TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

BAĞLANTILI ARAÇLARDA NESNELERİN İNTERNETİ SİBER SALDIRILARININ ADLİ BİLİŞİM AÇISINDAN İNCELENMESİ

Özgür ÖNEY

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
YÜKSEK LİSANS TEZİ

DANIŞMAN
Prof. Dr. Refik SAMET

ANKARA
2023

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

BAĞLANTILI ARAÇLARDA NESNELERİN İNTERNETİ SİBER SALDIRILARININ ADLİ BİLİŞİM AÇISINDAN İNCELENMESİ

Özgür ÖNEY

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
YÜKSEK LİSANS TEZİ

DANIŞMAN
Prof. Dr. Refik SAMET

ANKARA
2023

ETİK BEYAN

Ankara Üniversitesi
Sağlık Bilimleri Enstitüsü Müdürlüğü'ne,

Yüksek Lisans tezi olarak hazırlayıp sunduğum "Bağlantılı Araçlarda Nesnelerin İnterneti Siber Saldırılarının Adli Bilişim Açısından İncelenmesi" başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin fikir/hipotezi tümüyle tez danışmanım ve bana aittir. Tezde yer alan deneysel çalışma/araştırma tarafımdan yapılmış olup, tüm cümleler, yorumlar bana aittir.

Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı: Özgür Öney
Tarih:
İmza:

KABUL VE ONAY

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü
Disiplinlerarası Adli Bilimler Anabilim Dalı
Adli Bilişim İkinci Öğretim Tezli Yüksek Lisans Programında

Özgür ÖNEY tarafından hazırlanan
"Bağlantılı Araçlarda Nesnelerin İnterneti Siber Saldırılarının Adli Bilişim Açısından İncelenmesi" adlı tez çalışması
aşağıdaki jüri tarafından **YÜKSEK LİSANS TEZİ** olarak
OY BİRLİĞİ ile kabul edilmiştir.

21.07.2023

Prof.Dr. Refik SAMET
Ankara Ü. Mühendislik Fakültesi
Jüri Başkanı

Doç.Dr. Hüseyin ÇAKIR
Gazi.Ü. Gazi Eğitim Fakültesi
Üye

Dr.Öğr.Üyesi Yılmaz AR
Ankara Ü. Mühendislik Fakültesi
Üye

Tez hakkında alınan jüri kararı, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulu tarafından onaylanmıştır.

Prof.Dr. Fügen AKTAN
Sağlık Bilimleri Enstitüsü Müdürü

İÇİNDEKİLER

ÖNSÖZ

Son yıllarda teknolojinin hızla gelişmesi, çeşitli endüstrileri dönüştüren çok sayıda yeniliğin yolunu açmıştır. En dikkate değer gelişmelerden biri, cihazlarla ve çevremizdeki dünyayla etkileşim şeklimizde devrim yaratan Nesnelerin İnterneti olgusunun ortaya çıkışıdır. Nesnelerin İnterneti, çok sayıda cihazı sorunsuz bir şekilde birbirine bağlayarak ve benzeri görülmemiş düzeyde rahatlık ve verimlilik sağlayarak günlük hayatımızın ayrılmaz bir parçası haline gelmiştir.

Araçlar giderek artan bir şekilde Nesnelerin İnterneti yetenekleriyle donatıldıkça, otomotiv endüstrisi de bu dijital devrimin bir istisnası olmaktan çıkmıştır. Bu birbirine bağlı sistemler, gelişmiş güvenlik özellikleri, geliştirilmiş araç performansı ve gelişmiş eğlence sistemleri gibi çok çeşitli avantajların kilidini açmıştır. Bununla birlikte, Nesnelerin İnterneti teknolojilerinin otomobillere hızlı bir şekilde entegre edilmesiyle, yeni ve endişe verici bir tehdit ortamı ortaya çıkmıştır: *siber saldırılar.*

Araçlar birbirleri, çevreleri ve diğer sistemler ile bağlantılı olma özelliğini edindikçe ve dolayısıyla Nesnelerin İnterneti teknolojilerine bağımlı hale geldikçe, bu sistemlerdeki güvenlik açıklarından yararlanan kötü niyetli faaliyetlere karşı da savunmasız olabilme ihtimalini de üzerlerinde bulundurmaktadırlar. Bu tür siber saldırıların potansiyel sonuçları, kişisel mahremiyet ve güvenliği tehlikeye atmaktan önemli finansal kayıplara neden olmaya kadar oldukça çeşitli bir spektrumda olabilmektedir. Bu nedenle, bu gelecek vaat eden alanın sürekli büyümesini ve gelişmesini sağlamak için otomotiv endüstrisindeki siber güvenlik engellerini anlamak ve ele almak çok önemlidir.

"Otomobil Endüstrisinde Nesnelerin İnterneti Siber Saldırıları ve Saldırıların Adli Bilişim Kapsamında İncelenmesi" başlıklı bu tez, özellikle bağlantılı araçları hedef tahtasının ortasına koyan Nesnelerin İnterneti konusu ile ilgili siber saldırılar literatürünü incelemeyi amaçlamaktadır. Bu araştırmanın birincil odak noktası,

bağlanabilirlik özelliğini haiz araçlara karşı gerçekleştirilebilecek çeşitli saldırı türlerini keşfetmek, bu saldırıların altında yatan mekanizmaları anlamak ve yine bu saldırıların endüstri, tüketiciler ve bilişim sektöründeki etkilerini değerlendirmektir. Akabinde, bu saldırıların önüne geçilebilmesi için bir çerçeve model önerisi sunulmuştur.

Ayrıca bu tez, siber saldırıların soruşturulmasında, incelenmesinde ve faillerin tespit edilmesinde kritik bir rol oynayan adli bilişim alanını da ele alacaktır. Adli bilişim uzmanları, bu saldırıların geride bıraktığı kanıtları analiz ederek saldırıları failleri ile ilişkilendirmeye, saldırı vektörlerini anlamaya ve gelecekteki riskleri azaltmak için sağlam karşı önlemler geliştirmeye yardımcı olan değerli içgörüleri ortaya çıkarabilir.

Mevcut literatürün, olay incelemelerinin ve ampirik analizin kapsamlı bir incelemesiyle bu tez, Nesnelerin İnterneti teknolojileri, siber saldırılar ve otomotiv endüstrisindeki adli soruşturmalar arasındaki karmaşık etkileşime ışık tutmayı amaçlamaktadır. Yürüttüğüm işbu araştırmanın; Nesnelerin İnterneti teknolojisini barındıran araçlarda siber güvenliğin sağlanmasında karşılaşılan zorlukların daha derinden anlaşılmasına katkıda bulunurken aynı zamanda bu tür saldırıları araştırmak ve önlemek için kullanılan teknikler ve yöntemlere ilişkin içgörü sağlamasını umuyorum.

Bu araştırma sürecinde rehberlikleri ve destekleri için danışmanım Sayın Profesör Doktor Refik Samet'e, konu hakkında fikirlerini sorduğum iş ve okul arkadaşlarıma ayrıca içten şükranlarımı sunmak isterim. Uzmanlıkları ve değerli katkıları bu tezin içeriğini ve yönünü şekillendirmede etkili olmuştur. Bir diğer teşekkürü de kısıtlı kaynaklar ile *Devrim Arabalarını* üreterek bu değerli coğrafyanın değerli işgücü kaynağının varlığını bir kez daha gösteren, geniş sektörde bu coğrafyanın da pay alabileceğini ispatlayan, daha sonraki tüm otomotiv hamlelerine başat, bana da ilham kaynağı olan kıymetli yönetici ve mühendis büyüklerime sunmak isterim.

Son olarak, bilgi ve yenilik arayışlarını yönlendiren ilgi ve merak sahibi kişiler olduklarından, bu tezin okuyucularına şükranlarımı sunmak istiyorum. Bu araştırmanın, Nesnelerin İnterneti siber güvenliği ve adli bilimler üzerine tartışılmakta olan söylemlere katkıda bulunarak nihayetinde otomotiv endüstrisi ve paydaşları için daha güvenli ve daha güvenli bir geleceği teşvik etmesi dileği ile…

Ankara, Türkiye
Temmuz, 2023

SİMGELER VE KISALTMALAR

2FA	İki faktörlü Doğrulama (*İng. Two Factor Authentication)*
ABD	Amerika Birleşik Devletleri
ABS	Kilitlenme Önleyen Fren Sistemi (*İng. Anti-lock Braking System)*
ADAS	Geliştirilmiş Sürüş Destek Sistemleri (*İng.* Advanced Driving Assistance Systems*)*
CIS	İnternet Güvenliği Merkezi (*İng.* Center for Internet Security)
CAN	Denetleyici Alan Ağı (*İng. Controller Area Network*)
DDOS	Dağınık Servis Reddi (*İng.* Distributed Denial of Service)
ECU	Elektronik Kontrol Ünitesi, Beyin (*İng.* Electronic Control Unit)
EV	Acil durum aracı (itfaiye, ambulans vb.) (*İng. Emergency Vehicle*)
GDPR	Genel Veri Koruma Yönetmeliği (*İng. General Data Protection Regulation)*
GPS	Küresel Konumlandırma Servisi (*İng.* Global Positioning System)
IDPS	İhlal Tespit ve Koruma Sistemi (*İng. Intrusion Detection and Prevention System)*
IT	Bilgi Teknolojileri (*İng. Information Technology)*
IoT	Nesnelerin İnterneti *(İng.* Internet of Things)
LIDAR	Lazer Görüntülü Tespit ve Mesafelendirme Sistemi (*İng.* Laser Imaging Detection and Ranging*)*
MFA	Çokfaktörlü Kimlik Doğrulama (*İng.* Multifactor Authentication)
NAT	Ağ Adresi Çevirisi (*İng.* Network Address Translation)
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü (*İng.* National Institute of Standards and Technology)
OBD	Araç Teşhis Uygulamaları (*İng.* On-board Diagnostic)
PCI-DSS	Ödeme Kart Endüstrisi Veri Güvenliği Standardı (*İng. Payment Card Industry Data Security Standard)*
RFID	Radyo Frekansı Kimliklendirmesi (*İng.* Radio Frequency Identification)
SDLC	Yazılım Geliştirme Hayat Döngüsü (*İng.* Software Development LifeCycle)

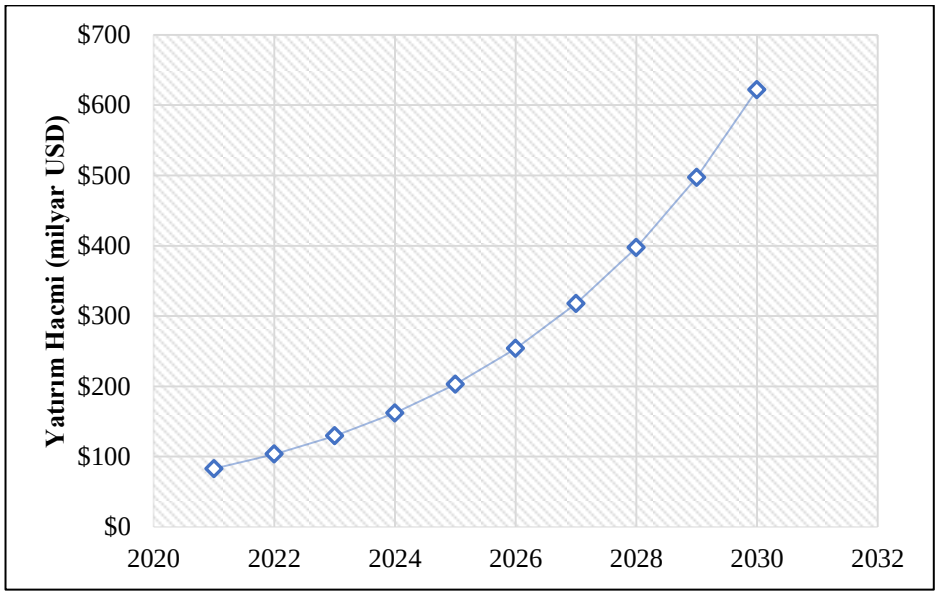
SSH	Güvenli Kabuk (*İng. Secure SHell)*
TLS	Taşıma Katmanı Güvenliği (*İng. Transport Layer Security)*
V2I	Araçtan Altyapıya İletişim (*İng.* Vehicle-to-Infrastructure)
V2V	Araçtan Araca İletişim (*İng.* Vehicle-to-Vehicle)

ŞEKİLLER

ÇİZELGELER

1. GİRİŞ

Otomotiv sektörünün temel yapıtaşı olan otomobiller, silikon çiplerin bu mecrada da kullanılmaya başlanmasından sonra bilhassa son yıllarda Nesnelerin İnterneti de dahil olmak üzere çeşitli teknolojilerin araçlara eklemlenmesi ile hızlı bir dijital dönüşüm geçirmiştir. Gartner'ın araştırmasına göre, 2022 yılındaki Amazon AWS, Google, Alibaba veya Tencent gibi dijital devlerin araç teknolojisindeki ayak izlerini sürekli olarak genişletmelerinden ve bu alanda yaptıkları yatırımları artırmalarından hareketle, 2028 yılına kadar yollardaki araçların onda yedisi bir bütüncül bilişim ekosisteminin parçası olacaktır (Gartner, 2022). Precedence Research isimli araştırma şirketinin yayınladığı rapora göre ise, 2014 yılından bu yana hızla büyümekte olan Nesnelerin İnterneti pazarı ile otomotiv sektörünün kesişimi düşünüldüğünde, 2021 yılında 82,7 milyar dolar büyüklüğünde olan Nesnelerin İnterneti pazarının, 2030 yılında neredeyse 621 milyar dolarlık pazar hacmine ulaşması (Şekil 1.1) ve kümülatif şekilde yıllık yüzde 25 civarında büyümesi öngörülmektedir (Precedence Research, 2022).



Şekil 1.1. 2021-2023 Yılları arasında otomotiv endüstrisinde Nesnelerin İnterneti pazar büyüklüğü.

Araçlardaki Nesnelerin İnterneti uygulamaları, geleneksel yöntemler çerçevesinden düşünüldüğünde her ne kadar kulağa ilk aşamada oldukça uzak gelse de pratik kullanımda sıklıkla yer edinmiştir, üstelik yüksek yakıt verimliliği, lastik basıncı gibi parametrelerde araca dair bilgi sağlaması neticesinde sürücünün araca hakimiyetini kolaylaştırması, trafiğin veya benzin istasyonlarının konumunu keskinlikle sunabilmesi neticesinde hızlı ve verimli rota oluşturma ve artırılmış güvenlik de dahil olmak üzere çok çeşitli avantajlar sunmaktadır (Manjunath ve ark., 2018). Ancak, araçların bağlanabilirliğindeki bu artış diğer tarafta aynı zamanda yeni güvenlik sorunları da ortaya çıkarmaktadır. Bağlanabilirlik, dışarıdan müdahale edilmesi için fiziksel temas gerektiren mekanik sistemlerin aksine, uzaktan müdahale edilebilirlik ihtimalini üretmektedir. Dolayısıyla bu durum, herhangi bir şekilde Nesnelerin İnterneti uygulamalarını kullanan araçlarda yalnızca araca veya sürücülere dair bilgilerin ele geçirilmesini değil, eş zamanlı olarak aracın hırsızlık sonucunda tamamen ele geçirilebilmesine imkân tanımaktadır (Becsi ve ark., 2015). Buna ek olarak, bağlanabilirlik imkânı ile istismar edilmeye yatkın alanların sayısı da artmaktadır, çünkü bir ağ üzerinden sunuculara, son kullanıcılara, üreticiye yahut diğer araçlara bağlanmak aracın işleyişine dışarıdan müdahale etme olasılığını sunan kapıların sayıların artışı anlamına gelmektedir. Buradan çıkarımla beklenen şekilde, suçlular araç sistemlerini tehlikeye atmak, araç kullanıcılarının kişisel nitelikte verilerini ele geçirmek veyahut araçların işleyişlerini sekteye uğratmak adına Nesnelerin İnterneti kategorisindeki cihazların güvenlik açıklarını her sene artan sayıda hedeflemektedir (Greenwood, 2015). Bu durumun, sürücü ve yolcuların güvenliği ile otomotiv endüstrisinin finansal istikrarı için kayda değer seviyede önemli ve göz ardı edilemeyecek bir tehdit oluşturduğu doğal olarak söylenebilir. Sonuçta otomotiv endüstrisindeki siber saldırıları önlemek, tespit etmek ve olası siber güvenlik olaylarını nitelikli şekilde inceleyerek yeni olayların oluşmasının önüne geçebilmek adına etkili ve verimli siber güvenlik önlemlerine ve adli soruşturma tekniklerine artan bir ihtiyaç mevcuttur.

Bu tezin amacı, bağlantılı araçlarda Nesnelerin İnterneti siber saldırılarını bütüncül seviyede incelemek, bağlantılı araçlarda siber saldırıları araştırmak ve azaltmak için kullanılabilecek adli bilişim çerçevelerini araştırmak ve ilgili bağlamda

verimli bir adli bilişim çerçevesinin kurulumuna katkı sağlamak olacaktır. Genel olarak tez, bağlantılı araçlarda Nesnelerin İnterneti siber saldırılarının yanı sıra bu tür saldırıları tespit etmek ve önlemek için kullanılabilecek adli soruşturma teknikleri ve araçları hakkında kapsamlı bir anlayış sağlamayı amaçlamaktadır. Bu duruma ek olarak tez, bağlantılı araçlarda etkili siber güvenlik önlemlerinin geliştirilmesine katkıda bulunacak ve sürücülerin ve yolcuların emniyetinin ve güvenliğinin sağlanmasına yardımcı olacaktır.

Tez, dijitalleşmeye doğru evrimi de dahil olmak üzere otomotiv endüstrisine ve geçmişine genel bir bakış sunarak başlayacaktır. Bakışın amacı, kronolojik bilgi sağlayarak bağlamın bütüncül olarak korunmasının sağlanması olacaktır. Otomobilin tarihine dair genel bilgiyi, otomobillerin dijitalleşmesine dair bilgilendirmeler ve Nesnelerin İnternetine dair bilgilendirmeler takip edecektir. Bu iki ayrık alana dair altyapı niteliğindeki bilgilerin sunumunu takiben, Nesnelerin İnterneti uygulamalarının otomotiv sektöründeki karşılıkları tartışılacaktır. Bu kapsamda, kullanılan Nesnelerin İnternetinin otomotiv endüstrisindeki rolü ve Nesnelerin İnterneti cihazlarının araçlardaki muhtelif uygulamalarından bazıları incelenecektir. Ardından da otomobillerde yürütülen Nesnelerin İnterneti operasyonlarının sahip olabileceği potansiyel güvenlik açıklarının analizi ve siber suçluların saldırı başlatmak için bu güvenlik açıklarından nasıl yararlanabileceğine dair yaklaşımlar, Nesnelerin İnternetinin araçlarda kullanılması neticesinde oluşturdukları saldırı yüzeyi ekseninde ele alınacaktır.

Tez çalışması, bahsi geçen saldırı yüzeylerinin kapsamının detaylı şekilde betimlenmesi ve saldırılardan bahsedilmesinin üzerine, bu saldırılardan öğrenilen derslerin aktarılması ile devam edecektir. Öğrenilen dersler kısmında, şu ana kadar hem kullanıcılar hem üreticiler hem de denetleyici ve düzenleyici otoriteler tarafından yapılan muhtelif hataların aktarılması ve bu hatalardan öğrenilen derslerin kapsamı, öğrenilen derslerin verimliliği üzerine görüşler ile değerlendirilecektir. Çalışmanın bu kısmını, bağlantılı araçlarda Nesnelerin İnterneti kullanımının güncel teknolojiler ile değerlendirileceği potansiyel problemler alt başlığı takip edecektir.

Çalışmanın olgunlaştığı alt başlıklardan ilki, Nesnelerin İnterneti kullanımlarının otomotiv sektöründe yaygınlaşmasının doğuracağı potansiyel problemlere dair sunulacak önlem yöntemleri olacaktır. Bu önerilecek yöntemlerde, çalışmanın olası problemler daha oluşmadan önüne geçmesi amacı güdülmektedir. Burada altı çizilmesi gerekir ki, önlem yöntemleri yalnızca tek bir paydaş tarafından değil, birden çok paydaşı niteleyecek biçimde olacaktır: kullanıcıların alması gereken önlemler, üreticilerin alması gereken önlemler ve diğer otoriteler tarafından alınması gereken önlemler.

Tez çalışmasında sunulacak ve potansiyel sorunlar yaşanmadan bu sorunların önüne geçmesi amacıyla üretilecek önerilecek önlemlerin alınabilmesi için zaruri olan ölçütlerden bahsedilmesi kısmı, bu aşamada çalışmanın devamını oluşturacaktır. Burada, on iki farklı alt başlık halinde, önlemlerin alınabilmesi için gerekli parametre ve kriterlerin tanımlaması yapılacaktır. Bu parametre ve kriterler, şu şekilde olacaktır: Anlaşılabilirlik, Bütçe, Yönetişim, Yönetim, Risk Değerlendirmesi ve Analizi, Güvenli Mimari ve Tasarım, Erişim Kontrol ve Kimlik Doğrulama Mekanizmaları, Güvenlik Testi ve Denetimi, Olay Müdahale ve Felaket Kurtarma Planı, Çalışanlar İçin Güvenlik Farkındalığı ve Eğitimi, Sürekli İzleme ve İyileştirme, Sektör İçinde İşbirliği ve Bilgi Paylaşımı.

Çalışmanın sonraki adımını bir önceki aşamada sunulan önlemlerin bütüncül olarak benimsenmemesi yahut tekil olarak eksik benimsenmesi senaryosunda karşılaşılabilecek olası tehlikelerden bahsedilmesi oluşturacaktır. Önem sırasına göre sunulacak olan bu tehlikelerin ilki, beşerî tehlikeler alt başlığında incelenecektir. Beşerî tehlikeleri, can güvenliği riskleri ve kişisel verilerin kaybedilmesi ekseninde değerlendirmek çalışmanın bu noktada eksenini oluşturacaktır. Burada aktarılan bilgileri, trafik kazaları ve güven alt başlıklarında incelenecek olan maddi tehlikeler başlığı takip edecektir.

Çalışmanın son kısmında, Nesnelerin İnterneti mecrasında yapılan siber saldırılar, bu durumun bağlantılı araçlara izdüşümleri, önerilen aksiyonlar ve önerilen aksiyonlara dair uygulamalar yürütülmemesi durumunda oluşabilecek tehlikelerin

göz önünde bulundurulması başlıklarının tek bir potada eritilmesi ile elde edilen Önerilen çerçeve ve modelden bahsedilecektir. Aktarıldığı şekilde model, Nesnelerin İnterneti uygulamalarını geliştiren üreticiler, kullanan son kullanıcı bireyler ve bu akışın denetleme ve düzenlemesinden sorumlu otoritelerden bahsedecektir.

Tez çalışması, süreç içerisinde kullanılan kaynaklar başta olmak üzere ilgili diğer verilerin ve bilgilerin sunulması ile sonlandırılacaktır.

1.1. Otomobil Sektörünün Geçmişi

Otomobil sektörünün başlangıcına atfedilen tarihin, Sanayi Devriminin itici gücü olan buhar makinesinin bir tekerlekli araç üzerinde güç kaynağı olarak kullanıldığı 1672 olduğu söylenebilir. Nitekim bu gelişmeyi, bireysel taşımacılıkta ilk kez buhar motorunun kullanılması ile gerçek manada bir otomobile çeviren kişi ise, 1769 yılında aldığı inisiyatif ile Fransız girişimci Nicolas-Joseph Cugnot olmuştur (Eckermann ve ark., 2011). Ancak, üzerinde bulundurduğu bir itki makinesinden güç alarak yolcularını, itki mekanizmasını ve itkiye kaynak oluşturan yakıtı üzerinde taşıyan otomobillerin, buhar makinelerinin oldukça ağır ve katı yakıtla çalışması neticesinde fazla hacim ihtiva etmesi ve seri üretime dair zorluklar, kullanımının yaygınlaşmasının önüne geçmiştir ve 19. Yüzyılın ortalarına değin otomobiller sınırlı sayıda el emeği ile üretilen ve geniş kitlelere erişme hedefinden oldukça uzakta konumlanan hobi araçları olagelmiştir. Bu sorunun kök nedeninin çözülmesine yardımcı olacak, benzini yakıt olarak kullanarak devinim sağlayan bir içten yanmalı motor yardımı ile yol alan ilk araba, “Benz Patent Motorwagen” adı ve üç tekerlekli bir araç olarak, 1886 yılında Karl Benz tarafından Almanya’da üretilmiştir. Bu ilk adımı, 1886'da Gottlieb Daimler ve Wilhelm Maybach tarafından, daha optimize bir sürüş vaat etmesi nedeniyle dört tekerlekli olarak tasarlanıp üretilen "Daimler Motorlu Araba"nın markete çıkışı izlemiştir. Bahsi geçen ilk ve sonraki on yıllık süreçte onları takip eden selef araçlar, öncelikle ulaşım için kullanılmaktaydı ancak zamanla zenginlik, özgürlük ve ilerlemenin önemli bir sembolü haline geldiler.

20. yüzyılın başlarında otomotiv endüstrisi seri üretim endüstrisi olarak şekillenmeye başlamıştır. 1908'de Amerikalı çağdaş iş yaşamındaki yenilikçi girişimci (Landes, 2008), yatırımcı ve mucit Henry Ford, araçların üretim süreçlerini "baştan sonuna kadar tek bir çizgiyi izleyen, her bir işçinin yalnızca üzerine düşen basit bir görev tanımı ile parça eklemesi ile oluşturulan ve parçaların hızlı bir şekilde montajlanmasına olanak sağlayan" şekilde değiştirmiş geliştirmiş, bu mühendislik optimizasyonu neticesinde de önceki araçlara nazaran ortalama gelire sahip bir bireyin satın alabileceği kadar uygun fiyatlı ve güvenilir bir araba olan Model T'yi tanıtmıştır. Ford'un otomobillerin verimli ve hızlı üretimine izin veren bu montaj hattı uygulaması, yalnızca o dönemde satılan otomobil sayısının, otomobillerin halkın ulaşabileceği seviyeye kadar düşmesi ile satış patlaması yaşamasına yardımcı olmamış; aynı zamanda otomotiv endüstrisinin global ölçekte diğer sektörler ile boy ölçüşebilecek rekabet altyapısının tamamlanmasına ve bu sebeple günümüze kadar ulaşan süreçte makineleşmiş toplumların belkemiğini oluşturan bir endüstriyel kol oluşumuna katkı sağlamıştır.

Devamlı akan üretim bandı yaklaşımının akademik yaklaşımlar ile sürekli geliştirilmesine ek, özellikle endüstri devriminden sonra gıdaya ulaşımın kolaylaşması ve tıbbı gelişmeler ile insanlık nüfusunun üstel şekilde artmaya başlaması neticesinde emeğin ucuzlaması, otomotiv sektörünü yüksek ivmeyle büyümeye sevk etmiştir. Sektörde yer alan üreticilerin potansiyel alıcı kitlesi niceliksel açıdan büyüdükçe otomobil üreticilerinin sayısı da artmıştır. Birinci Dünya Savaşı gibi küresel ölçekte pazarları etkileyen gelişmeler yaşansa, bu savaşın önemli aktörlerinin Avrupa kıtasında yer alması neticesinde, Uzak Asya ülkelerinde ve Amerika kıtasındaki ABD ve Kanada'da otomotiv endüstrisine dair gelişmelerin bu gelişmelerden olabildiğince soyutlandığını söylemek de yersiz olmayacaktır.

1918 senesinde Birinci Dünya Savaşının sonlanması ve büyük Avrupa ülkelerinde de artık diğer ülkeleri takip edebilecek otomotiv endüstrisi yaklaşımlarının benimsenmesi neticesinde bu dönem, otomotiv endüstrisinde altın niteliğinde gelişmelerin yaşandığı bir sürecin başlangıcı olmuştur. Bu dönemde gerçekleşen mekanik geliştirmeler ve icatlar, otomotivlerdeki verimliliğin

artırılmasına ön ayak olan temel yapı taşları olarak karşımıza çıkmaktadır. Bu durumlara ek olarak, araçların güç ünitelerinin konumlandırılmasına dair sektör çapında sessiz bir mutabakat sağlanmış, motor tiplerinin deneysellikten öteye gidemediği önceki on yılların aksine, genel geçer motor tiplerinin standardizasyonuna dair aksiyonlar yine bu dönemde alınmıştır. Örneğin, bir önceki on yılda satılan arabaların 10'da 9'unun açık tavanlı, bu on yılda satılan arabaların ise 10'da 9'unun kapalı tavanlı olduğu düşünüldüğünde (Georgano) bu dönemde inovasyon açısından sert bir değişim rüzgârı estiğinden bahsedilebilir. Bu geliştirme döneminin bir diğer artısı da özellikle Birinci Dünya Savaşı'nda rekabet etmiş ülkelerin, savaşta yer aldıkları taraftan bağımsız şekilde, diğer ülkelerin sahip olduğu teknolojik gelişmelerden geri kalmamak adına araştırma ve geliştirme çalışması yürüten kişi ve kurumları desteklemesi olmuştur. Rekabetçi anlayış, pazardaki gelişmelere gözle görülür seviyede kalite de katmıştır.

Üretim, araştırma ve geliştirme noktasında adeta patlama yaşanan bu dönemin sonunu, o yıllarda dünya finansının yeni dünyadaki başkenti olan New York borsasının 1929 yılındaki sert düşüşleri getirmiştir. Neredeyse on yıl kadar sürecek olan, yirminci yüz yılın en uzun, en derin ve en yaygın krizi olarak da bilinen ekonomik kriz (Duhigg, 2008), özellikle dünyada üretim araçlarının kısıtlanmasına sebep olduğu gibi, daha sonrasında tetikleyici bir faktör üstlenerek İkinci Dünya Savaşı'nın patlamasına sebebiyet verecektir. Her ne kadar bu süreç, özellikle otomotiv endüstrisinin gelişimi açısından durağan geçse de otomobillerin günümüzde kullandığımız birçok temel bileşeninin icat edilmesi ve yaygınlaşması da yine bu dönemde olmuştur.

İkinci Dünya Savaşı sırasında, otomotiv endüstrisinde yer alan her oyuncu; üreticiler, mavi yaka üretim hattı çalışanları ve pazarlamacılar, odağını savaş çabaları için araç üretmeye kaydırmıştır. Ayrıca bu dönemde, otomotiv satın almaya düşük bir talep yaşanması, ülkeler arası para birimi değişim kısıtlamaları kabul edilebilir satış performanslarının görünmesinin önüne geçmiştir (Wilkins ve ark., 2011). Savaşın iki ana tarafını oluşturan devletler tek tek ele alındığında, Alman hükümetinin savaş sürecinde otomotiv endüstrisine çoğunlukla askeri kara araçları

üretme talimatını verdiği anlaşılabilmektedir. Buna ek olarak, Almanya'da yer alan hükümetin savaş öncesinde halk nezdinde politik karşılık toplamak adına görece uygun fiyatlı otomobil üretme çabası da sektör adına kayda değer bir gelişme olarak değerlendirilebilir. Öte taraftan, savaşın karşı cephesindeki oyuncular, bilhassa ABD ve İngiltere, coğrafi konumlarının gereklilikleri dolayı otomotiv şirketlerini çoğunlukla hava aracı üretmeye teşvik ettiğinden, otomotiv endüstrisinde durağan bir süreç geçirmiştir.

Büyük savaştan sonra endüstri sivil araç üretmeye geri dönmüş ve araba sahipliğinin popülaritesi artmaya devam etmiştir. Savaşın, 1929 senesinde yaşanan büyük çaptaki ekonomik krizin etkilerini ülkelerin yoğun mecburi harcama örüntüsü neticesinde sonlandırması, farklı ülkelerdeki insanların tüketim alışkanlıklarının savaşın psikolojik etkileri nedeni ile daha yoğun bir şekilde harcama ve az birikim yapma yönüne değişmesi bu dönemde endüstride geçerli olan alışkanlıkların ve üretim adetlerinin de hızla değişmesine ön ayak olmuştur. Her ne kadar ABD, yılda 8 milyondan fazla araç üreterek bu konuda üretimi kendi üzerinde yoğunlaştırmış gibi gözükse de (Catalan Vidal), İtalya ve İngiltere gibi ülkelerde, irili ufaklı birçok firma, farklı seviyede kompakt boyutlarda otomobillerin üretimine öncülük ederek maliyetleri daha da aşağıya çekmiş, bu yolla kişilerin otomobillerin ulaşımda sağladığı ferahlığı erken yaşta fark etmesi sağlanarak hayatlarının büyük bölümünde otomobillerin kullanımı sebebi ile tüketici statüsünde daha uzun vakit geçirmeleri sağlanmıştır.

1960 ve 1970'lerin on yıllık süreçleri, otomotiv endüstrisinin hafızasında iz bırakan olayların gelişimine sebebiyet vermiştir. Maden ve metalürji alanındaki teknolojilerin gelişimi ile birlikte düşen petrol keşif ve çıkarma maliyetleri, piyasada uzun vadeli bir petrol ucuzluğuna neden olmuş, bu durum bilhassa Amerikan üreticilerinde yüksek yakıt tüketimine paralel yüksek güç çıktısı üreten araçların üretilmesine, sektörde birçok oyuncunun, geliştirdiği teknolojinin verimliliğinden bağımsız olarak tutunabilmesine ve başta ABD vatandaşları olmak üzere satın alma gücü yüksek bireylerin ulaşım alanındaki birincil tercihlerinin otomobile kaymasına yol açmıştır. 1973 senesinde üreticilerin petrol üretiminde kısıtlamaya gitmesi

neticesinde yaşanan petrol krizi ve ekonomik çalkantıların artması, dünyanın 16 büyük ekonomisinin 10 tanesinde durgunluk görülmesi (Maddison) üreticilerin büyük maliyet yükümlülükleri ile karşı karşıya kalmasına, düşük işçilik maliyetleri ile üretim yapan Japonya ve Çin gibi ülkelerin üretim pastasında kendi ülkeleri ve dünya çapında ağırlığının artmasına neden olmuştur. Buna paralel, başta ABD menşeili üreticilerin bir kısmı olmak üzere otomobil üreticileri yeniden yapılanmaya, küçülmeye veya kapanmaya zorlanmıştır. Netice olarak, otomotiv sektörü özelinde, 1970'lerin bunalımı, Japonya'nın dünya çapında en çok otomobil üreticisi olarak o zamana kadarki tartışmasız lider ABD'yi geçmesiyle sonuçlanmış, Japonya'nın üretimi 1985'te 12 milyon birimi aşarken (Tablo 1.1), ABD üretimi bu sayının hemen altında kalmıştır (Amsden, 1989).

Çizelge 1.1. Ülke bazında en büyük otomobil üreticilerinin 3 örneklemde değişimi.

