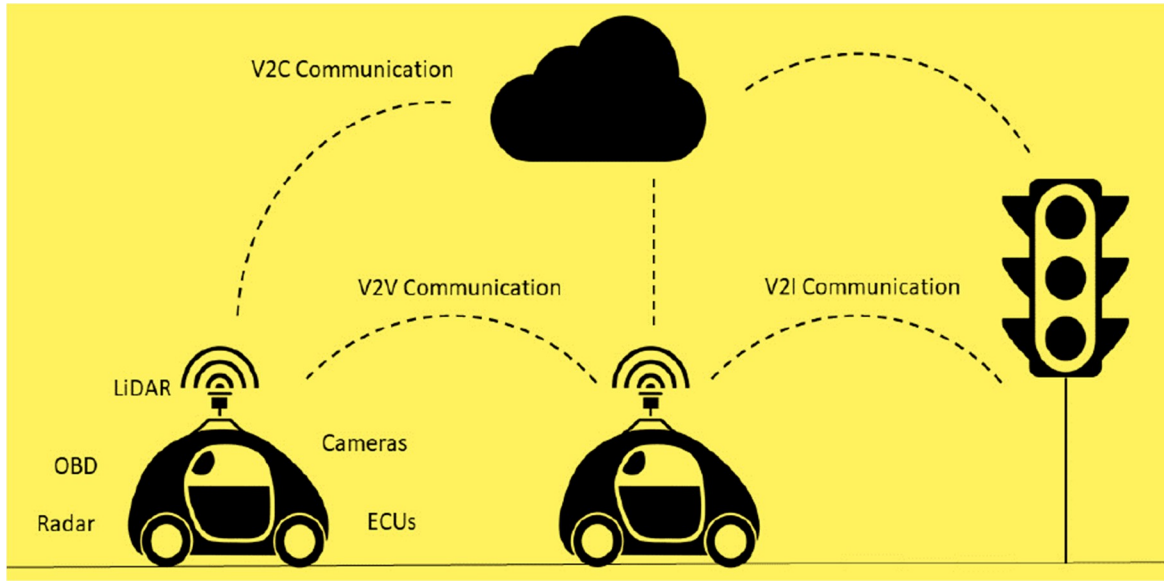
yanlış alarmları engelleyebilmektedir [13,14]. Araçlara yönelik kötü niyetli saldırılar yolcular, yayalar ve diğer araçlar için güvenlik sorunları oluşturabilir. Bu nedenle, araçların siber güvenliği için gerçek zamanlı yanıt hayati önem taşımaktadır. Bununla birlikte, araç içi sistem, hareket halindeki zaman ve alan kaynaklarındaki kısıtlamalar nedeniyle gerçek zamanlı olarak yanıt veremez. Bu durum, mevcut sınırlı kaynaklar dahilinde performans gösteren yüksek doğrulukta gerçek zamanlı bir saldırı tespit sistemi (IDS) tasarlama gerekliliğini ortaya çıkarmaktadır [15].

Alıcı düğümler, kaynağı belirtilmeyen alınan bir paketin yetkili olup olmadığını doğrulamadığı için CAN veri yolu sisteminin teknik kusurları olduğu gösterilmiştir [16]. Bilgisayar korsanları ECU'ları kullanarak kimliği doğrulanmamış CAN paketleri gönderebilirler. Bu tür kusurlar CAN veri yolu sistemlerini savunmasız hale getirir ve saldırılardan sorumlu düğümleri tanıyamaz. Bu nedenle, CAN veri yolu için güvenlik sistemleri önemlidir [17].

Ancak, otomotiv araştırma alanında yeni oldukları için ağ tabanlı saldırılarda birçok zorluk ortaya çıkmaktadır [18]. CAN protokolünü değiştirme fırsatı olduğundan, protokoldeki herhangi bir değişikliğe uyum sağlamak için örnekler aracılığıyla öğrenme yeteneği sayesinde bir saldırı tespit yöntemi uygulamak için bir makine öğrenimi yaklaşımı kullanılabilir. Birçok çalışma, konuşlandırıldığında denetim gerektiren makine öğrenimine bağlı IDS'yi benimsemiştir. Bu tür çalışmalarda kullanılan verilerin kapsamlı bir şekilde etiketlenmesi gerekir ki bu da gerçek zamanlı CAN tarafından üretilen milisaniye başına büyük miktarda veri göz önüne alındığında pratik değildir [19,20]. Sonuç olarak, denetimsiz makine öğrenimi yaklaşımına dayalı bir tespit sistemine ihtiyaç duyulmaktadır.

ABD'de Google, sürücüsüz araçları incelemeye 2009 yılında CAV'ların yol testleri ile başlamıştır [21]. Tesla [22] yol üstü CAV sürüş araçları tasarlamış ve bunları ticari amaçlarla dağıtmıştır; örneğin Michigan Üniversitesi [23] Mcity alanında test etmiştir. Avrupa'da BMW, Audi ve Mercedes Benz gibi büyük şirketler CAN sistemleri geliştirmeye başlamıştır [24]. Çin'de CAN sistemi Şangay'da test edilmiş [25], Baidu ise 2019 yılında Apollo CAV çerçevesini tasarlamaya başlamıştır [26]. Bazı çalışmalar CAV'lerde izinsiz girişleri tartışmaya çalışmıştır. Ciddi siber saldırılardan ikisi olan spoofing ve flood saldırılarının sahte mesajlar gönderdiği belirtilmiştir [27]. CAV'lerdeki siber saldırılar pasif ve aktif saldırılar olarak kategorize edilmiştir.

Giriş şifresi, bilgi edinme saldırıları, birbirine bağlı bilgisayar ağlarına yapılan saldırı türleridir [28]. Geleneksel otomobil araçlarındaki çeşitli saldırı kaynakları aslında ses sistemine veya mobil uygulamalara yönelik siber saldırılar ve CAN'a yönelik saldırılar olmak üzere iki türde sınıflandırılmıştır [29]. İkinci saldırı türü ilkinde göre daha risklidir çünkü CAN frenler, klima sistemleri ve direksiyon simidi gibi araç içi donanım parçalarıyla bağlantılıdır. CAV'ler, bilgisayar ağları ve sıradan otomobillerden farklı olarak, tüm ulaşım altyapısına bağlı hem donanım hem de sanal yazılım bileşenleriyle entegre edilmiştir. Sonuç olarak, bir araca yönelik her türlü saldırı CAV'lerde meydana gelebilir. Ayrıca, otonomi ve bağlanabilirlik arttıkça, daha fazla güvenlik açığı ve saldırı noktası ortaya çıkacaktır [30]. Sistemi, elektronik veya fiziksel olarak etkinliğini etkileyebilecek siber saldırılara karşı güvence altına almak için siber güvenlik gereklidir. Şekil 3'te açıklanan yapay zeka modeli tabanlı CAV mimarisini kullanarak, başlangıç aşamasında CAV'lara yönelik farklı saldırı türlerini tespit etmek, tanımlamak ve kategorize etmek hayati önem .



Şekil 3. İletişim yoluyla saldırı noktaları.

## 2. İlgili Çalışmalar

CAN üzerinde saldırı tespit sistemleri üzerine yapılan en son araştırma çalışmaları bu bölümde ele alınmaktadır. Song ve diğerleri [31] araç içi ağ trafiği verilerini saldırılara karşı eğiterek izinsiz girişleri tespit etmek için bir başlangıç-ResNet modeli kullanmıştır. Sonuçlar uzun kısa süreli hafıza, sinir ağı (NN), destek vektör makinesi (SVM) yaklaşımı, naif Bayes yaklaşımı, k-en yakın komşu (KNN) modeli [32] ve karar ağacı algoritmaları [33] gibi çeşitli mevcut modellerle karşılaştırılmıştır. Zhang ve diğerleri [34] CAN yolunu saldırılara karşı yönetmek için bir saldırı tespit sistemi geliştirmiş ve yazarlar saldırı mesajlarının sınıflandırılması için gradyan iniş momentumu ve uyarlanabilir kazanç gibi bir hybrid modeli kullanmışlardır. Liang ve diğerleri [35] CAN veri yolu mesaj çerçevesini izlemek için derin sinir ağı tabanlı saldırı tespitini uygulamıştır. Eğitim süreci için kullanılan derin öğrenme modeli, önerilen sistemin doğruluğunun %98'e ulaştığı gösterilen derin inanç ağı işleviydi. Hoppe ve diğerleri [36], yeni ağ paketlerinin desenini bulmak için ağ trafiğini analiz etmek üzere CAN veri yolunda bir IDS sistemi geliştirmiş ve bunları IDS sistemindeki desenlerle karşılaştırmıştır. Sistem geleneksel sistemle karşılaştırılmış ve sistemlerinin yüksek doğruluk elde ettiği belirtilmiştir. Taylor ve diğerleri [37] CAN veri yolu saldırılarını tespit etmek için bir LSTM modeli sunmuştur. Wang ve arkadaşları [38] dağıtık bir anomali sınıflandırması tasarlamak için hiyerarşik bir zamansal memory algoritması sunmuştur. Ampirik sonuçlar, modelin saldırıları tespit etmek için daha fazla zaman gerektirdiğini göstermiştir. CAN veri yolu üzerindeki izinsiz girişleri tahmin etmek için derin sinir ağı [39,40], uygulamalı Evrişimsel Sinir Ağları (CNN'ler) [41] ve yapay sinir ağları (YSA'lar) kullanılarak çeşitli makine öğrenimi (ML) ve derin öğrenme (DL) algoritmaları uygulanmıştır [42].

Araçların siber güvenliği konusunda farkındalık yaratmak için 2015 yılında bir Jeep Cherokee uzaktan hacklenmiştir [43]. Yakın zamanda yapılan bir çalışma [44], saldırılara karşı koruyan bir güvenlik sistemine sahip bir araç üretmenin imkansız olması nedeniyle araştırmanın ana odağının saldırıları önlemek olmaması gerektiği sonucuna varmıştır. Aksine, saldırıları tespit eden ve buna göre yanıt veren bir sistemin tasarlanmasına dikkat edilmelidir.