		1973			**1985**			**2015**
1	ABD	12638	**1**	Japonya	12135	**1**	Çin	24503
2	Japonya	7081	**2**	ABD	11538	**2**	ABD	12100
3	B. Almanya	3949	**3**	B. Almanya	4554	**3**	Japonya	9278
4	Fransa	3242	**4**	Fransa	3083	**4**	Almanya	6033
5	BK	2164	**5**	Sovyetler B.	2249	**5**	G. Kore	4556
6	İtalya	1960	**6**	Kanada	1931	**6**	Hindistan	4126
7	Sovyetler B.	1604	**7**	İtalya	1571	**7**	Meksika	3565
8	Kanada	1575	**8**	İspanya	1386	**8**	İspanya	2733
9	Belçika	1016	**9**	BK	1349	**9**	Brezilya	2429
10	İspanya	823	**10**	Belçika	1035	**10**	Kanada	2283
11	Brezilya	733	**11**	Brezilya	966	**11**	Fransa	1970
12	Avustralya	410	**12**	İsveç	463	**12**	Tayland	1915
13	İsveç	383	**13**	Avustralya	438	**13**	BK	1682
14	G. Afrika	295	**14**	Meksika	425	**14**	Rusya	1394
15	Meksika	283	**15**	Polonya	388	**15**	Çek Cumh.	1304

1970’li yıllarda yaşanan ekonomik buhranların neticesinde, otomobil üreticilerinin ve üretiminin odak noktası, müşteri talepleri neticesinde, performanstan ziyade, düşük yakıt tüketimi, bakım ve sürdürülebilirlik maliyetleri görece düşüklüğü ve kullanım süresinin daha yüksek olması olmuştur. Bahsi geçen bu gereksinimleri sağlayan otomobilleri, o yıllarda en iyi şekilde üreten ülkeler Asya ülkeleri

olduğundan, 1980'li yıllardan itibaren, otomotiv endüstrisinde üretim sayılarındaki ağırlık günümüze doğru geldikçe Batı Avrupa ve ABD'den Doğu Asya ülkelerine doğru kaymaya başlamıştır. Çizelge 1.1'de de görülebilecek bu değişim ile önce Japonya, ardından sırasıyla Çin, Güney Kore ve Tayland büyük üretim adetlerine ulaşmaya başlamıştır. Bu durum, önceden benimsenen trendlerin ve önceliklendirilen girdilerin de değişmesine neden olmuştur. Ancak, üretim için gerekli olan fikri ve sınai mülkiyet haklarının halen büyük oranda Batı ülkelerinde olmasından hareketle, üretimde karar mekanizmasının yine bu ülkelerde olduğunu ve üretimin odağı noktasındaki Doğu Asya ülkelerinin bu yıllarda üretim tecrübesi kazanarak ve tersine mühendislik uygulamaları ile yetkinlik biriktirdiğini söylemek yerinde olacaktır.

1990'lı yılların sonu ve 2000'li yılların başları, otomotiv endüstrisinde dijitalleşmenin yaygın hale geldiği ilk yıllar olarak değerlendirilebilir. Daha önceleri, 80'li yılların başında, barındırdığı muhtelif amaçlı sensörlerden aldığı verileri bütünleştirip işleyerek sürüş güvenliğine, yakıt ekonomisine veya konfora yardımcı olmaya çalışan üreticilerin varlığı bulunsa da bu üreticiler kahir ekseriyetle pahalı ürünler sattığından ve ekonomik piramidin tepesinde yer alan müşteri kitlesi fiyatlara dair yukarı yönlü esneklik gösterebildiğinden dolayı bu otomotiv çözümleri karşılık bulabilmiştir. İlerleyen yıllar ile silikon tabanlı ürünlerin (sensörler, güç kontrol üniteleri vb.), çiplerin üretim maliyetlerindeki düşüşle birlikte üreticiler tarafından teşhis, tespit ve onarım aşamasında sağladığı kolaylıklardan dolayı benimsenmesi neticesinde, bu uygulamalar standart uygulamalar halini almış ve neredeyse günümüzde bulunan her otomobilin vazgeçilmez bir parçası haline gelmiştir.

2010'lu yıllardan itibaren endüstri, artık içten yanmalı güç ünitelerine sahip otomobiller yerine, sadece elektrik motorlarından devinim sağlayan ve şarj edilebilen bir bataryadan güç alan araçlara şahitlik etmeye başlamıştır. Bu durum, doğal olarak yüz seneyi geçkin zamandan beri içten yanmalı motorlar üzerine geometrik mimariler, altyapı çalışmaları ve üretim süreçleri yürüten büyük şirketlerin birçoğunun bocalamasına sebebiyet vermiştir ve günümüzde de halen vermektedir. Öte taraftan, Çin gibi yoğun bilişim üretim altyapısına ve elektrikli araçların bataryalarında kullanılan nadir toprak elementlerinin maden cevher yataklarına sahip

bir ülkenin pazarda sağladığı hakimiyet, ilerleyen süreçte şu ana kadar ekonomik dengeyi korumakta başarılı gözüken Batılı üreticilerin zorlanabileceğine işaret etmektedir. Bu hususta, Batılı ülkelerin üretimi yazılım üzerinden şekillendirme ve pazar paylarındaki dengeyi koruma çabaları göze çarpmaktadır.

Netice olarak, geçen yüz yılı aşkın süre içerisinde, üretim yaklaşımları, üretici ülkelerin Pazar payları, karlılıklar ve maliyetler, üretilen ürünün muhteviyatı ve kalitesi sürekli olarak değişkenlik gösterse de otomotiv endüstrisinin sıklıkla kendi içinde evrimler geçirdiğini görmek makul bir çıkarım olacaktır. Buradan hareketle, özellikle yazılım alanındaki son dönemde yaşadığı ve günümüze yansıyan gelişmelerin neden olabileceği potansiyel değişimlerin bu endüstriyi de bahsi geçen girdi ve çıktılar kapsamında değiştirebileceğini söylemek yerinde olacaktır. Bu durumu daha iyi inceleyebilmek adına, otomobillerdeki dijitalleşmenin de benzer şekilde değerlendirilmesi gerekmektedir, takip eden bölümde buna dair inceleme devam ettirilecektir.

1.2. Otomobil Sektörünün Dijitalleşmesi

Dijital teknolojilerin çok yüksek bir ivme ile gelişmesi, değişmesi ve güncellemesi nedeniyle otomotiv sektörü son yıllarda köklü bir değişim geçirmiştir. Buna ek olarak, otomotiv sektöründe dijitalleşmenin ortaya çıkışı, otomobillerin marketteki potansiyel alıcılar tarafından nasıl tasarlandığı, üretildiği, çalıştırıldığı ve deneyimlendiği konusunda çarpıcı değişikliklere yol açmıştır. Dolayısıyla değişimin alıcıları, alıcıların işe değişimi karşılıklı olarak geri besleme yoluyla zenginleştirdiği iddia edilebilir. Dijitalleşme, tam otonom sürücüsüz arabalardan bağlantılı araçlara, akan trafik düzenlemelerinden akıllı hareketlilik çözümlerine kadar otomotiv endüstrisinde yenilikçi, verimli ve çevre dostu uygulamaların geliştirilmesinde kilit bir faktör olmuştur. Bu başlık altında, otomotiv sektöründeki dijitalleşmenin geçmişi, bugünü ve geleceğine ek olarak gelecekte gelişmesi beklenen farklı alanlarda uygulamalarının varlığından bahsedilecek ve detaylandırmalar sağlanacaktır.

1.2.1. Otomobillerde Dijitalleşmenin Geçmişi

Otomasyona yönelik erken başlangıçlardan bugün gördüğümüz en son teknolojilere kadar, otomotiv sektöründeki dijitalleşmenin geçmişi birkaç on yılı kapsamaktadır. Otomobil endüstrisi, üretim, otomobil özellikleri, bağlantı ve tüketici deneyimlerindeki değişiklikler de dahil olmak üzere dijitalleşmenin bir sonucu olarak önemli bir değişim geçirmiştir. 1970'lerde ve 1980'lerde bilgisayarlı teknolojiler ilk kez otomobillerde yer almaya başladığında, otomotiv endüstrisi dijitalleşmeye başladığı söylenebilir. Araçlarda sayısal olarak ölçülmesi beklenen, fren sistemleri, yakıt enjeksiyonu ve motor performansı dahil olmak üzere çeşitli süreçleri izlemek ve yönetmek için girdilere ait özelliklerin çoğu bir elektronik sistem veya alt sistem olarak entegre edilmiştir. Bu elektronik sistemleri koordine etmek için araç üreticileri Elektronik Kontrol Üniteleri (*İng. Electronic Control Unit,* ECU) tanıtmıştır. Bir ECU temel olarak, hesaplamalar ve aktif firmware değişikliklerinden oluşan gerekli görevi için sensörlerden girdiler alır ve verileri hesaplar. (Alam ve ark., 2019) Bu yaklaşım, araç elektroniğinin daha da kapsamlı hale gelmesine ve dijital teknolojide daha fazla gelişme için zemin hazırlamıştır.

Giderek daha ileri teknolojilerin dahil edilmesi, 1990'larda dijitalleşmeye ivme kazandırmıştır. Araçların elektronik kontrol ünitelerine dışarıdan bir cihazla bağlanarak, araca ait verilerin tutulduğu hafızaya erişmek ve anomalileri tespit etmek amacı güden Araçta Teşhis (*İng. On-board Diagnostic,* OBD) sistemlerinin geliştirilmesiyle araç teşhisi ve sorun giderme mümkün hale getirilmiştir. Hava yastıkları ve ABS (kilitlenmeyi önleyici fren sistemleri), mikrodenetleyicilerin ve sensörlerin geliştirilmesiyle mümkün kılınan ve 90'larda hemen her markanın benimseyerek alışılageldik hale getirdiği iki diğer gelişmiş güvenlik önlemidir. Yine aynı yıllarda, otomotiv endüstrisi tarafından araçların içinde kullanımı benimsenen 8 bitlik dijital ekranlar ve bilgi-eğlence sistemleri, müşteriler için sürüş deneyimini iyileştirmiştir.

Dijitalleşme, 2000'lerin başında, çoğunlukla gömülü sistemlerin ve ağların geliştirilmesi sayesinde muazzam ilerlemeler kaydetmiştir. CAN (Denetleyici Alan

Ağı) gibi araç içi iletişim protokollerinin geliştirilmesi, çeşitli araç bileşenlerinin kesintisiz veri alışverişi yapmasını mümkün kılmıştır. Bu veri akışı yöntemi, konuşma tanıma teknolojisi, Bluetooth ağı ve GPS kullanan navigasyon gibi sıradaki teknolojilerin araçlara dahil edilmesini kolaylaştırmıştır. GPS teknolojisinin kullanımı ve hemen ardından gelen otomobil üreticilerinin sunduğu telematik hizmetleri sayesinde araçlar acil yardım, uzaktan teşhis ve araç izleme gibi hizmetler için dış ağlarla dahi iletişim kurabilir standarda erişmiştir.

Geriye dönüp bakıldığında, otomobillerdeki dijitalleşmenin araçları sürücüler adına başka bir boyuta taşıdığından bahsedilebilir. Bütün bu gelişmelerin, neredeyse sadece otuz senede gerçekleşmesi, üreticilerin, entegre devre başına bileşenlerin yoğunluğunu düzenli aralıklarla ikiye katladıklarını ve bunu göz alabildiğince yapmaya devam edeceklerini söyleyen Moore yasası (Schaller, 1997) kapsamında değerlendirilse de özellikle sektöre yapılan yatırımların bu beklentiyi bile aştığını gözlemlemek mümkündür.

1.2.2. Otomobillerde Dijitalleşmenin Bugünü

Araçların içindeki neredeyse her sürecin dijitalleştiği, Otomotiv endüstrisi son zamanlarda bağlantılı ve akıllı araçlar çağını benimsemiştir. Bulut bilişim, yapay zekâ ve yüksek hızlı internet bağlantısının ortaya çıkışı, dijital dönüşüm için yeni fırsatlar yarattı. Güvenliği artırmak için sensör teknolojilerinden, kameralardan ve algoritmalardan yararlanan ve uyarlanabilir hız sabitleyici ve şerit tutma yardımı gibi yarı otonom sürüş özelliklerini etkinleştiren gelişmiş sürücü destek sistemleri (*İng. Advanced Driving Assistance Systems,* ADAS), çağdaş araçlarda standart donanımdır.

Günümüzde, müşteri deneyimi dijitalleşme yardımı ile büyük oranda dönüşüme uğramıştır. Akıllı telefon entegrasyonu, sesle etkinleştirilen kontroller ve özelleştirilmiş bilgi-eğlence sistemleri gibi teknolojilerin dahil edilmesiyle otomobil üreticileri, araçlardaki kullanıcı arayüzünü ve bağlanabilirliği geliştirmeye

odaklanmaktadır. Dijital çözümler ayrıca elektrikli arabaların büyümesine ve bunların şarj edilmesi için altyapıya katkıda bulunarak etkili enerji yönetimi ve uzaktan şarj etme yetenekleri sağlamıştır.

1.2.3. Gelecek Öngörüleri ve Muhtemel Senaryolar

İleriye baktığımızda da görebileceğimiz gibi, otomobil sektöründe gelecekteki dijitalleşme daha da fazla potansiyele sahiptir. Özellikle, son dönemde ismini sıklıkla duyduğumuz 5G iletişim teknolojisinin yıldırım hızında bağlantısı ve düşük gecikme süresi, akıllı otomasyondaki ilerlemeler için gerek şarttır: Nesnelerin İnterneti, Yapay Zekâ, sürücüsüz arabalar, dijital gerçeklik, blok zincir ve henüz aklımıza bile gelmemiş olan gelecek buluşları (Attaran, 2021). Araçtan araca (V2V) ve araçtan altyapıya (V2I) iletişim, 5G bağlantısının yaygın hale gelmesi gelişecek ve daha iyi güvenlik ve trafik yönetimi için gerçek zamanlı veri alışverişini mümkün kılacaktır. Yapay zekâ ve makine öğrenimi algoritmalarındaki gelişmeler sayesinde sürücüsüz arabalar gerçek olacaktır. Dijitalleşme, yalnızca araçların kendisi ile sınırlı kalmayacak, otomobil sektörünün ürünlerini üretme şeklini de değiştirmeye devam edecektir. Daha etkili üretim hatları ve tedarik zinciri yönetimi, robotik, otomasyon ve veri analitiğinin entegrasyonundan kaynaklanacaktır. Gerçek zamanlı izleme, önleyici bakım ve optimize edilmiş üretim, ekipman ve sistemlerin birbirleriyle kesintisiz iletişim kurduğu "akıllı fabrikalar" fikriyle mümkün hale gelecektir.

1.2.3.1. Bağlantılı Araçlar: Akıllı ve Bağlantılı Araçlar Çağı

Bağlantılı araçlar terimi, bir aracı çevresine bağlayan uygulamaları, hizmetleri ve teknolojileri ifade eder. Bağlantılı araç, temel olarak, aynı araç içinde bulunan diğer cihazlara ve/veya araç dışındaki cihazlara, ağlara, uygulamalara ve hizmetlere bağlanan cihazların bir araçta bulunmasıdır. Bahsi geçen bu uygulamalar, trafik güvenliği ve verimliliği, bilgi-eğlence, park yardımı, yol yardımı, uzaktan

teşhis ve telematikten otonom kendi kendine giden araçlara ve küresel konumlandırma sistemlerine (GPS) kadar her şeyi içermektedir (Uhlemann, 2015).

Bağlantılı otomobillerin, özellikle internet bağlantı teknolojilerinin geliştirilmesi, gerekli donanım ve yazılım altyapılarının rekabetçi fiyatlar neticesinde markette yerine alması ve güvenlik başta olmak üzere birçok alanda duyulan ihtiyaçlar neticesinde kullanıma sunulmasıyla birlikte otomotiv sektörü büyük bir değişim geçirmektedir. Bu araçlar tanımda aktarıldığı şekilde, bulundurdukları yüksek teknoloji sensörler, internet bağlantısı ve bütünleşik yazılım sistemleri sayesinde birbirleriyle, altyapıyla ve yayalarla iletişim kurabilmektedir. Artan sürüş güvenliği ve sürüş verimliliğinden, kişiye özel olarak planlanmış seyahatlere kadar her alanda görülen yansımalarla bağlantılı otomobillerin ortaya çıkışı, otomotiv endüstrisi ile dijital dünyanın buluşmasına işaret etmektedir (Paritala, Manchikatla ve Yarlagadda, 2017). Akıllı ve bağlantılı otomobillerin modern çağını tanımlayan göze çarpan özelliklere ve örneklere bakmak gerekirse, günümüzün bağlantılı araçlarında çeşitli kullanışlı olanaklara ve yardımcı hizmetlere erişilebilir. Önceleri yalnızca büyük Amerikan şehirlerinde yol bulmanın kolaylaştırılması amacıyla geliştirilen ancak ilerleyen süreçte cep telefonu ve dijital asistanların kullanımı ile daha geniş amaçlara da hitap ederek geliştirilen harita uygulamaları barındıran gelişmiş bütünleşik navigasyon sistemleri, araçlarda bulunan internet bağlantısı sayesinde sürücüleri trafik koşullarından haberdar edebilmekte, rotalarını optimize edebilir ve yol boyunca ilginç durakları vurgulayabilmektedir. Örneğin, bağlantılı bir araba, gerçek zamanlı trafik verilerine dayalı olarak zaman kazandıran, güç ünitesinin daha az sürede yahut daha verimli kullanıldığı (ve bu yolla enerji tasarrufu sağlayan) ve trafik sıkışıklığından kaçınan rota önerileri sunabilir.

Ayrıca, akıllı telefonlar ve giyilebilir cihazlar gibi akıllı araçlar, bağlantılı araçlara kolayca entegre edilebilmektedir. Müzik akışı hizmetleri, eller serbest telefon görüşmeleri ve akıllı ev ekipmanlarının uzaktan yönetimi, sesli komutlar ve dokunmatik ekranlar aracılığıyla sürücülere sunulan kolaylıklardan sadece birkaçıdır (Piccinini ve ark., 2015). Ortaya çıkan ağ bağlantılı ekosistem hem verimlilik hem de konfor açısından hareketliliği geliştirmektedir. Araçtan araca (V2V) ve araçtan

altyapıya (V2I) iletişim, bağlantılı arabaların birbirleriyle ve altyapıyla konuşmalarını sağlayan bir diğer önemli özelliğidir. Örneğin güvenlik söz konusu olduğunda, ağa bağlı bir araba, olası kazaları önlemeye veya hafifletmeye yardımcı olmak için bölgedeki diğer arabalarla veri paylaşabilir (Piccinini ve ark., 2015). Araçtan altyapıya (V2I) iletişim, araçların trafik işaretleri ve işaretleri gibi yol kenarındaki altyapıyla iletişim kurmasını sağlayarak trafiği düzene sokar ve çarpışma olasılığını azaltır. Bağlantılı araçlar tarafından üretilen büyük hacimdeki verilerin, araç üzerindeki donanımla mümkün olmayan ancak başka veri depolama merkezlerinde sağlanacak tasnif ve analizleri, faydalı iç görüler ve yeni hizmetler sağlayabilmektedir. Örneğin, araçlarda uzaktan teşhis izleme, önleyici bakım ve hızlandırılmış onarımların yolunu açar. Bu durumun hem sürücüler hem de üreticiler için artan araç güvenilirliği, araçların önceden tespit edilecek potansiyel sorunların tespiti ile arızalı oldukları ve kullanılamadıkları sürelerin düşürülmesi ve bilhassa araçların ticari saiklerle kullanılması senaryolarında gözle görülür seviyede düşük işletme maliyetleri yaratılması gibi birçok avantajı vardır (Radanliev ve ark., 2019).

1.2.3.2. Otonom Sürüş: Dışarıdan Müdahalesiz Sürüş Teknolojisi

Tamamen otonom, yani yolda herhangi bir insan müdahalesi olmadan ilerleyebilen araçların hipotetik olarak ortaya çıkışı, otomotiv endüstrisi ve ulaşım hakkında insanlığın düşünme şekli için bir oyun değiştirici olmuştur. İnsan müdahalesi olmadan hareket edebilen ve çalışabilen araçlara sahip olmanın, daha iyi trafik akışı, daha güvenli yollar ve daha rahat ulaşım dahil ancak bunlarla sınırlı olmamak üzere birçok avantajı vardır.

Otonom sürüşün merkezinde; Yapay zekâ (AI), başta LIDAR olmak üzere çeşitli sensörler ve görüntü işleme gibi karmaşık algoritmalar yer almaktadır. Bu teknolojilerin kullanımı, araçların çevrelerini anlamlandırıp anlamalarına, değişen koşullara gerçek zamanlı olarak yanıt vermelerine, gerektiğinde kendi kendilerine park edebilmelerine, sıkışık yollarda başarılı bir şekilde ilerlemelerine ve hatta aracın etrafındaki trafik kazalarından kaçınmalarına olanak tanımaktadır. Kameralar,

LIDAR ve radar, engelleri, yayaları ve yol koşullarını belirlemek için kullanılabilen sensör örnekleridir; yapay zekâ sistemleri daha sonra aracın ne yapması gerektiğini belirlemek için bu verileri analiz eder.

Geliştirilmiş yol güvenliği, otonom araçların önemli bir diğer avantajıdır. Kendi kendine giden araçların, insan sürücülerden daha güvenilir ve daha hızlı tepki vermesi amaçlanarak kaza olasılığını azaltılmaya çalışılmaktadır. Kendi kendine giden arabalar çevrelerini ölçülü bir şekilde tarayabilir, potansiyel tehlikeleri önceden görebilir ve çarpışmaları önlemek yahut çarpışma sonrası hasarları asgariye indirmek adına önleyici tedbirler alabilir (Rossini ve ark., 2015). Bu yenilik, trafikle ilgili ölümleri ve yaralanmaları büyük ölçüde azaltabilir. Ayrıca otonom sürüş, trafik sıkışıklığını azaltma ve dolaşımı artırma potansiyeline sahiptir. Otonom araçlar ile yol kenarı altyapısı arasındaki bağlantı, daha iyi rota planlamasına ve trafik akışlarının koordinasyonuna olanak tanır. Daha iyi koordinasyon sayesinde daha iyi trafik akışı, daha az gecikme ve daha yüksek üretkenlik mümkündür. Örneğin kendi kendine giden arabalar, akan trafiği barındıran şeritlerin birleşmesini kolaylaştırmak ve sıkışıklığa neden olan dur-kalk trafiğinin etkisini azaltmak için hızlarını ve mesafelerini koordine edebilir (Shah ve Sengupta, 2020).

Otonom sürüş teknolojileri, ayrıca araçlara erişilebilirliği büyük ölçüde iyileştirebilir. Yaşı, engeli veya başka sebeplerden dolayı motorlu taşıt kullanamayanlar, otonom sürüşün gelişimi ve yaygınlaşması ile başka bir ulaşım seçeneğine sahip olmaya adaydır; nitekim otonom araçların temel amaçlarından biri de yakıt tüketimini, kazaları ve tıkanıklığı azaltmayı amaçlanın yanında engelli ve yaşlı insanlar için hareketliliği iyileştirmektir (Yaqoob ve ark., 2020). Toplu taşımaya veya diğer insanların yardımına güvenerek sınırlananlar, otonom araçlarda daha fazla özgürlük ve bağımsızlık bulabileceğinden dolayı araçları tercih sebebi haline getirebilecektir.

1.2.3.3. Veriye Dayalı Yenilikçilik: Otomobillerde Büyük Veri Kullanımı

Dijitalleşmenin ortaya çıkışı sayesinde veri kavramı, otomotiv endüstrisi de dahil olmak üzere birçok sektörde önemli bir yenilik kaynağı haline gelmiştir. Otomotiv endüstrisi, yeniliği desteklemek ve otomobil yaratma, çalıştırma ve bakımını yapma sürecinde köklü değişiklikler gerçekleştirmek için büyük veri olgusunu da kullanmaktadır. Verilerle beslenen yenilikçilik yeni çözümler sunmakta, karar süreçlerinin verimliliğini artırmakta ve yeni pazarlar açmaktadır.

Bir arabanın ömrü boyunca kullanıcılar ve araç tarafından çok büyük miktarda veri üretilmektedir. Araç performansı, sürüş alışkanlıkları, üretim yöntemleri, tedarik zinciri faaliyetleri ve müşteri ilişkileri bu bilgilerin kapsadığı birçok alandan sadece birkaçıdır. Otomobil üreticileri, bu verileri verimli bir şekilde toplayarak, analiz ederek ve kullanarak birçok önemli alanda yeniliği ilerletebilir.

Araç tasarımı ve geliştirme, otomobil sektöründe büyük verilerin kullanıma sunulduğu bir alandır. Veriler, otomobil üreticilerinin trendleri ve müşteri tercihlerini tespit etmelerine yardımcı olarak, müşterilerin sürekli değişen istek ve ihtiyaçları ile daha uyumlu araçlar üretmelerine olanak tanımaktadır. Örneğin, araç sürüş destek yardımları gibi defaatle üzerinde çalışılması gereken konular, sürücülerin verilerinin toplanması, derlenmesi ve analiz edilmesi yöntemiyle optimal hale getirilebilmektedir. (Stellios ve ark., 2018). Araçlar, benzer şekilde ECU üzerinde bulunan ölçüm araçları ile sürekli olarak veri toplayıp analiz ederse, yakıt verimliliğini artırabilir, ne zaman bakıma ihtiyaç duyacaklarını tahmin edebilir ve güvenilirliklerini artırabilir. Örneğin, gerçek zamanlı motor verilerini kullanan araçlar, motor ayarlarını sürüş koşullarına göre ayarlayarak hem yakıt ekonomisini hem de çevre dostluğunu geliştirebilir (Bin Aris ve ark., 2015). Ek olarak, günümüzde yüksek giriş bedeli talep eden, işletme maliyetleri açısından verimsiz ve düşük karlılıkla çalışan otomobil temsilcilik ve bayi sistemi, otomobil üreticilerinin ve işletmecilerin gelişimini ciddi şekilde etkilemiş ve işletmeler ile kullanıcılar arasındaki ilişkiyi kısıtlayarak düşük marka bilinirliğine neden olmuştur. Bu durum karşısında mevcut otomobil pazarlama sitelerinin ilgili araştırmalarına başvurularak

büyük veri uygulamasına dayalı otomobil pazarlama sisteminin tasarlanması ve uygulanmasının zorunlu olduğu düşünülerek, veriye dayalı içgörüler üreten bir pazarlama sistemine dair deneysel çalışmalar da yürütülmektedir (Lv, 2020). Bu yolların yaygınlaşması ve gündelik alanda uygulamaların karşılık bulması ile otomobil şirketleri, demografik özelliklerini, satın alma alışkanlıklarını ve çevrimiçi etkinliklerini analiz ederek belirli alıcı gruplarını hedefleyebilecek, sonuç olarak, pazarlama çabaları daha fazla meyve verecek, tüketici katılımı ve marka sadakati artacaktır.

1.2.3.4. Gelişmiş Kullanıcı Deneyimi: Kişiselleştirme ve Kullanım kolaylığı

Günümüzün bilgi çağında, otomobil sektörü yalnızca araçların mekanik işleyişini veya sürüş kalitelerine dair girdileri iyileştirmekle değil, bir bütün olarak sürüş deneyimini de iyileştirmekle ilgilenmektedir. Dijital teknoloji, önceleri otomobillerde kişiselleştirmelere ve basitleştirilmiş yol tarifi gibi olanaklara izin vererek araç içi deneyimi şekillendirmeye başlamıştır. Otomobil üreticisi şirketler, deneyim şekillendirmelerinden aldıkları olumlu geri bildirimler nezdinde bilgi-eğlence sistemlerine, uyarlanabilirlik altyapılarına ve araç kişiselleştirmesine önem atfetmektedir.

Sürücülerin kendi belirledikleri seyahat parametrelerini kendilerinin seçebileceği bir dokunuş eklemek, kullanıcı deneyimini iyileştirmek adına oldukça sağlıklı bir yoludur. Otomobil üreticileri, müşterilerin direksiyon başındaki deneyimlerini kişiselleştirmelerine olanak tanıyan seçenekleri, git gide daha fazla modele dahil etmekte ve daha fazla çeşitlendirmektedir. Örneğin, sürücünün vücut ölçülerine göre koltuğun konumunun belirlenmesi, araç içi kabin sıcaklığının kontrol edilmesinde ve ses ayarlarında yapılan otomatik ayarlamalar sürücüler nezdinde daha rahat ve keyifli bir yolculuk sağlamaktadır. Müzik, navigasyon rotaları ve kişi listeleri gibi kullanıcıya özel bilgileri öğrenebilen ve kaydedebilen bilgi-eğlence

sistemleri ile hem kullanıcı keyfi hem de kullanım kolaylığı artırılmaktadır (Tran ve ark., 2022).

Kullanıcı deneyimlerini geliştirmek, büyük ölçüde bağlantılı hizmetlerle ilişkilendirilebilmektedir. Hem sürücüler hem de yolcular, araçlarının dijital ekosisteme bağlı olmasının rahatlığından bu eksende faydalanabilmektedir. Akıllı telefon entegrasyonunun mümkün kıldığı eller serbest telefon görüşmeleri, mesajlaşma ve müzik akışı, sürücülerin dikkatlerini yoldan ayırmadan sosyal hayatlarını sürdürmelerine yardımcı olmaktadır (Vachálek ve ark., 2017). Ses kontrolü ve doğal dil işleme, hava durumu güncellemeleri, trafik koşulları ve yakındaki ilgi çekici yerler gibi gerçek zamanlı veriler sağlayarak otomotiv endüstrisindeki kullanıcı deneyiminde de devrim yaratmıştır. Amazon'un Alexa'sı veya Google'ın Asistanı gibi sesli asistanların yardımıyla, sürücüler ve yolcular otomobillerini yalnızca sesli komutlarla kontrol edebilmektedir. Bu eller serbest ve anlaşılır arayüz, kullanıcıların yalnızca komutlarını söyleyerek iklim, müzik ve internet araması gibi özellikleri kontrol etmelerine olanak tanımaktadır (Vachálek ve ark., 2017).

1.2.3.5. Elektrikli Ulaşım: Elektrikli Araçların Yükselişi ve Sürdürülebilir Ulaşım

Son yıllarda içten yanmalı araçlara göre çevreci bir ulaşım seçeneği olduğundan, iklim değişikliği hassasiyeti göz önünde bulundurularak; devletler ve idari diğer birlikler nezdinde elektrikten güç alan hareketliliğe çok fazla destek sağlanmaktadır. Emisyonları şehrin dışına taşıması yoluyla insan sağlığına faydaları, azaltılmış karbondioksit ve azot temelli zararlı emisyonlar neticesinde çevresel faydaları, teknolojideki ilerlemeler ve destekleyici hükümet mevzuatı nedeniyle elektrikli araçlar (EV'ler) açıkça popülerlik kazanmaktadır. Elektrikli araçların artan popülaritesi, daha çevre dostu ulaşım yöntemlerine doğru atılmış bir adımdır.

Elektrikli araçlar, hareket için ihtiyaç duydukları enerjilerini şebekeden veya aracın içinde bulunan pillerden almaktadır. Elektrikli mobilitenin çeşitli faydaları vardır, ancak en dikkate değerlerinden biri, dünyanın karbon ayak izini azaltma yetenekleri oluşturmaktadır. Elektrikli arabaların egzoz emisyonu yoktur, bu nedenle çevre için daha tercih edilir hale gelmektedirler ve geleneksel içten yanmalı motorlu araçlara göre iklim değişikliğini yavaşlatmaya yardımcı olurlar. Bu nedenle elektrikli mobilite, çevre dostu seyahatin önemli bir parçasıdır.

Ayrıca elektrikli araçların enerji verimliliği, içten yanmalı motorlu araçlara göre daha fazladır, nitekim elektrik enerjisinin mekanik harekete dönüştürülmesi elektrikli aktarma organlarında daha verimlidir. Bu verimliliğin bir sonucu olarak EV kullanıcıları yakıttan tasarruf edebilir ve çevreye daha az zarar veren alternatifleri daha uygun fiyatlara kullanabilir (Wedeniwski, 2015). Pil teknolojisindeki gelişmeler, elektrikli araçların artan popülaritesine katkıda bulunmuştur. Şarj altyapısı iyileştirilmiş ve araçlarda lityum-iyon pil kapasiteleri artırılarak daha uzun menzilli sürüşler mümkün hale getirilmiştir. Şarj altyapısını açmak gerekirse, alternatif akım yerine direkt akım kullanan hızlı şarj ağlarının oluşturulması, elektrikli araç sahiplerinin araçlarını hızlı bir şekilde şarj etmelerine izin vererek uzun mesafeli seyahatleri düşük şarj süreleri ile mümkün kılmıştır. Bu duruma ek, elektrikli ulaşımın kapsamı bireysel otomobillerin çok ötesine geçmektedir. Giderek daha fazla insan elektrikli otobüsler, iş araçları ve hatta elektrikli bisikletler gibi daha yeşil ulaşım biçimlerini tercih eder hale gelmiştir (Pacheco ve Hariri, 2016). Ticari sektörde de elektrikli araçlar, kış aylarında yaşadıkları kayda değer menzil düşüşlerine rağmen işlevselliklerini kanıtlamışlardır (Wikström ve ark., 2015)

Sonuç olarak, gelecek açısından artan kullanım oranları ve iyileştirilen altyapı neticesinde otomobillerde elektrik kullanımı ile gelen dijitalleşmenin daha da yaygınlaşabileceğini ve ilerleyen yıllarda bu sektörün sıklıkla bahsi geçen bir ana oyuncu oluşturacağını söylemek mümkündür.

1.2.3.6. Endüstri 4.0: Üretim ve Tedarik Zinciri Süreçlerinde Devrim

Sanayi tanımsal olarak, büyük oranda otomatikleştirilmiş, nihai hedefi maddi metalar üretmek olan bir imalat kolunun genel adıdır. İngiltere'de başlayan Sanayi devriminin başlangıcından bu yana, üretim hatlarında yaşanan teknolojik sıçramalar, günümüzde "endüstriyel devrimler" olarak adlandırılan paradigma kaymalarına yol açmıştır: Üretimin insan gücünden mekanik şekle bürünmesine 1. Sanayi Devrimi, elektrik enerjisinin mekanik hatlarda yoğun kullanımı 2. sanayi devrimi ve üretim hatlarının bilgisayar kontrolüne geçerek dijitalleşmesine ise 3. sanayi devrimi isimleri yakıştırılmıştır. Fabrikalardaki ileri dijitalleşme temelinde, "akıllı" nesneler (makineler ve ürünler) alanında İnternet teknolojileri ile geleceğe yönelik teknolojilerin birleşimi, endüstriyel üretimde yeni bir temel paradigma değişikliğine yol açacak gibi görünmektedir. Gelecekteki üretim vizyonu, modüler ve verimli üretim sistemlerini içermektedir ve ürünlerin kendi üretim süreçlerini kontrol ettiği senaryoları karakterize etmektedir (Lasi ve ark., 2014). Bu kapsamda, sıradaki sayı olan dört ile yeni bir sanayi devrimi iddiasında bulunulmaktadır.

Dördüncü Sanayi Devrimi veya Endüstri 4.0, imalat ve tedarik zinciri endüstrilerini temelden değiştirme iddiasına sahiptir. Hem elemanları birbiri ile haberleşebilen hem de kendi içinde karar verebilme yetisine sahip akıllı bir sistem oluşturmak için Nesnelerin İnterneti, yapay zekâ, robotik ve veri analitiği gibi güncel teknoloji çözümleri harmanlanarak kullanılmaktadır.

Bu noktada ilerleyen yıllarda Endüstri 4.0 tarafından sağlanan pratiklerin imalat sektörüne yansımasını otomobile sektörü nezdinde de gözlemlemek mümkün olacaktır. İlerleyen süreç içerisinde, müşterilerin talepleri doğrultusunda tamamen dijital ortamdan verilen kişiselleştirilmiş siparişler, satın alma uygulamaları ile tam bütünleşik şekilde imalata ve üretim süreçlerine yansıtılacaktır. Bu yolla, şu anda üretim aşamasında maliyetlerin düşmesi sağlanacak, bu durum otomobil üreticilerinde ilkin fiyatları aşağı yönlü güncelleme ihtiyacını tetikleyecek ve otomobillerin ulaşım sektöründeki payı, elbette diğer şartlar göz ardı edildiğinde, maliyet avantajları sebebiyle artacaktır. Öte taraftan, gittikçe daha düşük maliyetli

üretim yapmaya çalışan firmaların, aşağı yönlü fiyat güncellemeleri yerine artan kar marjlarını araştırma ve geliştirme faaliyetlerine yönlendirmesi senaryosunda ise, otomobil sektöründeki dijitalleşme adımları yukarı yönlü üstel şekilde ivmelenerek artışa geçecektir.

Endüstri 4.0 arayışları çerçevesinde, tedarik zincirinde yaşanan aksaklıkların daha hızlı ve etkin şekilde giderilebileceği ve bu yolla araç arzında olan potansiyel problemlerin yaşanmadan engellenebileceği öngörülebilir. Tedarik zincirinde yaşanan bozulmaların araç arzını negatif olarak etkilemesine en yakın örnek, 2019 yılında başlayan salgın sürecinde fabrikaların üretim hatlarını kapatmasına neden olan kapatmaların çip üretimine engel olması ve araç fiyatlarının arz eksikliği sebebiyle göreceli olarak artması senaryosunda görülebilmektedir. Bir aracın üretimi için yüzlerce mikroçip gerekmektedir, bu süreçte hem COVID-19 salgınından hem de ticari sürtüşmelerden etkilenen otomotiv endüstrisindeki yukarı yönlü çip tedarikçileri ve sonraki otomobil üreticileri arasındaki uzun vadeli sıkı arz ve talep dengesinin endüstriyel zincir normalliği bozulmuştur. 2020'nin ikinci yarısından itibaren birçok otomobil üreticisinin çip tedarik sorunlarından etkilenen kısmi üretim hatlarını kapatmaktan başka çaresi kalmamıştır. Örneğin Volkswagen ve Toyota, Çin'de Chengdu ve Guangzhou'daki bazı üretim hatlarını kapatmıştır (Wu ve ark., 2021). Dolayısıyla, araç tedariğinde sıkıntılar yaşanmıştır. Ancak, üretim hatlarının tam otomatize olması senaryosunda, üretimin durmaksızın devam edeceği düşünüldüğünde, bu sıkıntıların ve bu sıkıntılar tarafından tetiklenen diğer sorunların ortadan kısmi olarak kalkacağı açık şekilde görülmektedir.

Tüm bu gelecek beklentilerinin ışığında netice olarak, otomotiv endüstrinde gelecek yıllarda yaşanabilecek gelişmelerin neredeyse tamamında, araçların bağlanılabilirlik özelliklerinin artırılması ve bu yolla kullanıcı ile son ürün arasındaki illiyet bağının artırılması, deneyimin güçlendirilmesi ve memnuniyetlerin varlığının olgunlaştırılması otomotiv sektöründeki üreticiler tarafından hedeflenmektedir. Bu durum, otomotiv endüstrisinin geleceğinin, bugünden çok daha çevrimiçi bağlantı ihtiyacına sahip olacağını göstermektedir. Buradan hareketle, Nesnelerin İnterneti uygulamalarının güncel artış ivmesinin korunacağı ve Nesnelerin İnterneti

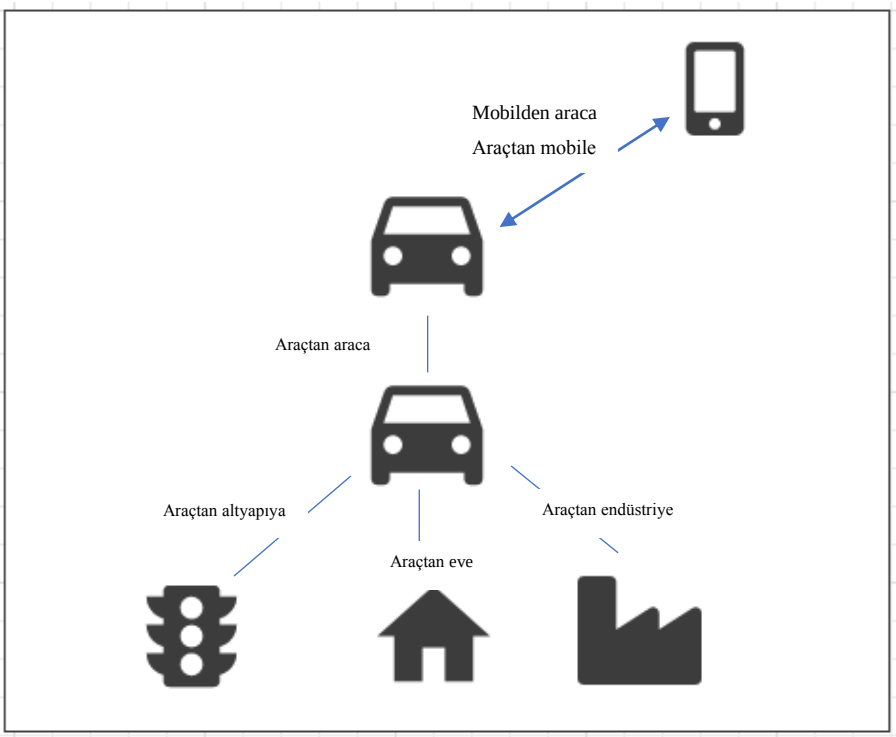
sektöründe görülmesi beklenen kötü niyetli saldırılara açık yüzey alanlarının genişleyeceği öngörülebilir.

1.3. Nesnelerin İnterneti ve Otomobil Sektöründe Nesnelerin İnterneti Uygulamaları

Nesnelerin İnterneti elektronik, yazılım, sensörler ve bağlantı ile gömülü fiziksel cihazlar, araçlar, binalar ve diğer öğelerden oluşan ve bu nesnelerin birbirine bağlanmasını ve veri alışverişini sağlayan bir ağ olarak tanımlanmaktadır. Bu ağa bağlı cihazlar, bulundukları ortamlar ve yaptıkları eylemler hakkında veri toplayıp paylaşabilmekte, böylece birbirleriyle ve diğer sistemlerle iletişim kurmalarına olanak tanımaktadır. Kesintisiz bağlantı oluşturmak için bulut ve uç bilişimi entegre eden Nesnelerin İnternetinin, dijitale öncelik veren bir dünyanın temelini desteklediğine inanılmaktadır. Teknoloji üzerine teknik danışmanlık raporlarının yanı sıra alanda vizyonun sınırlarını da çizmesi ile bilinen kurumsal şirket Gartner'e göre, 2029 yılına kadar kurumsal ağlarda 15 milyardan fazla Nesnelerin İnterneti cihazının konuşlandırılmış olacağını tahmin edilmektedir (Gartner, 2021). Geleceğinin oldukça yaygın bir başarı hikayesi olması beklenen Nesnelerin İnterneti cihazlarının şu ana kadar sergiledikleri de oldukça ümit vericidir. Nitekim, Nesnelerin İnternetinin oluşturduğu olgusallık, şimdiye kadar üretim ve sağlık hizmetleri de dahil olmak üzere birçok alanda başarıya ulaşmıştır. Otomobil sektörü de neredeyse bir istisna değildir (Llopis-Albert, 2021).

Otomobillerde Nesnelerin İnterneti uygulamaları, yalnızca araçların üzerine bütünleştirilmiş elektronik parça veya sistemlerin birbirleri ile haberleşmesi gerçeği ile sınırlı değildir. Bu alt sınırlamanın farkında olarak, otomobillerde Nesnelerin İnternetinin henüz üst sınırının da tanımlanmadığını belirtmek gerekir. Halihazırda farklı başlıklar altında değerlendirilebilseler de, otomobillerde Nesnelerin İnterneti uygulamaları Şekil 1.2'de belirtildiği üzere temelde mobil uygulamaların araçlar ile, araçların diğer araçlar ile, araçların trafik altyapı kümesinde yer alan diğer cihazlar

(trafik ışıkları, uyarıcılar vb.), araçların binalar ile ve araçların endüstri paydaşları ile olan iletişimini kapsamaktadır.



Şekil 1.2. Otomobillerde nesnelerin interneti paydaşları.

Tezin bundan sonra yer alacak kısmında, otomotiv endüstrisinde Nesnelerin İnterneti uygulamalarının kullanımına dair güncel bilgiler verilecek ve durum betimlemesi yapılmaya çalışılacak, ardından otomotiv endüstrisinde Nesnelerin İnterneti kullanımının beraberinde getirdiği potansiyel olumsuz etkiler aktarılacaktır. Bu çaba ile otomotiv endüstrisindeki geniş çerçevede ne gibi sorunlar oluştuğuna ve bu sorunların çözümünde alınması gereken inisiyatiflerin kapsamına dair fikir oluşturulmaya çalışılacaktır.

1.3.1 Otomotiv Endüstrisinde Nesnelerin İnternetinin Güncel Durumu

Otomotiv endüstrisi, çoğunlukla mekanik aksiyonların irdelendiği ve geliştirilme aşamasında dikkate alındığı bir sektör olarak karşımıza çıkar. Bu durum,

özellikle detayları belirtilen tarihçe kapsamında 1950'ler ve 1960'lar sürecine kadar bir nebze de olsa geçerli olmuştur. Lakin, ilerleyen süreçte, özellikle araç güvenlik sistemlerinin silikon devrim neticesinde yeniden şekillendirilmesi ile, ABS gibi otomobiller için kritik önemi haiz teknolojilerin araçlardan ayrılamayacağı anlaşılmış ve doğal olarak dijitalleşmenin araçlardaki ilk adımları atılmıştır. Sonrasında, internetin askeri düzlemden alınıp sivilleştirilmesi ile yaygınlaşması da otomobillerin bu süreçten bağımsız kalamayacağının bir nişanesi olagelmiştir. Günümüz dünyasında, başlıkta bahsi geçen Nesnelerin İnterneti de otomobillerin internet ile kesişim noktasında duran bir olgusallık olarak karşımıza çıkmaktadır. Otomobil endüstrisi nezdinde Nesnelerin İnterneti konseptlerinin uygulanması henüz emekleme aşamasında gibi gözükmektedir ancak akıllı cihazların artan yaygınlığı sayesinde bu alanda yüksek ivmeli bir artış söz konusudur. İnternet bağlantısının sektörde henüz yaygın olmayan varlığı, geleceğin otomobillerinin birbirleriyle ve sürücüleriyle devamlı veri alışverişinde bulunabileceği anlamına gelmektedir. Akıllı telefon üzerine indirilen bir uygulama vasıtasıyla aracın uzaktan çalıştırılıp hareket ettirilebilmesi yahut aracın her gün çalıştırılacağı vakitten önce ısıtma/soğutma panelinin çalıştırılması ile kullanıcı arabaya girdiğinde iklimlendirilmenin zaten önceden sağlanmış olması gibi modern kolaylıklar, günümüzün yeni nesil otomobillerinde bulunan geleceğe yönelik özelliklere örnek olarak gösterilebilir.

1.3.2. Otomotiv Endüstrisinde Nesnelerin İnterneti Uygulamalarının Örnekleri

Nesnelerin İnternetinin otomobil sektöründeki uygulamaları alanına mercek tutulduğunda, birçok farklı olasılık ve bu olasılıkların kombinasyonlarının görüntüsü karşımıza çıkmaktadır. Nesnelerin İnterneti cihazlarının pragmatist kullanımları neticesinde araçların bütüncül ve kısmi tasarımları, performansları, verimlilikleri ve üretim maliyetleri hem üretici hem de tüketici açısından iyileştirilebilmekte ve en yüksek kalite kontrol standartları korunabilmektedir. Bu duruma ek, yapay zekayı ağ teknolojisiyle birleştiren Endüstri 4.0, Nesnelerin İnternetinin yaygın olarak

benimsenmesine zemin hazırlamış, ayrıca araçların birbirleriyle kablosuz veri alışverişi yapmasına olanak sağlamıştır (Tawalbeh ve ark., 2020).

1.3.2.1 Filo Yönetimi

Nesnelerin İnterneti uygulamaları, birden çok aracın aynı anda aktif trafikte görev aldığı senaryolarda araçların verimli şekilde takip edilmesi adına kullanılabilir. Nesnelerin İnterneti uygulamaları, uzaktan filo yönetimini sağlayabilmek adına RFID cihazları, GPS teknolojisi ve OBD-II üzerinden veri alışverişine izin veren teknolojileri kullanmaktadır. Bir aracın anlık olarak nerede olduğu, aracın yanına gitmeden araçta oluşabilecek sorunların teşhisi ve diğer sensörlerden gelen veriler, bu teknolojiler kullanılarak gerçek zamanlı olarak izlenebilmektedir. Araca ait hız, rölanti süresi ve rota sadakatindeki değişikliklerden haberdar olunmasını sağlamak için ivmeölçerler ve jiroskoplar gibi hareket sensörlerinden bilgi derlenmektedir.

Özellikle büyük hacimde yük taşıyan ve bu sebeple kanuni sınırlara tabi ticari araçlarda, yükleme işlemi sonrası gerçek ağırlıkların belirlenmesi oldukça zor bir işlem olarak karşımıza çıkar, nitekim yüklü araçların ağırlığını kaldırabilecek ölçüm cihazları oldukça pahalıdır ve araçlara yüklenebilecek ürünün net ağırlık hesaplamalarının yapılabilmesi adına spesifik hacim ve öz kütle bilgilerinin bulundurulması gerekmektedir (Opoku, 2021). Nesnelerin İnterneti sistemleri tarafından sağlanan teknolojik yenilikler neticesinde, araç üstündeki anlık gerçek ağırlığı da belirlemek için basınç sensörleri kullanılır. Aks üzerine montelenen sensörler, bir kamyon veya treyler tarafından taşınan gerçek yükü yerinde ve anlık olarak ölçebilmektedir. Bu uygulama, bir ticari aracın ağırlığını belirlemek için dijital tartılara uygun bir alternatiftir, böylece para cezalarından kaçınılabilir.

1.3.2.2 Gerçek Zamanlı Navigasyon Kullanımı

Ticari veya kişisel kullanım için olması farketmeksizin, navigasyon kullanımı araçlarda uzunca zamandır var olan bir teknolojidir. Ancak aktif olarak kullanılan navigasyon altyapısı, yalnızca navigasyon ve haritalandırmadan sorumlu şirketin çoğunlukla yine aynı yazılımı kullanan diğer kişilerin taşınabilir cihazlarından aldıkları bilgiler doğrultusunda bir rota ve varış süresi hesaplaması sağlamaktadır. Nesnelerin İnterneti kullanımı neticesinde, otomobillerde üretim hattında eklenen gerekli modüllerin varlığı ve bu modüller tarafından gönderilen ve trafikte var olan her aktif aracın katkıda bulunduğu veri havuzunun aktif olarak işlenmesi ile, trafiğin akışındaki değişiklikler anlık olarak ve daha yüksek keskinlikle görülebilmektedir. Bu yolla, özellikle trafikte bekleme sürelerinin azaltılması ve trafik odaklı en optimal yolun seçilmesi olanaklarının varlığı ile hem yakıt hem de vakit açısından verimlilik artırılabilmiştir.

1.3.2.3 Otomotiv Bakım Sistemi

Otomobiller, bir kısmı hareketli olmak üzere yüzlerce farklı parçanın bir araya gelmesi ile oluşan karmaşık birer mühendislik çözümüdür. Bu mühendislik çözümlerinin işlevselliğinin korunabilmesi adına otomobiller kullanıldıkları veya kullanılmadıkları süreden bağımsız olarak, başta hareketli parçaları olmak üzere, kapsamlı bakım ve onarım faaliyetlerine ihtiyaç duymaktadır. Bakım ve onarıma tabi olacak parçaların ve nesnelerin kapsamlı bir çetelesini tutmak oldukça meşakkatlidir, nitekim her bir parçanın sahip olduğu görevle ilintili olarak farklı bakım periyotları vardır. Örneğin kauçuk materyalden üretilen lastikler, çoğunlukla beş yıl veya altmış bin kilometre kullanım ömrüne sahip iken, aracın ön veya arka camında yer alan ve yine kauçuk materyalden üretilen sileceklerinin senede bir kez değiştirilmesi üreticiler tarafından önerilen uygulamadır. Bu karmaşık durum, beklenen şekilde bakım ve onarım aralıklarının sıklıkla son kullanıcılar tarafından atlanmasına veya bazı bakımların toplu şekilde yapılmak istenmesi sonucunda önerilen sıklıkta yapılamamasına sebebiyet vermektedir.

Nesnelerin İnterneti uygulamalarının araçlarda benimsenmesi neticesinde, araç üzerinde yer alan sensörler anlık olarak verileri okuyup kullanıcının sıklıkla irtibatta olduğu araç göstergesi veya bilgi-eğlence sistemi ekranına bu verilerin gerçek zamanlı aktarılmasının önü açılmıştır. Ayrıca kendi üzerinde internete bağlanma altyapısı bulunan bazı araçlar, bu bilgileri gerçek zamanlı olarak araç servisleri ile paylaşmaktadır. Bu durum, araçların bakım ve onarım süreçlerinin hem kullanıcıya hem de bakımdan sorumlu olan servise şeffaf bir şekilde aktarılabilmesine ve bakım onarım faaliyetlerinin olması gereken sıklıkta sağlanabilmesine yardımcı olmaktadır.

1.3.2.4 Kaza Tespiti ve Acil Yardım Uygulamaları

Tüm dünyada trafik sıkışıklığı, acil durum hizmetlerinin sağlanması için acil durum araçlarının (*EV*) doğru zamanda bulunmaması nedeniyle can ve mal kaybına yol açabilen önemli bir sorundur (Wedel ve ark., 2009). Bu nedenle, ivedi şekilde gerekli tıbbi hizmetleri sağlamak için acil durumda kullanılan araçların sorunun gerçekleştiği bölgeye hızla ulaşımını kolaylaştırmanın ne kadar önemli olduğu göz önünde bulundurulmalıdır.

Günümüzde, Nesnelerin İnternetinin araçlarda kullanımı ile iki farklı yönde acil durum olaylarına müdahale hızlarının artırılması sağlanmıştır. İlkin, araçlarda bulunan ivmeölçer, hızölçer ve konum sensörleri sayesinde, aracın ivmesinde negatif yönlü bir gelişme kaydedilir ve aracın hızı sıfırlanır ise, araçta bulunan konum sensörleri bir kaza olduğunu varsayıp devreye girerek aracın anlık konumunu ilgili makamlarla paylaşabilmektedir. Bu durumda, araç sürücüsünde iletişime engel herhangi bir sağlık durumu olması sebebiyle olaylara müdahale edilememe ihtimali ortadan kaldırılmaktadır.

Ayrıca, güncel trafik verisine göre hızlı rota oluşturma teknolojisi, acil durum araçlarına entegre edilerek farklı ve hızlı bir rota oluşumu kolaylaştırılmaktadır. Aynı zamanda, bazı ülkelerde pilot olarak geliştirilip bireysel kullanıcı araçlarına

tanımlanan Nesnelerin İnterneti teknolojisinin yardımı ile, trafikteki diğer araçlara bir acil durum olduğu bilgisi iletilmekte, bu yolla acil durum araçlarının önünün trafik sıkışıklığı ile kapanması ve müdahale süresinin uzaması ihtimalinin önüne geçilmektedir. Ek olarak bu teknoloji, acil durum araçlarının ilerlemesi süresince trafik geçiş üstünlüğünü, trafik altyapısı ile bütünleşme sağlayıp izlenen rotadaki bütün trafik ışıklarının düzenlenmesine yardımcı olarak acil durum araçlarına vermekte, müdahale süresine bir katkıda daha bulunmaktadır.

1.3.2.5 Hırsızlık Tespiti

Araçların hırsızlık kurbanı olması, neredeyse otomobillerin tarihi kadar eski bir fenomendir. Özellikle değerli araçlar veya değerli metaların taşınmasından sorumlu olan araçlar (örneğin bankalar arası para transferinde görev alan ticari araçlar veya kargo taşıyan ticari araçlar gibi) bu tarz hırsızlık teşebbüslerinin birincil hedefi olarak karşımıza çıkmaktadır. Bu teşebbüslerin önüne geçmek amacıyla, uzunca zamandır araçları hırsızlığa karşı korumaya yönelik özellikler üreticiler tarafından tanıtılmakta veya kullanıcılar tarafından önlem mahiyetinde benimsenmektedir. Günümüzde bu özellikler, aracı daha uygun maliyetli, güvenli ve güvenilir hale getirmek için Nesnelerin İnterneti teknolojisi eklenerek geliştirilmiştir (Mukhopadhyay ve ark., 2018). Nesnelerin İnterneti yardımıyla geliştirilen hırsızlık önleme sisteminden yararlanan çalıntı bir aracın sahibi, internet bağlantısına sahip herhangi bir cihaz vasıtasıyla aracının tam konumunu hızlı bir şekilde tespit edebilir. Bu teknolojiye ek olarak geliştirilen bir diğer teknoloji ise, bir akıllı cihaz uygulaması ve failin aracı kullanırken çekilmiş fotoğrafını dijital kanıt olarak yakalayabilen direksiyona gömülü bir kamera kullanılarak sahibi tarafından uzaktan kontrol edilebilen başlatma özellikleri nedeniyle daha fazla güvenilirlik sağlamaktadır (Chandra Shreyas ve ark., 2018).

1.3.2.6 Sürücü Davranış Yönetimi

Sürücüler, şüphe olmaksızın trafikte en ağır sorumluluk sahibi paydaşlardan bir tanesidir. Sürücülerin sürüş esnasındaki tutum ve davranışları, karayollarında gerçekleşen kazalarda en önemli ve belirleyici etkenlerden bir tanesidir.

Çoğu durumda, sürücünün neden olduğu kaza, genellikle araç kullanmak için tatmin edici fiziksel ve zihinsel sağlık kriterlerinin bulunmamasının bir sonucudur (Rahim ve ark., 2021). Nesnelerin İnterneti teknolojisi, sürücünün fiziksel durumunu gözlemlemek için kullanılabilir. Aracın gösterge paneli hizasına yorgunluk tespit edici sistemler, sürücü koltuğuna Elektromiyogram (EMG) ve Elektrokardiyogram (EKG) bilgileri sağlayan sensörler monte edilerek ölçümlerin sağlanması, buradan elde edilen bilgilerin daha sonra yine Nesnelerin İnterneti teknolojisi yardımıyla ilgili kişi ve kurumlara aktarılması ve hatta aracın kullanımının bu bilgilerin işlenmesi neticesinde sürücünün sürüşe engel durumu giderilene kadar engellenmesi mümkündür.

Sonuç olarak, Nesnelerin İnterneti kavramı daha önceden betimlendiği şekilde gelecek zamanlarda iletişim altyapısına yapılan yatırımlar ve potansiyel sebebiyle oldukça gündemde olacağa benzemektedir. Halihazırda, fazla sayıda araca ev sahipliği yapan ticari filoların verimli ve sürdürülebilir düzlemde yönetilmesinden hırsızlık gibi istenmeyen olayların çözümlenmesine kadar birçok farklı Nesnelerin İnterneti uygulaması, otomotiv sektöründe kendine yer bulmuştur. Birinci bölümde altı çizilen şekilde, sürücülerin aidiyet bağının oluşturulması ve devam ettirilebilmesi adına şu anda güncel olarak kullanılan bazı teknolojilerin de bağlanabilirlik kullanılarak güncellenmesi, yeni eklenecek teknolojilerin yine uzaktan yönetilebilmesi adına Nesnelerin İnterneti çözümlerine ihtiyaç duyulacağı gerçeği gibi durumlar göz önünde bulundurulduğunda, ilerleyen süreçte oldukça yüksek bir ivme ile işbu teknoloji kullanımının niceliksel büyümesinin görülebileceği durumu ortadadır.

1.4. Nesnelerin İnterneti Uygulamalarına Saldırı Yüzeyi

Saldırı yüzeyi, saldırganların Nesnelerin İnterneti ortamlarının güvenliğini tehlikeye atmak için hedefleyebilecekleri giriş noktalarını veya güvenlik açıklarını ifade eder. Nesnelerin İnterneti alanında saldırı yüzeyleri, birbirine bağlı cihazların ve sistemlerin güvenlik açığı ve potansiyel istismarında önemli bir rol oynar. Nesnelerin İnterneti saldırı yüzeylerinin farklı yönlerini anlamak, potansiyel zayıflıkları belirlemek ve etkili güvenlik önlemleri uygulamak için çok önemlidir (Pacheco ve Hariri, 2016).

Sensörler ve aktüatörlerden akıllı ev cihazlarına, endüstriyel kontrol sistemlerine ve sağlık bakım cihazlarına kadar farklı bir spekturumda yer alan tüm Nesnelerin İnterneti ekosistemi cihazları bir saldırı yüzeyinin merkezinde yer alır. Bu cihazlara ait olası güvenlik açıkları, güvenli olmayan varsayılan ayarlardan, zayıf kimlik doğrulama mekanizmalarından, yama uygulanmamış yazılımlardan veya yetersiz şifreleme protokollerinden kaynaklanabilmektedir (Wedeniwski, 2015). Saldırganlar, yetkisiz erişim elde etmek, cihaz işlevselliğini değiştirmek veya hassas verileri çıkarmak için bu zayıflıklardan yararlanabilmektedir. Bilindiği üzere Nesnelerin İnterneti sistemleri, cihazlar ve arka uç (*İng. Back-end)* sistemleri arasında veri iletmek için iletişim protokollerine ve ağlarına dayanmaktadır. Dolayısıyla saldırı yüzeyleri, Wi-Fi veya Bluetooth gibi kablosuz protokollerdeki güvenlik açıklarından veya şifrelenmemiş veya kötü şifrelenmiş bağlantılar gibi güvenli olmayan iletişim kanallarından da kaynaklanabilmektedir. Saldırganlar, Nesnelerin İnterneti cihazlarından akan verilerinin bütünlüğünü ve gizliliğini tehlikeye atmak için iletişimi dinleyebilir, kötü amaçlı komutlar enjekte edebilir veya ortadaki adam saldırıları gerçekleştirebilir (Wedeniwski, 2015).

Birçok Nesnelerin İnterneti dağıtımı; veri depolama, işleme ve analizi için bulut platformlarından yararlanır. Bulut altyapısı da Nesnelerin İnterneti saldırıları için uygun şekilde güvenli hale getirilmezse bir saldırı yüzeyi haline gelebilir. Zayıf erişim denetimleri, yanlış yapılandırılmış izinler veya bulut içindeki verilerin yetersiz şekilde şifrelenmesi, saldırganların hassas bilgilere yetkisiz erişim elde etmesi veya

bulut hizmetlerini kesintiye uğratması için fırsatlar sağlayabilir. Nesnelerin İnterneti cihazlarından akan verileri yöneten ve işleyen arka uç (*İng. Back-end)* sistemleri, saldırı yüzeyinin bir diğer önemli bileşenleridir (Vachálek ve ark., 2017). Bu sistemler veri tabanlarını, uygulama sunucularını ve veri analitiği platformlarını içerebilir. Bu sistemlerdeki zayıf kimlik doğrulama mekanizmaları, yama uygulanmamış yazılımlar veya yetersiz güvenlik denetimleri, saldırganların verileri manipüle etmesine, kötü amaçlı kod enjekte etmesine veya yetkisiz eylemler gerçekleştirmesine olanak sağlayabilir.

Kullanıcıların mobil uygulamalar veya web portalları gibi Nesnelerin İnterneti cihazlarıyla etkileşime geçtiği, veri girişi veya veri okuma operasyonlarının gerçekleştirildiği kullanıcı arayüzleri de saldırı yüzeyleri sunabilir. Bu saldırılar, neredeyse tamamen web arayüzü üzerinden gerçekleştirilen saldırıların benzeri olduğundan, konuyla ilgili kötü niyetli kişilerin bu noktada ekstra bilgisine ihtiyaç duyulmadığından daha geniş bir saldıran kitlesine hitap edebilmektedir. Güvenli olmayan kimlik doğrulama mekanizmaları, geliştirilmesi veya kullanılması sürecinde güvenlik açığı barındıran uygulama kodları veya giriş doğrulama operasyonlarının yetersiz şekilde yapılması; yetkisiz erişime, veri sızıntısına veya kötü amaçlı komutların eklenmesine yol açabilmektedir (Vachálek ve ark., 2017).

Son olarak da DDoS olarak isimlendirilen, en bilineni Mirai Botnet saldırısı olan dağıtık mimari üzerinde gerçekleşen hizmet reddi yahut ilintili diğer Nesnelerin İnterneti saldırıları oldukça olağan gözükmektedir, nitekim bu cihazların internet ile olan arayüzleri neticesinde cihazlara ulaşmak, örnek olarak bu cihazlar üstündeki port yönlendirme mekanizmaları yardımıyla, teorik olarak mümkün gözükmektedir. Ancak, kendileri üstünden internete direkt olarak erişilemeyen, bir diğer deyiş ile NAT'lerin arkasında kalan cihazlar da aynı şekilde güvenli değildir (Acar ve ark., 2018). 2018 yılında Princeton Üniversitesinde yürütülen bir çalışmada, Nesnelerin İnterneti cihazları ile aynı LAN (*İng. Local Area Network)* kümesinde yer alan bir kullanıcı, kötü amaçlı JavaScript kod parçası bulunduran bir web sitesini ziyaret etmiş şeklinde bir senaryo üzerinden; saldırganın HTTP endpointlerini kullanarak yerel aygıtları keşfedebildiği ve yerel cihazlara erişim sağlayabildiği bir saldırı başarı

ile simule edilmiştir (Acar ve ark., 2018). Bu durum, internete direkt arayüzü olmayan Nesnelerin İnterneti cihazlarının da saldırı yüzeyi kapsamında bulunabileceğini ispatlamıştır.

1.5. Nesnelerin İnterneti Siber Saldırı Türleri

Nesnelerin İnterneti ekosistemindeki birbirine bağlı cihazların sayısı artmaya devam ettikçe, bu cihazları ve güvendikleri ağları hedef alan siber saldırı potansiyeli de artmaktadır. Saldırganlar, yetkisiz erişim elde etmek, veri bütünlüğünden ödün vermek, hizmetleri bozmak veya diğer kötü niyetli faaliyetleri başlatmak için Nesnelerin İnterneti sistemlerindeki güvenlik açıklarından yararlanır (Tran ve ark., 2022). Yaygın Nesnelerin İnternetin siber saldırı türlerini anlamak, etkili güvenlik önlemleri uygulamak için çok önemlidir. Siber saldırılara karşı bir savunma stratejisi sağlamak için öncelikle çeşitli saldırı senaryoları ve saldırı türleri araştırılmalıdır (Aslan ve Samet, 2017). Öte taraftan, Nesnelerin İnterneti yaklaşımsal ve tanımsal olarak cihazların birbirleri ile iletişimini önceliklendirdiğinden, bu sektör nezdinde yapılacak siber saldırıların çoğunlukla iletişim altyapısı üzerinden yürütüldüğü de göz ardı edilmemelidir. Nesnelerin İnterneti ağı üzerinde gerçekleştirilen yaygın saldırılar, türlerine göre temel başlıklar halinde gruplanabilmektedir:

1.5.1. Fiziksel Saldırılar

Nesnelerin cihazlarına yapılan fiziksel saldırılar, cihazların işlevselliğinden ödün vermek adına fiziksel erişim sağlamayı içerir. Fiziksel erişim sağlanması adına saldırgan, Nesnelerin İnterneti cihazının fiziksel bütünlüğünü bozabilir, muhtelif görülür veya görünmez etkilerle cihazı işlevinin dışında davranmaya zorlayabilir yahut cihaza ekstra yetenekleri fiziksel olarak sağladıktan sonra (örneğin, cihaza dışarıdan bir veri yolu eklemek, dışarıdan bir depolama aracı takmak vb.) saldırıyı gerçekleştirebilir. Fiziksel saldırılar, yedi temel başlık altında gruplanıp özetlenebilir (Deogirikar and Vidhate, 2017):

1) Node Tampering: Yabancı dilde *Node* olarak bilinen düğümler, Nesnelerin İnterneti akış şemasında verinin geçtiği her bir alt sistemi temsil etmektedir. Node tampering saldırılarında saldıran kişi, güvenliği ihlal edilen düğümü fiziksel olarak değiştirir ve şifreleme anahtarı gibi hassas bilgileri elde edebilir.

2) RFID ünitelerde radyo dalgası paraziti yayımı: Saldırgan, RFID cihaz ve sistemlerin iletişimi için kullanılan radyo frekansı sinyalleri üzerinden, iletişimi karıştıran gürültü sinyalleri göndererek hizmet reddi saldırısı gerçekleştirir ve böylece hizmet vermesi beklenen cihaz veya sistem kullanılmaz hale gelir.

3) Kablosuz iletişimde Node Jamming: Saldırgan, sinyal karıştırıcı veya sinyal bozucu kabiliyette "jammer" olarak da bilinen cihazları kullanarak kablosuz iletişimi bozabilir. Hizmet reddi saldırısına neden olur.

4) Kötü Amaçlı Düğüm Enjeksiyonu: Saldırgan, birbiriyle haberleşen cihazların arasına bir ekstra adım mahiyetinde cihaz ekler ve veri iletişiminin bu cihaz üzerinden gerçekleşmesine sebep olur. Eklenen yeni cihaz, iletişime dair detayları görebilir, manipüle edebilir ya da yok edebilir. Ortadaki adam saldırılarının fiziksel cihazlar yardımıyla yapılan sürümüdür.

5) Fiziksel Hasar: Saldırgan, Nesnelerin İnterneti sisteminin bileşenlerine fiziksel olarak zarar verir ve DoS saldırı tipi ile sonuçlanır.

6) Sosyal Mühendislik: Saldırgan, bir Nesnelerin İnterneti sisteminin kullanan gerçek kişiler ile, o kişilerin iletişim numaraları, e-posta adresleri, ev adresleri gibi kanalları kullanarak fiziksel olarak etkileşime girer ve kişileri, hedeflerine ulaşmak için hassas bilgiler elde etme amacıyla manipüle veya ikna eder.

7) Kötü Amaçlı Kod Enjeksiyonu: Saldırgan fiziksel olarak eriştiği Nesnelerin İnterneti sisteminin bir parçasına (düğümüne) kötü amaçlı bir kod enjekte eder ve sistemin kontrolünü kısmen ya da tamamen ele geçirme iradesi ortaya koyar.

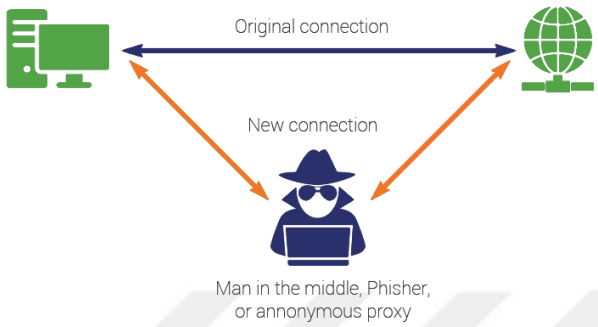
1.5.2. Ağ Saldırıları

Ağ saldırıları, Nesnelerin İnterneti cihazlarının aralarındaki iletişimi hedef alan saldırılardır. Ağ saldırıları, hedef aldıkları iletişim altyapısı düğümlerine göre değişik tiplerde ve değişik boyutlarda değerlendirilebilir.

Ağ saldırı tipinin en yaygını, hiç şüphe yok ki Botnet üzerinden DDOS saldırılarıdır. Botnet saldırıları, bir kişi veya grup tarafından, genellikle spam e-posta, sahte nitelikte siteler, phishing gibi saldırılar üzerinden zararlı yazılım yardımıyla ele geçirilmiş bilgisayarların bir araya gelerek oluşturduğu ağlar tarafından yapılan saldırılardır. Örgütlenmiş saldırganlar tarafından kontrol edilen ve art niyetli eylemin sonucunda kontrolü yitirilmiş bilgisayarlara zombiler veya "robot" kelimesinin kısaltılması ile türetilen botlar da denmektedir. Bu terim, İnternet üzerinden otomatik bir görev olarak çalışan, çalıştırdığı yazılım hakkında fikri olmaksızın, sorgulamadan sadece uygulayan yazılım uygulamalarına gönderme yapmaktadır. Bir komuta ve kontrol (C2 veya C&C) altyapısı altında, bir grup bot, botnet adı verilen kendi kendine yayılan, kendi kendini organize eden ve otonom bir çerçeve oluşturabilmektedir (Liu ve ark., 2009). Bu otonom çerçeve ile, saldırganlar tarafından ele geçirilen cihazların tek bir sunucuya istek atması, bu yolla sunucunun dakika veya saniye başına daha önceden tanımlanmış işlem limitini doldurması ile diğer isteklere cevapsız kalması amaçlanmıştır. Nesnelerin İnterneti cihazları, internete bağlı, sayıca tekil kullanıcı cihazlarından çok daha fazla sayıda ve istek atmaya müsait oldukları için, bu saldırılar için biçilmiş birer kaftandır.