Bu nedenle, bu çalışma, araçlara enjekte edilen mesajlardan kaynaklanan saldırıları ve anormal davranışları gerçek zamanlı olarak uygun doğrulukla tespit eden bir model önermektedir. Saldırı verilerini tespit etmek ve sınıflandırmak için hiyerarşik veri analizi olarak bilinen bir teknik uygulanmıştır. Ayrıca, saldırı tespit modelini uygun şekilde eğiterek yanlış tespit ve tespit edilmemeyi en aza indirmek için bir makine öğrenimi algoritması kullanılmıştır. Gerekli hiper parametreleri elde etmek için bir simülasyon ortamı sağladık ve seçilen veri kümesine uygun bir algoritma kullandık. Daha spesifik olarak, bir saldırıyı anında tespit eden bir yöntem

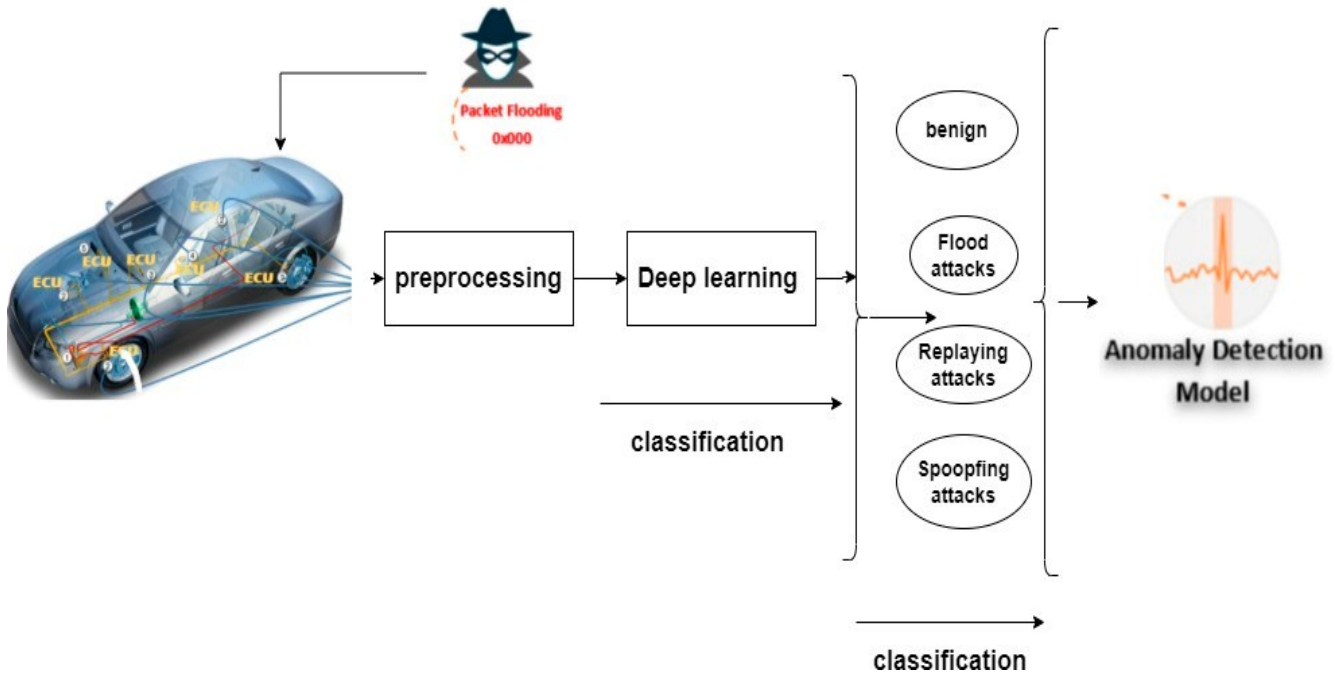
gerçek zamanlı olarak mevcut saldırı önerilmiştir [45–47]. Bu, CAN veri davranışı aracılığıyla elde edildi. Modeli gerçek bir ortamdaki araçlar için doğrulamak için doğruluğunu artırdık ve sınırlı kaynaklarla işlevini sağladık. Modelin doğruluğunu ölçmek için F1 puanı ve tespit süresi güvenilir ölçütler olarak kullanıldı. Çalışmamızın deneysel sonuçları, bir CAN veri yolundan gelen saldırı mesajlarını tespit etmek için diğer son teknoloji yaklaşımlarla karşılaştırıldığında derin öğrenme yaklaşımlarıyla optimum doğruluk gösterdi [48].

### 3. Katkı

Önerilen sistemin temel motivasyonu, potansiyel saldırı mesajlarını tespit ederek ve CAV siber güvenliğini başlatarak CAV'lerde bilgi güvenliğinin zorluklarını ele almaktır. Yapay zeka çerçevesi, IVN'lerin iletişimine yönelik siber tehditlerle yüzleşmek için sağlam bir yapıya yönelik bir çözümdür. CAV'lerin birçok ülkede gelişmekte olan bir teknoloji haline geldiği ve günlük sosyal hayata dahil edildiği göz önüne alındığında, IVN'lerin işlevinden yeni saldırı tespiti önemlidir. Araç içi CAN otobüslerine yönelik saldırıları tespit etmek için önerilen derin öğrenme yaklaşımlarının geliştirilmesi çalışmanın temel amacıdır. Bu yöntem, mevcut sistemlere kıyasla tüm saldırı türlerinin tespit doğruluğunu büyük ölçüde geliştirmiştir. Önerilen sistem iki tür saldırının tespitinde üstün doğruluk elde etmiştir. Ayrıca, derin öğrenme yaklaşımı bir CAN veri yolundaki saldırı mesajlarını tespit etmiştir. Önerilen sistem, CAV siber güvenliği için güncel gerçek veri kümeleri kullanılarak incelenmiştir.

### 4. Materyaller ve Yöntemler

Sürücüsüz araçlar hızla geliştirilirken, birçok şirket CAV sisteminin saldırılara karşı korunmasıyla ilgili zorluklarla karşılaşmış ve yolda çeşitli sorunlar yaratmıştır. Birkaç çalışma, sistemlerin güvenliğini sağlamak için yaklaşımları tartışmıştır, ancak yüksek performans elde etmek için algoritmada hala bir boşluk vardır. Bu çalışmada, gerçek CAV veri kümeleri üzerinde derin öğrenme yaklaşımlarını kullandık. Şekil 4, bir CAV ağına yönelik saldırıları tespit etmek için önerilen çerçeveyi göstermektedir.



Şekil 4. Önerilen çerçeve.

#### 4.1. Veri Seti

CAV veri kümesi, sahtekarlık, sel ve yeniden oynatma saldırıları ve iyi huylu paketler dahil olmak üzere gerçek CAN trafik verilerinden toplanmıştır. Veri kümesi, aktarılan mesajların çeşitli saldırı mesajlarını enjekte ettiği gerçek bir CAV'dan bir CAN trafiği OBD-II portu oluşturularak tasarlanmıştır. CAN paket üretici Open Car Testbed and Network Experiments (OCTANE) kullanılmıştır. Saldırıları her 3 ila 5 saniyede bir enjekte edilmiş ve CAV trafiği 30 ila 40 dakika sürmüştür. Tablo 1 CAN trafiğinin enjeksiyon saldırısını göstermektedir. Veri setine bu bağlantıdan ulaşılabilir: <https://ocslab.hksecurity.net/Datasets/CAN-intrusion-dataset> (erişim tarihi 20 Kasım 2021).

**Tablo 1.** CAN veri yolu saldırıları.

Saldırılar	Açıklama
Sel Saldırısı	CAN'dan farklı ECU düğümlerine flood mesajları gönderme. Saldırıları her 0,3 ms'de bir enjekte edilmiştir.
Saldırıyı Tekrar Oynatma	Tekrarlama saldırıları CAN'a daha önce gönderilmiş bir mesaj gönderir tekrar oynatma saldırıları içeren CAN mesajları enjekte eden kullanıcılar tarafından. Enjeksiyonlar her 0,5 ms'de bir gerçekleşmiştir.
Spoofing Saldırısı (RPM/dişi)	RPM/vites bilgileriyle ilgili CAN mesajlarına saldırı enjekte etme. Her 1 ms'de bir enjekte edildi.

#### 4.2. Ön işleme

Veri kümesi, saniye cinsinden zaman damgası, onaltılık ve DLC cinsinden veri ve hakem kimliği özellikleri ve 0'dan 8'e kadar veri baytları bilgilerini içeriyordu (Tablo 2). Veri kümesinin etiketleri, iyi huylu ve normal paketlerin yanı sıra spoofing, flood ve replaying saldırıları olmak üzere üç saldırı aldı (Tablo 3). Sistemi çalıştırmak için, ECU cihazlarından CAN'a gönderilen mesajlar da dahil olmak üzere veri ve tahkim kimliği özelliği kategorik değişkenlerdir. Bu nedenle, izinsiz girişi tanımlamak ve sınıflandırmak için bu değişkenleri sayısal hale dönüştürdük. Kategorik değişkenler dönüştürüldükten sonra, büyük veri kümelerinin ele alınmasından kaynaklanabilecek eğitim sürecindeki olası bir çakışmayı önlemek için veriler maksimum-minimum normalizasyon yöntemleri kullanılarak işlenmiştir.

Kullanılan normalizasyon yönteminde aynı aralıktaki veri kümesi için 0 ile 1 arasında bir ölçeklendirme aralığı kullandık.

$$z_n = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \left( \frac{x}{x_{\min}} (Yeni_{maks} - Yeni_{m(i)(n)(x)}) + Yeni_{m(i)(n)(x)} \right) \quad (1)$$

Nerede?

- $x_{mi(n)}$ : verilerin minimum değeri
- $x_{m(a)(x)}$ : verilerin maksimum değeri
- $New_{min_x}$ : minimum sayı (0)
- $New_{max_x}$ : maksimum sayı (1).

**Tablo 2.** Veri kümesinin özellikleri. Veri kümesinin özellikleri.

Özellik	
Zaman Damgası	kaydedilen zaman (s)
CAN KİMLİĞİ	CAN mesajının HEX cinsinden tanımlayıcısı
(örn. 043f) DLC	0'dan 8'e kadar veri bayt sayısı
VERİ [0~7]	veri değeri (bayt)

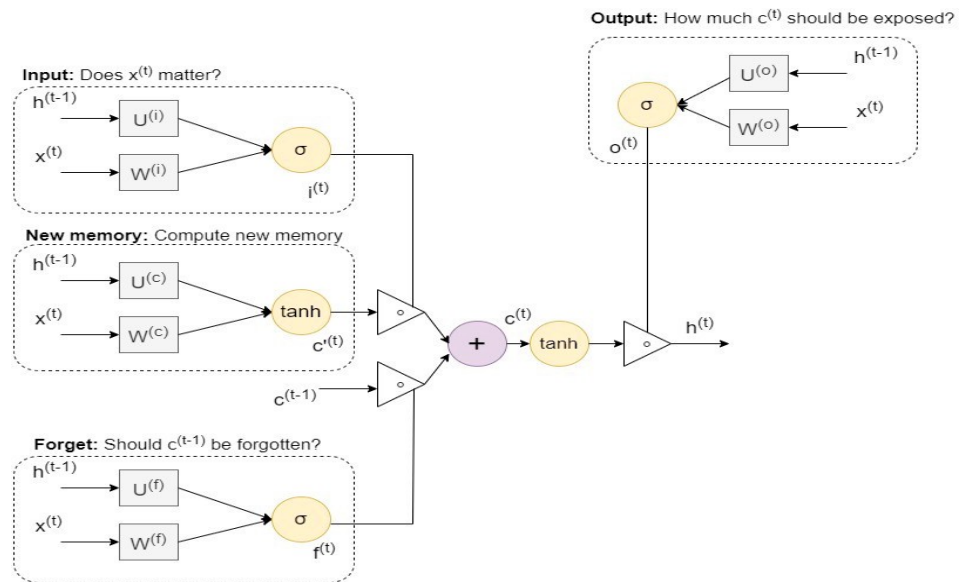


**Tablo 3. Her sınıf için Her sınıf için eğitim veri kümeleri.**

#Etiketler	Cilt
Sel saldırısı	38,657
Tekrarlanan saldırı	13,294
Spoofing saldırısı	2890
Normal paketler	739,679
Fuzzing	22,527