İkinci yoğun şekilde görülen Nesnelerin İnterneti ağ saldırıları tipi, ortadaki adam saldırılarıdır. Ortadaki adam (*İng. Man in the Middle, MitM)* saldırıları, iletişim sağlayan iki taraf arasına, Şekil 3.2'de aktarılan şekilde yetkisiz bir üçüncü kişinin girmesi ile tüm iletişim trafiğini kayıt altına alması, değiştirmesi, manipüle etmesi gibi zararlı faaliyetlerde bulunması ile iletişim trafiğinin ele geçirilmesini ifade eden bir saldırı tipidir. Nesnelerin İnterneti sistemlerinde yapılan ortadaki adam saldırılarında, saldırganlar Nesnelerin İnterneti cihazları arasındaki veya cihazlar ile arka uç sistemleri arasındaki iletişimi keser ve manipüle eder. Saldırganlar, veri

paketlerini ele geçirerek ve değiştirerek hassas bilgilere kulak misafiri olabilir, kötü amaçlı komutlar enjekte edebilir veya aktarılan verileri manipüle edebilir (Shah ve Sengupta, 2020).



Şekil 1.3. MitM saldırılarının genel işleyişi.

RFID cihazlarının klonlanması veya taklit edilmesi (spoofing) saldırıları da iletişim ağı üzerinde gerçekleştirilen saldırılardan bir diğeridir. Cihazların klonlanması, cihazların yaydığı elektromanyetik sinyallerin tespit edilerek bir başka cihaza aktarılması yöntemi ile gerçekleştirilir. Özellikle içinde RFID çipleri taşıyan kimlik kartlarının, ortamlara fiziksel girişte kullanılan yetki kartlarının klonlanması oldukça sık görülmektedir. Aynı şekilde, etrafa sinyal yayan cihazların sinyallerinin şiddet ve frekansları üçüncü parti cihazlar üzerinden tespit edilerek birebir taklit edilebilmektedir.

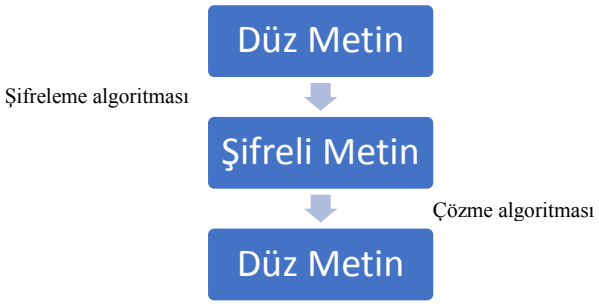
1.5.3. Yazılım Saldırıları

Nesnelerin İnterneti sistem ve cihazlarına, yetkisiz erişim sağlayan veya kötü amaçlı eylemler gerçekleştiren amaçlı üçüncü parti yazılımlar bulaşabilir. Kötü amaçlı yazılım, Nesnelerin İnterneti sistemleri ile aynı LAN üzerinde yer alan kullanıcılara gönderilen şüpheli içerikli e-posta ekleri, lisanssız ve internetten rastgele indirilmiş ve güvenliği ihlal edilmiş üçüncü taraf uygulamaları, virüs veya malware içeren sözde yazılım güncellemeleri veya tamamen bağımsız şekilde,

fiziksel *bus* cihazları üzerinden çeşitli yollarla aktarılabilir. Nesnelerin İnterneti cihazları bir kez virüs bulaştıktan sonra kötü amaçlı yazılımı yaymak veya diğer koordineli saldırılara katılmak için kullanılabilir (Stellios ve ark., 2018). Bu enfeksiyonlara örnek olarak, dünya çapında bilinirliği ile Stuxnet saldırısı örnek gösterilebilir. 2010 yılı haziran ayında, İran'ın nükleer tesislerinin bir tanesinde, nükleer sistemlerde çalışan pompa, kayar bant, servo motor gibi elemanların direkt insan müdahalesi olmaksızın yürümesinden sorumlu olan SCADA tabanlı robotik otomasyon sistemlerinde, sistemin işleyişine aykırı hareket etmesine sebebiyet veren bir yazılım tespit edilmiştir. Bu yazılım, öncelikle <*Rootkit.TmpHider*> ismiyle rapor edilmiştir. Yapılan incelemelerde, yazılım iddia edilene göre, nükleer bir tesisin bahçesine atılan USB taşınabilir diski üzerinden sisteme bulaş sağladığı, oldukça incelikle geliştirilmiş bu yazılımın, Windows bilgisayarlar üzerine ilk aktarım yaptıktan sonra, enfekte etmesi gereken Siemens üretimi SCADA sistemlerine bulaşı sağlayana kadar kendini gizlediği ve ancak bulaşı hedefi tutturulduktan sonra çalışmaya başladığı gözlemlenmiştir (Langner, 2011). Yazılımın, İran'ın nükleer faaliyetlerinden rahatsız olan kişi, grup veya ülkeler tarafından geliştirildiğine dair hipotezler halen canlıdır, ancak hem bu iddialara hem de verdiği zararın kapsamına dair herhangi bir resmî açıklama yapılmamıştır.

1.5.4. Şifreleme Saldırıları

İletişim altyapısının kapalı devre olarak kabul edilmeyen tüm ögeleri, iletişimin sağlıklı ve her iki taraftan anlaşılabilir ancak üçüncü bir taraftan anlaşılamaz olması için şifreleme pratikleri kullanmaktadır (Şekil 3.3). Saldırganlar, bu şifreleme pratiklerini manipüle ederek, tersine mühendislik ile etkisiz hale getirerek veya tamamen devre dışı bırakarak Nesnelerin İnterneti üstünde saldırılar gerçekleştirebilmektedir.



Şekil 1.4. Şifreleme akış şeması.

Kriptanaliz Saldırıları, şifreleme saldırılarının ilk yöntemidir. Bu saldırı yönteminde saldırgan, şifreleme anahtarını düz metin halinde herhangi bir şifreye maruz kalmamış şekilde veya şifreli metin halinde ele geçirmektedir. Kullanılan yönteme bağlı olarak, farklı türde kriptanaliz saldırıları vardır (Andrea ve ark., 2015):

a) Yalnızca Şifreli Metin (*Ciphertext*) Saldırısı: Bu saldırıda saldırgan, bir yere kaydedilmiş veya iletişim altyapısı üzerinde iletim halinde olan şifreli metne erişir ve bu şifreli metne karşılık gelen anlamlı metni elde eder. Bu süreç, tek tek tüm harf, rakam veya özel karakter kombinasyonlarının denenmesi (*brute force*) yöntemi ile olabileceği gibi farklı algoritmaların tersine mühendisliği ile de sağlanabilmektedir.

b) Bilinen Düz Metin Saldırısı: Saldırgan, ele geçirdiği şifreli metnin bazı bölümlerinin şifresi çözüldüğünde neye benzediğini bilir ve bu bilgiyi kullanarak şifreli metnin kalan kısmını çözmek amacıyla saldırıya geçer.

c) Seçilmiş Düz Metin Saldırısı: Saldırganın elinde şifreli bir metin vardır, bu kapsamda saldırgan bütün düz metinlere saldırır ve hangi düz metnin elindeki şifreyle uyumlu olduğunu gözlem ile tespit eder, neticede şifreleme anahtarını bulur ve gelecek saldırılarda potansiyel olarak bu şifreleme anahtarını kullanır.

d) Seçilmiş Şifreli Metin Saldırısı: Saldırgan, seçilen şifreli metnin düz metnini mevcuttur, bütün şifreli metinlere saldırıda bulunup ele geçirdikten sonra düz metin ile şifreli metin arasındaki ilişkiden şifreleme anahtarını bulabilir.

1.5.5. Tedarik Zinciri Saldırıları

Nesnelerin İnterneti ekosistemine ait cihazlar, son kullanıcılara ulaşmadan önce karmaşık tedarik zincirlerinden geçer. Örneğin bir bebek monitörünün tasarımı bir ülkede, içindeki mikroistemcilerinin üretimi bir başka ülke ve fabrikada, en son birleştirme aşaması ise bambaşka bir konumda gerçekleşebilir. Tedarik zinciri saldırıları, cihazların üretim, dağıtım veya kurulum sırasında ele geçirilmesini içerir. Bu, saldırganların cihazlara arka kapılar, kötü amaçlı yazılımlar veya diğer kötü amaçlı bileşenleri sokmasına olanak tanıyarak güvenliklerini baştan tehlikeye atar (Shah ve Sengupta, 2020).

1.6. Nesnelerin İnterneti Saldırı Yüzeylerinden Yararlanılması: Güvenlik Açıkları ve Riskler

Nesnelerin İnterneti sistemlerinde düşmanların yararlanabileceği güvenlik açığı noktalarına atıfta bulunan Nesnelerin İnterneti saldırı yüzeyleri, kötü niyetli kişiler tarafından istismar edildiklerinde güvenlik açıklarına sebebiyet vermektedir. Nesnelerin İnterneti saldırı yüzeyleriyle ilişkili güvenlik açıklarını anlamak, potansiyel riskleri belirlemek ve etkili güvenlik önlemleri uygulamak için çok önemlidir. Nesnelerin İnterneti saldırı yüzeylerinden yararlanmaya ilişkin bazı yaygın güvenlik açıkları ve belirtilen güvenlik açıklarının oluşturdukları ilintili riskler şu şekilde sıralanabilir:

1.6.1. Zayıf Kimlik Doğrulama ve Yetkilendirme

Birçok Nesnelerin İnterneti cihazı ve sistemi, basit parolalar veya hiç kimlik doğrulaması olmaması gibi varsayılan veya zayıf kimlik doğrulama mekanizmalarına hâlâ güvenmektedir. Saldırganlar, kimlik bilgilerini kolayca tahmin ederek veya giriş yapılması için gerekli kimlik doğrulama uygulamalarında tek tek denemeler yürütülmesi yöntemini uygulayarak, cihazlara yetkisiz erişim sağlayabilmekte ve dolayısıyla ilişkili sistemler üzerinde kontrol sağlayabilmekte, sözüm ona bu güvenlik açıklarını istismar edebilmektedir. Bu durum, yetki olmayan kişilerin Nesnelerin İnterneti üzerinde dolaşan muhtelif nitelikteki verilere erişimine, cihaz manipülasyonuna ve hatta ağ güvenliğinin bütüncül olarak ihlal edilmesine yol açabilmektedir (Paritala, Manchikatla ve Yarlagadda, 2017).

1.6.2. Güvenli Olmayan İletişim Kanalları

Nesnelerin İnterneti cihazları genellikle, uygun şekilde korunmadıkları takdirde güvenlik açıklarına neden olabilecek Wi-Fi veya Bluetooth gibi kablosuz iletişim protokolleri üzerinden haberleşme sağlamaktadır. Saldırganlar, cihazlar ve arka uç sistemleri arasında değiş tokuş edilen verilerin gizliliğini ve bütünlüğünü tehlikeye atarak araya girebilmekte, bahsi geçen verileri bu yolla manipüle edebilir veya iletişime kötü amaçlı komutlar ekleyebilmektedir. Bu durum yine yetkisiz erişime, veri sızıntısına veya cihaz davranışının manipüle edilmesine neden olabilmektedir (Paritala, Manchikatla ve Yarlagadda, 2017).

1.6.3. Yamasız Yazılım ve Ürün Yazılımı

Yamalar, sorunları tespit edilen yazılım ve donanım çözümlerinin üreticileri veya bağımsız kullanıcıları tarafından sorunların giderilmesi adına üretilen ekstra yazılım çözümleridir. Birçok Nesnelerin İnterneti cihazında düzenli yazılım güncellemeleri yapılmamakta ve yama yönetimine dair süreçler sağlıklı şekilde

yürütülmemektedir ve bu durum cihaz ve sistemleri bilinen güvenlik açıklarına karşı savunmasız bırakmaktadır. Saldırganlar, yetkisiz erişim elde etmek, cihazın amacı dışında eylemlere sebebiyet veren kodları çalıştırmak veya cihazların işlevselliğini tehlikeye atmak için bu yama uygulanmamış güvenlik açıklarından yararlanabilmektedir. Bu durum, yetkisi olmayan kişilerin cihazları kontrol etmesine, veri ihlallerine veya güvenliği ihlal edilmiş cihazların daha fazla saldırı için giriş noktası olarak kullanılmasına yol açabilir (Piccinini ve ark., 2015).

1.6.4. Yetersiz Şifreleme ve Veri Koruma

Nesnelerin İnterneti cihazları, kişisel sağlık bilgilerinden iş açısından kritik verilere kadar çok miktarda hassas veri üretmekte ve bu verileri gerek cihazlar arasında gerekse cihazdan arka taraf sunucularına iletmektedir. Bu veri akışı sürecinde zafiyeti bilinen şifreleme algoritmaları kullanılarak şifreleme yapılması veya şifreleme sonrası süreçlerde tuzlama (*İng.* salting) süreçleri gibi tamamlayıcı süreçlerde eksiklikler bulunması, bu verileri yetkisiz erişime ve manipülasyona açık hale getirmektedir. Saldırganlar bu eksiklikler üzerinden hassas nitelikte ve kişisel verileri yakalayabilir ve sızdırabilmekte, bu istenmeyen durum da ayrıca gizlilik ihlallerine, finansal kayıplara veya itibar kaybına neden olabilmektedir (Radanliev ve ark., 2019).

1.6.5. Güvenli Cihaz Yönetimi Eksikliği

Birçok Nesnelerin İnterneti dağıtımı, güvenlik güncellemelerini uygulamayı, cihaz sağlığını izlemeyi veya güvenlik olaylarına yanıt vermeyi zorlaştıran sağlam cihaz yönetimi uygulamalarından yoksundur. Saldırganlar, cihazları tehlikeye atmak, yapılandırmalarını manipüle etmek veya tüm Nesnelerin İnterneti ekosistemi üzerinde yetkisiz kontrol elde etmek için bu yönetim eksikliğinden yararlanabilir (Piccinini ve ark., 2015).

Yukarıda sağlanan bilgilere ek, saldırı yüzeyleri, saldırı türleri, güvenlik açıkları ve bu güvenlik açıklarının neden olabileceği risklerin öğrenilmesinden sonra, siber saldırıların gerçekleştirilmesi senaryolarında karşılaşılabilecek etkilerin öğrenilmesi, bu etkiler nezdinde önerilen tedbirlerin sunulması ve bu etki-tedbir zincirinin canlandırılmasını kolaylaştırmak adına örneklendirilmesi önem arz etmektedir. Akabinde, bu siber saldırılara dair edinilen öngörülerin otomobil sektörü düzleminde türevinin alınması, üretilecek çerçevenin verimliliği adına katkı sağlayacaktır.

1.7. Nesnelerin İnterneti Siber Saldırılarının Etkileri

Nesnelerin İnterneti alanında gerçekleştirilen siber saldırılar, bireysel tüketicilerden kritik altyapıya kadar çeşitli sektörlerde önemli hasara ve aksamaya neden olma potansiyeline sahiptir. Bu saldırıların etkisini anlamak, kuruluşlar ve bireyler için sağlam güvenlik önlemlerinin önemini kavramak için önem arz etmektedir. Siber saldırıların üretebileceği sorunlar, akademik literatürde altı farklı başlık altında gruplandırılarak incelenmektedir.

1.7.1. Finansal Kayıplar

Nesnelerin İnterneti siber saldırıları bireyler, işletmeler ve hatta ülkeler için önemli mali kayıplara yol açabilir. Örneğin, Nesnelerin İnterneti cihazlarını hedef alan fidye yazılımı saldırıları, saldırganların güvenliği ihlal edilmiş cihazlara veya verilere erişimi geri yüklemek için ödeme talep ettiği haraç girişimleriyle sonuçlanabilmektedir (Rossini ve ark., 2015). Ayrıca siber saldırılara maruz kalan işletmeler, hizmetlerin kesintiye uğraması, müşteri güveninin kaybedilmesi ve Nesnelerin İnterneti güvenlik ihlalleriyle ilişkili olası yasal sonuçlar nedeniyle mali kayıplara maruz kalabilmektedir.

1.7.2. Veri İhlalleri ve Gizlilik Endişeleri

Nesnelerin İnterneti cihazları, kişisel bilgiler ve hassas iş verileri dahil olmak üzere çok büyük miktarda veri toplar ve iletir. Başarılı bir Nesnelerin İnterneti siber saldırısı, veri ihlallerine yol açarak bu bilgileri yetkisiz erişime veya hırsızlığa maruz bırakabilir. Bu tür ihlallerin sonucunda gerçekleşecek yetkisiz erişim yahut veri çalıntı/sızıntılarının; hassas nitelikte kişisel verilerin istenmeyen kişilerin eline geçmesi, dolandırıcılık, itibar zedelenmesi ve mahremiyet düzenlemelerinin ihlali gibi ciddi sonuçları olabilmektedir. Mahremiyetin ve kişisel bilgiler üzerindeki kontrolün kaybı, bireyler ve kuruluşlar üzerinde uzun süreli etkilere sahip olabilir.

1.7.3. Hizmet ve Operasyonların Aksaması

Nesnelerin İnterneti siber saldırıları, temel hizmetlerin ve operasyonların kesintiye uğramasına veya bozulmasına neden olabilir. Örneğin, akıllı şebekeleri, sağlık sistemlerini veya ulaşım ağlarını hedef alan saldırılar elektrik kesintilerine, sağlık hizmetlerinde aksamalara ve hatta kazalara neden olabilmektedir (Stellios ve ark., 2018). Sanayi sektöründe bağlantılı üretim sistemlerine yönelik saldırılar, üretimi durdurarak önemli mali kayıplara ve tedarik zinciri kesintilerine yol açabilir.

1.7.4. Güvenlik ve Fiziksel Zarar

İnternete bağlı otomobiller veya tıbbi cihazlar gibi belirli bağlamlarda Nesnelerin İnterneti siber saldırıları, fiziksel güvenlik ve sağlık için riskler oluşturabilmektedir. Örneğin, internete bağlı bir aracın güvenlik açıklarını kullanarak aracın fren sisteminin işlevselliğini tehlikeye atmak veya tıbbi bir cihazın ayarlarını değiştirmek, insan yaşamını tehdit eden sonuçlara yol sebebiyet verebilecektir. Aynı şekilde, internet bağlantısını haiz güvenlik kameraları gibi Nesnelerin İnterneti uygulamalarının siber saldırılara maruz kalması, bu cihazların sağladığı güvenlik konfor alanının ihlali anlamına geleceğinden; kişilerin veya ilgili teknolojinin

kullanıldığı güvenli alana ihtiyaç duyan meskenlerin güvenliğini tehdit edici niteliğe sahiptir.

1.7.5. Kritik Altyapıda Hasar

Gündelik toplumsal hayatın sağlıklı devamını sağlamak adına temel yapıtaşlarını oluşturan elektrik şebekeleri, yer altı atık sistemleri, su arıtma tesisleri veya ulaşım sistemleri dahil olmak üzere kritik altyapıyı hedef alan Nesnelerin İnterneti siber saldırılarının toplum üzerinde kademeli etkileri olabilir (Lee, 2020). Bu temel hizmetlerdeki uzun süreli kesintiler; birincil seviyede önemli olan insan sağlığına zarar verebilir, çevredeki diğer canlıların yaşamını devam ettirmesine engel olabilir, önemli ekonomik kayıplara ve kamu güvenliği açısından potansiyel risklere yol açabilir.

1.7.6. Güven ve İtibar Kaybı

Nesnelerin İnterneti siber saldırıları cihazlara, hizmetlere ve markalara olan güveni aşındırabilir. Örneğin, yakın zamanda gerçekleşen bir siber saldırı olayında, bebek telsizleri üreticisinin yaşadığı saldırı neticesinde şirketin marketteki payında büyük hacimli düşüşler meydana gelmiştir. Müşteriler, Nesnelerin İnterneti ürün ve hizmetlerine olan güvenlerini kaybederek benimseme oranlarının düşmesine ve işletmelerin gelirlerinin düşmesine neden olabilmektedir. Önemli bir siber saldırıdan sonra güveni yeniden oluşturmak, güvenlik önlemlerine ve iletişim çabalarına önemli yatırımlar gerektirerek zor olabilir.

1.8. Nesnelerin İnterneti Güvenliği için Önleyici Tedbirler ve En İyi Uygulamalar

Nesnelerin İnterneti ekosisteminde sağlam ve sürdürülebilir güvenliğin sağlanması, birbirine bağlı cihazları, ağları ve ürettikleri verileri korumak için kritik

öneme sahiptir. Kuruluşlar, önleyici tedbirleri uygulayarak ve en iyi uygulamaları takip ederek Nesnelerin İnterneti siber saldırı riskini önemli ölçüde azaltabilir.

1.8.1 Güvenli Cihaz Tasarımı

Güvenlik, başından itibaren Nesnelerin İnterneti cihaz tasarımının ayrılmaz bir parçası olmalıdır. Bu, güçlü kimlik doğrulama mekanizmalarının uygulanmasını, güvenli iletişim protokollerini ve hassas verilerin şifrelenmesini içerir. Varsayılan kimlik bilgileri benzersiz ve güçlü olmalı ve cihazlar düzenli güvenlik güncellemelerini ve yamalarını alma özelliğine sahip olmalıdır (Li, 2019).

1.8.2 Düzenli Yazılım Güncellemeleri

Nesnelerin İnterneti cihazlarını ve ilişkili yazılımları güncel tutmak, bilinen güvenlik açıklarını ele almak ve ortaya çıkan tehditlere karşı korunmak için çok önemlidir. Kuruluşlar, cihaz üreticileri ve yazılım satıcıları tarafından sağlanan güvenlik yamalarını ve güncellemeleri düzenli olarak izlemek ve uygulamak için süreçler oluşturmalıdır.

1.8.3 Güçlü Kimlik Doğrulama ve Erişim Kontrolleri

Çok faktörlü kimlik doğrulama gibi sağlam kimlik doğrulama mekanizmalarının uygulanması, yalnızca yetkili kişilerin Nesnelerin İnterneti cihazlarına ve sistemlerine erişebilmesini ve bunları kontrol edebilmesini sağlamaya yardımcı olur (Llopis-Albert, 2021). Erişim kontrolleri, her kullanıcı veya cihaz için gereken en az ayrıcalığı verecek şekilde uygun şekilde yapılandırılmalıdır.

1.8.4 Ağ Segmentasyonu

Nesnelerin İnterneti cihazlarını ayrı ağlara veya alt ağlara bölmek, güvenliği ihlal edilmiş bir cihazın potansiyel etkisini sınırlayabilir ve ağ içinde yanal hareketi önleyebilir. Bu ayrım, saldırıların kontrol altına alınmasına yardımcı olur ve kritik sistemlere ve verilere yetkisiz erişim riskini azaltır.

1.8.5 Şifreleme ve Veri Koruma

Nesnelerin İnterneti cihazları hassas veriler üretip ileterek, bu bilgilerin gizliliğini ve bütünlüğünü korumak için şifrelemeyi zorunlu hale getirir (Llopis-Albert, 2021). Veriler, yetkisiz erişimi veya manipülasyonu önlemek için hem aktarılırken hem de dururken şifrelenmelidir.

1.8.6 Güçlü Satıcı ve Tedarik Zinciri Yönetimi

Kuruluşlar, Nesnelerin İnterneti cihaz satıcılarını seçerken kapsamlı bir durum tespiti yapmalı ve tedarik zinciri boyunca uygun güvenlik uygulamalarının izlendiğinden emin olmalıdır (Tawalbeh ve ark., 2020). Satıcıların ve tedarikçilerin düzenli denetimleri ve güvenlik değerlendirmeleri, potansiyel risklerin ve güvenlik açıklarının belirlenmesine yardımcı olabilir.

1.8.7 Güvenlik İzleme ve Olay Müdahalesi

Nesnelerin İnterneti cihazlarının, ağlarının ve arka uç sistemlerinin sürekli izlenmesini uygulamak, anormalliklerin ve potansiyel güvenlik olaylarının erken tespit edilmesini sağlar (Weyer, vd., 2016). Bir güvenlik ihlali durumunda atılması gereken adımları özetleyen bir olay müdahale planı oluşturmak, kuruluşların etkiyi azaltmak için hızlı ve etkili bir şekilde yanıt vermesine yardımcı olur.

1.9. Bağlantılı Araçlara Yapılan Siber Saldırılar

1.9.1 Amaç

Nesnelerin İnterneti aracılığıyla bağlantılı araçlara yönelik siber saldırılar, internete bağlı diğer paydaşlar ile kurulan iletişimin kararlılığını, sağlamlığını, gerçek zamanlılığını, güvenliğini ve gizliliğini azaltan ve yeteneğini kaybetmesine neden olan karıştırma, parazit oluşturma, gizli dinleme ve benzer diğer farklı yöntemlerle çeşitli yönlerde olabilmekte, çok çeşitli amaçlara hizmet edebilmekte, bağlantılı araçların olması gerektiği şekilde hizmetler sunma yeteneğinin kaybolmasına ve hatta ciddi kazalara neden olabilmektedir (Sun ve ark., 2015). İlk amaç olarak, saldırganlar potansiyel sürüş tehlikeleri yaratarak bir aracın işlevselliğine zarar vermeye çalışabilmektedir. Kötü niyetli kişiler veya organizasyonlar, araçlara yerleştirilmiş Nesnelerin İnterneti cihazlarını tehlikeye atabilirlerse sürücülerin, yolcuların ve çevredekilerin hayatlarını tehlikeye atabilirler. İkincisi, bilgisayar korsanları dahili ağlarına giriş elde etmek için sıklıkla otomobilleri hedefler. Potansiyel olarak güvenliği ihlal edilmiş Nesnelerin İnterneti cihazları, bir saldırganın kapıların kilidini açmasına, motoru çalıştırmasına veya önceden sürücü tarafından kullanılan GPS koordinatlarını kurcalamasına izin verebilir (Paritala, Manchikatla ve Yarlagadda, 2017). Araç hırsızlığı, yasa dışı casusluk ve hatta terör eylemleri, bu tür yetkisiz girişlerle kolaylaştırılabilir. Son olarak, otomotiv sektörü, özel bilgilere, finansal belgelere veya fikri mülkiyete erişim elde etmek isteyen siber suçlular için potansiyel bir hedeftir. Bu yüksek nitelikte kişisel bilgiler, tümü karanlık ağdan satın alınabilen kimlik hırsızlığı, dolandırıcılık ve iş casusluğu için oldukça değerli olabilmektedir. Siber saldırılar, otomobil sektörünü çapında ses getirmek, araç firmalarının üretimini durdurmak veya tüketici güvenini sarsmak amacıyla sabotaj veya kötü niyetle de motive edilebilmektedir. Son olarak, bilgisayar korsanları, araç sistemlerini şifreleyip otomobilleri kullanılmaz hale getirdikten sonra bu şifreleri çözmek için ödeme talep etme yolunu, yani fidye yazılımlarını kullanmakta ve böylece aslında teorik olarak çalışan araçları ellerinde rehin olarak tutabilmektedir (Paritala, Manchikatla ve Yarlagadda, 2017).

1.9.2 Kapsam

Otomobillerdeki pek çok farklı işleyiş, sistem ve sistemlere ait parça, Nesnelerin İnterneti üzerindeki zafiyetleri kullanan bilgisayar korsanları tarafından hedef alınabilir. Veri paylaşımı ve iletişim için Nesnelerin İnterneti olgusundan çerçevelendiği için telematik ve bağlantılı araçlar birincil hedeflerdir. Bu sistemlerdeki güvenlik açıkları, siber suçlular tarafından yetkisiz erişim elde etmek veya aracın özelliklerini değiştirmek için kullanılabilmektedir. Öte taraftan niyetinden bağımsız siber saldırı icra eden kimseler, otomobillerdeki kullanıcı arayüzlerini, bilgi-eğlence ve çoklu ortam sistemlerini; bu sistemler kullanışlılığı artırmak adına üreticiler tarafından internete veya internet bağlantısı sahibi mobil cihazlara doğrudan veya dolaylı bağlı olacak şekilde üretildiği için hedef alabilmektedir. Yolcuların kendilerine eğlence, navigasyon ve bağlantı sağlayan bu cihazlara internet aracılığı ile zoraki erişimi, siber suçlular için bir fırsat penceresi açmaktadır denilebilir. Nesnelerin İnterneti ekosistemi, araç ticaretinin varlığını sürdürdüğü bayiler, tamirciler ve teknisyenler tarafından kullanılan teşhis ve bakım ekipmanlarını da içermektedir. Bu ekipmanlar, çoğunlukla araçların bütünlüğünü ve güvenliğini sayısal olarak kontrol eden sensör ve okuyuculardan veri toplayarak bu verileri insanların anlayabileceği halde, tercihen taşınabilir bir arayüz üzerinden sunan ve ekseriyetle teşhis aşamasında kullanılan donanım ve yazılım çözümleridir. Bu kullanılan ekipmanların güvenliğinin ihlal edilmesi durumunda, bilgisayar korsanlarının servis veya onarım yapılırken araç sistemlerine erişmesi ve muhtemelen bu sistemleri manipüle etmesine açık kapı bırakılabilmektedir.

Nesnelerin İnterneti teknolojilerine dayanmaları nedeniyle otonom ve yarı otonom araçlar da keza bilgisayar korsanları için kolay hedeflerdir. Otonom araçların dayandığı omurga iletişimi odak noktasına koymaktadır, bu durum yine bahsi geçen şekilde saldırı yüzey alanını genişleterek bir diğer zafiyet alanı yaratmaktadır. Bilgisayar korsanlarının otonom sürüş sistemlerindeki zayıflıklardan yararlanma yoluyla araçların kısmi veya bütüncül kontrolünü ele geçirme veya operasyonlarını kesintiye uğratma potansiyeli, önemli güvenlik endişeleri oluşturmaktadır.

Otomobil şirketleri, çoğunlukla tedarik zinciri kurarak üretim süreçlerini desteklemektedirler. Bu durumda, şirketlerin alt yüklenici diğer şirketler üzerinden gerçekleştirdiği üretimlerin de kayda değer seviyede önemli olduğundan bahsedilebilir. Dışarıdan sağlanan hizmetlerin bir alt başlığı da yazılım ve iletişim altyapısının kurulmasında gerekli olan çözümlerdir. Kusurlu donanım veya yazılım, bitmiş ürünün güvenliğini tehlikeye atabileceğinden, bir araca tedarik zinciri yoluyla dahil edilebilecek güvenlik kusurları da siber güvenlik zafiyetlerinin kapsamı dahilindedir.

1.9.3 Örnek Olaylar

Otomobil sektöründe siber güvenlik olaylarının şeceresi, dijitalleşmenin ilk başladığı yıllardan itibaren tutulamasa da araştırmalara göre elde edilen veriler, siber güvenlik olaylarının sayılarının yıllar geçtikçe arttığını göstermektedir. Bu kapsamda, sektör nezdinde yankı uyandıran siber güvenlik olaylarının dikkat çekenleri paylaşılarak öngörü oluşturulması sağlanmalıdır.

1.9.3.1 Jeep Cherokee (2015) Örneği

2015'te siber güvenlik alanında çalışmalar yürüten araştırmacılar Charlie Miller ve Chris Vasalek, ABD pazarında oldukça popüler bir araç olan ve başarılı satış rakamları yakalayan Jeep Cherokee üzerinde temel bir kusurdan yararlanmanın ne kadar kolay olacağını gösterdiler ve bu da onların aracın kontrolünü uzaktan ele geçirmelerine olanak sağladı. Bilgisayar korsanları, Şekil 3.4'te gösterimi sağlanan ana ünitede bilgi eğlence sistemi tedarikçisi Harman Kardon tarafından üretilen bir güvenlik açığından yararlanarak (Miller, 2019) önce araca yetkisiz erişim sağladı, ardından CAN mesajlarının gönderiminin sağlanması için bir gateway çipini baştan programlayarak aracın gaz pedalını, frenlerini ve vites kutusunu kontrol edebildiler. Bu sorunun bir sonucu olarak, güvenlik yamalarının yüklenebilmesi için 1,4 milyon otomobilin geri çağrılması gerekti.

Şekil 1.5. 2014 model Jeep Cherokee aracın istismarına neden olan bilgi eğlence ekranı.

1.9.3.2 Tesla Model S (2016) Örneği

2016 yılında, Tencent Keen Security Lab çalışanlarından oluşan bir araştırma ekibi Tesla Model S'yi hem Park Etme hem de Sürüş modunda bir uzaktan erişim yöntemi izleyip kırarak farklı sistemlerini uzaktan manipüle etmelerinin yolunu açmıştır. Yürütülen bu uzaktan saldırı, karmaşık bir güvenlik açıkları zinciri kullanmıştır. Araştırmacılar, kablosuz ağ üzerinden (Wi-Fi/Hücresel) araca erişim sağlayabileceklerini, IC, CID ve Ağ Geçidi gibi birçok araç içi sistemi tehlikeye atabileceklerini ve ardından CAN Veriyoluna kötü amaçlı CAN mesajları ekleyebileceklerini kanıtladılar. Bilgisayar korsanları, yerleşik tarayıcısındaki Şekil 3.5'te de gösterilen açıklardan yararlanarak aracın kapılarını, ekranlarını ve diğer özelliklerini kontrol edebilmiştir. Zafiyete tabi aracın üretici şirketi olan Tesla Inc., sorunları gidermek için aygıt yazılımını on gün içerisinde yama yayınlamak zorunda kalmıştır (Sen ve ark., 2017).

```
void JSArray::sort(ExecState* exec, JSValue compareFunction,
CallType callType, const CallData& callData)
{
    checkConsistency();
    ArrayStorage* storage = m storage;
    // ......
    // Copy the values back into m_storage.
    AVLTree<AVLTreeAbstractorForArrayCompare, 44>::Iterator
iter;
    iter.start iter least(tree);
    JSGlobalData& globalData = exec->globalData();
    for (unsigned i = 0; i < numDefined; ++i) {
        storage->m vector[i].set(globalData, this,
tree.abstractor().m_nodes[*iter].value);
        ++iter;
    }
    ......
}
```

Şekil 1.6. Tesla Model S marka aracın yerleşik tarayıcısındaki açıkları oluşturan fonksiyon.

1.9.3.3 Ransomware (Fidye Yazılımı) Saldırıları

Son yıllarda özellikle otomotiv endüstrisini hedef alan fidye yazılımı saldırıları gerçekleşmiştir. Bu saldırıların kapsamı genellikle otomobil üreticilerin yerel kaynakları ve hedefi genellikle hassas bilgiler veya fidye ödenene kadar şifrelenecek sistemlerdir. Bu tarz saldırıların olası sonuçları, ancak üretim gecikmeleri, bilgi sızıntıları ve parasal kayıplar gibi genellikle maddi yönden etkileyen noktalar olarak kalmıştır. Ancak otomobillere yapılacak olan saldırılarda farklı olan bir nokta vardır, birçok kişi muhtemelen kötü amaçlı yazılımın farkındadır, ancak en tehlikeli biçimi olan, yani bireylere fiziksel zarar verme, hatta ölüme neden olan kötü amaçlı yazılımın farkında olmayabilirler (Brody ve ark., 2018) ve otomobillere yapılacak olan saldırılar tam da bu kapsamda değerlendirilebilir. Ancak, otomobillerin tamamen kilitlenerek aracın sahibinden para istenmesi, şu ana kadar çok fazla örneği ile karşılaşılmamış ve raporlanmamış bir saldırı türü olarak durmaktadır. Her ne kadar şimdiye kadar çok fazla bir örnekle rastlanmasa da fidye yazılımı geliştiricilerinin otomobilleri hedeflemesi kaçınılmaz görünmektedir ve yine de ilgili riskin sistematik olarak değerlendirilmesine ilişkin araştırma eksikliği mevcuttur. Bu farkındalıkların ışığında, kötü amaçlı yazılım geliştiricileri bunları istismar etmeye çalışmadan önce, modern otomobillerdeki saldırı vektörlerini tanımamız ve ortadan kaldırmamız zorunludur (Bajpai ve ark., 2020).

1.9.3.4 Altyapı Saldırıları

Giderek daha fazla araç altyapı sistemlerine bağlandıkça, araçlar ile altyapı arasındaki iletişim kanallarına yönelik saldırı potansiyeli oluşmaktadır. Trafik akışının kesintiye uğraması, trafik sinyallerinin tahrif edilmesi ve kavşak güvenliğinin tehlikeye atılması, bu tür saldırıların olası sonuçlarıdır.