#### 4.3. Derin Öğrenme Algoritması için Önerilen Sistem

Bu çalışmada, CAN saldırılarını tespit etmek için derin öğrenme yaklaşımlarını uyguladık, [49] LSTM tekniğini uzun vadeli bilgi bağımlılığı için bir zaman tekrarlayan sinir ağı (RNN) olarak sunduk. LSTM'nin akışı RNN'ninkiyle karşılaştırılabilir. LSTM ve RNN teknikleri arasındaki fark, LSTM durumunda hücrelerin çalışma şeklidir [50]. Her LSTM birimi dört kapıdan oluşur: giriş, aday, unutma ve çıkış. Unutma kapısı, verileri atılmaları veya kaydedilmeleri gerekli gerekmedikine göre sınıflandırır. Giriş kapısı hücreleri yeniler ve LSTM'deki gizli durum her zaman çıkış kapısı tarafından belirlenir. Ayrıca LSTM, RNN öğrenme sürecindeki hem kaybolma hem de patlama-gradyan zorluklarını çözmesine olanak tanıyan gömülü bir bellek bloğu ve kapı yapısı içerir [51]. LSTM tekniğinin yapısı Şekil 5'te görülebilir.

**Şekil 5. LSTM tekniğinin yapısı.**

aşağıdaki gibidir:

Şekil 5'teki LSTM yapısı ile ilişkilendirilen hesaplama denklemleri

$f_i =$

$$\sigma(W_{(f)} \cdot X_t + W_{(f)} \cdot h_{(t-1)} + b_f) \quad (2)$$

$$i_t = \sigma(W_{(i)} \cdot X_t + W_{(i)} \cdot h_{(t-1)} + b_i) \quad (3)$$

$$S_t = \tanh(W_{(c)} \cdot X_t + W_{(c)} \cdot h_{(t-1)} + b_c) \quad (4)$$

$$C_t = i_t * S_t + f_t * C_{t-1} \quad (5)$$

$$o_t = \sigma(W_{(o)} \cdot X_t + W_{(o)} \cdot h_{(t-1)} + V_{(o)} \cdot C_t + b_o) \quad (6)$$

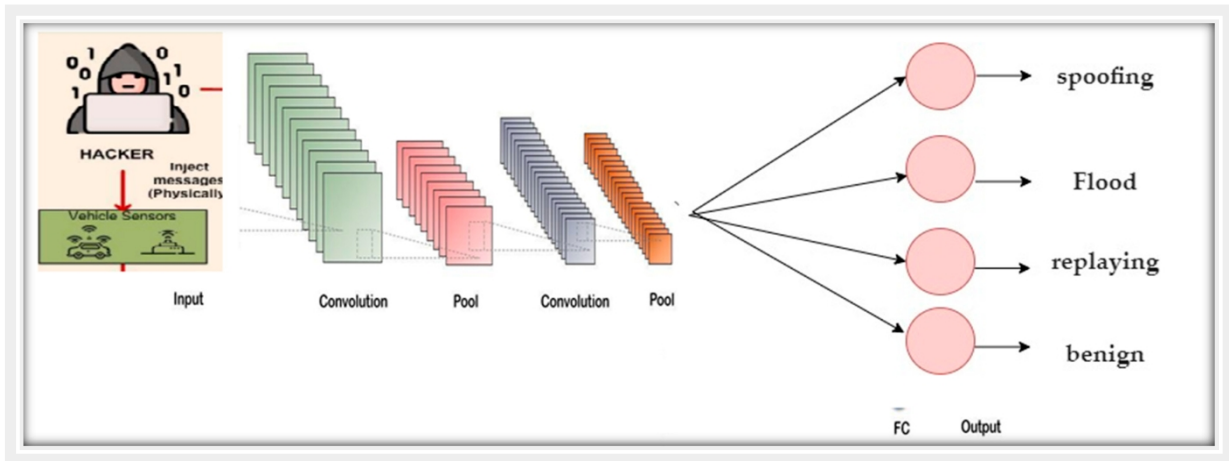
$$h_{(t)} = o_t + \tanh(C_{(t)}) \quad (7)$$

Yukarıdaki formüllerde yer alan aritmetik gösterimler aşağıdaki gibi gösterilebilir:

$X_t$ ,  $t$  zamanında bellek hücresine iletilen giriş verilerinin vektörüdür;  $W_i$ ,  $W_f$ ,  $W_c$ ,  $W_o$  ve  $V_o$  ağırlık matrislerini ifade eder;

$b_{ij}$ ,  $b_{(j)}$ ,  $b_c$  ve  $b_o$  önyargı vektörlerine işaret etmektedir;  
 $h_t$ ,  $t$  zamanında bellek hücresinin belirtilen değerini gösterir;  
 $S_t$  ve  $C_t$  sırasıyla bellek hücresinin aday durumunun ve bellek hücresinin  $t$  zamanındaki durumunun tanımlanmış değerleridir;  
 $\sigma$  ve  $\tanh$ , LSTM sinir ağındaki aktivasyon fonksiyonlarını temsil eder;  
 $i_t$ ,  $f_t$  ve  $o_t$  sırasıyla  $t$  zamanında giriş kapısı, unutma kapısı ve çıkış için elde edilen değerlerdir. Bu kapılar doğrusal olmayan sigmoid aktivasyon fonksiyonu üzerinde 0 ile 1 aralığında değerlere sahiptir.

CNN, uzamsal girdileri dikkate alan derin öğrenme sinir ağının bir tekniğidir. CNN nöronları, diğer sinir ağlarında olduğu gibi, eğitilebilir ağırlıklara ve önyargılara sahiptir. Ayrıca, CNN çoğunlukla bilgiyi ızgara düzeniyle yönetmek için kullanılır ve bu da onu diğer mimarilerden ayırır [52]. CNN, girişten çıkışa doğru tek yönde veri akışı olan ileri beslemeli bir ağıdır [53]. CNN modeli temel olarak üç katmandan oluşur: konvolüsyonel, havuzlama ve tam bağlı. Veri boyutluluğunu ve hesaplama maliyetini azaltmak için konvolüsyon ve havuzlama katmanları kullanılır. Tamamen bağlı katman ise önceki katmanların çıkışına bağlanan katlanmış katmandır. CNN'in yapısında maksimum, ortalama ve global havuzlama gibi farklı teknikleri bulunmaktadır. Bunlardan maksimum havuzlama yaygın olarak kullanılır ve bir havuzlama penceresinden maksimum değeri seçerek çalışır. Şekil 6'da CNN modelinin yapısı gösterilmektedir.



Şekil 6. CNN modelinin yapısı. CNN modelinin yapısı.

CNN-LSTM, sinir ağları tekniklerine dayanan entegre bir derin öğrenme algoritmasıdır. Görsel zaman serisi tahmini sorunlarını çözmek ve görüntü dizilerinden metin oluşturmak için oluşturulmuştur. CNN katmanları, giriş verilerinden bir çıkarma özelliği olarak kullanılırken, LSTM, CNN-LSTM sisteminde sıralı tahmine izin vermek için CNN ile birleştirilir. CNN uzamsal verilerden bilgi alır, açıklamayı oluşturmak için LSTM yapısına uygular [54,55] ve saldırı tespit sistemini sınıflandırır. CNN-LSTM ağı, uzamsal-zamansal ilişkileri etkili bir şekilde korur ve deney sonuçlarına göre yağış tahmininde bağlantılı LSTM (FC-LSTM) modelini sürekli olarak yener. CNN-LSTM modelinin yapısı Şekil 7'de gösterilmektedir. CNN-LSTM modelinin önemli parametreleri Tablo 4'te sunulmuştur. CNN-LSTM algoritmasının sözde kodu Algoritma 1'de sunulmuştur.