Trafik altyapısında ne gibi zafiyetler görülebildiğini göstermek adına, Michigan Üniversitesi'nden Alex Halderman liderliğindeki bir grup güvenlik araştırmacısı, Amerika Birleşik Devletlerindeki Michigan şehrinde yüzden fazla trafik ışığı sinyalini kontrol etmek için yalnızca bir dizüstü bilgisayar ve hazır bir radyo vericisi kullanmayı nasıl başardıklarına dair bir çalışma yayınlamıştır (Buchanan, 2014). Çalışma sürecinde etik olabilmek ve can güvenliği riskini barındıran sağlıksız trafik akışının önüne geçmek adına ilgili kurumlardan alınan izinler sonrasında yürütülen ve trafikteki sürücüler için herhangi bir tehlike gerçekleşmemesini garanti altına alan çalışmada amaç, yaygın olarak satılan tüketim malzemeleri ile trafik altyapısını ele geçirmenin kolay olabileceğinin gösterilmesidir.

Gerçekleştirilen saldırının anlaşılabilmesi adına, öncelikle ülkede hüküm süren teknik trafik iletişim altyapısının detaylarının tespiti yapılmıştır. ABD'de, trafik ışığı denetleyicileri tarafından kullanılan radyo frekansı; tipik olarak endüstriyel, bilimsel ve tıbbi kullanımların bandı olan 900 MHz veya 5,8 GHz'dir. Araştırmacıların tespit ettiği güvenlik açığı, şifrelenmemiş radyo sinyallerinin kullanıldığı zayıf kablosuz güvenlik olmuştur. Bu zafiyet, olası davetsiz misafirlerin, trafik ışığı denetleyicilerine giden ve bu denetleyicilerden kablosuz radyo sinyalleri üzerinden geçen ağ trafiğini gizlice dinlemelerine olanak tanıdığı anlamına gelmektedir. Bu şekilde, kullanılan kullanıcı adlarını ve parolaları görmek mümkün olmuş ve kullanılan kullanıcı adlarının ve parolaların, fabrika varsayılanlarına ayarlı olduğu ve internette basit aramalar neticesinde bulunabileceği görülmüştür. Bu duruma ek olarak, denetleyicilerin hata ayıklama için fiziksel olarak erişilebilen ve kolayca ele geçirilebilen fiziksel bir bağlantı noktasına sahip olduğu tespit edilmiş,

bu yolla trafik ışıklarının kontrolü sağlanmış ve trafik ışıklarına ele geçiren kişinin istediği durumu atamak mümkün hale gelmiştir.

1.10. Çalışmanın Amacı

Verilen bilgilerin ışığında, otomobillerin geçmişten günümüze gelen süreç içerisinde dijitalleşme olgusunu hızlıca benimsediği söylenebilir. Bu gerçekliğe paralel ancak bu gerçeklikten görece bağımsız şekilde, internet altyapısının yaygınlaşması, internete bağlanabilen cihaz sayısındaki artış ve internet erişim hızlarının artması ile birlikte, son kullanıcıların talepleri doğrultusunda farklı endüstrilerde ve kullanım alanlarında yer alan cihazların internete bağlı olarak kişiselleştirilebilmesini ve kontrol edilmesini ifade eden Nesnelerin İnterneti olgusunun ortaya çıktığı da görülebilmektedir.

Son dönemde, Nesnelerin İnterneti olgusunun otomobil sektörü ile iç içe geçmesi neticesinde, internet aracılığı ile muhtelif son kullanıcı faydaları üreten akıllı araçlar yaklaşımı karşımıza çıkmaktadır. Araçlarda artan bağlantı özellikleri, araçların, araç kullanıcısı olan kişiler haricinde kimseler tarafından erişilebilir olmasının da önünü açmaktadır. Saldırı yüzeyi olarak adlandırılan bu sanal alandaki genişleme, bağlantıya sahip otomobillerde, yani akıllı araçlarda, başta kullanıcıların can güvenliği olmak üzere muhtelif sorunlara neden olabilecektir. Bu durumun önüne geçilmesi adına, sorunun teşhisi, tasnifi ve çözümüne dair adımlar atılmalıdır.

Çalışmanın bu kısmına kadar olan bölümünde, ilkin otomobillerin tarihinden yola çıkılarak geleceğe dair bir öngörü sunulması amaçlanmıştır. Bu kapsamda, gelecek süreçte otomobillerin sayısal tabanlı özellik kümelerinin genişleyeceği tahmininde bulunulmuştur. Nesnelerin İnterneti olgusunun tanımlanması, çalışmanın akışında sıradaki amacı betimler. Bu iki tanımsal yaklaşımdan hemen sonra, otomobillerin artan bağlantı arayışı ile birlikte artık “akıllı araçlar” statüsünde değerlendirilebilmesi amaçlanmaktadır.

Akıllı araçlara dair tanımlamalar ve durum tespitleri, kendi içinde sıradaki durum tespit olan akıllı araçların da saldırı kapsamına girebileceği fikrini uyandırmayı amaçlamaktadır. Saldırı olgusunun daha derin şekilde irdelenebilmesi ve saldırı olgusuna dair çözüm önerilerinin belirlenebilmesi adına, saldırıların tipleri, nedenleri, etkileri ve önleyici faktörlere değinilmiştir. Ayrıca bu aşamada, akıllı araçlar nezdinde gerçekleştirilen saldırıların bir çerçevesi çizilmeye çalışılmış, doğrudan akıllı araçlara gerçekleşen saldırıların örneklendirilmesi sağlanmaya çalışılmıştır.

Çalışmanın ilerleyen kısmında, akıllı araçlar üzerinde gerçekleştirilen siber saldırıların önlenmesi adına akademik eksende yürütülen araştırmalar ve adli bilişimin iyi uygulamalarının da müdahil olduğu bir sentez sürecinin neticesinde damıtılan yeni bir model önerisi ile birlikte çalışma esnasında elde edilen fikir ve üretilen çıktıların tartışılmasına dair hazırlanan zemine dair bilgi paylaşımı gerçekleştirilecektir.

2. GEREÇ VE YÖNTEM

Bağlantılı araçlarda kullanılan Nesnelerin İnterneti uygulamalarında rastlanan, **Tartışma** ve **Bulgular** alt başlıklarında detayları okuyucu ile paylaşılan ve ilgili noktaları aktarılan siber saldırıların önlenmesi noktasında kullanılabilecek kapsayıcı bir çerçeve önerisinin ihtiyacı açıktır, bu kapsamda adli bilişim tabanında elde edilen dersler ile birlikte değerlendirilerek güncel uygulamaların üstüne çıkması beklenen bir çerçeve bu kısımda oluşturulacaktır.

2.1. Yöntem

Mevcut araştırma, sistematik titizlik ve kapsamlılık ile şekillendirilen ve mevzubahis araştırma alanının detaylı bir şekilde incelenmesine yardımcı olan metodolojik bir çerçeve kullanmaktadır. İlk aşama, konu ile ilgili akademik literatürün seçici ve ayrıntılı bir tespiti, incelemesi ve eleştirel değerlendirmesi ile kesin araştırma hedeflerine ulaşılması şeklinde aktarılabilir. Bu aşama, çalışmayı daha geniş akademik söylem bağlamı içine etkili bir şekilde yerleştiren temel dayanağı oluşturmaktadır. Sonraki aşamayı, çağdaş *iyi uygulama* çerçevelerinin, yöntemsel kontrol listelerinin ve mevcutta sektörde gerçekleştirilen uygulamaların özetlenmesi ve paradigmaların yöntemli bir araştırması oluşturmaktadır. Bu çok yönlü bulguların tespiti, takibi, tasnifi, incelenmesi ve birleştirilmesi neticesinde; yaygın olarak kullanılan iyi uygulamaların ve probleme yaklaşımların panoramik bir anlayışına ulaşılmakta ve böylece sonraki analizler için sağlam bir temel sağlanmaktadır.

Bu yöntemsel çerçevenin kendine özgü boyutu, bağlantılı araçlar endüstri ekosisteminde faaliyet gösteren paydaşların karmaşık rollerine, ilişkilerine ve sektör katkılarına yönelik yapılan sorgulamadır. Burada gerçekleştirilen belirleyici ayırt etme yaklaşımı, farklı bakış açılarının, örgütsel rollerin ve alan uzmanlığının sentezini gerektirmektedir. Çalışma, bu çok çeşitli bakış açılarını bütünleştirerek,

endüstri fotoğrafını karakterize eden karmaşık karşılıklı ilişkileri tespit etmeye, anlamaya, bir manada çözmeye ve bu çözümleme neticesinde bu ilişkileri makul düzlemde bağdaştırmaya çalışmaktadır.

Netice olarak çalışma akışının bütününde; kapsamlı bir literatür taraması, daha önceden varlığını ve uygulanabilirliğini sağlamlaştırmış yöntemsel uygulamalar, çerçeve ve temellerin makul bir değerlendirmesi ve sınıflandırılan paydaşlar tecrübelerinin bir sentezini içeren bileşik metodoloji, net sonuçların ve makul tavsiyelerin birleşimini doğrulamak için bir araya gelmektedir. Bütüncül ve çok yönlü yaklaşım, araştırma alanının derinlemesine anlaşılmasını sağlamak ve mevcut bilgi birikimine anlayışlı katkılar sağlamak için tasarlanmıştır.

2.2. Önerilen Çerçeve

Günümüz dünyasında, örnekleri aktarılan senaryolar kapsamında, otomobillerin internet bağlantısı sahipliği git gide artmakta ve çok da uzak olmayan gelecekte, araçların internet bağlantısının olmadan kullanılabilirlik özelliklerinin büyük oranda tırpanlanacağı düşüncesi oldukça güçlü bir temsiliyete sahiptir. Bilhassa son 30 yılda yaşanan gelişmeler ile birlikte, araçlar önce elektronik altyapısında ciddi ilerlemeler kaydetmiş, bu elektronik ilerlemeleri yalnızca araç içinde ikame bilişim çözümleri izlemiş ve hemen ardından iletişim teknolojilerindeki gelişmeler ile birlikte araçlar artık bir bilişim altyapısı ile bütünleşik bir iletişim altyapısı sahibi olmuşlardır.

Bugün dünya otomobil pazarında satılan birçok farklı tipte, farklı ebatta ve farklı amaçlara hizmet eden otomobilde, bu durumun izleri görülebilmektedir. GPS sisteminden destek alan araca bütünleşik navigasyon sistemleri, acil durumlarda sürücülerin otoriteler ile anında irtibata geçmesine ve acil yardım alabilmesine yardımcı olan SOS sistemleri artık neredeyse standart hale gelmiştir. Otonom sürüşün hız sabitleme ile başlayan macerası, şeritlerin takip edilmesi, kör noktalarda bulunan araçların tespiti ve yazılım sistemlerinin direksiyona müdahalesi ile birlikte

tam otonom sürüşe doğru kararlılıkla ilerlemektedir. Avrupa'da araçları altyapı ile bağlama ve bu yolla emisyonları ve trafiği hafifletme fikri gündemde iken, ABD sınırlarında araçların uzaktan yazılım güncellemeleri alarak servise gitmesi yükümlülüğünden kurtulması gibi gelişmeler de izlenmektedir.

Bu kadar bağlanılabilirlik özelliği ile iç içe girmiş bir dünyada, artık bir yüzü internete dönmüş olan otomobillerin siber saldırılara maruz kaldığına dair malumat ortadadır. Çok geniş sayıda insanın ulaşımında temel gereç olan otomobillerin, siber saldırılar vasıtasıyla kullanılamaz hale gelmesi veya amacı dışında kullanılması, doğal olarak insan hayatını tehlikeye atabileceğinden ötürü önem arz etmektedir. Bu kapsamda, araçlarda gerçekleşmesi muhtemel siber güvenlik olaylarının anlaşılması, önlenebilmesi; eğer siber güvenlik olayları gerçekleşmiş ise de bu konuda çıkarılan dersler ile üretici ve kullanıcıların gerekli aksiyonları alabilmesi adına, bütüncül bir çerçevenin ihtiyacı hissedilmektedir.

Önerilen çerçeve, otomobil sektöründe bir çatı güvenlik kuruluşunun, üreticilerin inisiyatifi doğrultusunda kurulması ile temellendirilir. Bu çatı güvenlik kuruluşu, üreticilerin ticari şekilde paydaşlık yoluyla kurabileceği bir şirket olabileceği gibi, şirketlerden aldığı destek ve teşvikler yoluyla hayatta kalan bir dernek veya vakıf yapısı şeklinde örgütlenebilir. Ancak, koşullar ne olursa olsun, şirket içinde gerekli kontrol mekanizması sağlanarak denetim şeffaflığı yaratılmalı ve bu şirket nezdinde hiçbir paydaşın kafasında soru işareti oluşmamalıdır. Ayrıca bu çatı kuruluşun, gerektiğinde halka açık yayınlar yaparak kamuoyunu bilinçlendirmesi ve bilgilendirmesi yeteneğine sahip olması göz ardı edilmemelidir.

Çatı kuruluş, her ne kadar siber güvenlik olaylarının önlemi, tespiti ve idaresi konusunda gerekli, otomotiv sektörüne özgü çerçeveyi çizecek olsa da, ilgili kurum ve kuruluşlar olmadan bu çerçevenin çizilmesi oldukça hatalı ve eksik sonuçlara sebebiyet verebilir. Netice olarak çatı siber güvenlik olaylarını önleme kuruluşu, sürecin en başından itibaren desteklerine ve tecrübelerine başvurabileceği ilgili kuruluşlar ile dirsek temasında kalmalı, bu ilgili kurum ve kuruluşların, çatı kuruluşu hakkında gerekli bilgilendirmeye sahip olarak desteklerini esirgememeleri

sağlanmalıdır. Örnekleri şekilde belirtilen (NIST, ISO ve Metasploit) ilgili kuruluşların, daha önce siber güvenlik ile alakalı ortaya koyduğu çalışmalar, önerdikleri çerçeveler, sahip oldukları siber saldırı bilgi envanterleri; otomotiv sektörüne özgü çatı kuruluşun bilgi omurgasının oluşturulmasında oldukça kapsamlı bir yer edinecektir.

Kurulacak çatı kuruluşun bir diğer görevi de olası siber güvenlik zafiyetlerinin önüne geçmek adına kuruluşlara yol haritası göstermek ve bu yol haritasını detaylandırmak olacaktır. Bu noktada kuruluş, kendi paydaşı üreticiler ile irtibata geçerek arabalarda var olan ve siber zafiyete açık parçaların listesini tek tek yayımlayıp belirterek, tüm üreticilerin ve ilgili tedarikçilerin kendi risk envanterlerini buna göre güncellemesini sağlamalıdır. Elbette bu çalışmanın kapsamı risk faktörlerine göre genişletilmelidir. Örneğin, otomobillerin ABS kontrol modülleri yalnızca ECU üzerinden araç bilişim omurgasına bağlıyken, bu modüle dışarıdan siber saldırı yoluyla erişebilmek adına zafiyetin türetilmesi gerekmektedir, dolayısıyla önce ECU birincil seviyede ele geçirilmesi gereken zafiyet noktasını oluşturur ancak öte taraftan araç içi eğlence modülleri ekseriyetle Wi-Fi veya Bluetooth üzerinden haberleşme sağladıkları için birinci dereceden etkiye açıktır. Bu parametrelere göre üreticiler bir risk çalışması yürütmesi ve bunu da ilgili çatı kuruluşuna belgelendirdikten sonra ellerindeki riskleri tespit edip, detaylandırıp raporlamalıdır.

Bu noktada çerçevede irdelenmesi gereken yol ayrımı, siber olayların yaşanması veya yaşanmaması üzerinden ele alınmalıdır. Siber olayların yaşanması, adli bilişim süreçleri ile bir bütünleşme yaklaşımı gerektirir. Korkulan siber olayların yaşanmaması ise, kendi içinde ayrı sorumlulukları beraberinde getirmektedir. Her senaryoda, çatı kuruluş süreçlerin son halkasında var olmaya devam edecektir.

Siber saldırıların yaşanmadığı senaryoda, kurum ve kuruluşlar, kendi bütçelerinden çalışanlarına ve tedarikçilerine siber güvenlik saldırıları noktasında eğitim sağlamalıdır. Eğitimlerin kapsamı, daha önce yaşanmış veya tespit edilmiş olaylar olabileceği gibi, eskiden kullanılan çerçevelerde önerilen iyi uygulamalar,

olaya maruz kalabilecek bileşenlerin analizleri, risk değerlendirmeleri, etken analizleri, sorumluluk hatırlatmaları gibi başka konular da olabilir. Ayrıca eğitimlerin hedef kitlesi, belirtilen şekilde yalnızca kişiler değil, kurumlar da olabilir. Burada eğitimlerin tüm paydaşlara açık olmasının, yapıcı geri bildirimler bırakılması adına gerekliliği unutulmamalıdır.

Eğitimlerin bir çıktısı olarak, paydaş şirketlerin iş sürekliliği planları yaratması gerekmektedir. İş sürekliliği planları, otomotiv endüstrisi gibi üretim bandının devamlı çalışması gerekliliği olan sektörlerde, işlerin aksamasına sebebiyet verebilecek dış etkenlerin detaylandırılarak bu olumsuz potansiyeldeki etkenlerin önlendiği çalışma senaryolarıdır. Bu noktada, iş sürekliliği planlarına bilişim ile alakalı eylemler de eklenmeli, şirketlerin bilişim altyapıları iş sürekliliği planları çerçevesinde güncellenmelidir. Örneğin, otomobil şirketlerinden birinin başına gelebilecek olası bir sel baskınında şirketin verilerinin bulunduğu veri merkezinin durumu ve bu veri merkezinin bu senaryoda ayakta kalabilmesi için yedeklenmesi gerekliliği bu planlarda detaylandırılmaktadır. Bu planların içine, siber olayların da, eğer mevcut değillerse eklenmesi, önerdiğimiz çerçevenin bir diğer maddesidir.

Sürekli takip, tespit, denetimler ve iyileştirme operasyonları, önerilen çerçevenin sıradaki adımının katılımcılarını oluşturur. Otomobil şirketi üzerinde gerçekleşen bilişim faaliyetleri, iletişim altyapısı, araçlar üzerinde ikame sistemlerin sağlığı gibi kritik noktalar, şirketler bünyesinde kurulması gereken bir sürekli takip operasyon merkezi tarafından otomatize edilmiş yazılımlar ile izlenmelidir. Bu yazılımların çıktıları ve diğer tüm bilişim süreçleri, şirketler bünyesinde yer alacak IT ekipleri tarafından güncel iyi uygulamalar takip edilerek denetlenmelidir. Denetim faaliyetlerinin en önemli çıktısı olan uygunsuzluk raporları, önereceğimiz çerçeve kapsamında üçüncü gözler tarafından irdelenmeli, uygunsuzluk maddeleri alışılagelmiş şekilde çözümleri için takip edilmeli ve süreçlere dair sertifikasyon sağlanmalıdır. Denetimlerden elde edilen bulgular, akışın başında yer alan kişi ve kurumlara sağlanan eğitimlere bir girdi olarak da kullanılabilmeli, bu yolla sürekli iyileştirme sağlanmalıdır. Aynı zamanda, çatı kuruluşun varlığı ile belirlenen ortak

çalışma güdüsünün sağlanabilmesi ve şeffaflığın korunabilmesi adına şirketler nezdinde yapılan denetimlerin çıktıları çatı kuruluş ile paylaşılmalıdır.

Siber saldırıların bağlantılı araçlarda yaşanmasına dair senaryolarda takip edilecek akış şeması da değişecektir. Siber saldırılar gerçekleştikten hemen sonra aksiyon alınabilmesi için standartların, dönüş noktası ve dönüş zamanı hedeflerinin açık şekilde uzlaşı yoluyla belirlenmesi ve denetleyici düzenleyici kurum tarafından ilgili paydaşlara aktarılması gerekliliği ortadadır. Siber saldırı sonrası ilk mesele, otomobillerin insan can güvenliğinden sorumlu olabileceği güdüsünden hareketle felaket kurtarma planlarının uygulamaya alınmasıdır. Otomobil sektörüne atılan bakışta, çoğunlukla siber olaylardan sonra felaket kurtarma planlarının devreye alınamadığı, devreye alınsa bile bu planların güncelleme yoksunluğu veya pratik eksikliği nedeniyle verimli olamadığı izlenimi edinilmiştir. Bu kapsamda, çerçevenin felaket kurtarma planlarına işlevsellik kazandırmak adına ekstra bir rol daha üstlenmesi gerektiği çıkarımı yapılabilir. Bu nedenle, felaket kurtarma planlarını şablonlaştırılmalı, felaket kurtarma tatbikatlarının yapılması ve bu tatbikatların gerçekçi senaryolar üzerinden gerçekleştirilmesi için üreticilere gerekli sınırlar çizilmelidir.

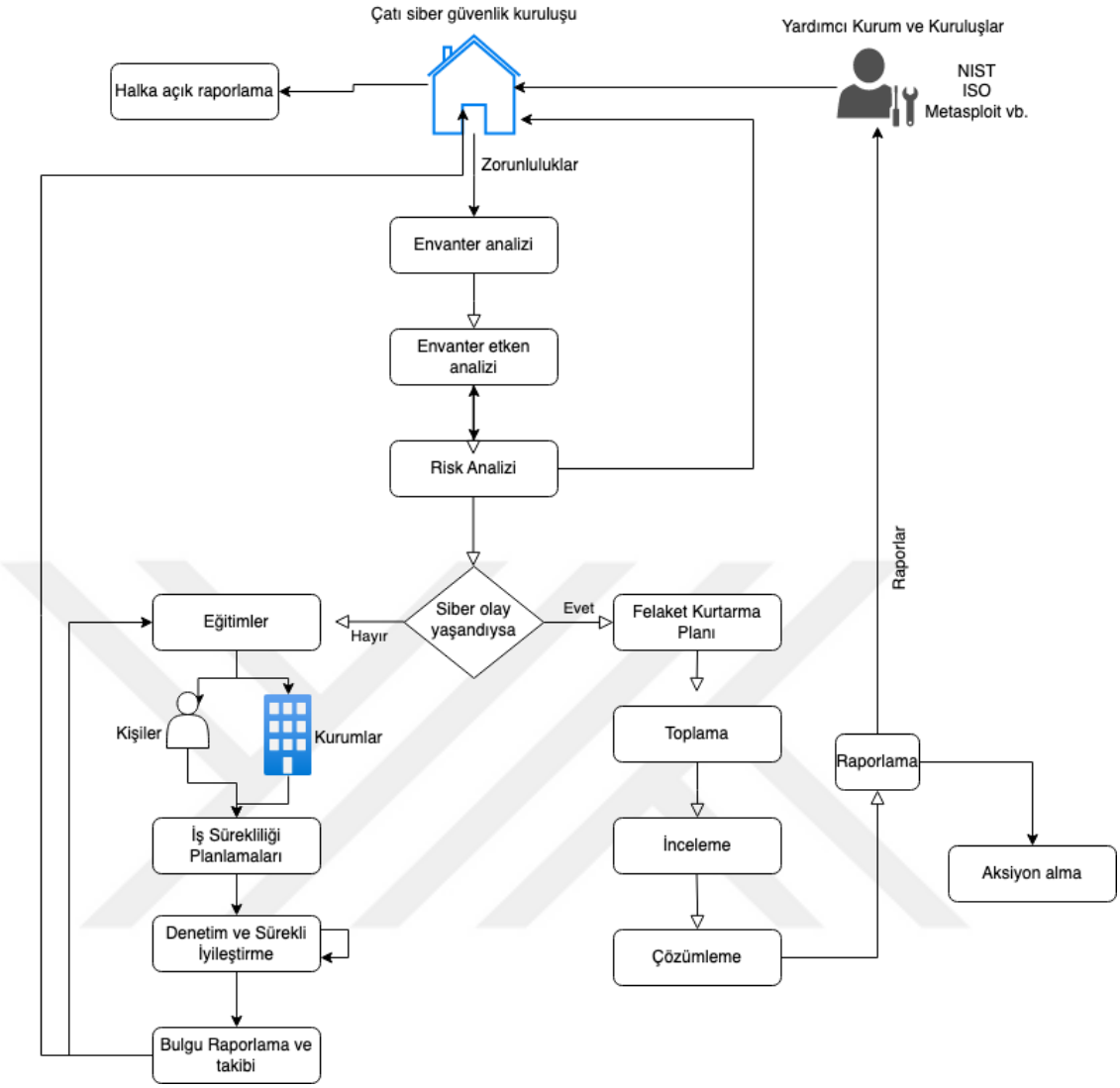
Siber saldırıların yaşanmasından ve ilgili felaket kurtarma planları başarı ile devreye alındıktan sonra, adli bilişim nezdinde irdelenmesi gereken adımlar çerçeve içinde takip edilmelidir. Şu ana kadar kullanılan iyi uygulamaların bütününde, siber güvenlik olaylarının önlenmesine dair adımlar aktarılmış, siber güvenlik olaylarının iş sürekliliği kapsamında değerlendirilmesi gerektiği belirtilmiş; ancak siber güvenlik olayları gerçekleştikten sonra bilhassa otomotiv gibi zaman-kritik sektörlerde adli bilişimin rolüne dair tanımlamalar göz ardı edilmiştir. Bu kapsamda, çerçevenin adli bilişim konusunda diğer iyi uygulamalardan farklı bir yaklaşım edindiği söylenebilir. Toplama çalışmaları, otomobillere yapılan siber saldırıların ardından otomobillerden gerekli verilerin bütünlüğünün korunarak alınabilmesi ekseninde önem arz etmektedir. Bu kapsamda, farklı üreticilere ait farklı masaüstü yazılımları olduğu ve bu yazılımların araç teşhisinde kullanıldığı bilinmektedir. İlgili çerçeve, bu araç teşhis uygulamalarına verilerin dondurularak ihraç edilmesi uygulamasını zorunlu

kılacak, bu yolla etkilenen araçlara ilk müdahale edilecek servislerde araçların hafızası sağlıklı bir biçimde edilip incelenebilecektir.

Adli bilişim nezdinde otomobillerdeki siber güvenlik olaylarının incelenmesinde ikinci adım, toplanan verilerin incelemesidir. Bu noktada, verilerin incelemesinin sınırlar içinde kalarak, Toplama aşamasında bütünlükle elde edilen verilerin varsa üzerindeki şifreleme işlemleri gibi gizlilik sağlayan donelerden arındırılmasını, elde edilen bütünlüğü korunmuş verilerin değerlendirilmesini ve yine bütünlüğünün korunarak olayla ilgili verilerin ve çıkarılmasını içermektedir. İnceleme aşaması, yine adli bilişimin temel pratiklerinden olan sterilizasyon esası göz önünde bulundurularak yapılmalı, dışarıdan müdahalelere izin verilmemeli ve bu yolla anlaşılabilirlik korunmalıdır.

Çözümleme aşaması, raporlamanın bir önceki adımı olarak oldukça önem arz etmektedir. Otomobillerde gerçekleşen siber güvenlik olaylarının "neden" gerçekleştiği durumu, şu ana kadar yalnızca siber güvenlik olaylarının gerçekleştiği otomobil şirketinin ilgisini çeken bir nokta olarak kalagelmiştir. Ancak çatı kuruluşun varlığı ile, önceden de belirtilen 5N1K soruları, endüstri ile paylaşabilmek adına sorulmalı ve detaylandırılmalıdır, bu yolla siber güvenlik olaylarının nedenleri olması gerektiği gibi ele alınacaktır.

Siber güvenlik olayını tecrübe eden şirketlerin, adli bilişim süreçleri kapsamında bir sonraki yapması gereken işlem, raporlama işlemidir. Burada çatı kuruluşun bir faydası daha görülebilir, çatı kuruluşa sunulacak raporların şablonu önceden belli olmalı; veri ihlalleri, bütünlüğün bozulması, gizliliğin ihlali, uygunluğun bozulması gibi alt başlıkların altında üretilecek raporlar bu yolla kolay anlaşılabilir ve sınıflandırılabilir olmalıdır. Olayı tecrübe eden şirket, bu rapor sonrasında gerekli aksiyonu, ki bu aksiyon geri çağırma, uzaktan müdahale, servise çağırma gibi senaryoları içerebilir, alarak siber güvenlik olayının kovuşturması sürecinde çatı kuruluşun inisiyatifini beklemelidir. Çatı kuruluşu, yaşanan olayları resmi ağızdan kamuoyu ve otoriteler ile paylaşmalı, olayların bir daha yaşanmaması için kendi örneklem kümesini güncellemeli ve çerçevesini düzenlemelidir.



Şekil 2.1. Önerilen adli bilişim odaklı siber güvenlik çerçevesi.

Özetle, güvenlik önlemlerinin bir çatı kuruluşunun oluşturduğu çerçeve (Şekil 2.1) kapsamında alınması, yaşanan güvenlik ihlallerinin adli bilişimin iyi uygulamaları göz ardı edilmeden karşılanması, incelenmesi ve raporlanması, otomotiv endüstrisinde Nesnelerin İnterneti siber saldırılarına karşı önleme yöntemlerinin uygulanmasında kritik bir faktördür. Paydaşlar, güvenlik politikalarının, yönergelerinin ve eğitim programlarının netliğini ve erişilebilirliğini geliştirerek, etkili güvenlik önlemlerinin uygulanmasında etkin iletişim ve iş birliği yapma becerilerini geliştirebilir.

3. BULGULAR

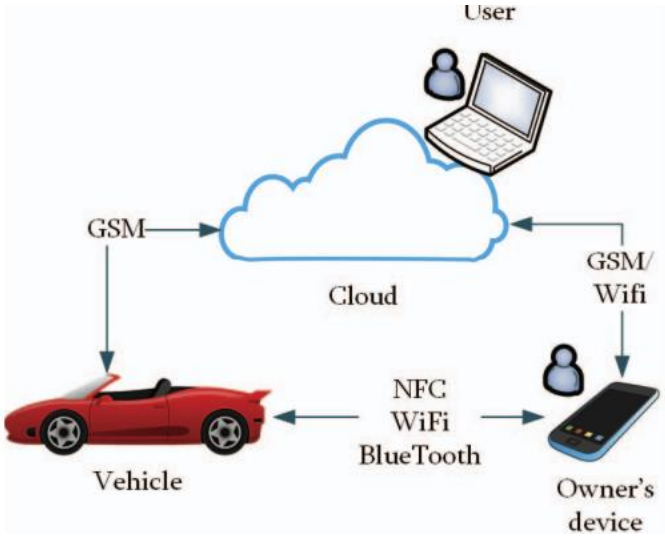
Nesnelerin İnterneti siber saldırıları, Nesnelerin İnterneti paydaşı olan cihaz, sistem ve uygulamalarda kendiliğinden (*İng.* built-in) bulunan yahut sistem entegrasyonu neticesinde ortaya çıkan güvenlik açıklarından yetkisiz erişim elde etmek, hassas niteliğe sahip bilgileri sahip rızası olmadan elde etmek, operasyonları kesintiye uğratmak veya zarar vermek ya da diğer kötü niyetli faaliyetleri başlatmak için yararlanmaya yönelik kötü niyetli girişimlerin bütününü ifade etmektedir. Bu saldırılar, bağlantılı arabalar, akıllı ev aletleri, endüstriyel kontrol sistemleri ve tıbbi cihazlar dahil olmak üzere çok çeşitli Nesnelerin İnterneti cihazlarını hedef alabilir.

Nesnelerin İnterneti artan sayıda cihaz ve sistemi birbirine bağlayarak genişlemeye devam ettikçe, bu birbirine bağlı ağları hedef alan siber saldırı riski de üstel bir şekilde artmaktadır. Öte yandan, Nesnelerin İnterneti siber saldırıları bireyler, kuruluşlar ve kritik öneme sahip altyapılar için önemli tehditler oluşturmaktadır. Dolayısıyla, risk olgusunu, bir istenmeyen durumun oluşma ihtimali ve oluşan durumun vereceği hasarın direkt çarpanı olarak ele aldığımızda (Denklem 3.1), Nesnelerin İnterneti üzerine yaşanacak bu saldırıların yaratacağı sıkıntıların üstel şekilde fazla olduğu sonucuna varılabilir.

$$Siber\ Risk = (Riskin\ gerçekleşme\ ihtimali)\ x\ (Potansiyel\ etki) \quad (3.1)$$

Nesnelerin İnterneti üzerinde kötü niyetli kişilerce gerçekleştirilecek saldırıların doğasını anlamak, etkili güvenlik önlemleri uygulamak adına fevkalade önem arz etmektedir. Nesnelerin İnterneti siber saldırıları, Nesnelerin İnterneti cihazlarındaki, ağlarındaki veya uygulamalarındaki güvenlik açıklarından yararlanmayı amaçlayan kötü niyetli faaliyetleri ifade eder (Patel ve Doshi, 2018). Bu saldırıların finansal kazanç, veri hırsızlığı, hizmetlerin aksaması ve hatta sabotaj dahil olmak üzere çeşitli nedenleri olabilir. Büyük ölçekli dağıtım, çeşitli cihaz türleri ve birbirine bağlanabilirlik gibi Nesnelerin İnterneti sistemlerinin benzersiz özellikleri, düşmanların yararlanabileceği karmaşık bir saldırı yüzeyi oluşturur.

Nesnelerin İnterneti siber saldırılarıyla ilgili temel endişelerden biri, hedefledikleri saldırı yüzeyidir. Nesnelerin İnterneti'nin saldırı yüzeyi, saldırganların sistemin güvenliğini tehlikeye atmak için yararlanabilecekleri giriş noktalarını veya güvenlik açıklarını kapsar. Nesnelerin İnterneti cihazları, sensörler, iletişim kanalları, bulut platformları ve hatta ürettikleri verilerin tümü potansiyel saldırı yüzeyleri haline gelebilecektir (Şekil 3.1). Bu saldırı yüzeyleri, yetkisiz erişim elde etmek, kötü amaçlı yazılım saldırıları başlatmak, verileri manipüle etmek veya hizmet reddi saldırıları gerçekleştirmek için kullanılabilir (Patel ve Doshi, 2018).



Şekil 3.1. Otomobillerde Nesnelerin İnternetinde zafiyete tabi taraflar.

Netice olarak, siber güvenlik riskinin iki sac ayağı olan ihtimal ve etki, Nesnelerin İnterneti siber saldırıları için de geçerlidir ve artan teknolojik yatırımların bu alana kaydırılması ile birlikte önem arz etmektedir. Bundan sonraki bölümde, siber güvenlik dürbününden Nesnelerin İnterneti uygulamalarının kırılganlığa tabi tarafları aktarılacak, bu kırılgan noktaları hedef alan siber saldırıların türleri, güvenlik açıklarına sebebiyet veren olgular, ve son olarak bu olguların riskleri belirtilecektir.

3.1. Bağlantılı Araçlarda Siber Saldırıların Önemi

Otomobil sektöründe gerçekleşmesi düşünülen veya gerçekleştiği bilinen saldırılar, Nesnelerin İnterneti ağı ve bileşenlerine yapılan saldırılardan bağımsız şekilde düşünülemez. Otomobillerin günlük işleyişte ulaşım ayağında en önemli payı tutmasının yanı sıra, ev aletleri gibi internete bağlı cihazlardan temel bir diğer farkı da içinde taşıdığı kişi veya kişilerin can güvenliği riskini dair zafiyetler barındırmasıdır. Bu kapsamda, otomobil sektöründe yaşanacak Nesnelerin İnterneti siber saldırılarını, diğer saldırılara gösterilen dikkatin daha da üstünde bir dikkat ve önemle ele almak bir zorunluluktur. Bu başlıkta, Nesnelerin İnterneti saldırılarını otomobiller üzerindeki yansımalarının amaçları ve kapsamı örneklerle çeşitlendirilerek gerekli altyapının kurulmasına dair çalışmaların temellendirilmesi amaçlanmaktadır.

3.2. Olayların tespiti

Otomotiv endüstrisindeki Nesnelerin İnterneti siber saldırı olaylarını tespit etmek için çeşitli güvenlik önlemlerini ve teknolojileri entegre eden çok katmanlı bir yaklaşım benimsenmektedir. Genel olarak siber saldırıların tespitinde de bu çok katmanlı model uygulanmaktadır, dolayısıyla diğer sektörler veya alanlarda gerçekleşen siber saldırıların da otomotiv sektöründe yaşanan siber saldırılardan farklı olduğu düşünülemez. Bu çok katmanlılığın, siber saldırılar yaşandıktan sonra olayların daha kolay tespit edilebilmesi ve kök neden analizlerinin daha kolay yapılabilmesi amaçları taşıdığı söylenebilir.

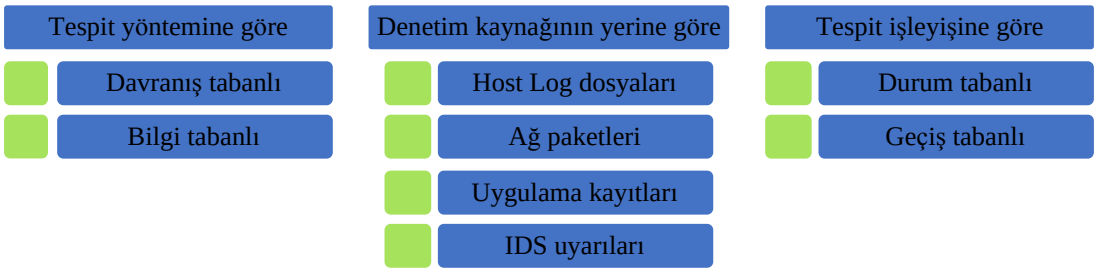
Çok katmanlı güvenlik mimarisinde kullanılan araç ve uygulamalar, spesifik teknolojileri bünyesinde barındıran karmaşık çözümler olarak da görülebilir. Nitekim bu alanda işlevsel bulunan her bir paydaş, yapay zekadan makine öğrenmesine, büyük veri analizinden algoritma optimizasyonuna kadar geniş bir yelpazede güncel veya güncelin de ötesinde çözümleri, art niyetli saldırganlardan daha önde olmak adına kullanmak durumunda kalmıştır. Siber olayların tespitinde kullanılan araçlara

genel bir bakış atıldığında, üç farklı alt başlık ile gruplandırma yapmak mümkün hale gelmektedir.

3.2.1. Saldırı Tespit Sistemleri (IDS)

Saldırı Tespit Sistemleri (*İng.* Intrusion Detection Systems) çözümleri, siber güvenliğe nesne olması muhtemel sistemlerin verilerini aktardığı havuzların üstünde konumlanarak, sistemlerdeki anormal veya kötü amaçlı ağ trafiğini ortaya çıkarılabilen yazılım çözümleridir. Bu sistemlerde, önceden yaşanan siber güvenlik ilintili olayların ağ iletişim örüntüleri tanımlanmış olup, ağ üzerinde gerçekleşen veri alışverişi anlık olarak izlendiğinden, herhangi bir şekilde önceden yaşanan siber güvenlik olayına benzeyen örüntü tespit edilir ise uyarılar üretilmesi sağlanabilir veya tanımlanan özerkliğe bağlı olarak ağ trafiği tamamen kapatılabilir.

Saldırı tespit sistemleri özellikleri kapsamında değerlendirildiğinde Şekil 3.6'da belirtildiği gibi üç farklı şekilde tasnif edilebilmektedir:



Şekil 3.2. Saldırı tespit sistemi sınıflandırmaları.

Tespit yöntemine göre sınıflandırma, esasında ağı analiz eden yazılımın özelliklerini tanımlamaktadır. Saldırı tespit sistemi, izlediği sistemin normal davranışı hakkında bilgi kullandığında, bu durum davranışa dayalı olarak nitelendirilmektedir. Saldırı tespit sistemi saldırılarla ilgili bilgileri kullandığında ise, bu durum bilgiye dayalı olarak nitelendirilmektedir.

Davranış üstünden tespit yöntemi, izinsiz giriş tespit sisteminin saldırılara verdiği yanıtı tanımlamaktadır. Düzeltici (delikleri kapatma) veya proaktif (olası saldırganların oturumunu kapatma, hizmetleri kapatma) eylemleri alarak saldırıya aktif olarak tepki verdiğinde, izinsiz giriş tespit sisteminin aktif olduğu söylenir. İzinsiz giriş tespit sistemi yalnızca alarmlar (çağrı gibi) üretiyorsa, bu sistemin pasif olduğu söylenir.

Denetim kaynağı konumu, saldırı tespit sistemlerini analiz ettikleri girdi bilgilerinin türüne göre ayırır. Bu girdi bilgileri, bir ana bilgisayardaki denetim izleri, sistem günlükleri, ağ paketleri, uygulama günlükleri veya diğer izinsiz giriş tespit sistemleri tarafından oluşturulan izinsiz giriş tespit uyarıları olabilir.

Tespit işleyişi, izinsiz giriş tespit sistemi tarafından kullanılan tespit mekanizmasını tanımlar. Saldırı tespit sistemleri, durumları (güvenli veya güvensiz) veya geçişleri (güvenliden güvensize) değerlendirebilir (Debar, 1987).

3.2.2. Güvenlik Olay ve Olay Yönetimi (SIEM) Sistemleri

Muhtemel siber saldırıları tespit etmek ve ilişkilendirmek, çeşitli kaynaklardan güvenlik olayı kayıtlarının toplanmasını ve analiz edilmesini gerektirir. SIEM çözümleri, çok çeşitli Nesnelerin İnterneti cihaz ve sistemlerinden veri toplayıp analiz ederek şüpheli etkinliğin tespit edilmesine ve güvenlik duruşunun kapsamlı bir görünümünün sağlanmasına yardımcı olur.

3.2.3. Tehdit İstihbaratı ve Bilgi Paylaşımı çözümleri

Nesnelerin İnternetine izinsiz girişleri tespit etme yeteneğinin geliştirilmesine, tehdit istihbaratlarının paylaşıldığı forumlara katılarak ve en son güvenlik açıkları ile saldırı metodolojilerini takip ederek yardımcı olunabilir. İşletmeler, diğer kişi, kurum veya kuruluşlar ile beraber çalışarak ve yeni riskler

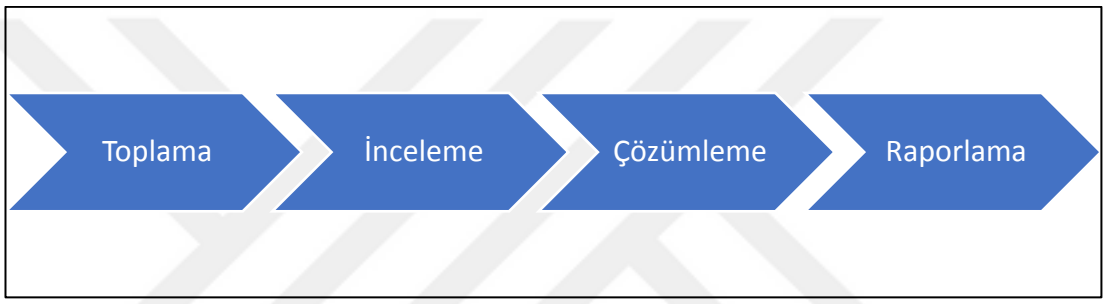
hakkında istihbarat paylaşarak herhangi bir saldırıya karşı daha iyi hazırlanabilir ve yanıt verebilir.

Sonuç olarak, Nesnelerin İnterneti alanında yaşanan genişlemeyi siber güvenlik olaylarından ayrı şekilde değerlendirmek oldukça güçtür. Bu kapsamda incelendiğinde, otomobillerde kullanılan bağlanılabilirlik özelliklerinin de siber olaylardan etkilendiği, sunulan örnekler değerlendirildiğinde görülebilmektedir. Her ne kadar örnek olaylar çeşitli amaçlara hizmet etse de, saldırıların kapsamı genellikle ortaktır. Siber olayların gerçekleşmesinden hemen sonra, tespit edilebilmeleri olayların önlenebilmesi adına önem arz etmektedir, nitekim tespit edilemeyen saldırıların varlığı retoriktir. Bu konuda geliştirilen farklı çözümler mevcuttur.

3.3. Olayların İncelenmesi

Bir Nesnelerin İnterneti siber saldırısının doğasını anlamak, etkilerini azaltmak ve sorumlu tarafları belirlemek, otomotiv endüstrisinde meydana geldiğinde kapsamlı bir araştırma gerektirir. Otomotiv endüstrisine yönelik siber saldırıların araştırılması, her siber saldırı alt başlığında olduğu gibi, günümüzün dijital çağında büyük önem taşımaktadır. Nitekim, bu saldırıları soruşturmanın önemini anlamak hem sürücülerin hem de yolcuların emniyetini ve güvenliğini sağlamak için önem arz etmektedir. Ayrıca olayların incelenmesi süreci, endüstrinin sistemlerindeki zayıflıkları belirlemesine ve ele almasına, savunmaları güçlendirmesine ve sağlam siber güvenlik önlemleri geliştirmesine olanak tanımaktadır. Otomotiv endüstrisine yönelik siber saldırıların soruşturulması, faillerin tespit edilmesini de kolaylaştırarak yasal işlem yapılmasına olanak tanır ve bu tür saldırılara müsamaha gösterilmeyeceğine dair güçlü bir mesaj vermektedir. Sonuç olarak, olayların incelenmesi durumunda alınacak kapsamlı inisiyatifler, yalnızca can güvenliğinin birincil kaygı olduğu otomotiv sektöründe bu kaygıların gelecekte yaşanmamasına yardımcı olmaz, üstüne otomotiv üreticilerinin itibarını korumaya, tüketici güvenini artırmaya ve bağlantılı ve otonom araçların geleceğini korumaya yardımcı olur.

Olayların incelenmesi süreci, farklı kaynaklarda farklı işleyişlerin gözlenebileceği bir aşamadır. Ancak, mesleki düzlemde siber olayların incelenmesine dair yapılan çalışmalar, çoğunlukla iyi uygulamaları ve bu konuda hazırlanmış rehber, yayın, akademik çalışma ve kontrol listesi gibi envanterin takip etmesi şeklinde gerçekleşmektedir. Bu bağlamda, sektörde en çok başvurulan kaynak, ABD menşeili NIST tarafından yayımlanan yönergedir. Bu yönergede, siber güvenlik olaylarının incelenmesi süreci dört temel adımdan oluşmaktadır (Şekil 4.1) ve bu farklı düzlemdeki dört temel adım ile siber güvenlik olayları uçtan uca değerlendirilebilir (Kent ve ark., 2006):



Şekil 3.3. NIST tarafından önerilen Adli Bilişim Süreci.

Bu akış şemasında belirtilen başlıkların açıklaması ise şu şekildedir (Dimitriadis ve ark., 2020):

Toplama: Toplama eyleminin temel amacı, siber olayla ilgili potansiyel veri kaynaklarını belirlemek, ardından bu veri kaynaklarını etiketlemek ve kaydetmektir. Daha sonra bu kaynaklarda yer alan veriler, kaynakların bütünlüğü korunarak elde edilmelidir. Burada, adli bilişimin bütünlüğü koruma ilkesi göz önünde bulundurulmalı, veriler toplanmadan önce cihazların rasgele erişimli hafızalarında ikame bulunan verilerin kaybının önüne geçilmesi adına cihazlara elektrik akımı kesilmemesine dikkat edilmelidir.

İnceleme: Toplama aşamasında bütünlükle elde edilen verilerin varsa üzerindeki şifreleme işlemleri gibi gizlilik sağlayan donelerden arındırılmasını, elde edilen bütünlüğü korunmuş verilerin değerlendirilmesini ve yine bütünlüğünün

korunarak olayla ilgili verilerin çıkarılmasını içermektedir. İnceleme aşaması, yine adli bilişimin temel pratiklerinden olan sterilizasyon esası göz önünde bulundurularak yapılmalı, dışarıdan müdahalelere izin verilmemeli ve bu yolla anlaşılabilirlik korunmalıdır.

Çözümleme: Elde edilen verilerin ışığında, *5N1K* olarak da bilinen, sırasıyla "ne, neden, nerede, nasıl, ne zaman ve kim", sorularını yanıtlamak veya hiçbir sonuca varılamayacağını veya bu verilerden bu soruların cevaplarının kısmen çıkarılabileceğini belirlemek için incelemeden çıkarılan bilgileri incelemeyi içeren analiz sürecidir. Burada adli bilişim pratikleri kapsamında dikkat edilmesi gereken, ilgili çözümleme yapılırken mantık hatalarından, ön yargılardan ya da kalıplaşmış düşünce birikimlerinden uzak durulmasıdır.

Raporlama: Raporlama safhası, soruşturmada uçtan uca kullanılan prosedür, yöntem ve araçların, analiz aşamasından elde edilen anlamlı veya anlamsız sonuçlarla birlikte hazırlanması ve sunulması sürecidir. Raporlama safhasında dikkat edilmesi gereken önemli bir husus da şeffaflık ve anlaşılabilirlik ilkelerinin korunmasıdır.

Netice olarak, olayların incelenmesi süreci de her siber güvenlik sorunu gibi çok katmanlı bir yapıdan oluşmaktadır ve süreç içerisinde önceden üretilmiş şablonların takip edilmesi büyük önem arz etmektedir.

3.4. Alınan Dersler

Her siber olayda olduğu gibi, otomotiv sektöründe Nesnelerin İnterneti sistemlerine yapılan siber saldırı ve müdahalelerde de olayın gerçekleşmesi, incelenmesi ve sonuçlanması döngüsünden hemen sonra, alınan derslerin aktarılması oldukça büyük önem arz etmektedir. Önceki bölümlerde sunulan olaylar ve geçmişte yaşanan örnekler göz önünde bulundurulduğunda, siber güvenlik saldırılarının adli bilişim açısından tarafsızca değerlendirilebilmesi ve yeni bir çerçevenin sağlıkla

oluşturulabilmesi için, bu olaylardan alınan derslerin kesinlikle dikkate alınması gerekmektedir. Alınan dersler, sunulan farklı başlıkların altında detaylandırılabilir:

İyi Uygulamalar Kullanılarak Sistem Tasarımlarının Gerçekleştirilmesi

Nesnelerin İnterneti üzerindeki siber saldırıların birincil seviyedeki sebebi, Nesnelerin İnterneti sistemleri kurulurken yaşanan eksiklikler, açıklar, gözden kaçırmalar ve hatalardır. Bu durumların önüne geçilmesi adına, iyi uygulamaların sistem tasarım aşamasında ele alınması ve bu yolla sistem mimarisinde temelin sağlam tutulması gerekmektedir.

Güvenli Yazılım Geliştirme Yaşam Döngüsünün (SDLC) Önemi

Nesnelerin İnterneti üzerindeki siber saldırılar, güvenliği yazılım oluşturma sürecinin her aşamasına yerleştirme ihtiyacını gün ışığına çıkarmıştır. Özellikle fiziksel olmayan siber güvenlik saldırılarında (ağ, şifreleme ve yazılım kapsamına giren saldırılar) güvenli yazılım geliştirme döngüsünün takip edilmemesine dair izler görebilmek mümkündür. Güvenli kodlama uygulamalarını uygulamak ve sıkı güvenlik değerlendirmeleri yapmak, alınan derslerin örnekleridir. Güvenlik, geliştirmenin başlangıcından itibaren en yüksek önceliğe sahipse, üretime sunulmadan önce güvenlik açıkları bulunabilir ve yama yapılabilir.

Düzenli Güvenlik Değerlendirmeleri ve Penetrasyon Testi

Nesnelerin İnterneti sistemlerindeki güvenlik açıkları, yalnızca düzenli güvenlik denetimleri ve sızma testleri yoluyla bulunabilir. Kurumsal güvenlik açıkları, gerçekçi saldırı senaryoları simüle edilerek gerçekten kullanılmadan önce keşfedilebilir ve düzeltilebilir. Testler düzenli olarak yapılırsa, güvenlik açıkları kötü aktörler tarafından kullanılmadan önce bulunabilir ve yamalanabilir.

Üreticiler ve Güvenlik Araştırmacıları Arasındaki İş birliği

Otomobil üreticileri ve güvenlik uzmanları arasındaki iletişimi kolaylaştırmak esastır. Üreticiler, yetkin kişilerin açıkları tespit etmesi halinde ödüllendirildiği mekanizmalar ile ifşa programları oluşturarak ve araştırma topluluğuyla iş birliği yaparak güvenlik açıklarını bulmak ve Nesnelerin İnterneti sistemlerinin güvenliğini artırmak için dış bilgilerden yararlanabilir. Güvenlik araştırmacılarıyla yakın iş birliği yapılması, güvenlik açıklarının düzeltilmesini hızlandırabildiği gibi son kullanıcıların güvenini artırabilmektedir.

Yazılım Güncellemeleri

Sisteme ait yazılımların ve ürün üzerinde koşan yazılımının zamanında güncellenmesi, güvenlik sorunlarını gidermek ve bilinen güvenlik açıklarını gidermek adına önem arz etmektedir. Önceki siber saldırılardan alınan dersler, hem üreticiler hem de kullanıcılar tarafından hızlı güncelleme kurulumunun önemini vurgulamaktadır. Güncellemeler, Nesnelerin İnterneti cihazlarının ve sistemlerinin sürekli güvenliğini, var olan güvenlik açıklarını devamlı kapatarak açık kapıları kapatmak suretiyle korumaktadır.

Son Kullanıcıların Nesnelerin İnterneti Güvenlik Riskleri Hakkında Eğitimi

Nesnelerin İnterneti cihazlarını ve altyapısını kullanırken önlem almanın önemi konusunda tüketicileri eğitmek de ayrıca önem arz etmektedir, çünkü bu uygulamaları ve sistemlerin kullanılması noktasında birincil seviyede inisiyatif alma yeteneği kullanıcılardadır. Kullanıcılara, uygun güvenlik uygulamaları konusunda rehberlik sağlanırsa, güçlü parolalar kullanmaları teşvik edilirse ve araçlarını düzenli olarak yükseltmeleri teşvik edilirse, Nesnelerin İnterneti özellikli araçlarının güvenliğini artırmaya yardımcı olabilir. Güvenlik konusunda daha bilinçli ve eğitimli bir kullanıcı tabanı, güvenlik açıklarını azaltmada uzun bir yol kat edecektir.

3.5. Saldırıların Önlenmesi İçin Gerek Şartlar

Günümüzün küresel olarak birbirine bağlı, teknoloji ile harmanlanmış topluluklarına sahip bütünlükçü dünyasında, siber saldırıları engellemek için önlemler almak her zamankinden daha fazla önem arz etmektedir. Teknoloji geliştikçe ve siber tehditler değiştikçe sistemleri, verileri ve gizliliği korumak için gerekli hale gelen siber güvenlik önlemleri de benzer şekilde değişmek zorunda kalacaktır, dolayısıyla bu alanda benimsenecek ileriye etkili yaklaşım da benzer şekilde göz önünde bulundurulması gereken bir girdi olarak karşımıza çıkar (Tran ve ark., 2022). Siber tehditlerin önlenmesi, parasal faktörlerden insan faktörüne kadar geniş bir yelpazede katılım gerektiren ve on bir farklı başlık halinde akademik literatürde sınıflandırma ve değerlendirmeye tabii unsurlara bağlıdır:

i. Bütçe

Bütçelendirmeye dair eksiklikler, hiç şüphe yok ki hem siber güvenlik olaylarının yaşanmasının bir numaralı müsebbibi hem de siber güvenlik olaylarının önlenmesi yönünde gerekli olan bir numaralı sorunsaldır. Siber güvenlik alanındaki saldırılar elbette tamamen önlenemese de gerekli bütçelerin ayrılmasına binaen güçlenecek her parametre, siber güvenlik olaylarının yaşanması ve tekrar etmesi yönünde kötü niyetli kişilerin önüne konulacak bir engel oluşturur.

ii. Yönetişim

Sağlam bir güvenlik yönetişim mimarisi ve verimli yönetim prosedürleri oluşturmak, siber güvenlik olaylarının önlenebilmesi adına önem arz etmektedir. Yönetişim, bir karar veya aksiyonun, kurum ve kuruluşlar nezdinde üst yönetimdeki temsiliyetini, kabullenilmesini ve uygulanma iradesini anlatan terimdir. Üst yönetimlerin siber güvenlik olaylarının önlenmesine dair kararlı tavrı neticesinde, uzman çalışanların işe alınmasını, açık yetki sınırlarının oluşturulmasını ve yeni protokol ve uygulamaların getirilmesini içeren siber güvenlik önlemleri, sağlam

şekilde işleyebilecektir. Yine üst yönetim tarafından dayatılacak uyumluluk ve sürekli iyileştirme, düzenli güvenlik denetimleri ve risk değerlendirmeleri yapılarak, siber güvenlik olaylarının daha az yaşanması sağlanabilir (Llopis-Albert, 2021). Şirketin maliyetlerini artıracak ve bu sebeple ancak üst yönetim kararı ile tercih edilebilecek bir siber sigorta ürünü, hem sigorta şirketinin risk profillerini incelemeleri neticesinde altyapının güçlendirilmesine hem de siber saldırganların gönülsüz davranmasına yardımcı olabilecektir.

iii. Yönetim

Yönetim faaliyetleri, yönetişim politikaları kapsamında alınan kararların daha ufak boyuttaki birimlere, ekiplere ve kişilere dikte edilmesini ifade etmektedir. Her ne kadar yönetişim faaliyetleri kapsamıyla üst yönetimlerin siber güvenlik dirençliliğine dair irade ve azmi ortaya konulsa da kurum ve kuruluşlarda alt seviyede çalışan kişilere bu irade ve azmin yöneticileri vasıtasıyla aktarılması, siber güvenlik olaylarının en büyük yüzey alanını oluşturan kişilerin risk matrisinde yerinin aşağılara doğru kaymasına sebebiyet verebilmektedir. Yöneticiler, işlemlerinin içeriğinden bağımsız olarak siber güvenlik riskini göz önünde bulundurarak hareket etmeli, alınan kararlarda siber güvenlik risklerine dair danışmanlık veya görüş alınmalıdır. Aynı zamanda yöneticiler hem kendilerinin hem de çalışma arkadaşlarının yönetişim çerçevesi kapsamında belirlenen gerekli eğitim faaliyetleri konusunda eksiklik yaşamadıklarını, iş yerlerinde risklere dair bilgilendirmelerin sürekli yapıldığını garanti altına almalıdırlar.

iv. Risk Değerlendirmesi ve Analizi

Siber güvenlik olaylarının önüne geçilebilmesi adına, öncelikle zayıf noktaları ve olası giriş noktalarını belirlemek için kapsamlı risk değerlendirmeleri yapılmalıdır. Sistemler, ağlar ve uygulamalar, kuruluşların güvenlik açıklarını belirleyebilmesi ve bunları azaltmak için öncelikler belirleyebilmesi için değerlendirilmelidir. Bu, bilgisayar korsanlarının verebileceği hasarı hesaplamak ve ilgili riskleri azaltmak için bir plan yapmak gibi şeyler yapmayı gerektirir. Siber

saldırılar hala sıklıkla insan hatası içermektedir. Personeli, paydaşları ve son kullanıcıları siber güvenlik için en iyi uygulamalar konusunda eğitmek çok önemlidir. Güvenlik farkındalığı programlarına dahil edilmesi gereken şeylerden bazıları, kimlik avı, sosyal mühendislik, iyi parola uygulamaları ve güvenli web taramasıdır. Başarılı saldırılar, insanlara olası tehditleri fark etmelerine ve bunlara yanıt vermelerine yardımcı olacak düzenli eğitim verilerek azaltılabilir.

v. Güvenli Mimari ve Tasarım

Siber tehditleri önlemek, sistemlerin, ağların ve cihazların güvenli bir şekilde yapılandırılmasını gerektirmektedir. En iyi güvenlik uygulamaları uygulanarak, kullanılmayan hizmetler kapatılarak, yetki sınırlandırmaları ile ve güvenlik duvarları ve izinsiz giriş tespit sistemleri kurularak saldırı yüzeyi büyük ölçüde azaltılabilir. Ağları alt ağlara ve bölümlere ayırmak ve dışarıdan izole etmek, ihlallerin önlenmesine yardımcı olmaktadır ve siber saldırıların neden olduğu hasarı azaltır (Tawalbeh ve ark., 2020). Saldırganlar tarafından yanal hareket etme riski, önemli sistemleri halka açık ağlardan izole ederek ve ağları kullanıcı rollerine ve veri hassasiyetine göre bölümlere ayırarak azaltılabilir.

Hassas bilgileri şifreleyerek ve güvenli iletişim yöntemleri kullanarak aktarılan verileri korumak ayrıca önem arz etmektedir. TLS ve SSH protokolleri tarafından sağlanan şifreleme ve kimlik doğrulama, açık ağlar üzerinden iletilen bilgilerin gizliliğini ve gerçekliğini korur (Weyer ve ark., 2016). Kuruluşlar, kapsamlı izleme yöntemleri oluşturdukları takdirde olası siber saldırıları hızlı bir şekilde fark edebilir ve bunlara yanıt verebilir. Ağ etkinliği, sistem günlükleri ve kullanıcı davranışları gibi aksiyonlara; izinsiz girişleri izleyen ve bunlara alarm üretmek suretiyle yetkili kişileri uyararak ya da kendi inisiyatifi içerisinde yanıt veren sistemlere saldırı tespit ve önleme sistemleri (IDPS) aracılığı ile göz kulak olmak, herhangi bir şüpheli etkinliğin tespit edilmesine ve aynı etkinliğin durdurulması için hızla tepki vermeye yardımcı olabilmektedir.

Siber saldırıların etkileri, düzenli veri yedeklemeleri ve çalışırlığı ispatlanmış sağlamlıkta felaket kurtarma stratejileri kullanılarak da azaltılabilir. Veri bütünlüğünü korumak için yedekler güvenli bir yerde tutulmalı ve sık sık denetlenmelidir. Güvenli yedeklemelere ve net bir kurtarma stratejisine sahip olmanın, bir siber saldırının işletmeler üzerindeki etkisini azaltmaya yardımcı olduğu söylenebilir (Ullah ve ark., 2021). Siber saldırıların önlenmesi için geçerli endüstri normlarına ve standartlarına uygunluk esas teşkil etmektedir. Farklı kurum ve kuruluşlar tarafından ilgili sektöre dayatılan Genel Veri Koruma Yönetmeliği (GDPR), Ödeme Kartı Sektörü Veri Güvenliği Standardı (PCI-DSS) ve diğer yayımlar dahil olmak üzere işletmelerin bilmesi ve bunlara uyması gereken bir dizi düzenleme mevcuttur. Hangi güvenlik önlemlerinin alınacağına ve hassas verilerin nasıl güvende tutulacağına ilişkin bilgiler ise uyumluluk çerçevelerinde bulunabilmektedir (Ullah, Imtiaz ve Qusay Mahmoud, 2021).

vi. Erişim Kontrol ve Kimlik Doğrulama Mekanizmaları

Dışarıdan bakışları sistemlerden ve hassas nitelikte kişisel bilgilerden uzak tutmak adına, güvenilir erişim kısıtlamaları oluşturmalıdır. Parola karmaşıklığı gereksinimleri, 2FA-MFA gibi kimlik doğrulama mekanizmaları ve erişim ayrıcalıklarının rutin incelemeleri ve iptallerinin tümü bu kategoriye girmektedir. Rol tabanlı erişim denetimleri, kullanıcıları işlerini gerçekleştirmek için gerçekten ihtiyaç duydukları veri ve özelliklerle sınırlamaktadır (Llopis-Albert, 2021). Bilinen güvenlik açıklarını yazılımların, işletim sistemlerinin ve uygulamaların en güncel sürümlerini kullanarak yamalamak bilahare öneme sahiptir. İşletmeler, güvenlik yükseltmelerini zamanında devreye almak için verimli yama yönetimi süreçlerine ihtiyaç duyar ve bu sorunu çözmek amacıyla üretilen otomatik güncelleme mekanizmaları, sistemleri modern tehlikelerden korumaya yardımcı olur.

vii. Güvenlik Test ve Denetimleri

Sistemlerdeki ve ağlardaki güvenlik açıkları, rutin güvenlik denetimleri ve sızma testleri yoluyla bulunabilmektedir. Bu değerlendirmeler, gerçek saldırıları

birebir yöntem ve araçlar taklit edip kötü niyetli saldırganların yararlanabileceği güvenlik açıklarını ortaya çıkarmaktadır. Kuruluşlar, güvenlik açıklarını proaktif olarak ele alarak, potansiyel tehlikelerle ilgili kaynakları ve bilgileri bir araya toplayarak güvenlik ihlallerini daha iyi tahmin edebilir ve başarılı siber saldırı olasılığını büyük ölçüde azaltabilir (Soe, 2020). Bu duruma ek olarak, bu konuda aksiyon almak isteyen kurum ve kuruluşlar birlikte çalışarak savunmalarını geliştirebilir ve sürekli değişen siber tehditlerle daha iyi başa çıkabilir.

viii. Olay Müdahale ve Felaket Kurtarma Planı

İşletmelerin kendilerini siber tehditlerden korumak için kapsamlı olay müdahale stratejilerine sahip olmaları gerekmektedir. Bahsedilen bu planlar, bir ihlal durumunda, olayı bildirmek, sorunu çevreleyerek yalnızlaştırmak, düzeltmek ve zarardan kurtarmak gibi alınacak önlemleri detaylandırmaktadır. Planlarda aktarılan siber olay müdahale yöntemleri geliştirilebilmekte ve koruma sürecindeki boşluklar ve eksiklikler, simüle edilmiş saldırı senaryoları kullanılarak yapılan düzenli testlerle belirlenebilmektedir. Satıcıların ve tedarikçilerin güvenlik uygulamalarındaki bulunabilecek potansiyel güvenlik açıkları, bu kurumlarla iş ilişkisinde bulunan bir kuruluşu tehlikeye atabilir, dolayısıyla bu aktif çözümlere dair hamleler yapmak önem arz etmektedir (Saleem ve ark., 2017).

ix. Çalışanlar İçin Güvenlik Farkındalığı ve Eğitimi

Çalışanlar nezdinde gerçekleştirilecek siber güvenlik pratiklerine dair çalışmalar, otomotiv sektörü paydaşları için şüphe olmaksızın en iyi yatırımlardan biri olacaktır. Çalışanlardan önce, işe alım sürecinde aday kişilerin adli sicil ve geçmiş iş kayıt kontrolleri, işe alma sürecinde gerçekleştirildiğinde en etkili olan çözümdür. Kişiler işe başladıktan sonra, içeriden gelen tehditlerin oluşturduğu tehlikeler, sıkı erişim kontrolleri, kullanıcı izleme ve düzenli çalışan farkındalık programları oluşturularak azaltılabilir. Şüpheli davranış, kullanıcı eylemlerinin rutin olarak izlenmesi ve denetlenmesi yoluyla ortaya çıkarılabilir. Bir kuruluşun güvenlik duruşu, etik bilgisayar korsanları istihdam edilerek veya kırmızı ekip etkinlikleri

yürütülerek iyileştirilebilir. Güvenlik açıklarının kötü niyetli olarak kullanılmasını önlemek için, etik korsanlar gerçek saldırıları çoğaltır.

x. Sürekli İzleme ve İyileştirme

Tehdit istihbaratı ve proaktif güvenlik izleme kullanılarak yeni siber riskler tespit edilebilir ve karşı konulabilir. Kuruluşlar, Güvenlik Bilgileri ve Olay Yönetimi sistemleri ve tehdit istihbaratı akışları gibi modern güvenlik teknolojilerini kullanarak saldırıları gerçek zamanlı olarak tespit edip önleyebilir. Yazılımda güvenlik açıklarının ortaya çıkmasını engellemenin en iyi yolu, güvenliği baştan dahil etmektir (Roopak ve ark., 2019). Güvenli kodlama uygulamalarını takip etmek, düzenli kod incelemeleri gerçekleştirmek ve zorlu testler gerçekleştirmek, güvenlik sorunlarını erkenden tespit edip düzeltmeye büyük ölçüde yardımcı olur. Hem yazılım hem de donanım geliştirme sırasında güvenliğe öncelik verildiğinde, güvenlik açıklarının ortaya çıkma olasılığı daha düşüktür.

Sistemlerdeki ve ağlardaki güvenlik açıkları, rutin güvenlik denetimleri ve sızma testleri yoluyla bulunabilir. Bu değerlendirmeler, gerçek saldırıları taklit eder ve bilgisayar korsanlarının yararlanabileceği güvenlik açıklarını ortaya çıkarır. Kuruluşlar, güvenlik açıklarını proaktif olarak ele alarak başarılı siber saldırı olasılığını büyük ölçüde azaltabilir (Soe, 2020).

xi. Sektör İçinde İş birliği ve Bilgi Paylaşımı

İşletmeler, devlet kurumları ve siber güvenlik grupları arasındaki iletişimi ve iş birliğini teşvik etmenin gerekliliği ortadadır, nitekim farklı gruplar tarafından yaratılabilecek beyin fırtınasının niteliksel ve niceliksel faydaları mevcuttur. İşletmeler, potansiyel veya yaşanmış tehlikelerle ilgili kaynakları ve bilgileri bir araya toplayarak güvenlik ihlallerini daha iyi tahmin edebilecek ve önleyebilecektir. Yine işletmeler birlikte çalışarak savunma mekanizmalarını iyileştirebilir, geliştirebilir ve sürekli değişen siber tehditlerle daha iyi başa çıkabilir.

3.6. Geçmiş Önlem Pratikleri

Otomobillerde siber güvenlik pratiklerinin oluşturulması, test edilmesi ve sürekli güncellenerek pekiştirilmesi adına, daha önceden muhtelif çözümler ve çerçeveler önerilmiştir. Bu farklı spektrumdaki çerçeveler, çoğunlukla problemlerin otomotiv sektörü uygulamaları göz ardı edilerek tek taraflı değerlendirilmesi neticesinde kendi içinde döngüsel açıklar barındırabilmekte ve nitekim buradan hareketle kusursuz uygulanmaları senaryolarında bile güvenlik zafiyetlerine sebebiyet verebilmektedir.

Elde bulunan çerçeve havuzunda ise en geniş ve kapsamlı çalışmaları içeren ve dolayısıyla sektör tarafından en çok en iyi uygulamalara yakın olarak değerlendirilen çerçeve, İnternet Güvenliği Merkezi (CIS) tarafından oluşturulan ve işletmelerin siber güvenlik pratiklerini nasıl ve ne şekilde geliştirebileceklerine dair öneriler sunan *Critical Security Controls - CSC* çerçevesidir. Çerçeve içerisinde *Temel, Kuruluşsal/Örgütsel* ve *Organizasyonel* kategorileri altında değerlendirilen otuz iki adet farklı kontrol adımı mevcuttur ve yine bu sınıflandırma kapsamında, üç katmanda ele alınan kontrol adımları önlem pratiklerinin temelini oluşturmaktadır:

4.6.1. Birincil (Basit) Kontroller

Birincil kontroller, bilişim alanında çalışsın ya da çalışmasın, herhangi bir şirkette olması gereken temel korumalara dair çerçeve çizmektedir. Birincil kontrollere dair alt başlıklar ve açıklamaları ise şu şekildedir:

• Donanım ve Yazılım Varlıklarının Envanteri ve Kontrolü

BT ortamının görünürlüğü ve kontrolü hem yetkili hem de yetkisiz tüm donanım ve yazılımların güncel bir envanterinin tutulmasıyla sağlanabilir.

• Sürekli Güvenlik Açığı Yönetimi

Sistemlerdeki ve uygulamalardaki güvenlik açıklarını sürekli olarak değerlendirmek ve ele almak için otomatik güvenlik açığı taraması, yama yönetimi yöntemleri ve güvenlik açığı azaltma önlemleri uygulanmalıdır.

• Donanım ve Yazılım için Güvenli Yapılandırmalar

Siber saldırıların önemli bir kısmının kendiliğinden gelen yapılandırmaların istismarı üzerinden gerçekleşmesinden hareketle, saldırı yüzeyini ve güvenlik açıkları olasılığını azaltmak için, tüm donanım ve yazılım varlıkları için güvenli yapılandırma yönergeleri oluşturmak ve bu yönergeleri uygulamak önem arz etmektedir.

• Ayrıcalıkların Kontrollü Kullanımı

Ayrıcalıklar, şirkette çalışan gerçek ya da sanal kişilere, şirket sistemi üzerinde kolaylıklar tanıyan yetkilendirmelerin isimlendirilmesidir. Ayrıcalıklı erişimi yalnızca ihtiyacı olan kişilerle sınırlandırmak, yetkiye sahip personel sayısını en az ayrıcalık ilkesiyle sınırlandırmak ve bu hususta periyodik denetimler gerçekleştirmek, siber saldırı yüzey alanını azaltmakla kalmayacak, olası bir zafiyet durumunda kötü niyetli kişilerin eline asgari yetki geçmesini de sağlayacaktır.