**Algoritma 1. CNN-LSTM Algoritması**

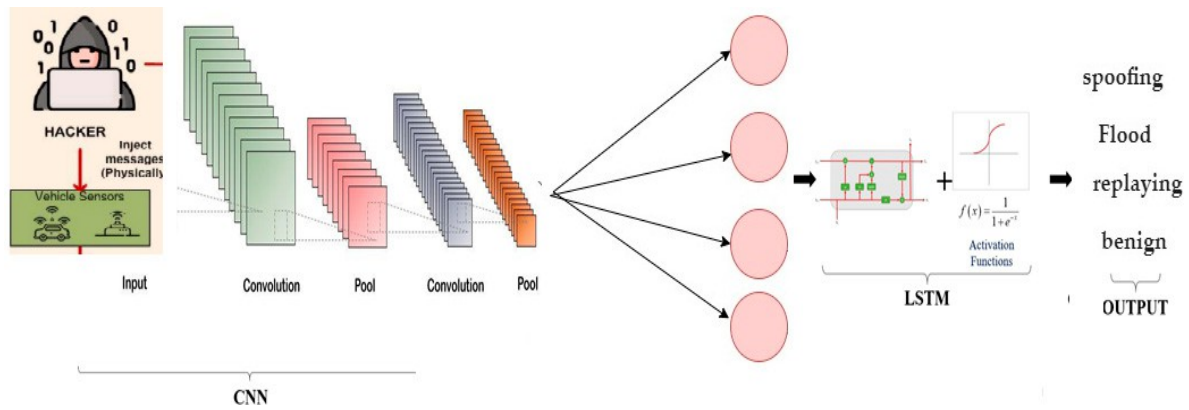

---

```

Veri ön işleme
Sınıf 4, giriş verileri 22222
Model = Sequential()
model. Add(Conv1D(filters= 128, kernel_size= 1, strides= 1, padding= 'same', input
shape = (train_data_st.shape [1], 1))
model. Add(Conv1D(filters= 128, kernel_size= 1, strides= 1, padding= 'same')) model.
Add(LSTM(64, activation = 'relu', return sequences = True))
model. Add(LSTM(64, dönüş dizileri= True)) model.
Ekle(Flatten())
model.add(Dense(128, aktivasyon= 'relu'))
model.add(Dense(256, aktivasyon= 'relu'))
Model Oluşturun
Giriş= Giriş(şekil= (train_data_st.shape[1],1))
C= Conv1D(filters= 32, kernel_size= 1, strides= 1)(inp)
C2= Conv1D(filters= 32, kernel_size= 1, strides= 1, padding= 'same')(C) A1 =
Activation("relu")(C11)
C3= Conv1D(filters= 32, kernel_size= 1, strides= 1, padding= 'same')(A11) S13 =
Add()([C12, C])
A1= Etkinleştirme ("relu")(S11)
M11= MaxPooling1D(pool_size= 1, strides= 2)(A12)
C3= Conv1D(filters= 32, kernel_size= 1, strides= 1, padding= 'same')(M11) A3 =
Activation("relu")(C21)
C4= Conv1D(filters= 32, kernel_size= 1, strides= 1, padding= 'same')(A21) S4 =
Add()([C22, M11])
A4= Etkinleştirme ("relu")(S11)
M4= MaxPooling1D(pool_size= 1, strides= 2)(A22)
C5= Conv1D(filters= 32, kernel_size= 1, strides= 1, padding= 'same')(M21) A5 =
Activation("relu")(C31)
C6= Conv1D(filters= 32, kernel_size= 1, strides= 1, padding= 'same')(A31) S5 =
Add()([C32, M21])
A5= Etkinleştirme ("relu")(S31)
M31= MaxPooling1D(pool_size= 1, strides= 2)(A32) F1 =
Flatten()(M31)
D1= Yoğun(32)(F1)
A66= Etkinleştirme("relu")(D1)
D22 = Yoğun(32)(A66)
D33= Dense(labels.shape[1])(D22) A77=
Activation("softmax")(D33)
model= Model(girdiler= inp, çıktılar= A7) #
opotimnasyon
Parametreler sabır= 3, verbose= 1, faktör= 0.5, lr= 0.00001 ve optimize edici= rms, epochs= 10 batch_size
= 64
İçin→ rms= keras.optimizers.rms= RMSprop(learning_rate= 0.001, rho= 0.9) history
= model.fit(x_train_cnn,y_train, batch_size= batch_size, steps_per_epoch =
x_train.shape[0]//batch_size,
epochs= epochs,
validation_data = (x_validate_cnn,y_validate),
#validation_split = 0.10,
callbacks= [learning_rate_reduction, checkpoint]

```

---



Şekil 7. CNN-LSTM modunun yapısı.

Tablo 4. Önerilen modelin parametreleri. Önerilen modelin parametreleri.

Parametreler	Değerlerin Boyutu
Konvolüsyon katmanı	128
Çekirdek boyutu	5
Maksimum havuzlama boyutu	5
Bırakma Boyutu	0.50
Tam bağlı boyut	256
Etkinleştirme işlevinin adı	tanh
Optimizier fonksiyonu	RMSprop
Öğrenme_oranı	0.001

#### 4.4. Değerlendirme Metrikleri

Önerilen sistemi değerlendirmek için doğruluk, geri çağırma, kesinlik ve F1-skor metriklerinin standart değerlendirmesi uygulanmıştır. Değerlendirme metrikleri, doğru-pozitif (TP), yanlış-pozitif (FP), doğru-negatif (TN) ve yanlış-negatif (FN) olmak üzere karışıklık metrikleri göstergeleri kullanılarak hesaplanmaktadır.

$$\text{Doğruluk} = \frac{TP + TN}{FP + FN + TP + TN} \times 100\% \quad (8)$$

$$\text{Hassasiyet} = \frac{TP}{TP + FP} \times 100\% \quad (9)$$

$$\text{F1-puan} = 2 \times \frac{\text{hassasiyet} \times \text{duyarlılık}}{\text{hassasiyet} + \text{duyarlılık}} \times 100\% \quad (10)$$

$$\text{Özgüllük} = \frac{TN}{TN + FP} \times 100\% \quad (11)$$

## 5. Deneyler

Önerilen derin öğrenme algoritmasının incelenmesi için eğitim verilerini toplamak üzere CAN paketleri üreticisi OCTANE kullanılmıştır. Bu deneyde, CNN ve CNN-LSTM olmak üzere iki derin öğrenme algoritması uyguladık.

### 5.1. Veri Kümesini Bölme

Veri kümesi eğitim için %70 ve test için %30 veriye bölünmüştür. Test verileri, aracın öz bakım sisteminden saldırı tespiti için modelimizi doğrulamak ve değerlendirmek için kullanılmıştır. Tablo 5 veri kümesinin bölünmesini göstermektedir.

**Tablo 5.** Veri kümesini bölme.

#Veri	#Instance Değerleri
Eğitim	490,526
Test	240,258
Doğrulama	70,076

Bu deneyde, ağ paketleri 800.860 idi. Test süreci, test verisi olarak kabul edilen 240.258 paket içeriyordu. Doğrulama süreci, eğitim sürecinde ortaya çıkan aşırı uyum sorunlarını önlemek için uygulanmıştır.

### 5.2. Ortam Kurulumu

Yapay zeka algoritmalarını kullanarak siber güvenlik sistemini geliştirmek için, sistemi başarılı bir şekilde elde etmek için donanım ve yazılım parçaları gerekiyordu. Tablo 6, önerilen güvenlik sisteminin geliştirilmesi için sistem gereksinimlerini özetlemektedir.

**Tablo 6.** Sistemin tasarımı için donanım ve yazılım gereksinimleri.

Donanım	Yazılım
8 GB RAM	Python
CPU I7	Jupyter
	İşletim Sistemi: Windows

### 5.3. Sonuçlar

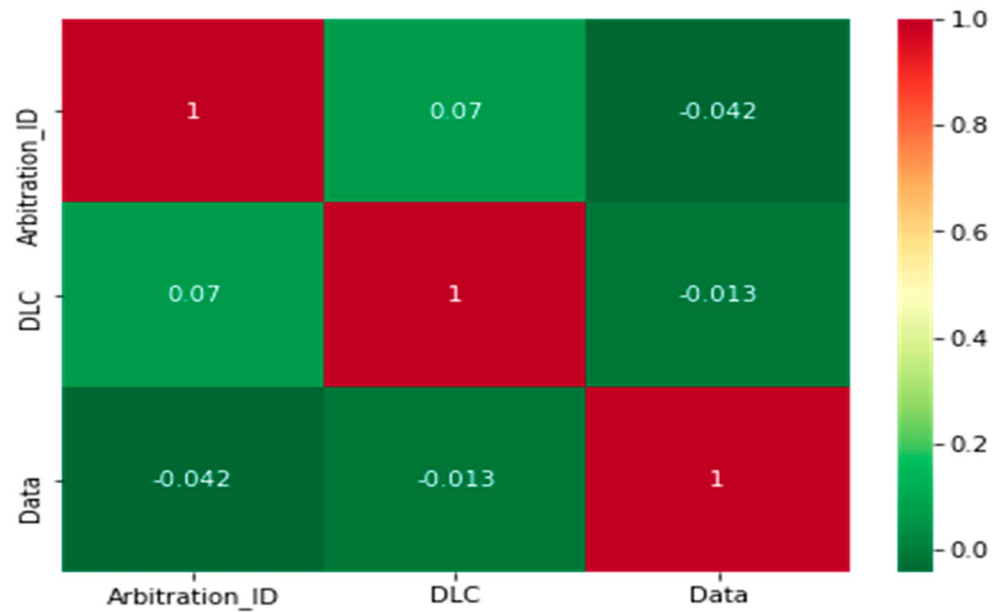
Önerilen derin öğrenme modelleri, araç ağından gelen saldırı mesajlarını tanımlamak için kullanılmıştır. Sistem, fuzzing, spoofing, replaying ve normal paketleri içeren gerçek bir ağ uygulanarak incelenmiştir. Veri kümeleri rastgele olarak %70'i eğitim ve %30'u test için ayrılmıştır. Sistemin veri tabanı eğitim aşamasında 486.640 mesaj ve test aşamasında 486.640 mesaj içeriyordu.

Tablo 7, veri kümelerinin istatistiksel analizini, ortalama, maksimum ve minimum değerleri ve belirli veri kümesi özellikleri için standart sapma metriklerini göstermektedir. İstatistiksel sonuçlar, özellikler ve etiketler arasında büyük bir fark olduğunu ortaya koymuştur. Bir CAN veri yolundaki saldırı mesajlarını tespit etmek için kullanılan geleneksel yaklaşımların uygun olmadığını belirttik. Şekil 8, veri kümelerinin özellikleri arasındaki korelasyonu göstermektedir. Ağın farklı özellikleri nedeniyle özellikler arasında bir boşluk vardır.

**Tablo 7. İstatistiksel analiz.** İstatistiksel analiz.

Özellikler	Ortalama	Standart Sapma	Minimum	Maksimum
Tahkim Kimliği	1.80	1.67	0.00	8.00
DLC	7.50	1.188	2.00	8.00
Veri	1.61	5.98	0.00	2.78

Tablo 8 saldırı tespiti için CNN modelinin sonuçlarını göstermektedir. Kesinlik (%0,86), geri çağırma (%100), özgüllük (%93) ve F1-skoru (%100) açısından iyi değerler elde edilmiştir. Ancak, CNN modeli saldırı paketlerini tespit etmekte başarısız olmuştur. Genel olarak, CNN modelinin bir CAN veri yolundan gelen saldırı mesajlarının tespitindeki performansı %86'dır. Daha önce de belirttiğimiz gibi, bir CAN veri yolunun trafiğinin izlenmesi büyük zorluklar yaratmaktadır, bu nedenle bu saldırılarla ilgilenen hibrit bir derin öğrenme modeli geliştirdik.

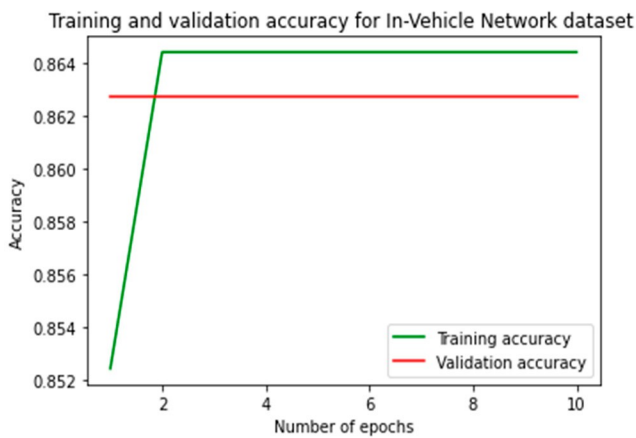


Şekil 8. Veri kümesinin korelasyon özellikleri.

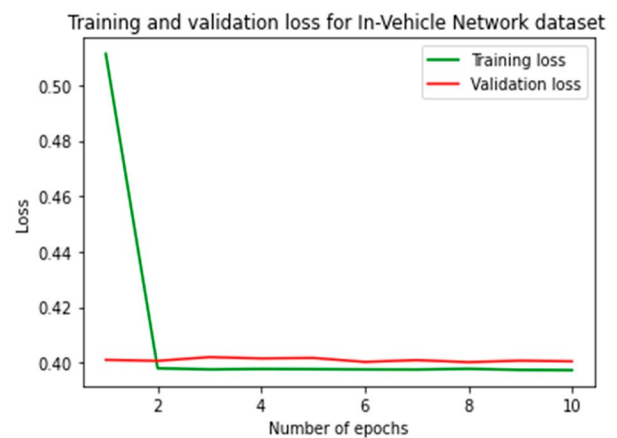
Tablo 8. Doğrulama aşaması için önerilen sistemin sonuçları.