• Güvenli Kullanıcı Kimlik Doğrulaması ve Parola Yönetimi

Kullanıcı hesaplarına yetkisiz erişimi önlemek için çok faktörlü kimlik doğrulama (MFA) gibi güçlü kimlik doğrulama teknikleri uygulanması ve güvenli parola yönetimi uygulamalarının zorunlu kılınmasıdır.

4.6.2. Kuruluşsal/Örgütsel Kontroller

Bu kısıtlamalar, daha yaygın siber suç biçimlerini engelleyerek, bir önceki başlıkta sunulan temel kontrolleri tamamlayıcı görev üstlenmektedir. Kuruluşsal/örgütsel kontroller şu şekilde alt başlıklara sahiptir:

• E-posta ve Web Tarayıcı Korumaları

Şirketin sunucularına dışarıdan gelen e-postalar için bir tarama yöntemi ve yine şirket sunucularının istek attığı web serverlarına tarama yöntemlerini uygulayarak kimlik avı dolandırıcılıklarını, kötü amaçlı yazılım indirmelerini ve diğer çevrimiçi tehlikelerin önlenmesini amaçlamaktadır.

• Kötü Amaçlı Yazılım Savunmaları

Anti-virüs olarak da isimlendirilen, kötü amaçlı yazılımdan koruma sağlayan yazılım ve ilgili diğer ürünleri şirket nezdinde dağıtarak ve sürdürerek kuruluşun veri altyapısını kötü amaçlı yazılımlardan korunmasının amaçlanmasıdır.

• Veri Kurtarma Yetenekleri

Bir sistem arızası veya veri kaybı durumunda, bir yedekleme ve kurtarma planının var olduğuna dair makul güvence sağlanması ve bu planın gerektiği şekilde çalıştığından emin olunmasıdır.

• Ağ Cihazları için Güvenli Yapılandırmalar

Aktarılan verilerin korunması, ağ tabanlı tehditlere maruz kalmayı sınırlanması ve yönlendiriciler (*router*), anahtarlar ve diğer ağ aygıtlarında güvenli yapılandırmalar kurarak yetkisiz kullanıcıların engellenmesidir.

• Sınır Savunması

Kötü niyetli eylemleri engellemek ve hassas bilgileri korumak için güvenlik duvarları ve izinsiz giriş tespit/önleme sistemleri kurularak, kullanılan ağın gelen ve giden verilerine ait paketlerin incelenmesi ve gözetlenmesi aktivitelerinin uygulanmasıdır.

4.6.3. Kurumsal Kontroller

Bu önlemler, yönetişimi ve risk yönetimini iyileştirerek bir kuruluş genelinde bir siber güvenlik kültürünü teşvik etmeyi amaçlamaktadır. Kurumsal kontroller için, isimle müsemma, kurumsal bir altyapı, kültür ve anlayış gereklidir. Kurumsal kontrollere dair başlıklar şu şekildedir:

• Risk değerlendirmesi

Siber güvenlik risklerinin, kuruluşun iş hedefleri, tehditleri, güvenlik açıkları ve yansımaları ışığında belirlenmesi ve bu risklerin öncelik sırasına koymak adına düzenli olarak değerlendirilmesidir.

• Güvenlik Farkındalığı ve Eğitim Programları

Personeli siber güvenlikle ilgili en iyi uygulamalar, tehlikeler ve güvenli bir ortam sağlama konusundaki sorumlulukları konusunda eğitmek önem arz ettiğinden, güvenlik farkındalığı ve eğitim programlarının çalışanlar nezdinde uygulanmasıdır.

• Olay Müdahalesi ve Yönetimi

Güvenlik sorunlarının hızlı bir şekilde tanımlanabilmesi, sorunlar ile başa çıkılabilmesi ve normal işleyişe dönülebilmesi için güvenlik sorunlarını ele alacak

bir plan ve planın işleyişinden sorumlu bir grup insanın ve sistemin oluşturulmasıdır. Ayrıca, deneyimler ve uygulamalar ışığında var olan bu planların test edilmesi ve gözden geçirme rutinine sahip olmasını içermektedir.

• Sızma Testi ve Kırmızı Takım Egzersizleri

Siber tehditleri daha iyi tespit etmek ve bunlara yanıt vermek için, güvenlik açıklarını ortaya çıkarmak ve güvenlik politikalarının etkinliğini değerlendirmek için düzenli sızma testlerinin yürütülmesi ve sisteme bazen sistem işletenleri bilecek şekilde, bazen ise tamamen spontane ve habersiz gelişen şekilde simüle edilmiş saldırılar gerçekleştirilmesidir.

• Güvenli Yazılım Geliştirme Yaşam Döngüsü (SDLC)

Güvenli olmayan yazılımların derlenmesi yahut çalıştırılmasından doğması muhtemel riskler; yazılım mimari tasarımı esnasında güvenlik hassasiyetinin ön planda tutulduğu *Security by Design* yaklaşımı, güvenli yazılım geliştirme araçlarının kullanılması, yazılım incelemeleri, sürekli yazılım testleri ve güvenlik açığı testlerini içeren yazılım geliştirme yaşam döngüsüne dahil edilmesi ile azaltılabilmektedir.

Kuruluşlar, CIS Kontrolleri çerçevesinde ayrıntılı olarak açıklanan kontrolleri uygulayarak siber güvenlik duruşlarını güçlendirebilir; nitekim kontroller, hayati sistemleri, verileri ve varlıkları siber tehditlerden korumak için geçmiş tecrübelerden faydalanılarak tasarlanmıştır. Ancak bu kontrollerin, şirketin faaliyet koluna, amaçlarına, eğer var ise fazladan sektör standartlarına ve karşı karşıya olduğu tehditlerin doğasına uygun hale getirilmesi gerekliliği de değerlendirilmelidir. Verimli bir siber güvenlik mimarisini sürdürmek ve gelişen siber tehditlere karşı sürekli korumayı garanti etmek, sürekli izleme, değerlendirme ve geliştirme gerektirmektedir.

Ek CIS Kontrolleri, *Critical Security Controls - CSC* çerçevesi kapsamında *Temel, Kuruluşsal/Örgütsel* ve *Organizasyonel* kategorileri altında bulunan kontrolleri destekleyen diğer ilintili kontrolleri içerir:

•Yapılandırma ve Güvenlik Açığı Yönetimi

Kuruluşlar, yapılandırma ve güvenlik açığı yönetimi ilkelerini uygulayarak güvenlik açıklarını daha iyi yönetebilir ve sistemleri güvende tutabilir. Bazı örnekler şu şekildedir:

• Kurumsal Varlıkların Güvenli Yapılandırması

İşletim sistemleri, uygulamalar ve ağ cihazları için güvenli yapılandırmalar ayarlayarak ve uygulayarak tehditlere maruz kalmayı azaltın ve kuruluşunuz genelinde tek tip güvenliği garanti edin.

• Sürekli Güvenlik Açığı Değerlendirmesi ve Düzeltme

İstismar olasılığını azaltmak için, güvenlik açıklarını tespit etmek ve önceliklendirmek için düzenli güvenlik açığı değerlendirmeleri yapmak önemlidir.

• Sızma Testi ve Kırmızı Takım Egzersizleri

Sistemlerde, ağlarda ve uygulamalarda güvenlik açıkları bulmak ve ardından bunları düzeltmek için düzenli sızma testleri ve saldırı simülasyonları gerçekleştirilmesidir.

Veri koruması

Kurum ve kuruluşlar, müşterilerinin güvenini korumak ve gizlilik yasalarına uyma zorunluluklarını karşılayabilmek adına müşterilerinin kişisel bilgilerinin

güvenliğini sağlamalıdır. Bu kapsamda, dayatılması gereken veri güvenliği önlemlerine bazı örnekler akademik literatürde alt başlıklar halinde şu şekilde özetlenebilir:

• Veri Güvenliği ve Gizlilik Politikaları

Gizlilik yasalarına uygun kalmak için kişisel bilgileri toplamak, depolamak ve göndermek için şeffaf protokoller oluşturun.

• Veri kaybı önleme

Veri kaybını önleme (DLP) önlemlerini devreye alarak hassas bilgileri çalınmaya, tehlikeye atılmaya veya kaybolmaya karşı koruyun.

• Şifreleme

Bekleyen ve aktarılan veriler, şifreleme araçlarıyla korunabilir, bu da bilgileri okunamaz hale getirir ve çalınsa bile bilgisayar korsanları için işe yaramaz hale getirir.

Olaya Müdahale ve Kurtarma:

Kurum ve kuruluşlar, siber güvenlik sorunlarını daha kolay tespit edebilmek, yanıtlayabilmek ve bu sorunları bertaraf etmek adına sağlam bir olay müdahalesine ve yerinde kurtarma kapasitesini barındırmayı hedeflemelidir. Olay Müdahale ve Kurtarma başlığı altında sağlanması gereken kontroller gruplandırılacak olur ise:

• Olay Müdahale Planı

Bir siber saldırı durumunda kimin neyi ve nasıl yapacağını belirleyen, siber saldırı olayındaki tüm paydaşları kapsayan bir olay müdahale stratejisi oluşturulmasıdır.

• Olay Tespiti ve Müdahale

Siber olayların yaşanmasından hemen sonra tespit edilmesi ve tespitin üzerine hızlı aksiyon alınması, olaydan asgari zarar ile çıkılması noktasında önem arz ettiğinden; izleme sistemleri, günlük olay analizi ve tehdit istihbaratı kullanılarak elde edilebilen tespit ve müdahale oluşturulmasına dair gerekliliğin belirtilmesidir.

• Yedekleme ve kurtarma

Bilişim sisteminin ele geçirilmesi veya tehlikeye girmesi durumunda, önceden alınan son yedeklemelerden hızlı ve kolay bir şekilde geri yükleme işlemi sağlanabilmektedir, bu nedenle önemli veriler ve verilerin akışında görev alan sistemlere dair detayların düzenli olarak yedeklenmesi, zararın kısmi ya da bütüncül olarak giderilebilmesi açısından önem arz etmektedir.

Güvenlik Yönetişimi

Yerinde sağlam bir güvenlik yönetişimi, yani kurum veya kuruluş üst yönetiminin güvenlik nezdindeki farkındalığı ve bu farkındalığı uygulama iradesinin mevcudiyeti; siber güvenliğin önceliklendirilmesi, iyi yönetilmesi ve kurum veya kuruluş hedefleri doğrultusunda olmasının önünü açmaktadır. Güvenlik yönetimiyle ilişkili bazı kontroller dört farklı alt başlıkta değerlendirilmektedir:

• Güvenlik Politikası ve Yönetişim Çerçevesi

Siber güvenlik girişimlerinize rehberlik edecek ve geçerli tüm yasalara ve standartlara uygun, her şeyi kapsayan bir güvenlik politikası oluşturulmasıdır.

• Risk yönetimi

Eğitimli kararlar almak ve kaynakları etkin bir şekilde tahsis etmek için siber güvenlik risklerini tespit edebilen, değerlendirebilen ve sıralayabilen bir risk yönetimi stratejisi uygulanmasıdır.

• Güvenlik Farkındalığı ve Eğitimi

Sık sık güvenlik farkındalığı ve eğitim oturumları düzenleyerek personellerin başta düzenleyici yönetmelik ve kanunlar olmak üzere, siber güvenlik riskleri, en iyi uygulamalar ve bireysel sorumlulukları hakkında bilgilendirilmesidir.

• Satıcı Risk Yönetimi

Dışarıdan sağlanan hizmetlere dair prosedürlerin değerlendirilerek, dış satıcıların ve tedarikçilerin kullanılmasıyla ilişkili güvenlik risklerinin bütüncül olarak yönetilmesidir.

Kuruluşlar, CIS kuralları çerçevesinde açıklanan kuralları benimseyerek siber güvenlik duruşlarını geliştirebilir ve siber saldırılara karşı savunmasızlıklarını azaltabilir. Ancak siber güvenlik, sürekli gelişen tehditlere ve zayıflıklara ayak uydurmak için sürekli değerlendirme, izleme ve ayarlama gerektiren devam eden bir süreçtir. İşletmeler, sürekli değişen siber güvenlik ortamına ayak uydurabilmek için güvenlik önlemlerinin etkinliğini düzenli olarak değerlendirmeli, prosedürlerini ortaya çıkan tehditleri hesaba katacak şekilde uyarlamalı ve güncellemeleri takip etmelidir.

4. TARTIŞMA

Nesnelerin İnterneti düzleminde gerçekleşen siber saldırılar, otomobil sektöründe Nesnelerin İnterneti uygulamalarının da var olduğu düşünüldüğünde, bütüncül bazda otomotiv endüstrisini etkilemiştir hipotezi kurulabilir. Bu kapsamda, otomobil sektörüne yapılan saldırıların, bahsi geçen saldırı yüzeyi, güvenlik açıkları ve riskleri, örnek olaylar ve son olarak da olayların tespiti başlıkları tarafından sağlanan bilgi envanteri ile bir tartışma yaratılarak, olayların adli bilişim açısından incelenmesi ve adli bilişim kapsamında üretilecek bir çerçevenin sürece dair sorunlara çözüm üretmesi gerekliliği ortadadır.

Sonuç olarak, bu çalışma boyunca sunulan kapsamlı analiz, araştırma ve verilerin ışığında değerlendirmek gerekirse, bağlantılı araçların siber güvenlik açısından değerlendirilmesinin bağlı gerçeklikler maddi boyutta göz önünde bulundurulduğunda oldukça niş kaldığı ve bu alandaki siber güvenlik uygulamalarının mevcut durumunun, kuruluşların karşı karşıya kaldığı sürekli büyüyen ve gelişen tehditleri ele almada ne yazık ki yetersiz olduğu görülmektedir. Bulgular, mevcut çerçeve ve uygulamalar içindeki kritik boşlukları, güvenlik açıklarını ve eksiklikleri net bir şekilde aydınlatarak, yeni ve kapsamlı bir yaklaşıma olan acil ihtiyacın görünürlüğüne işaret etmektedir.

Mevcut siber güvenlik uygulamalarında tespit edilen güvenlik açıkları, hassas bilgilerin ve kritik sistemlerin gizliliği, bütünlüğü ve kullanılabilirliği açısından önemli riskler oluşturmaktadır. Güncelliğini yitirmiş veya parçalanmış güvenlik protokolleriyle birleşen siber saldırıların artan karmaşıklığı ve sıklığı, bu riskleri daha da artırmaktadır. Başarılı bir siber saldırının potansiyel sonuçları, mali kayıplar ve itibar kaybından yasal sonuçlara ve tehlikeye atılmış kamu güvenliğine kadar uzanır.

Bu riskleri etkili bir şekilde azaltmak ve siber tehditlere karşı koruma sağlamak için yeni bir çerçeve zorunludur. Bu kapsamlı çerçeve, risk değerlendirmesi ve yönetiminden teknik kontrollere, farkındalık ve eğitim programlarına ve olay müdahale yeteneklerine kadar çeşitli temel boyutları ele almalıdır.

Kuruluşlar, güçlü bir risk değerlendirmesi ve yönetim metodolojisini entegre ederek, bağlamlarına özgü potansiyel güvenlik açıklarını ve tehditleri proaktif olarak tanımlayabilir ve öncelik sırasına koyabilir. Bu, kaynakların tahsis edilmesini ve riskleri etkili bir şekilde azaltmak için hedeflenen önlemlerin uygulanmasını sağlayacaktır.

Teknik altyapının modernleştirilmesi, yeni çerçevenin bir diğer önemli yönüdür. Kuruluşlar, gelişmiş güvenlik kontrollerini benimseyerek savunma mekanizmalarını geliştirebilir ve kritik sistemleri yeni ortaya çıkan siber tehditlere karşı güçlendirebilir. Şifreleme mekanizmaları, güvenli ağ mimarileri ve saldırı tespit sistemleri, hassas veri ve altyapının gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için entegre edilmesi gereken temel bileşenlerdir.

Siber güvenliğe öncelik veren bir organizasyon kültürü, herhangi bir çerçevenin başarısı için temeldir. Çalışanları ve paydaşları siber güvenliğin önemi, bilgi varlıklarını korumadaki rolleri ve tehdit algılama ve önleme için en iyi uygulamalar hakkında eğitmek için kapsamlı farkındalık ve eğitim programları uygulanmalıdır. Kuruluşlar, güvenlik bilincine sahip bir zihniyet geliştirerek insan hatası riskini önemli ölçüde azaltabilir ve her düzeyde sağlam güvenlik önlemlerinin benimsenmesini sağlayabilir.

Ek olarak, siber güvenlik olaylarının etkisini azaltmak için etkili bir olay müdahale planı hayati önem taşır. Olay tespiti, kontrol altına alma, yok etme ve kurtarma için iyi tanımlanmış prosedürler oluşturmak, hasarı en aza indirmek ve operasyonları hızla geri yüklemek için çok önemlidir. Olay müdahale planının

düzenli olarak test edilmesi, değerlendirilmesi ve iyileştirilmesi, ortaya çıkan tehditleri ele almadaki etkinliğini sağlayacaktır.

Özetle, mevcut siber güvenlik uygulamalarının yetersizlikleri göz önüne alındığında, bu özel alanda acilen yeni ve kapsamlı bir çerçeveye ihtiyaç duyulduğu tartışılmaz. Kuruluşlar böyle bir çerçeveyi uygulayarak siber dayanıklılıklarını güçlendirebilir, hassas bilgileri ve kritik sistemleri koruyabilir ve siber saldırıların potansiyel olarak yıkıcı sonuçlarını azaltabilir. Proaktif risk yönetimi, çağdaşlaştırılmış teknik kontroller, güvenlik bilincine sahip bir kurumsal kültür ve sağlam bir olay müdahale planı toplu olarak daha güvenli ve dayanıklı bir siber ortama katkıda bulunacaktır.

Otomotiv sektöründe yürütülen saldırılara dair, kapsam ve amaç ile birlikte örneklendirmeler ve potansiyel sorunlar da belirtilerek bir çerçeve çizmiştik. Bu noktada, saldırıların daha fazla yaşanmamaları ve mükerrer olmamaları adına gerekli önlemlerin alınmasının gerekliliği açıktır. Otomotiv endüstrisinde, aslında birçok farklı işten sorumlu paydaş olsa da paydaşları üretici ve tüketici-kullanıcı şeklinde iki ana başlık halinde gruplandırmak mümkündür. Bu paydaşlar; kullanıcılar ve üreticilerdir ve kendilerinden beklenen önlem yöntemlerine dair görüşler şu şekildedir:

Kullanıcılar tarafından otomobillerde yaşanan siber güvenlik olaylarında alınması beklenen önlemler niceliksel olarak oldukça sınırlıdır, nitekim siber güvenlik alanında medyan otomobil kullanıcıların bilgisinin sınırlı olduğu söylenebilir. Kullanıcı kitlesi, özellikle bu alan hakkında az bilgi sahibi olan kişiler, konu hakkında ancak kendilerine medya tarafından hangi noktalara dikkat çekiliyor ise o noktada bir bilgi edinimi sağlayabilmektedir. Medya tarafı ise, bu noktada yalnıza gerçekleşen olayları bildirmek için bir taraf seçiyor gibi gözükmektedir, zira basın mensuplarının da konuyla ilgisi oldukça sınırlıdır. Dolayısıyla medyada basın tarafından raporlanan olaylar ancak *gerçekleşmiş* olaylardır ve doğal olarak gerçekleşmiş olayların önüne geçmek veya gerçekleşmiş olaylara önlem mahiyetinde aksiyon almak mümkün değildir. Bu aşamada kullanıcılar, yalnızca badire atlatmış,

sorun yaşamış üreticilerden uzak durabilirler ancak bu da makul bir yol gibi gözükmemektedir, bilakis otomotiv endüstrisinde belli partilere talebi öldürmek olur, ki oyun teorisi kapsamında sektöre dair genel bir erozyona sebebiyet verebilir. Neticede, siber saldırı olaylarını tecrübe etmiş üreticiler de bu olayın gerçekleşmesini istemeyen üreticilerdir ve örneklerde görüldüğü gibi üretici sorun yaşandığı takdirde hemen önlem almaktadır. Dolayısıyla bu noktada kullanıcıların alması beklenen tek önlem, konuya dair bilinç kazanarak saldırı yüzey alanını daraltmak olarak not edilebilir. Örneğin, kullanıcının telefonunda aracı kontrol eden bir yazılım varsa, cep telefonuna kaynağı belirsiz uygulama yüklenmemesi konusunda dikkat edilmelidir ki aracın kontrolünün istenmeyen kişilerin eline geçmesi dolaylı yoldan engellenebilmelidir.

Otomotiv alanında Nesnelerin İnternetini hedefleyen siber saldırılara önlem alması gereken diğer paydaş, otomobil üreticileridir. Mekanik ve elektronik manada yürütülen araştırma ve geliştirme faaliyetlerinin yükünü çeken üreticilerin, son dönemde artan dijitalleşme ile birlikte bilişim teknolojilerinin otomobillere yansıması alanında da inisiyatif almaları zorunlulukları doğmuştur. Bu zorunluluklara binaen, gerçekleşen ve sayısı günden güne artan siber güvenlik olaylarının çözülebilmesi adına üreticilerin alması gereken başlıklar, maddi kaynaklar, destekler, üretim aşamasında dikkat edilmesi gereken parametreler ve insan kaynağına yapılması beklenen yatırımlar olarak özetlenebilir.

Üreticilerin önlem mahiyetinde sağlaması gereken ilk husus, doğal olarak bütçedir. Her ne kadar bilişim teknolojilerinin önemi diğer sektörlerde oldukça çabuk kavransa da otomobil sektörü yapısı gereği durağanlaşmaya müsaittir ve bu konudaki yatırımlara dair küresel şirketlerin üst yönetimleri en azından içinde bulunduğumuz dönemde oldukça temkinli yaklaşmaktadır. Sorunların önlenebilmesi adına maddi meselelere dair sınırların yukarı yönlü esnetilmesi, birincil derecede önem arz etmektedir. Ayrıca, özel sektör firmalarının karşılaştığı siber güvenlik riskleri ve olayları şu temel soruyu gündeme getirmektedir: Özel sektördeki bir firma siber güvenlik faaliyetlerine ne kadar yatırım yapmalıdır? Yukarıdaki soruyu yanıtlamak, ABD Kongre Duruşmalarının (ör. ABD İç Güvenlik Komitesi'nin 2007 Alt

Komitesi), akademik araştırmaların (Gordon ve Loeb, 2002) ve sektör oyuncularının arasındaki tartışmaların konusu olmuştur. Ne yazık ki, bu sorunun basit bir cevabı yoktur (Gordon ve ark., 2015).

Üreticiler tarafından sağlanabilecek bir diğer önlem adımı, otomobil sektöründe yaşanacak siber güvenlik saldırılarının ekonomisi, amacı, kapsamı, incelenmesi ve önlenmesine dair akademik çalışmaların desteklenmesidir. Bu alanda yapılan akademik çalışmalarda, geçtiğimiz on yılda bilişim teknolojilerinin eklemlendiği ilk yıllara göre daha fazla hareketlilik gözlemlenmiş ve bu durum aslında birçok teknolojik sistemin araçlara dahil edilmesiyle aynı zamana denk gelmiş olsa da sektörde yapılan akademik literatürün hala eksik olduğu gerçeği ortadadır. 1989'dan 2018'e kadar, araçlarda siber güvenlik literatüründeki katkı toplam yayınların %7,16'sını oluştururken, araç denetimi ve belgelendirme ile ilgili akademik yayınlar tüm literatürün hala %0,24'ünü oluşturmaktadır. Ayrıca, özel şirketler (%22,28) ve ağırlıklı olarak Kuzey Amerika ve Avrupa'da (%38,49 ve %35,84) bulunan diğer araştırma merkezlerine (%14,20) kıyasla üniversitelerden (%63,50) daha yüksek bir akademik katkıda bulunmuştur (Mateo Sanguino ve ark., 2020). Bu durum, akademik nosyonun halen dünya genelinde yaygınlaşmadığını ve uyarıcı söylemlerin ve yatırımların karşılık bulmadığının dolaylı bir göstergesi olarak ele alınabilir.

Siber güvenlik riski değerlendirme çalışmalarının, araç yazılımlarının geliştirme döngülerine direkt olarak eklenmemesi ve risk değerlendirme çalışmalarının, bütçe ve zaman önemli görülmesinden hareketle ikinci planda bırakılması, yaşanan siber güvenlik olaylarının bir diğer temel sebebidir. Buradan hareketle, kötü niyetli kişilerin olası siber güvenlik zaaflarını kullanarak araçlar üzerinde tahakküm elde etmesinin önüne olaylar yaşanmadan geçilebilmesi ve olaylar gerçekleştikten sonra da proaktif çözümlerin hızlıca alınarak can ve mal kaybına sebebiyet vermeden aksiyon alınabilmesi adına, geliştirme faaliyetlerini siber güvenlik risklerini düşünerek gerçekleştirmesi önem arz etmektedir.

Otomotiv sektörünün siber güvenlik olaylarına karşı önlem mahiyetinde alabileceği bir diğer mesele, sektörde yetişmiş insan gücüdür. Konuya azami önem gösteren ülkelerin hükümetleri, endüstri ve akademi, iyi gelişmiş siber güvenlik insan kaynakları açığının ele alınmasının kuruluşlar için bir öncelik haline geldiği konusunda büyük ölçüde hemfikirdir. Bu son derece uzmanlaşmış ancak kötü tanımlanmış iş gücünün, yetersiz yatırım yapılan eğitim süreçlerinden ve kopuk geliştirme programlarından mustarip olduğuna dair geniş bir kabul söz konusudur (Assante ve Tobey, 2011). Buradan hareketle, siber güvenlik operasyonlarının her bir safhasında yer alacak insan gücünün sağlanması noktasında otomotiv endüstrisi paydaşlarının, iş imkanlarını çeşitlendirmek, maddi konularda gerekli düzenlemeleri sağlamak ve yetenekli insanların konuya ilgisini cezbetmek adına harekete geçmesi için adımlar atmasına dair ihtiyaç bakidir.

Kullanıcıların satın alma işlemi öncesinde, sırasında ve sonrasında şeffaf şekilde bilgilendirilmesi, üreticiler tarafından alınabilecek bir diğer önlem yöntemidir. Bu yolla, kullanıcıların alabileceği önlemler için de bir temel hazırlanmış olur. Araç satın alımı öncesinde kullanıcılar, daha önce yaşanan siber güvenlik olaylarının şeffaf şekilde bildirilmesi ile ne gibi sorunların yaşanabileceği noktasında bilinç kazanabilmektedir. Benzer şekilde, araçların satın alımı esnasında teslimat süreçlerinde hazırlanabilecek bir kullanım kitapçığı ile potansiyel riskler işaret edilebilir. Son olarak da araçlar satın alındıktan sonra yaşanan siber güvenlik olaylarına anında müdahale sağlanmalı, araç sahipleri siber güvenlik olayına dair çeşitli kanallar üzerinden bilgilendirilmeli ve eğer araçlarda güncellemeye ihtiyaç duyulursa araçların ivedi şekilde ilgili servis hizmeti sağlayan işletmelere götürülmesi sağlanmalıdır.

Öte yandan Nesnelerin İnterneti teknolojisinin otomotiv sektöründe her geçen gün daha da artan sayıda farklı uygulamalarının görülmesi, bu alanı zafiyet olarak gören ve zafiyetlerden maddi yahut manevi çıkar elde etmeyi hedefleyen kişi veya grupların ilgisini cezbetmektedir. Bu kapsamda, ilerleyen bölümlerde detayları aktarılacak olan çalışmanın önemi anlaşılabilmesi adına, sunulan bilgilerin farklı bir

perspektif ile ele alınarak değerlendirilebilmesi ve gerekli etkinin yaratılabilmesi adına sunulan bilgiler gereklidir.

Nesnelerin İnterneti ekseninde siber olayların ve ilgili diğer güvenlik olaylarının temelden çözülmesi adına muhtelif hipotezler ortaya konulabilse de bu çözüm yöntemlerinin karşılaşabileceği potansiyel sorunlar değerlendirilmeden mantıksal çıkarım yapmak zordur. Nitekim, bu sorunların önceden bilinmesi ve adli bilişim kapsamında önerilecek yeni çerçevede bu sorunlara dair işaretlerin eklenmesi, sürecin sürekli iyileştirilmesi ve manalı çıktıların ivedilikle uygulamaya alınabilmesi adına oldukça önemlidir.

Otomobillerdeki Nesnelerin İnterneti sistemleri üzerinde gerçekleşmesi muhtemele siber güvenlik saldırılarının önlenmesi ve olaylar gerçekleştikten sonra ivedilikle aksiyon alınmasının önündeki engellerden ilki, yasal ve düzenleyici uyum sorunlarıdır.

Öncelikle, siber güvenlik olaylarının önüne geçilebilmesi adına ortaya konulması gereken dünya çapında bir iradedir. Ancak konuyla alakalı gerekli sorgulamalar yapıldığında, uluslararası bir dayatma eksikliği görülmektedir. Bu gerçekliğin yanında, doğal olarak ülkelerin kanunlar yerel çapta etkiye sahiptir. Kanun kapsamında konuyla ilişkili olarak veri sızıntıların önüne geçilmesine dair Avrupa Birliği ülkelerinde geçerli çatı kanun GDPR mevcut iken, ülkemizde bu gereklilik de 6698 sayılı Kişisel Verilerin Korunması Kanunu üzerinden sağlanmaktadır. Bu kanun, verilerin korunmasına dair oldukça güçlü sınırlar çizerek gereksinimleri sağlamaya yönelik adımlar atsa da kahir ekseriyetle değişiklikler öncelikle Batı Avrupa ülkelerinden kaynaklanmakta ve ülkemizde bu değişikliklerin yansımaları nispi olarak daha geriden gelmektedir. Bu duruma bir diğer örnek olarak, Birleşik Krallık verilebilir, zira Birleşik Krallık'ın Avrupa Birliği'nden çıkışına neden olan halk oylaması ayrılma lehinde sonuçlandıktan sonra, başta İngiltere olmak üzere Anglo-Sakson hukuk sistemini kullanan ülkeler, hukuk sistemlerinin içtihada dayalı olması neticesinde bocalamışlardır. Yasal ve Düzenleyici uyumlarından kaynaklanan uyumsuzluklara, ülkemizde otomobillerde yer alan acil

durum (SOS) modülünün kullanılması gösterilebilir. Düzenleyici kurum statüsündeki BTK, kişisel veriler konusunda yetkili kurum olan Kişisel Verileri Koruma Kurumundan aldığı danışmanlığa da binaen, ülkedeki yasal düzenlemeyi dayanak göstererek veri güvenliği ve gizliliği endişeleri yüzünden acil durum sisteminin kullanacağı araçlara dair verilerin (aracın konumu, durumu vb.) Türkiye'de tutulmalı şeklinde görüş beyan etmiştir. Üretici firmalar ise zaten Avrupa Birliği sınırlarında serbest dolaşım sebebiyle kendi veri tabanlarına sahip olmaları sebebiyle maliyetleri de gerekçe göstererek Türkiye Cumhuriyeti sınırları içerisinde ayrıca bir veri merkezi açmak istememektedir. Bu hukuki dayatmanın sonucunda da SOS modülleri, canlı trafik verisi; sürücü ve araç sahiplerinin verileri korunamaz ya da Türkiye Cumhuriyeti gerekli mercileri tarafından denetlenemez endişeleri ile kullanılamaz duruma gelmektedir.

Bu durumun aşılabilmesi adına, konunun uluslararası boyutta tartışılabilmesi, farklı birlik ve devletlerin bu konuda bir yönetişim iradesi göstermesi, ilgili kanunların uluslararası düzlemde belirlenmiş ve ülkeler tarafından imzalanmış çerçeveler nezdinde geliştirilmesi ve denetlenebilmesi için adımların atılması gerekliliği açıktır.

Otomobil üreticileri, henüz tam anlamıyla dijitalleşememiş ancak dijitalleşme yolunda büyük bir hızla adımlar atan sektörün gerçekliklerine uyum sağlamakta güçlük çekmektedir. Nitekim, otomobillerin barındırdığı Nesnelerin İnterneti modülleri nezdinde gerçekleşebilecek siber saldırılardan çıkarılan dersler, bu alana olması gereken özenin gösterilemediği yönündedir. Bu noktada, otomotiv endüstrisinin büyük oyuncularının bütçe yetersizlikleri, önerilecek bir iyi uygulama çerçevesinin karşısında önemli bir engel faktörü olarak ortaya çıkabilir.

Otomobil üreticilerinin sistemlerini, olası siber güvenlik meselelerine karşı düzenleyebilmesi için geliştirilen bir çerçeveye uyması, büyük bir güncelleme sorumluluğunu da beraberinde getirecektir. Şu anda kullanımda olan ve farklı firmalar tarafından farklı kronolojik gündem göz önünde bulundurularak geliştirilmiş sistemlerden bazıları, güncelleştirme sürecinde ait oldukları arabanın kullanılamaz

kalmasına neden olacak yahut uzaktan güncelleme imkânı mümkün olsa bile servis dışı kalarak en azından sınırlı bir süre için kullanılamaz durumda yer alacaktır. Bu durum, müşteri memnuniyeti açısından oldukça sıkıntılı bir atmosfer yaratacağı için, otomotiv şirketleri her türlü diğer parametrenin olumlu olduğu bir iyi uygulamalar sürecinden sonra dahi problem yaşamaya namzet olacakları için gönülsüz davranabileceklerdir.

Siber güvenlik iş gücü, ilgili eğitim süreçlerine yetersiz yatırım yapılmasından ve parçalanmış bir eğitim ve geliştirme programları kadrosundan mustariptir (Hoffman ve ark., 2012). Dünya çapında bilişim alanında fırsat gören veya bu alanda çalışmalar konusunda bilgi sahibi her bir hükümet, şirket ve akademik paydaş; siber güvenlik uzmanlarının eğitim ve gelişimini büyük ölçüde ulusal güvenlik önceliği olarak görmektedir. Tahmin edilene göre, ihtiyaç duyulan siber güvenlik alanında yetkin kişilerin sayısı, hali hazırda siber güvenlik alanında istihdam edilen kişi sayısının neredeyse yirmi beş katıdır, bu durumda siber güvenlik uzmanlarını eğitmek ve işe almak için kapsamlı, koordineli bir strateji gerektirecektir. Ancak, akademik literatürün paydaşlarından çıkarımda bulunulabileceği üzere, otomotiv endüstrisinde kâr marjının şu anda çok düşük seviyelerde seyretmesi sebebiyle, bu açığın otomotiv endüstrisi şirketlerinin istihdamı ile sağlanamayacağı ihtimali üzerinde düşünülmelidir. Bu durumda otomotiv endüstrisi şirketleri, dışarıda yetişmiş siber güvenlik insan kaynağını üzerine çekebilmek adına farklı stratejiler benimsemek durumunda kalabilecektir.

Otomotiv sektöründe gerçekleştirilen siber saldırılara dair bir araştırma yürütüldüğünde, bu saldırıların her birinin farklı kaynaklar üzerinde rapor edildiği ve farklı internet mecralarında bu saldırılar özelinde tartışmalar yürütüldüğü görülebilir. Nitekim, otomotiv siber saldırıları örnekleri de bu durumdan müstakil değildir, bu saldırılara dair detaylı bilgilendirmeler farklı internet siteleri veya forumlardan elde edilebilmiştir. Ayrıca, otomotiv sektöründeki Nesnelerin İnterneti siber saldırılarına dair not edilmesi gereken bir diğer nokta da bazı saldırıların mükerrer olduğu şeklindedir. Yapılan saldırılardan bazıları, tamamen aynı bileşenler üzerinden, aynı sonuçları hedefleyen ve bir kısmı da aynı yöntem akışını takip eden saldırılardır. Bu

durumda, otomotiv sektöründe siber saldırıların önlenmesi adına gerekli olan bilgi paylaşım ve koordinasyon alanında yetersizlik olduğu ihtimalinden söz edilebilir. Nesnelerin İnterneti alanında yaşanacak tersine devinimsel hareketlerin önüne geçebilmek adına, paydaşlar arasında bilgi paylaşıma dair gerekli altyapının kurulması gerekliliği, sorunların çözümü isteniyorsa oldukça önem arz edecektir.