Veri Seti	Hassasiyet (%)	Hatırlama (%)	F1-Skoru (%)
Normal	0.86	100	93
Saldırıları	0.00	0.00	0.00
Doğruluk		0.86	
Ağırlıklı ortalama	0.75	0.86	0.80

Şekil 9, bir araç ağındaki saldırıları tahmin etmek için CNN modelinin performansını, eğitim kaybını ve doğrulamasını göstermektedir. Şekil 9a, CNN modelinin 10 epokluk doğruluğunu göstermektedir. CNN modelinin doğruluğunun %84'ten %86'ya yükseldiğini ve daha sonra bir platoya ulaştığını gözlemledik. Bu nedenle, 10 epok olarak kabul ettik. Şekil 9b, CNN modelindeki eğitim kaybını göstermektedir. Azalan doğruluk performansı nedeniyle eğitim kaybının çok yavaş bir şekilde azaldığı, 0,52'den başlayarak 0,40'a ulaştığı belirtilebilir.



(a)



(b)

Şekil 9. CNN modelinin performansı. CNN modelinin performansı: (a) doğruluk performansı ve (b) eğitim kaybı ve doğrulama.

Eğitim doğruluğunu artırmak için, önerilen sistemin aşırı uyumunun üstesinden gelinmelidir. Bu nedenle, hibrit CNN-LSTM modeli uygulanmıştır. Tablo 9, bir CAN veri yolundan gelen saldırı mesajlarının tespitine ilişkin CNN-LSTM sonuçlarını özetlemektedir. Önerilen sistem tekrarlama ve sahtecilik saldırılarını tespit etmekte başarısız olmuştur. Ancak CNN-LSTM modeli flood, fuzzing ve normal paketlerin tespitinde üstün performans elde etmiştir. Sistemin aşırı uyumunun üstesinden hibrit bir derin öğrenme yaklaşımı kullanılarak gelinmiştir.

**Tablo 9. CNN-LSTM modelinin** CNN-LSTM modelinin bir CAN veri yolu veri kümesi üzerindeki tüm saldırıların tespitindeki sonuçları.

Saldırılar	Hassasiyet %	Hatırlama yüzdesi	F1-Skor %
İyi huylu	95	100	97
Sel	91	0.09	0.16
Tekrar Oynatılıyor	0.0	0.0	0.0
Spoofing	0.0	0.0	0.0
Fuzzy	96	100	98
Doğruluk		95.44%	
Ağırlıklı ortalama	93	95	93
Kayıp	0.20		

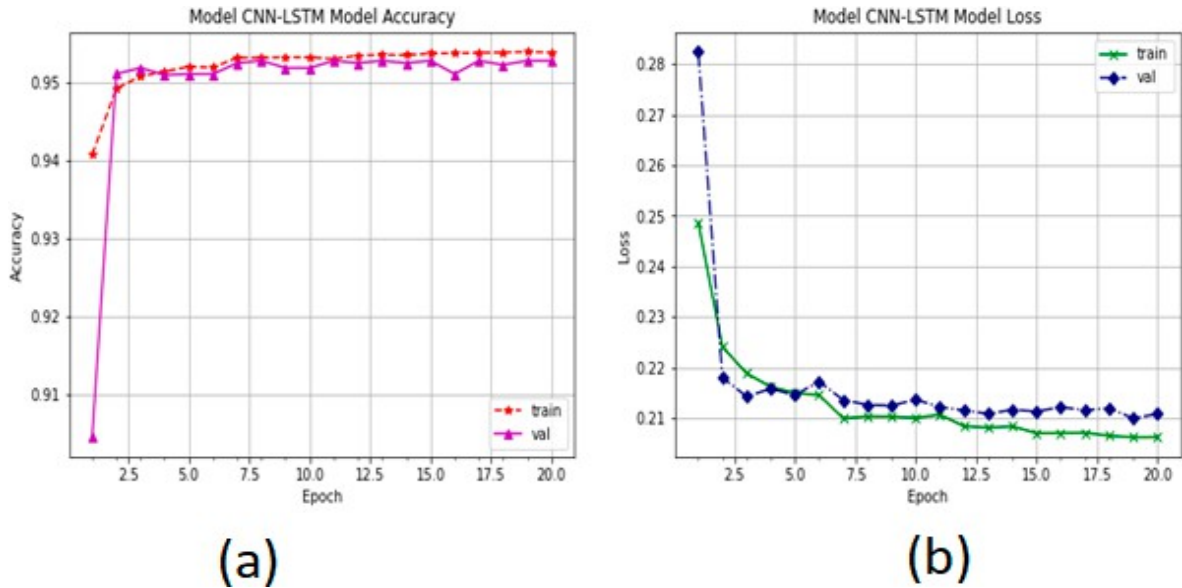
TP, FP, TN ve FN cinsinden karışıklık metrikleri, önerilen sistemdeki CAN mesajlarının değerlendirilmesinde ve sınıflandırılmasında önemlidir. Ayrıca, karışıklık metrikleri normal veya saldırı olarak doğru sınıflandırılan CAN mesajlarının sayısını hesaplar. CNN-LSTM modelinin karışıklık metrikleri Şekil 10'da sunulmuştur. Her bir sınıfa ait tahmin değerleri yüzde olarak sunulmuştur.



**Şekil 10. CNN-LSTM modelinin** CNN-LSTM modelinin karışıklık metrikleri.

Önerilen sistemin doğruluk performansı Şekil 11'de sunulmuştur. Y eksen, düzeltilmiş sınıflandırma yüzdesini temsil eder. Eğitim doğruluğu performans

doğrulama sisteminin. Sistemin doğruluğu 20 epoch'a çıkarmak için optimizasyonu durdurduğunu gözlemliyoruz. CNN-LSTM modelinin performansı %91'den %95,55'e yükselmiştir. Önerilen sistemin eğitim kaybını ölçmek categorical\_crossentropy fonksiyonu kullanılmıştır. Şekil 11b CNN-LSTM kaybını göstermektedir. Doğrulama kaybının 24'ten 20'ye düştüğü, eğitim kaybının ise 20 epok ile 25'ten 21'e düştüğü görülmektedir.



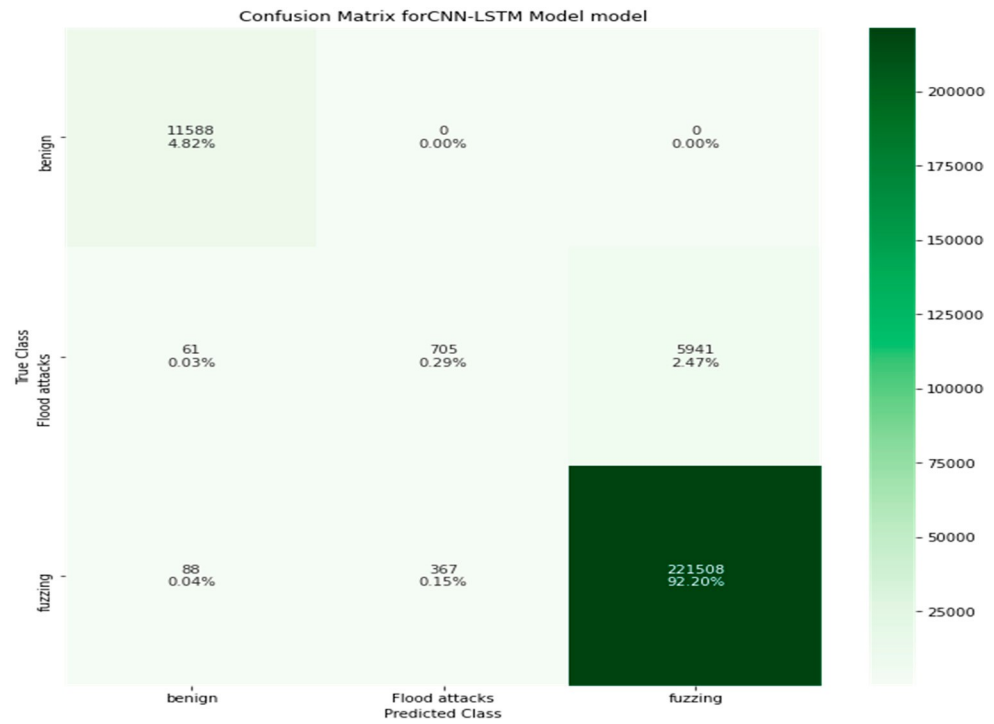
**Şekil 11. CNN-LSTM'nin performansı** CNN-LSTM'nin performansı: (a) doğruluk performansı ve (b) CNN-LSTM modelinin eğitim kaybı ve doğrulaması.

Tablo 10, CNN-LSTM modelinin flood ve fuzzing saldırıları ile normal paketlerin değerlendirilmesindeki deneysel sonuçlarını göstermektedir. Önerilen sistemin performansının arttığı görülmektedir. Ağırlıklı değerlerin değerlendirme metrikleri kesinlik (%97), geri çağırma (%97), F1-skoru (%96) ve doğruluktur (%97,30). Deneysel sonuçlar, tekrarlar ve sahtekarlık saldırıları kaldırıldığında sistemin doğruluğunun arttığını göstermiştir. Şekil 12, CNN-LSTM modelinin bir CAN veri yolundaki sel ve bulanıklaştırma saldırılarının ve normal paketlerin tespitindeki karışıklık metriklerini göstermektedir.

**Tablo 10. CNN-LSTM modelinin** CNN-LSTM modelinin bir CAN veriyolundaki sel, bulanıklaştırma ve normal paketlerin tespiti için sonuçları.

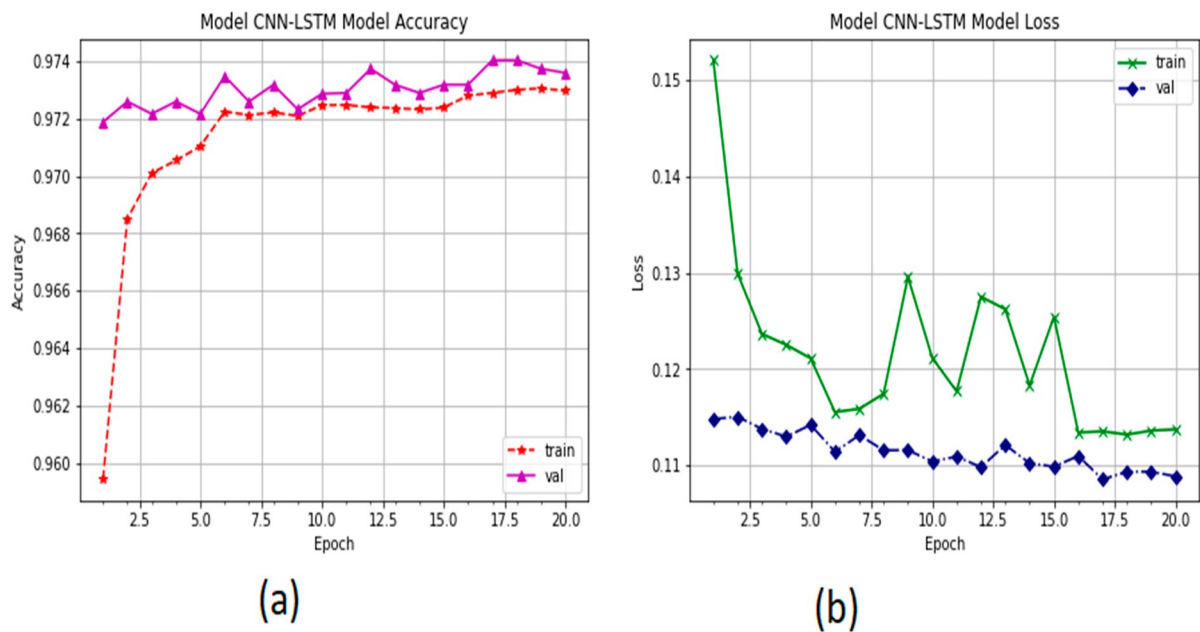
Saldırılar	Hassasiyet %	Hatırlama yüzdesi	F1-Skor %
İyi huylu	99	100	99
Sel	66	11	18
Fuzzy	97	100	99
Doğruluk		97.30%	
Ağırlıklı ortalama	97	97	96
Kayıp	0.11		





**Şekil 12.** CNN-LSTM modelinin bir CAN veri yolu ağındaki sel, bulanıklaştırma ve normal paketlerin tespitindeki karışıklık metrikleri.

Önerilen modelin bir CAN veri yolundaki bulanıklaştırma saldırılarını ve normal paketleri tanımlamak için doğrulama performansı Şekil 13'te sunulmuştur. Sistem, 20 epok ile %94'ten %97,74'e bir artış göstererek %97'lik bir doğrulama doğruluğu elde etmiştir. Doğrulama kaybı, sistemin çok hafif aşırı uyumu nedeniyle minimum düzeydedir ve çapraz entropi metrikleri kullanılarak doğrulama kaybı 0,11'e düşürülmüştür.



**Şekil 13.** CNN-LSTM'nin performansı CNN-LSTM'nin performansı: (a) doğruluk performansı ve (b) CNN-LSTM modelinin bir CAN veriyolundaki sel, bulanıklaştırma ve normal paketleri tespit etmedeki eğitim ve doğrulama kaybı.

## 6. Tartışma

CAV üretimindeki artışla birlikte, şirketler bakımı daha akıllı hale getiren yeni özellikler geliştiriyor ve ekliyor. Bu özellikler uzak ağlara bağlıdır, bu nedenle risk kaçınılmaz olarak artacaktır. Bilgisayar korsanları, yanlış bilgiler içeren sahte mesajlar göndererek CAN veri yolu sisteminde bir açık bulmaya çalışırlar. Otonom araç ağlarında izinsiz giriş tespiti, kötü niyetli trafiğin tespitinde ve farklı ECU'lar arasındaki normal ve anormal mesajların tanımlanması için CAN veri yolu sistemlerinin izlenmesinde önemli bir rol oynamıştır. IDS, yeni saldırıları tespit etmek için çok sayıda saldırı ve normal paket içeren veri tabanlarını işleyen makine öğrenimi ve derin öğrenme algoritmaları gibi yapay zeka modelleri kullanılarak geliştirilebilir.

Bu çalışmada, bir CAN veri yolundaki saldırı davranışlarını tanımlayan bir derin öğrenme modeli araştırılmıştır. Önerilen sistemi değerlendirmek amacıyla, bir CAN veri yolu sistemindeki saldırı mesajlarını tespit etmek için deneysel veriler kullanılmıştır. İlk olarak, veri kümesini iki etiketle tahmin etmek ve sınıflandırmak için bir CNN modeli uyguladık: normal veya saldırılar. Modelin daha fazla aşırı uyuma sahip olduğunu ve doğruluğun iyi olduğunu gözlemledik. İkinci deneyde, hibrit CNN-LSTM modeli flood, fuzzing, spoofing ve replaying saldırısı ve normal bir paket olmak üzere dört etiket/saldırı türü içeren bir veri kümesinden gelen saldırıları tanımlamak için uygulandı. Üçüncü deneyde, CNN-LSTM modelini flood, spoofing, fuzzing ve normal paketleri içeren bir veri kümesiyle uyguladık. Önerilen veri kümesinin performansı farklı bir veri kümesine kıyasla yüksekti. Tablo 11 önerilen sistemin nihai sonuçlarını göstermektedir.

**Tablo 11.** Derin öğrenme algoritmalarının karşılaştırma sonuçları.

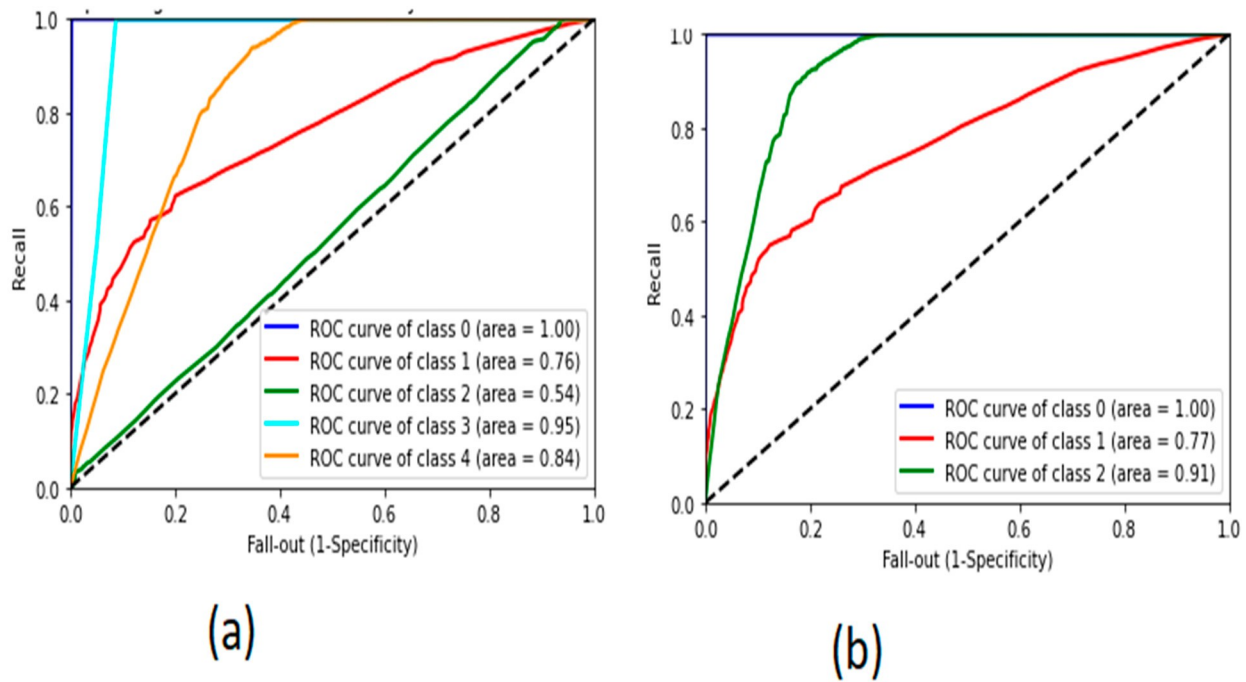
Modeller	Etiketler	Hassasiyet (%)	Hatırlama (%)	F1-Skoru (%)	Doğruluk (%)
CNN	İki	75	86	80	86
CNN-LSTM	Altı	93	95	93	95.44
CNN-LSTM	Üç	97	97	96	97.30

Önerilen sistem, flood, spoofing, fuzzing ve normal paketleri içeren dört sınıftan oluşan veri kümesinde en yüksek doğruluğu elde etmiştir. Alıcı işletim karakteristiği eğrisinin grafiksel gösterimi Şekil 14'te gösterilmekte ve modelin tüm sınıfların sınıflandırılmasındaki performansını ortaya koymaktadır.

Önerilen sistem ile mevcut modeller arasındaki karşılaştırmalı sınıflandırma performansı Tablo 12'de sunulmuştur. Önerilen çerçevenin doğruluğu %97 ile araç ağlarındaki IDS'leri tespit etmek için mevcut tüm sistemlerden daha iyi performans göstermiştir.

**Tablo 12.** Araç içi ağlar için saldırı tespit sistemi üzerine önerilen sisteme karşı son araştırmaların doğruluk performansını gösterir.

Ref.	Modeller	Doğruluk %	Saldırı Türleri
Ref. [56]	Derin öğrenme modeli	95%	Normal ve saldırılar (İki sınıf)
Ref. [57]	Derin öğrenme modeli	85%	DoS, Komut Enjeksiyonu, Kötü Amaçlı Yazılım saldırıları
Ref. [58]	Üretken çekişmeli ağlar	95%	DoS, Fuzzing ve Gear saldırıları
Ref. [59]	LSTM	80%	Spoofing, Replay ve Flooding saldırıları
Ref. [60]	Makine öğrenimi	90%	DoS, Fuzzing, Spoofing saldırıları
Ref. [61]	Sinir ağı-LSTM	90%	DoS, Fuzzing, Spoofing saldırıları
Önerilen model	CNN-LSTM	97%	DoS, Fuzzing, Spoofing, Replaying



**Şekil 14.** CNN-LSTM'nin alıcı işletim özellikleri eğrisi: (a) iki sınıflı veri kümesi ve (b) üç sınıflı veri kümesi.

## 7. Sonuçlar

Otomobil üretiminin ve Nesnelerin İnterneti teknolojisinin hızla gelişmesiyle birlikte, otonom araç ağı akıllı ve daha yerleşik hale geldi. Otonom araç, otomobili uydu navigasyonuna veya eğlence sistemlerine bağlayarak birçok kolaylık sağlamaktadır. Ancak bu kolaylıkları sağlayan otonom otomobiller, akıllı otomatik araç ağının uzaktan erişim için internete bağlanması nedeniyle uzaktan saldırı riskiyle karşı karşıya kalmaktadır.