Otomotiv endüstrisi, Nesnelerin İnterneti cihazları ve sistemleri için tek tip güvenlik gerekliliklerinden yoksun olduğu için bir zorluk ortaya çıkıyor. Tek tip kural kümesinin ve uygulamaların olmaması nedeniyle, farklı üreticiler ve tedarikçiler arasında benzer düzeyde bir güvenlik sağlamak zordur. Katı güvenlik standartlarının oluşturulmasıyla riskler azaltılabilir ve ekosistemdeki güvenlik iyileştirilebilir.

Nesnelerin İnterneti uygulamalarının otomotiv sektöründeki yansımalarında, olayların incelenmesi adli bilişim pratiklerinden bağımsız düşünülemez. Dolayısıyla, bu olayların incelenmesinde, toplama, inceleme, çözümleme ve raporlama paradigması ayrılmaz bir bütünlük oluşturmaktadır. Nesnelerin İnterneti saldırılarında daha bütüncül bir yaklaşım sergileyebilmek adına madalyonun öbür yüzünü, geçmişte yaşanan saldırılardan dersler çıkarılması oluşturmaktadır. Alınan derslerin etkisi büyük olsa da farklı eksendeki olası sorunlar, Nesnelerin İnterneti uygulama ve sistemlerindeki siber güvenlik olaylarının temelden çözülebilmesi iradesinin zarar görebilmesinin önünde bir engel olabilmektedir.

İşletmeler, güvenilir siber güvenlik uygulamalarını benimsemekte ve uygulamakta başarısız olduklarında, kendilerini çok çeşitli tehditlere ve olumsuz sonuçlara maruz kalma riskine sokarlar. Yeterli siber güvenlik önlemleri alınmadığında şirketlerin veri ihlallerine maruz kalma olasılığı daha yüksektir. Güvenlik açıkları, kötü kişiler tarafından müşteri kayıtları, ticari sırlar ve fikri mülkiyet dahil olmak üzere özel bilgileri çalmak için kullanılabilir (Opoku, 2021). Önemli parasal kayıplar, itibar zedelenmesi ve yasal yükümlülükler bir veri ihlalinden kaynaklanabilir.

Şirketler siber saldırılar sonucunda yıkıcı mali kayıplara maruz kalabilir. Adli soruşturmalar, sistem onarımları, yasal ücretler ve olası yasal para cezaları, bir olayın müdahalesi, kurtarılması ve iyileştirilmesi sonucunda ortaya çıkabilecek masraflardan sadece birkaçıdır (Weyer ve ark., 2016). Siber saldırılar aynı zamanda operasyonel aksamalara yol açarak iş, üretkenlik ve hizmetlerin sağlanması için harcanan zaman kaybına neden olabilmektedir. Bir şirketin müşterilerinin güveni ve markasının bütünlüğü siber saldırılara karşı savunmasızdır. Bir güvenlik olayı veya veri ihlaliyle ilgili, siber saldırı neticesinde elde edilen bilgi ve belgeler dahi, hızla yayılabilmekte, bu da kötü bir habere ve müşteri güveninin azalmasına neden olabilmektedir. Sonuç olarak müşteri sadakati, gelirler ve marka değeri darbe alabilmektedir. Bir halkla ilişkiler felaketinden sonra müşterilerin güvenini geri kazanmak zor ve pahalı olabilir.

Endüstri kurallarına ve veri koruma mevzuatına uyulmaması, yetersiz siber güvenlik önlemlerinden kaynaklanabilir. Genel Veri Koruma Yönetmeliği (GDPR) ve diğer kurallar, kişisel olarak tanımlanabilir bilgilerle ilgilenen işletmeler için katı kurallar koyar. Uyulmadığı için yasal sonuçlar, düzenleyici para cezaları ve kişinin itibarına zarar gelebilir. İşletmeler siber güvenlikten mahrum kaldıklarında, fikri mülkiyetlerini riske atarlar. Bilgisayar korsanları ticari sırlar, Ar-Ge verileri ve diğer gizli bilgiler gibi fikri mülkiyetleri çalabilir (Saleem, 2017). Bu nedenle, şirketin yenilik yapma ve pazarda rekabet etme yeteneği zarar görebilir ve rakipleri haksız bir avantaj elde edebilir.

Siber saldırıların kamu güvenliği ve enerji, ulaşım ve sağlık gibi sektörlerdeki temel altyapı üzerinde yıkıcı etkileri olabilir. Bilgisayar korsanları tarafından hayati altyapıya yapılan saldırılar, hayati hizmetlere güvenenlerin güvenliğini tehlikeye atarak operasyonları kesintiye uğratabilir. Güç şebekelerinin, ulaşım ağlarının veya tıbbi cihazların saldırıya uğradığı senaryolar bu kategoriye girer. Fidye yazılımı saldırıları artıyor ve her ölçekten ve her sektördeki işletmeleri etkiliyor. Fidye yazılımı, yeterli siber güvenlik önlemi almamış herhangi bir işletme için bir tehdittir; verileri şifreler ve kurban onu geri almak için bir fidye ödeyene kadar rehin tutar.

Fidye ödense bile verilerin kurtarılacağının garantisi yoktur ve yine de şirketin itibarı zedelenebilir (Radanliev ve ark., 2019).

Şirketler, dış satıcılara ve tedarikçilere güveniyorlarsa tedarik zinciri güvenlik açıklarına karşı savunmasızdır. Saldırganlar, tedarik zincirindeki güvenlik açıklarından yararlanarak sistemleri tehlikeye atabilir, kötü amaçlı yazılımlar yerleştirebilir veya ürün ve bileşenleri kurcalayabilir. Tedarik zinciri tehlikeye girerse, ürün ve hizmetlerin bütünlüğü ile hassas müşteri bilgilerinin güvenliği tehlikeye girebilir. Ortaklar, müşteriler ve müşteriler arasındaki iş birliği, günümüzün birbirine bağlı iş ekosisteminde olağan bir durumdur. Bu paydaşlar tarafından dayatılan güvenlik yükümlülüklerine uyulmaması, yeterli siber güvenlik önlemlerinin alınmamasından kaynaklanabilir. Bu, bir şirketin ticari fırsatları kaçırmasına, ilişkilerin zedelenmesine ve hatta yasal sorunlarla karşı karşıya kalmasına neden olabilir.

Saldırganların karmaşıklığı ve yaratıcılığı, siber tehdit ortamında süregelen değişimi yönlendiriyor. Siber güvenliğe yeterince yatırım yapmayan kuruluşlar, bilgisayar korsanları için daha kolay hedef haline gelebilir. Güvenlik açıkları daha uzun süre yama yapılmadan bırakıldığında başarılı saldırı ve saldırı olasılığı artar. Saldırı yöntemleri, teknolojik ilerlemeyle birlikte gelişir ve yeni güvenlik açıkları sıklıkla kötü niyetli aktörler tarafından hedef alınır. Kuruluşlar, bu yaklaşımlar kullanılmazsa, sürekli olarak etkisiz siber güvenlik prosedürlerini atlatmanın yeni yollarını arayan siber suçlular için kolay bir avdır.

Kuruluşlar, günümüzün birbirine bağlı iş ortamında ortak hedeflere ulaşmak için genellikle ortaklar, tedarikçiler ve müşterilerle birlikte çalışır. Ancak, tek bir şirket bile siber güvenliği göz ardı ederse, tüm ağın güvenliği tehlikeye girebilir. İş ortakları, rakipleri tarafından kullanılan güvenlik önlemleri hakkında şüpheleri varsa, birlikte çalışmaktan veya gizli bilgi alışverişinde bulunmaktan çekinebilir (Opoku, 2021). Bu, geliştirme beklentilerini bastırabilir ve nihayetinde şirketin beklentilerine zarar verebilir. Bir siber felaket durumunda çalışanların morali ve çıktısı ciddi bir darbe alabilir. İhlaller ve saldırılar meydana geldiğinde, çalışanların kendilerini

güvensiz, güvensiz ve endişeli hissetmelerine neden olabilir. Bilgisayar korsanlığı ve veri ihlalleri gibi güvenlik tehditlerine ilişkin endişeler çıktıyı azaltabilir ve yaratıcılığı engelleyebilir. Çalışanlar ayrıca yönetimin kendilerine insan ve işçi olarak bağlılığından şüphe etmeye başlayabilir, bu da moral ve işten ayrılma için kötüdür (Opoku, 2021).

Kuruluşlar, sektöre özgü birçok farklı siber güvenlik standardı ve yasasına uymalıdır. Kuruluşlar, bu gereklilikleri yerine getirmezlerse ve yeterli siber güvenlik önlemlerini almazlarsa yaptırımlara ve yasal sonuçlara maruz kalabilirler. Ek olarak, çeşitli politikaların şartları, işletmelerin belirli siber güvenlik önlemlerini yerinde tutmasını zorunlu kılar (Paritala, Manchikatla ve Yarlagadda, 2017). Bu koşulların sağlanmaması durumunda teminat reddedilebilir veya primler artabilir. Kuruluşlar, yeterli siber güvenlik önlemleri alınmadan siber saldırıları belirleyemeyebilir, kontrol altına alamayabilir ve azaltamayabilir. Bir saldırı çok uzun süre fark edilmezse, saldırganın zarar vermek için daha fazla zamanı olur. Uzun süreli sistem kesintisi, finansal kayıplar ve itibar kaybı yetersiz kurtarma süresinden kaynaklanabilir (Paritala, Manchikatla ve Yarlagadda, 2017).

Günümüzün dijital ekosistemindeki müşteriler yahut alıcılar, üreticiler ve iş ortağı satış kanallarına dair kararları verirken güvenliğe önem atfetmektedir. Siber güvenliğe gereken önemi vermeyen üretici şirketler, kazançlı sözleşmeleri, değerli ittifakları ve müteallik diğer fırsatları kaçırma riskini de almaktadır. Günümüz atmosferinde bir üretici kuruluş, siber güvenliğe olan bağlılığını göstererek rekabette öne çıkabilir ve pazardaki konumunu geliştirebilir. Siber güvenlik ayrıca yaratıcı problem çözme ve teknolojik büyümeyi teşvik etmek için önemlidir. Siber saldırıların barındırdığı ve önceki tecrübelerden çıkarımı yapılan muhtelif ölçekteki riskler ve potansiyel etkiler nedeniyle işletmeler, gerekli koruma şartları sağlanmadan veya çevresel etkilerin riskleri sınırlandırılmadan güncel ötesinde teknolojilerle ilgilenmek veya dallanabilecek yeni araştırma ve geliştirme alanlarına yatırım yapma konusunda kayıtsız ve isteksiz olabilmektedir. Sonuç olarak, şirketin büyüme ve değişen pazar ihtiyaçlarına yanıt verme yeteneği engellenebilir.

5. SONUÇ VE ÖNERİLER

Yıllar ilerledikçe teknoloji trendleri de önceki devirlere göre değişim hızlarını üstel şekilde artırmaktadır. Mekanik ile başlayan endüstriyel devrim, sırasıyla elektronik ve şimdi de yazılım devrimi olarak devam etmektedir. Bu teknolojik devinimin içerisinde, otomobil sektörü de yerini almakta, doğrudan ve dolaylı yoldan paydaşların tepkimesi ile yaşadığı gerçekliklerin algısını değiştirmektedir.

Nitekim bu düzlemde, Nesnelerin İnterneti teknolojilerinin, silikon tabanlı mikroişlemcilerin araçlarda kullanımının oldukça artması ve diğer taraftan da 5G gibi taşınabilir iletişim teknolojilerinin geliştirilmesi neticesinde, önce kullanımının artacağı daha sonra ise araçlardan koparılamaz bir teknoloji gerçekliği olabileceğinden söz edilebilir. Nesnelerin İnterneti teknolojilerinin araçların bütünlüğüne müdahil olması, doğal olarak, Nesnelerin İnterneti teknolojilerinin araçların bütünlüğüne zarar verebilecek eylemlerin de bir parçası olması anlamına gelmektedir. Bir de Nesnelerin İnterneti uygulamalarının, yalnızca fiziksel değil aynı zamanda sanal müdahalelere de açık kapı bırakması, yani aslında internet ağına bağlı uygulamalardan mürekkep olmaları, bu istenmeyen dış müdahale durumuna çanak tutmaktadır.

Nesnelerin İnterneti teknolojilerinde yaşanan çeşitli siber güvenlik olayları şu zamana kadar görülmüş ve tasniflendirilmiştir. İşbu tasniflendirmeler kapsamında, siber güvenlik olaylarının farklı düzlemlerde meydana geldiğini ve çeşitli önlemler ile bu olayların yaşanma frekansının düşürülebileceği ihtimali üzerinde düşünülmektedir. Aynı zamanda, siber güvenlik olayları sonrasında bu olayların incelenmesi kapsamında adli bilişim aktörlerinin rol aldığı görülmektedir. Ancak, yapılan incelemeler ve yürütülen araştırma neticesinde, siber güvenlik olaylarının öncesi, bugünü ve sonrası olarak da açıklayabileceğimiz üç evresinin, adli bilişim pratiklerinden soyutlanmış bazı çerçeveler tarafından ele alınmaya çalışıldığı görülmüştür.

Sunulan bilgilerin ışığında, otomobiller nezdinde gerçekleşen siber saldırıların adli bilişim bakış açısı ile harmanlanmış ve oluşturulmuş bir çerçevenin tedrisatından geçmesi gerekliliği açıktır. Ancak bunu sağlayabilmek için, siber olayların önlem yöntemlerinin ve önlem yöntemlerinin uygulanabilmesi için gerek şart oluşturan faktörlerin açıklanması, yayılması, öğrenilmesi ve değerlendirilmesine dair adımların atılması gerekmektedir.

Önerilen çerçeve, hem gerek şart oluşturan faktörlere dair atılması gereken adımları, hem siber güvenlik düzenlemelerinde eksik kalan muhtelif kısımları hem de güncel kontrol denetimlerinin sağladığı proaktif yaklaşımların uyumuna dair kapsayıcı bir sonuç oluşturma gayesi ile hazırlanmıştır. Özellikle farklı araç üretici ve bu üreticilere ait sağlayıcıların çok girift bir matris oluşturduğu araç endüstrisinde, bu paydaşların sağlıklı kontrollerinin sağlanabilmesi adına çatı çerçeve kurumunun oluşturulması ve bu oluşumun denetleme ve düzenleme görevlerine sürekli iyileştirme faaliyetlerinde otorite teşkil etmesi fikri, daha önce farklı yüzleri ile değerlendirilse de şu aşamaya kadar değerlendirilmemiş bir yaklaşımın temsilidir. Aynı zamanda, siber güvenlik olaylarının adli bilişim yaklaşımlarına aynı çerçeve nezdinde aktarılması anlamlandırması da yine sektör paydaşları tarafından daha önce denenmemiş ve uygulanmamış bir gerçek olarak karşımıza çıkmaktadır.

Çerçevenin diğer iyi uygulamalardan farkları birçok noktadan oluşsa da burada temel çekirdeğin adli bilişim uygulamalarının iyi uygulamalar ile birleştirilerek çözüm arayışı oluşturulmasından bahsedilebilir. Bu çalışmada çalışmanın başlığına istinaden adli bilişim teorisinin, pratiklerinin, iyi uygulamalarının ve adli bilişim ile ilgili vaka analiz yöntemlerinin çerçevenin şekillenmesinde azami ölçüde göz önünde bulundurulduğu söylenebilir. İlerleyen süreçte, önerilen çerçevenin üzerine getirilecek kritikte, inşa edilecek yeni çerçevelerde yahut yine aynı çerçeve üzerinde yapılması beklenen değişikliklerde, bu durumun göz önünde bulundurulmasının gerekliliği açıktır.

Çalışmanın akışı içerisinde başta önerilen çerçeve olmak üzere siber saldırıların adli bilişim açısından değerlendirilmesi kriteri ön planda tutularak

aksiyon alınmış ve araştırmalar sağlanmıştır. Siber olayların adli bilişim açısından incelenebilmesi yetisine ek, aynı zamanda engellenmesi, tespit edilmesi, raporlanması ve yönetilmesine dair çalışmaların literatür kapsamında ele alınmasına ihtiyaç ise açıktır. Bu kapsamda, gelecekte gerçekleştirilebilecek çalışmaların kapsamını, bahsedilen bu başlıklar üzerinden ele almak potansiyel olarak mümkün gözükmektedir.

Ülkemizde otomobil üretimi oldukça eskilere dayansa da, akıllı araçların bir bütün olarak ele alınması ve üretim aşamalarının yüksek teknolojiye dayanan ihtiyaçlarının da yine ülkemiz nezdinde gerçekleştirilmesine dair adımlar oldukça yakın tarihlidir. Ayrıca, siber güvenlik süreçlerinin uçtan uca ele alınması, irdelenmesi ve yönetilmesi yaklaşımını benimseyen çalışmalar da literatürde uzunca süredir yer bulsa da sektör tarafından pratikte uygulanmaya başlaması görece yenidir. Bu iki bağımsız olgunun birleşiminden yola çıkılarak, ülkemizde akıllı araçların siber saldırı maruziyeti tanımı üzerinden hareketle gerekli akademik çalışmaların yürütülmesi, betimleyici ve tamamlayıcı aksiyonların alınabilmesi adına bilahare önem arz etmektedir.

Öte taraftan, daha önceden kullanılan veya günümüzde de kullanılmaya devam eden çerçevelerin de bu kapsamda üzerinden geçilmesinin ihtimali üzerinde düşünülmelidir. Bu konuda gerekli yardımlaşma, yine bu tez üzerinde sunulan yapılması gereken faaliyetler ve dikkat edilmesi gereken hususlar gibi altı çizilmiş noktaların yorumlanması üzerinden gerçekleştirilebilecektir.

ÖZET

Bağlantılı Araçlarda Nesnelerin İnterneti Siber Saldırılarının Adli Bilişim Açısından İncelenmesi

Otomotiv sektörü, alandaki ilk görülür araştırma ve geliştirme faaliyetlerinin yaşandığı on dokuzuncu yüzyıl sonlarından 1980'lere kadar neredeyse yüz sene boyunca, mekanik gelişmelerin diğer sektör ve alanlardaki gelişmelere nazaran daha baskın sayıda görüldüğü bir çalışma alanını temsil etmektedir. Öte yandan, dijitalleşme ile görülen yenilikçi adımların, 80'li yılların sonundan günümüze kadar otomotiv sektöründeki değişim ve ilerlemenin temelinde yer aldığını ise söylemek mümkündür. Günümüze kadarki son kırk yılı kapsayan süreç içerisinde, öncelikle araçlarda çift haneli sayılarda kendine yer edinen bilgisayarların var olduğu, sonrasında ise araçların çevreyle etkileşiminin tasarlandığı bağlantılı araç olgusunun sektörün merkezine oturtulduğu görülmektedir. Artan işlem yükünün bir sonucu olarak niceliksel olarak fazlalaşan işlem ünitelerinin varlığı, araçların yapısal güvenliği başta olmak üzere birçok alanda tehdit unsuru haline gelmesine sebebiyet verebilecek potansiyelde saldırı yüzey alanı oluşturmaktadır. Nesnelerin İnterneti fenomeninin sektörde kendine yer edinmesi ile otomobillerin kontrollerinden sorumlu yapıların diğer otomobiller ve/veya diğer ilgili cihazlar ile bağlantı kurmaları durumu ise, halihazırda var olan bu yüzey alanının ayrıca genişlemesine sebebiyet vermektedir. Sonuç olarak, bağlantılı araç elemanları arasındaki bağlantı sayısındaki artış ile üstel şekilde genişleyen saldırı zafiyet yüzeyinin akademik mercekte yeteri kadar irdelenmediği ve bu yolla ilerleyen süreç içerisinde sektör nezdinde duyulan ihtiyacı karşılamakta güçlük çekebileceği tespiti yapılmış olup; bu tez çalışması kapsamında bağlantılı araçlarda Nesnelerin İnterneti kullanımının kullanım alanları belirtilerek, işbu kullanım alanlarının oluşturduğu zafiyetler ve başta zafiyetlerin engellenmesi olmak üzere çözüm önerilerine dair teknikler araştırılmaktadır ve sonuç olarak bir çerçeve önerilmektedir.

Anahtar Sözcükler: Adli bilişim, Güvenlik açıkları, Nesnelerin İnterneti, Bağlantılı Araçlar, Siber saldırı

SUMMARY

Investigation of Internet of Things Cyber Attacks in Connected Vehicles in scope of Computer Forensics

The automotive sector represents a field of study where mechanical developments were more dominant than developments in other sectors and fields for almost a century, from the late nineteenth century, when the first visible research and development activities in the field were experienced to the 1980s. On the other hand, it is possible to say that the innovative steps seen with digitalization have been at the heart of the change and progress in the automotive industry since the end of the 80s. In the process covering the last forty years from those dates to the present, it is seen that first, there are computers that have a place in the vehicles in double-digit numbers, and then the connected vehicle phenomenon, in which the interaction of the vehicles with the environment is designed, has been placed at the center of the sector. The presence of quantitatively increased processing units because of the increased processing load creates a potential attack surface area that can cause vehicles to become a threat in many areas, especially in the structural security of vehicles. The fact that the Internet of Things phenomenon has taken its place in the sector and that the structures responsible for the controls of the automobiles connect with other automobiles and/or other related devices causes the existing surface area to expand further. In consequence, it has been determined that the attack vulnerability surface, which expands exponentially with the increase in the number of connections between the connected vehicle elements, has not been adequately examined in the academic scope, and in this way, it may be difficult to meet the need in the sector in the future; Within the scope of this thesis, by specifying the usage areas of the use of the internet of things in connected vehicles, the vulnerabilities created by these usage areas and the techniques for solution proposals, especially the prevention of vulnerabilities, are investigated and as a result, a framework is proposed.

Keywords: Computer Forensics, Security Vulnerabilities, Internet of Things, Connected Vehicles, Cyber attacks

KAYNAKLAR

ACAR, G., HUANG, D. Y., LI, F., NARAYANAN, A., & FEAMSTER, N. (2018). Web-based attacks to discover and control local IOT devices. *Proceedings of the 2018 Workshop on IoT Security and Privacy*. doi:10.1145/3229565.3229568

ALAM, M. S., IQBAL, S., ZULKERNINE, M., & LIEM, C. (2019). Securing vehicle ECU Communications and stored data. *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. doi:10.1109/icc.2019.8762043

AMSDEN, A. H. (1989). In *Asia's next giant South Korea and late industrialization*. essay, New York: Oxford University Press.

ANDREA, I., CHRYSOSTOMOU, C., & HADJICHRISTOFI, G. (2015). Internet of things: Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication (ISCC)*, 180–187. doi:10.1109/iscc.2015.7405513

ASLAN, O., & SAMET, R. (2017). Mitigating cyber security attacks by being aware of vulnerabilities and bugs. *2017 International Conference on Cyberworlds (CW)*. doi:10.1109/cw.2017.22

ASSANTE, M. J., & TOBEY, D. H. (2011). Enhancing the Cybersecurity workforce. *IT Professional*, **13**(1): 12–15. doi:10.1109/mitp.2011.6

ATTARAN, M. (2021). The impact of 5G on the evolution of Intelligent Automation and Industry Digitization. *Journal of Ambient Intelligence and Humanized Computing*, **14**(5): 5977–5993. doi:10.1007/s12652-020-02521-x

AUTOMOTIVE IOT MARKET (By Communication: Vehicle To Vehicle, In Vehicle Communication, Vehicle To Infrastructure; By Offering: Hardware, Software, Services; By Connectivity Form: Embedded, Tethered, Integrated; By Application: Navigation, Infotainment, Telematics; By End User: Oem, Aftermarket) - Global Industry Analysis, Size, Share, Growth, Trends, Regional Outlook, And Forecast 2022-2030. (2022, Temmuz). *Automotive IoT Market*. Erişim: https://www.precedenceresearch.com/automotive-iot-market Erişim Tarihi: 25 Mayıs 2023

BAJPAI, P., ENBODY, R., & CHENG, B. H. C. (2020). Ransomware targeting automobiles. *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security*. doi:10.1145/3375706.3380558

BECSI, T., ARADI, S., & GASPAR, P. (2015). Security issues and vulnerabilities in connected car systems. *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*. doi:10.1109/mtits.2015.7223297

BIN ARIS, I., SAHBUSDIN, R. K., & AMIN, A. F. (2015). Impacts of IOT and Big Data to automotive industry. *2015 10th Asian Control Conference (ASCC)*. doi:10.1109/ascc.2015.7244878

BRODY, R. G., CHANG, H. U., & SCHOENBERG, E. S. (2018). Malware at its worst: Death and destruction. *International Journal of Accounting & Information Management*, **26**(4): 527–540. doi:10.1108/ijaim-04-2018-0046

BUCHANAN, W. J. (2014). Traffic light hacking shows the Internet of Things must come with better security

CATALAN VIDAL, J. (2016). The stagflation crisis and the European automotive industry, 1973–85. *Business History*, **59**(1): 4–34. doi:10.1080/00076791.2016.1237505

CHANDRA SHREYAS, P., ROOPALAKSHMI, R., KARI, K. B., PAVAN, R., KIRTHY, P., & SPOORTHI, P. N. (2018). IOT-based framework for automobile theft detection and driver identification. *International Conference on Computer Networks and Communication Technologies*, p.:615–622. doi:10.1007/978-981-10-8681-6_56

CHRIS GREENWOOD, D. M. C. C. (2015). Increasing number of cars being stolen after thieves simply bypass security devices. Erişim: https://www.dailymail.co.uk/news/article-2938793/Car-hackers-driving-motors-Increasing-numbers-stolen-thieves-simply-bypass-security-devices.html

DEBAR, H. (1987). Introduction to intrusion detection systems. *Advances in Security Technology*, 53–54. doi:10.1016/b978-0-409-90052-1.50012-5

DEOGIRIKAR, J., & VIDHATE, A. (2017). Security attacks in IOT: A survey. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. doi:10.1109/i-smac.2017.8058363

DIMITRIADIS, A., IVEZIC, N., KULVATUNYOU, B., & MAVRIDIS, I. (2020). D4I - digital forensics framework for reviewing and investigating cyber attacks. *Array*, *5*, 100015. doi:10.1016/j.array.2019.100015

DUHIGG, C. (2008). Depression, you say? Check those safety nets. Erişim: https://www.nytimes.com/2008/03/23/weekinreview/23duhigg.html

D.S. LANDES, (2008). Dynasties fortune and misfortune in the world's great family businesses, Penguin, London.

ECKERMANN, E., & ALBRECHT, P. L. (2001). *World history of the Automobile*. Warrendale, PA: SAE International.

Gartner identifies top Five automotive technology trends for 2022. (n.d.). Erişim: https://www.gartner.com/en/newsroom/press-releases/2022-02-17-gartner-identifies-top-five-automotive-technology-trends-for-2022

GEORGANO, G. N. (2002). *From the early years to the Golden Era of coachbuilding*. Broomhall, PA: Mason Crest Publishers.

GORDON, L. A., & LOEB, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, **5**(4): 438–457. doi:10.1145/581271.581274

GORDON, L. A., LOEB, M. P., LUCYSHYN, W., & ZHOU, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*. doi:10.1093/cybsec/tyv011

HOFFMAN, L., BURLEY, D., & TOREGAS, C. (2012). Holistically building the Cybersecurity workforce. *IEEE Security & Privacy Magazine*, **10**(2): 33–39. doi:10.1109/msp.2011.181

KENT, K., CHEVALIER, S., GRANCE, T., & DANG, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. doi:10.6028/nist.sp.800-86

LANDES, D. S. (2008). *Dynasties fortune and misfortune in the world's great family businesses*. London: Penguin.

LANGNER, R. (2011). Stuxnet: dissecting a cyberwarfare weapon. *IEEE Security & Privacy Magazine*, **9**(3): 49–51. doi:10.1109/msp.2011.67

LASI, H., FETTKE, P., KEMPER, H.-G., FELD, T., & HOFFMANN, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, **6**(4): 239–242. doi:10.1007/s12599-014-0334-4

LEE, I. (2020). Internet of things (IOT) cybersecurity: Literature review and IOT cyber risk management. *Future Internet*, **12**(9): 157. doi:10.3390/fi12090157

LI, H., CHEN, Y., & HE, Z. (2012). The survey of RFID attacks and defenses. *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*. doi:10.1109/wicom.2012.6478720

LIU, J., XIAO, Y., GHABOOSI, K., DENG, H., & ZHANG, J. (2009). Botnet: Classification, attacks, detection, tracing, and preventive measures. *EURASIP Journal on Wireless Communications and Networking*, *2009*(1). doi:10.1155/2009/692654

LLOPIS-ALBERT, C., RUBIO, F., & VALERO, F. (2021). Impact of digital transformation on the automotive industry. *Technological Forecasting and Social Change*, **162:** 120343. doi:10.1016/j.techfore.2020.120343

LV, S. (2020). Design of the automobile marketing system based on the big data. *Advances in Intelligent Systems and Computing*, 1713–1719. doi:10.1007/978-981-15-2568-1_241

MADDISON, A. (1991). *Dynamic forces in capitalist development: A long-run comparative view*. Oxford u.a.: Oxford Univ. Press.

MANJUNATH, P., SOMAN, R., & GAJKUMAR SHAH, DR. P. (2018). IOT and Block Chain Driven Intelligent Transportation System. *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)*. doi:10.1109/icgciot.2018.8753007

MATEO SANGUINO, T. DE, LOZANO DOMÍNGUEZ, J. M., & DE CARVALHO BAPTISTA, P. (2020). Cybersecurity certification and auditing of Automotive Industry. *Advances in Transport Policy and Planning*, 95–124. doi:10.1016/bs.atpp.2020.01.002

MILLER, C. (2019). Lessons learned from hacking a car. *IEEE Design & Test*, **36**(6): 7–9. doi:10.1109/mdat.2018.2863106

MUKHOPADHYAY, D., GUPTA, M., ATTAR, T., CHAVAN, P., & PATEL, V. (2018). An attempt to develop an IOT based vehicle security system. *2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS)*, 195–198. doi:10.1109/ises.2018.00050

OPOKU, D.-G. J., PERERA, S., OSEI-KYEI, R., & RASHIDI, M. (2021). Digital Twin Application in the construction industry: A literature review. *Journal of Building Engineering*, **40:** 102726. doi:10.1016/j.jobe.2021.102726

PACHECO, J., & HARIRI, S. (2016). IOT security framework for Smart Cyber Infrastructures. *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W)*. doi:10.1109/fas-w.2016.58

PARITALA, P. K., MANCHIKATLA, S., & YARLAGADDA, P. K. D. V. (2017). Digital manufacturing- applications past, current, and future trends. *Procedia Engineering*, **174**: 982–991. doi:10.1016/j.proeng.2017.01.250

PATEL, C., & DOSHI, N. (2018). Security challenges in IOT Cyber World. *Security in Smart Cities: Models, Applications, and Challenges*, 171–191. doi:10.1007/978-3-030-01560-2_8

PICCININI, E., HANELT, A., GREGORY, ROBERT. W., & KOLBE, L. M. (2015). Transforming industrial business: the impact of digital transformation on automotive organizations. *Thirty Sixth International Conference on Information Systems*, 1–20.

RADANLIEV, P., MANTILLA MONTALVO, R., NICOLESCU, R., HUTH, M., CANNADY, S., & DE ROURE, D. (2019). *Analysing IOT Cyber Risk for Estimating IOT Cyber Insurance*. doi:10.20944/preprints201903.0110.v1

RAHIM, MD. A., RAHMAN, MD. A., RAHMAN, M. M., ASYHARI, A. T., BHUIYAN, MD. Z., & RAMASAMY, D. (2021). Evolution of IOT-enabled connectivity and

applications in Automotive Industry: A Review. *Vehicular Communications*, 27, 100285. doi:10.1016/j.vehcom.2020.100285

ROOPAK, M., YUN TIAN, G., CHAMBERS, J. (2019). Deep learning models for cyber security in IOT Networks. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. doi:10.1109/ccwc.2019.8666588

ROSSINI, M., SPENA, P. R., CORTESE, L., MATTEIS, P., & FIRRAO, D. (2015). Investigation on dissimilar laser welding of advanced high strength steel sheets for the automotive industry. *Materials Science and Engineering: A*, **628**: :288–296. doi:10.1016/j.msea.2015.01.037

SALEEM, J., ADEBISI, B., ANDE, R., HAMMOUDEH, M. (2017). A state of the art survey - impact of cyber attacks on SME's. *Proceedings of the International Conference on Future Networks and Distributed Systems.* doi:10.1145/3102304.3109812

SCHALLER, R. R. (1997). Moore's law: Past, present and future. *IEEE Spectrum*, **34**(6): 52–59. doi:10.1109/6.591665

SEN, N., LING, L., & YUEFENG, D. (2017). FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS. *Black Hat USA 25*, 1–16.

SHAH, Y., & SENGUPTA, S. (2020). A survey on classification of cyber-attacks on IOT and IIOT devices. *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. doi:10.1109/uemcon51285.2020.9298138

STELLIOS, I., KOTZANIKOLAOU, P., PSARAKIS, M., ALCARAZ, C., & LOPEZ, J. (2018). A survey of IOT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, **20**(4): 3453–3495. doi:10.1109/comst.2018.2855563

SUN, Y., WU, L., WU, S., LI, S., ZHANG, T., ZHANG, L., … XIONG, Y. (2015). Security and privacy in the internet of vehicles. *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)*. doi:10.1109/iiki.2015.33

TAWALBEH, L., MUHEIDAT, F., TAWALBEH, M., QUWAIDER, M., & SALDAMLI, G. (2020). Predicting and preventing cyber attacks during COVID-19 time using data analysis and proposed secure IOT layered model. *2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA)*. doi:10.1109/mcna50957.2020.9264301

TRAN, M.-Q., ELSISI, M., LIU, M.-K., VU, V. Q., MAHMOUD, K., DARWISH, M. M., … LEHTONEN, M. (2022). Reliable deep learning and IOT-based monitoring system for secure computer numerical control machines against cyber-attacks with

experimental verification. *IEEE Access*, *10*, 23186–23197. doi:10.1109/access.2022.3153471

UHLEMANN, E. (2015). Introducing connected vehicles [connected vehicles]. *IEEE Vehicular Technology Magazine*, **10**(1): 23–31. doi:10.1109/mvt.2015.2390920

VACHALEK, J., BARTALSKY, L., ROVNY, O., SISMISOVA, D., MORHAC, M., & LOKSIK, M. (2017). The digital twin of an industrial production line within the industry 4.0 concept. *2017 21st International Conference on Process Control (PC)*, *21*. doi:10.1109/pc.2017.7976223

WEDEL, J. W., SCHÜNEMANN, B., & RADUSCH, I. (2009). V2X-based traffic congestion recognition and avoidance. *2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks*. doi:10.1109/i-span.2009.71

WEDENIWSKI, S. (2015). In *The mobility revolution in the automotive industry: How not to miss the digital turnpike* 1–47. Heidelberg: Springer.

WEYER, S., MEYER, T., OHMER, M., GORECKY, D., & ZÜHLKE, D. (2016). Future modeling and simulation of CPS-based factories: An example from the automotive industry. *IFAC-PapersOnLine*, **49**(31): 97–102. doi:10.1016/j.ifacol.2016.12.168

WIKSTRÖM, M., HANSSON, L., & ALVFORS, P. (2015). An end has a start – investigating the usage of electric vehicles in commercial fleets. *Energy Procedia*, **75:** 1932–1937. doi:10.1016/j.egypro.2015.07.223

WILKINS, M., & HILL, F. E. (2011). American Enterprise . In *American business abroad: Ford on six continents*, 270–285, Cambridge England: Cambridge University Press.

WU, X., ZHANG, C., & DU, W. (2021). An analysis on the crisis of "chips shortage" in automobile industry ——based on the double influence of covid-19 and trade friction. *Journal of Physics: Conference Series*, **1971**(1): 012100. doi:10.1088/1742-6596/1971/1/012100

YAQOOB, I., KHAN, L. U., KAZMI, S. M., IMRAN, M., GUIZANI, N., & HONG, C. S. (2020). Autonomous driving cars in smart cities: Recent advances, requirements, and challenges. *IEEE Network*, **34**(1): 74–181. doi:10.1109/mnet.2019.1900120