CAN'ın trafik davranışı doğası gereği bir yayın alanıdır. Etkili bir güvenlik sisteminin geliştirilmesi birçok zorlukla karşı karşıya kalmıştır. Bu nedenle, yapay zeka modellerine dayalı saldırı tespit sistemi, araç ağlarının artan riskine karşı çözümler sunmuştur. Yapay zeka algoritmalarına dayalı IDS, olası saldırganlardan gönderilen CAN mesajlarında herhangi bir değişiklik olması durumunda sistemi güncelleyebilir.

Bu makalede, CAN veri yoluna yönelik saldırılar için, sahtecilik, sel ve tekrarlamalı saldırılarının yanı sıra iyi huylu paketleri de içeren büyük bir gerçek veri kümesi kullanarak yeni bir saldırı tespit sistemi önerdik. OCTANE kullanılarak sistemin değerlendirilmesi için farklı zaman aralıklarında gerçek bir veri kümesi oluşturmak amacıyla CAN veri yolu sistemine çeşitli türlerde saldırı mesajları enjekte edilmiştir.

Deneysel sonuçlar, önerilen CNN-LSTM ve CNN modellerinin saldırı mesajlarını tespit ettiğini ortaya koymuştur. Önerilen sistemlerin CAN veri yolunu korumak için anormal paket tespitini verimli bir şekilde gösterdiği doğrulanmıştır. Ayrıca, güvenli veri işleme için otonom araç ağlarının karmaşık altyapıları içindeki diğer güvenlik sistemleri tasarımlarına da genişletilebilirler.

Genel olarak, önerilen sistemler %97,30'luk bir doğruluk puanı elde etmiştir. Bu deneysel sonuçlar mevcut sistemlerle karşılaştırılmış ve onlardan daha iyi performans göstermiştir. Gelecekte, gelişmiş yapay zeka kullanarak sistemimizi geliştirmeye devam edeceğiz.

**Yazar Katkıları:** Kavramsallaştırma, T.H.H.A. ve .A.; metodoloji, T.H.H.A.; yazılım, T.H.H.A.; doğrulama, T.H.H.A. ve H.A. biçimsel analiz, T.H.H.A. ve H.A. araştırma, T.H.H.A. ve H.A. kaynaklar, T.H.H.A. veri kütüphanesi, T.H.H.A. ve H.A.; yazı-orijinal taslak hazırlama, T.H.H.A. ve H.A.; yazım-inceleme ve düzenleme, .A.; görselleştirme, T.H.H.A. ve .A. gözetim,

T.H.H.A.; proje yönetimi, T.H.H.A. ve H.A.; fon temini, T.H.H.A. ve H.A. Tüm yazarlar makalenin yayınlanan versiyonunu okumuş ve kabul etmiştir.

**Finansman:** Bu araştırma ve APC, Kral Faysal Üniversitesi Bilimsel Araştırmalar Dekanlığı tarafından NA00036 numaralı hibe kapsamında mali destek için finanse edilmiştir.

**Kurumsal İnceleme Kurulu Beyanı:** Geçerli değil.

**Bilgilendirilmiş Onam Beyanı:** Geçerli değil.

**Veri Kullanılabilirlik Beyanı:** Bu çalışmada sunulan verilere <https://ocslab.hksecurity.net/Datasets/datachallenge2019/car> adresinden ulaşılabilir.

**Teşekkür:** Yazarlar, NA00036 numaralı proje aracılığıyla bu araştırma çalışmasını finanse ettiği için Kral Faysal Üniversitesi Bilimsel Araştırma Dekanlığı'na teşekkürlerini sunar.

**Çıkar Çatışmaları:** Yazarlar herhangi bir çıkar çatışması yaşamadıklarını beyan etmişlerdir.

## Referanslar

- Hartenstein, H.; Laberteaux, K.P. *VANET: Vehicular Applications and Inter-Networking Technologies*; John Wiley & Sons: Chichester, İngiltere, 2009.
- Zeng, W.; Khalid, M.A.S.; Chowdhury, S. Araç İçi Ağlara Genel Bakış: Başarılar ve Zorluklar. *IEEE İletişim. Hayatta Kalma. Eğitim.* **2016**, *18*, 1552-1571. [CrossRef]
- Mehedi, S.T.; Anwar, A.; Rahman, Z.; Ahmed, K. Elektrikli Araç Ağları için Derin Transfer Öğrenme Tabanlı İzinsiz Giriş Tespit Sistemi. *Sensörler* **2021**, *21*, 4736. [CrossRef]
- Kiencke, U.; Dais, S.; Litschel, M. Otomotiv Seri Denetleyici Alan Ağı. *SAE Trans.* **1986**, *95*, 823-828.
- Vasudev, H.; Das, D.; Vasilakos, A.V. IoVs iletişim bileşenleri için güvenli mesaj yayma protokolleri. *Hesaplama. Elektrik Müh. Eng.* **2020**, *82*, 106555. [CrossRef]
- Du, R.; Santi, P.; Xiao, M.; Vasilakos, A.V.; Fischione, C. The Sensable City: Akıllı Şehir İzleme için Dağıtım ve Yönetim Üzerine Bir Araştırma. *IEEE İletişim. Hayatta Kalma. Eğitim.* **2019**, *21*, 1533-1560. [CrossRef]
- Barletta, V.; Caivano, D.; DiMauro, G.; Nannavecchia, A.; Scalera, M. Akıllı Şehir Entegre Modelinin Akıllı Program Yönetimi ile Yönetilmesi. *Appl. Sci.* **2020**, *10*, 714. [CrossRef]
- Baldassarre, M.T.; Barletta, V.S.; Caivano, D. Akıllı Bir Şehirde Akıllı Program Yönetimi. Proceedings of the 2018 AEIT International Annual Conference, Bari, Italy, 3-5 October 2018; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, ABD, 2018; pp. 1-6.
- Zhou, J.; Dong, X.; Cao, Z.; Vasilakos, A.V. Bulut Tabanlı Araç DTN'leri için Güvenli ve Gizliliği Koruyan Protokol. *IEEE Trans. Bilgi Güvenliği. Forensics Secur.* **2015**, *10*, 1299-1314. [CrossRef]
- Baldassarre, M.T.; Barletta, V.; Caivano, D.; Scalera, M. Yazılım geliştirmede güvenlik ve gizliliğin bütünleştirilmesi. *Softw. Qual. J.* **2020**, *28*, 987-1018. [CrossRef]
- Zhou, J.; Cao, Z.; Dong, X.; Vasilakos, A.V. Bulut Tabanlı IoT için Güvenlik ve Gizlilik: Zorluklar. *IEEE İletişim. Mag.* **2017**, *55*, 26-33. [CrossRef]
- Challa, S.; Das, A.K.; Gope, P.; Kumar, N.; Wu, F.; Vasilakos, A.V. bulut destekli siber-fiziksel sistemlerde kimlik doğrulamalı anahtar anlaşma şemasının tasarımı ve analizi. *Future Gener. Hesaplama. Syst.* **2020**, *108*, 1267-1286. [CrossRef]
- Sommer, F.; Duerrwang, J.; Kriesten, R. Otomotiv Güvenlik Saldırılarının Araştırılması ve Sınıflandırılması. *Bilgi* **2019**, *10*, 148. [CrossRef]
- Caivano, D. İstatistiksel Süreç Kontrolü yoluyla Sürekli Yazılım Süreci İyileştirme. Proceedings of the Ninth European Conference on Software Maintenance and Reengineering, Manchester, UK, 21-23 March 2005; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, ABD, 2005; s. 288-293.
- Baldassarre, M.T.; Barletta, V.S.; Caivano, D.; Raguseo, D.; Scalera, M. Siber güvenlik eğitimi: Hack-space entegre modeli, CEUR Çalıştay Bildirileri. *ITASEC, Üçüncü İtalyan Siber Güvenlik Konferansı Bildirileri, Pisa, İtalya, 13-15 Şubat 2019*; University of Bari Aldo Moro: Bari, İtalya, 2019; Cilt 2315.
- Lokman, S.F.; Othman, A.T.; Abu-Bakar, M.-H. Otomotiv Kontrolör Alan Ağı (CAN) veri yolu sistemi için izinsiz giriş tespit sistemi: Bir inceleme. *EURASIP J. Wirel. İletişim. Netw.* **2019**, *2019*, 184. [CrossRef]
- Carsten, P.; Andel, T.R.; Yampolskiy, M.; McDonald, J.T. Araç İçi Ağlar. Proceedings of the 10th Annual Cyber and Information Security Research Conference on-CISR '15, London, UK, 6-8 April 2015; Association for Computing Machinery (ACM): New York, NY, USA; pp. 1-8.
- Gmidien, M.; Gmidien, M.H.; Trabelsi, H. Araç içi CAN veri yolunun güvenliğini sağlamak için bir saldırı tespit yöntemi. Proceedings of the 2016 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), Sousse, Tunisia, 19-21 December 2016; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, ABD, 2016; s. 176-180.
- Young, C.; Zambreno, J.; Olufowobi, H.; Bloom, G. Otomotiv Denetleyici Alan Ağı İzinsiz Giriş Tespit Sistemleri Araştırması. *IEEE Des. Test Comput.* **2019**, *36*, 48-55. [CrossRef]

20. Qu, X.; Yang, L.; Guo, K.; Ma, L.; Sun, M.; Ke, M.; Li, M. Denetimsiz Saldırı Tespiti için Kendi Kendini Düzenleyen Haritaların Geliştirilmesi Üzerine Bir Araştırma. *Mob. Netw. Uygulama* **2019**, *26*, 808-829. [\[CrossRef\]](#)
21. Yao, X.Q.; Tang, G.; Hu, X. SOM sinir ağına dayalı konteyner vinç motorunun mekanik durumunu tanıma yöntemi. *IOP Konferans Serisi* içinde: *Malzeme Bilimi ve Mühendisliği*; IOP: Londra, İngiltere, 2018; Cilt 435, s. 12009.
22. NCSL. *Autonomous Vehicles|Self-Driving Vehicles Enacted Legislation*; NCSL: Washington, DC, USA, 2019.
23. Madrigal, A.C. Waymo'nun Sürücüsüz Araçları Eğitmek için Kullandığı Gizli Dünyanın İçinde. *The Atlantic'te*; Carnegie Mellon Üniversitesi: Pittsburgh, PA, ABD, 23 Ağustos 2017.
24. Dikmen, M.; Burns, C.M. Gerçek dünyada otonom sürüş: Tesla Autopilot ve Summon ile deneyimler. Otomotiv Kullanıcı Arayüzleri ve Etkileşimli Araç Uygulamaları 8. Uluslararası Konferansı Bildirileri, New York, NY, ABD, 24 Ekim 2016; ACM: New York, NY, ABD, 2016; s. 225-228.
25. Eustice, R. *Michigan Üniversitesi'nin Otonom Araçlara Yönelik Çalışmaları*; Teknik Rapor; Michigan Üniversitesi: Ann Arbor, MI, ABD, 2015.
26. Fagnant, D.J.; Kockelman, K. Bir ulusu otonom araçlar için hazırlamak: Akıllı bağlantılı araçlar: Endüstriyel uygulamalar ve Çin'deki otomotiv değer zincirleri üzerindeki etkileri öneriler. *Transp. Res. Part A Policy Pract.* **2015**, *77*, 167-181. [\[CrossRef\]](#)
27. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Chekaway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; . Modern bir otomobilin deneysel güvenlik analizi. Güvenlik ve Gizlilik üzerine 2010 IEEE Sempozyumu Bildirileri, Berkeley/Oakland, CA, ABD, 16-19 Mayıs 2010.
28. Checkoway, S.; Damon, M.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S.; Koscher, K.; Czeskis, A.; Roesner, F.; Kohno, T. Otomotiv saldırı yüzeylerinin kapsamlı deneysel analizleri. USENIX Güvenlik Sempozyumu Bildirileri, San Francisco, CA, ABD, 8-12 Ağustos 2011.
29. Miller, C.; Valasek, C. *A Survey of Remote Automotive Attack Surfaces*; BlackHat: Las Vegas, NV, USA, 2014.
30. Song, H.M.; Kim, H.R.; Kim, H.K. Araç içi ağ için CAN mesajlarının zaman aralıklarının analizine dayalı saldırı tespit sistemi. Uluslararası Bilgi Ağı Konferansı (ICOIN) 2016 Bildiriler Kitabı, Kota Kinabalu, Malezya, 13-15 Ocak 2016.
31. Song, H.M.; Woo, J.; Kim, H.K. Derin evrişimli sinir ağı kullanarak araç içi ağa izinsiz giriş tespiti. *Veh. İletişim*. **2020**, *21*, 100198. [\[CrossRef\]](#)
32. Cover, T.M.; Hart, P. En Yakın Komşu Örüntü Sınıflandırması. *IEEE Trans. Inf. Teori* **1967**, *13*, 21-27. [\[CrossRef\]](#)
33. Quinlan, J.R. Karar Ağaçlarının İndüksiyonu. *Mach. Learn.* **1986**, *1*, 81-106. [\[CrossRef\]](#)
34. Zhang, Y.; Chen, X.; Jin, L.; Wang, X.; Guo, D. Ağ İzinsiz Giriş Tespiti: Derin Hiyerarşik Ağ ve Orijinal Akış Verilerine Dayalı. *IEEE Erişim* **2019**, *7*, 37004-37016. [\[CrossRef\]](#)
35. Liang, L.; Ye, H.; Li, G.Y. Akıllı Araç Ağlarına Doğru: Bir Makine Öğrenimi Çerçevesi. *IEEE Internet Things J.* **2019**, *6*, 124-135. [\[CrossRef\]](#)
36. Hoppe, T.; Kiltz, S.; Dittmann, J. Otomotiv CAN ağlarına yönelik güvenlik tehditleri Pratik örnekler ve seçilen kısa vadeli karşı önlemler. *Reliab. Mühendislik. Syst. Saf.* **2011**, *96*, 11-25. [\[CrossRef\]](#)
37. Taylor, A.; Leblanc, S.; Japkowicz, N. Otomobil kontrol ağı verilerinde uzun kısa süreli hafıza ağları ile anomali tespiti. IEEE Uluslararası Veri Bilimi ve İleri Analitik Konferansı Bildirileri (DSAA 2016), Montreal, QC, Kanada, 17-19 Ekim 2016; s. 130-139.
38. Wang, C.; Zhao, Z.; Gong, L.; Zhu, L.; Liu, Z.; Cheng, X. HTM Kullanarak Araç İçi Ağ için Dağıtılmış Bir Anomali Tespit Sistemi. *IEEE Access* **2018**, *6*, 9091-9098. [\[CrossRef\]](#)
39. Bezemskij, A.; Loukas, G.; Gan, D.; Anthony, R.J. Bayesian Ağları Kullanarak Otonom Robotik Bir Araçta Siber-Fiziksel Tehditleri Algılama. 2017 IEEE Uluslararası Nesnelerin İnterneti (iThings) ve IEEE Yeşil Hesaplama ve İletişim (GreenCom) ve IEEE Siber, Fiziksel ve Sosyal Hesaplama (CPSCom) ve IEEE Akıllı Veri (SmartData) Konferansı Bildirileri, Exeter, İngiltere, 21-23 Haziran 2017; Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE): Piscataway, NJ, ABD, 2017; s. 98-103.
40. Kang, M.-J.; Kang, J.-W. Araç İçi Ağ Güvenliği için Derin Sinir Ağı Kullanan Yeni Bir İzinsiz Giriş Tespit Yöntemi. Proceedings of the 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), Nanjing, China, 15-18 May 2016; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, ABD, 2016; pp. 1-5.
41. Kalash, M.; Rochan, M.; Mohammed, N.; Bruce, N.D.B.; Wang, Y.; Iqbal, F. Derin Evrişimli Sinir Ağları ile Kötü Amaçlı Yazılım Sınıflandırması. Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, Fransa, 26-28 Şubat 2018; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, ABD, 2018; s. 1-5.
42. Lin, Z.; Shi, Y.; Xue, Z. IDSGAN: Generative Adversarial Networks for Attack Generation against Intrusion Detection. *arXiv* **2018**, arXiv:1809.02077.
43. Miller, C.; Valasek, C. Değiştirilmemiş Bir Binek Aracın Uzaktan İstismarı. Black Hat USA 2015 Bildiriler Kitabı, Las Vegas, NV, ABD, 1-6 Ağustos 2015; s. 1-91.
44. Miller, C. Bir arabayı hacklemekten alınan dersler. *IEEE Des. Test Comput.* **2019**, *36*, 7-9. [\[CrossRef\]](#)
45. Petit, J.; Shladover, S.E. Otomatik araçlara yönelik potansiyel siber saldırılar. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 546-556. [\[CrossRef\]](#)
46. He, Q.; Meng, X.; Qu, R. CAV'ın siber güvenliği üzerine araştırma. *Kooperatif Konumlandırma ve Hizmet (CPGPS)*; IEEE: Harbin, Çin, 2017; pp. 351-354.

47. Otonom Araç Emniyeti ve Güvenliğinin Bütünleştirilmesi. 2017. Çevrimiçi olarak mevcuttur: [https://www.researchgate.net/publication/321323\\_032\\_Integrating\\_Autonomous\\_Vehicle\\_Safety\\_and\\_Security](https://www.researchgate.net/publication/321323_032_Integrating_Autonomous_Vehicle_Safety_and_Security) (10 Mart 2019 tarihinde erişilmiştir).
48. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Araç iletişiminde siber güvenlik zorlukları- tions. *Veh. Commun.* **2020**, *23*, 100214. [CrossRef]
49. Alkahtani, H.; Aldhyani, T.H.H. Nesnelerin İnterneti Uygulamaları için CNN-LSTM Modeli Kullanarak Botnet Saldırısı Tespiti. *Güvenlik. İletişim. Netw.* **2021**, *2021*, 3806459. [CrossRef]
50. Khan, M.A.; Karim, M.R.; Kim, Y. Evrişimsel-LSTM Ağına Dayalı Ölçeklenebilir ve Hibrit Bir Saldırı Tespit Sistemi. *Simetri* **2019**, *11*, 583. [CrossRef]
51. Alkahtani, H.; Aldhyani, T.; Al-Yaari, M. Siber uzayda uyarlanabilir anomali tespit çerçevesi modeli nesneleri. *Appl. Bionics Biomech.* **2020**, *2020*, 6660489. [CrossRef] [PubMed]
52. Kim, J.; Kim, J.; Kim, H.; Shim, M.; Choi, E. Hizmet Reddi Saldırılarına Karşı CNN Tabanlı Ağ İzinsiz Giriş Tespiti. *Elektronik* **2020**, *9*, 916. [CrossRef]
53. Zheng, Z.; Yatao, Y.; Niu, X. Akıllı Şebekelerin Güvenliğini Sağlamak için Elektrik Hırsızlığı Tespiti için Geniş ve Derin Evrişimsel Sinir Ağları. *IEEE Trans. Ind. Inform.* **2017**, *14*, 1606-1615.
54. Ullah, A.; Javaid, N.; Omaji, S. Akıllı Şebekenin Güvenliğini Sağlamak için Elektrik Hırsızlığı Tespiti için CNN ve GRU tabanlı Derin Sinir Ağı. 2020 Uluslararası Kablosuz İletişim ve Mobil Hesaplama Bildirileri, Limasol, Kıbrıs, 15-19 Haziran 2020.
55. Yao, R.; Wang, N.; Liu, Z.; Chen, P.; Sheng, X. Gelişmiş Ölçüm Altyapısında İzinsiz Giriş Tespit Sistemi: Bir Çapraz Katman Özellik-Füzyon CNN-LSTM Tabanlı Yaklaşım. *Sensörler* **2021**, *21*, 626. [CrossRef] [PubMed]
56. Kang, M.J.; Kang, J.W. Araç İçi Ağ Güvenliği için Derin Sinir Ağı Kullanan İzinsiz Giriş Tespit Sistemi. *PLoS ONE* **2016**, *11*, e0155781. [CrossRef] [PubMed]
57. Loukas, G.; Vuong, T.; Heartfield, R.; Sakellari, G.; Yoon, Y.; Gan, D. Araçlar için Bulut Tabanlı Siber-Fiziksel Saldırı Tespiti Using Deep Learning. *IEEE Access* **2017**, *6*, 3491-3508. [CrossRef]
58. Seo, E.; Song, H.M.; Kim, H.K. GIDS: Araç İçi Ağ için GAN Tabanlı İzinsiz Giriş Tespit Sistemi. IEEE Erişim 2018 16. Yıllık Gizlilik, Güvenlik ve Güven Konferansı (PST) Bildirileri, Belfast, İrlanda, 28-30 Ağustos 2018; s. 1-6. [CrossRef]
59. Zhu, K.; Chen, Z.; Peng, Y.; Zhang, L. Araç İçi Ağıın Mobil Kenar Destekli Edebi Çok Boyutlu Anomali Tespiti LSTM Kullanarak. *IEEE Trans. Veh. Teknol.* **2019**, *68*, 4275-4284. [CrossRef]
60. Avatefipour, O.; Al-Sumaiti, A.S.; El-Sherbeeny, A.M.; Awwad, E.M.; Elmeligy, M.A.; Mohamed, M.A.; Malik, H. Makine Öğrenimi Kullanarak Elektrikli Araçların CAN Veri Yolunda Siber Saldırı Tespiti için Akıllı Güvenli Bir Çerçeve. *IEEE Access* **2019**, *7*, 127580-127592. [CrossRef]
61. Yang, Y.; Duan, Z.; Tehranipoor, M. ECU Parmak İzi Sinyalinin Derin Özelliklerine Dayalı Olarak Araç İçi CAN Veriyolunda Sahtekarlık Saldırısının Belirlenmesi. *Akıllı Şehirler* **2020**, *3*, 17-30. [CrossRef]