Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Endüstri 4.0'ın Gelişim Sürecinde Unutulan Bileşen: Siber Güvenlik

Serkan GÖNEN [a], Ercan Nurcan YILMAZ [b,*], Seda ŞANOĞLU [b], Gökçe KARACAYILMAZ[c], Özge ÖZBİRİNCİ[a]

[a] *Mühendislik ve Mimarlık Fakültesi, İstanbul Gelişim Üniversitesi, İstanbul, TURKEY*
[b] *Fen Bilimleri Enstitüsü, Gazi Üniversitesi, Ankara, TURKEY*
[c] *Adli Bilimler, Hacettepe Üniversitesi, Ankara, TURKEY*
** Sorumlu yazarın e-posta adresi: enyilmaz@gazi.edu.tr*
DOI: 10.29130/dubited.905340

Öz

İnsanlık tarihi teknolojik açıdan önemli aşamalardan geçmiştir ve geçmeye devam etmektedir. Bu aşamaların en önemlilerinden birisi de Endüstri 4.0 sürecidir. Bu süreçle birlikte geleneksel sanayi üretimi yerini bilişim sistemlerinin ön planda olduğu bir yaklaşıma bırakmıştır. Endüstriyel haberleşme sistemleri ilk üretildikleri zamanlarda tamamen izole olarak yönetilmişlerdir. Zamanla iç ağlara (intranet) devamında ise internete bağlanmaları ile Endüstri 4.0 süreci başlamıştır. Bu süreçte siber-fiziksel sistemlerin ortaya çıkmasıyla birlikte, bu sistemler siber tehditlere karşı açık hale gelmişlerdir. Bu zafiyetler akıllı sistemleri ve Endüstri 4.0 sistemlerini saldırganların gözdesi haline getirmiştir. Her ne kadar bu sistemler verimlilik, sürat, işlerlik gibi insan hayatına önemli katkılar sağlasa da siber güvenlik açıklıkları uygun şekilde değerlendirilmezse, Endüstri 4.0'ın gerçek potansiyeline asla ulaşılamayabilir. Bu nedenle, çalışmada Endüstri 4.0'ın tüm bileşenleri ele alınarak, Siber Güvenlik bileşeni üzerine odaklanılmıştır. Çalışma, Endüstri 4.0'ın siber güvenlik boyutuna yönelik çalışmalara önemli katkı sağlayacaktır.

Anahtar Kelimeler: *Endüstri 4.0, Siber Güvenlik, Özerk Sistemler, IoT*

The Forgotten Component in the Development Process of Industry 4.0: Cyber Security

Abstract

Human history has passed through important technological stages and continues to do so. One of the most important of these stages is the Industry 4.0 process. With this process, traditional industrial production has left its place to an approach where information systems are at the forefront. Industrial communication systems were completely isolated when they were first produced. In time, the Industry 4.0 process started with their connection to internal networks (intranet) and then to the Internet. With the emergence of cyber-physical systems in this process, these systems have become vulnerable to cyber threats. These weaknesses have made smart systems and Industry 4.0 systems the favorite of attackers. Although these systems make significant contributions to human life such as efficiency, speed and operability, if cyber security vulnerabilities are not properly evaluated, the real potential of Industry 4.0 may never be reached. Therefore, the study focused on the Cyber Security component by considering all the components of Industry 4.0. The study will make a significant contribution to the studies on the cyber security dimension of Industry 4.0.

Keywords: *Industry 4.0, Cyber Security, Autonomous Systems, IoT.*

Geliş: 29/03/2021, Düzeltme: 22/04/2021, Kabul: 24/04/2021

I. GİRİŞ

İnsanlık tarihi insan hayatına yön veren önemli aşamalardan geçmiştir. Bu aşamalar çok farklı türde kategorilere ayrılmış olsa da temel de toplum yaşantısını etkileyen üç temel aşamaya ayrılabilir. İlki tarım toplumu, ikincisi sanayi toplumu ve üçüncüsü bilgi toplumudur. Hâlihazırda içinde bulunduğumuz bilgi toplumu, en geniş ağ olan "İnternetin" hayatımıza girmesiyle insan yaşantısında önemli değişikliklere yol açmıştır. Bankacılıktan, alışverişe, sağlık hizmetlerinden eğitime kadar tüm alanlar dijital dönüşüme sahne olmuştur. Bu süreci daha da hızlandıran ve siber-fiziksel sistemlerin ortaya çıkmasına neden olan diğer bir gelişme ise 4. Sanayi devrimi denilen Endüstri 4.0 sürecidir.

Endüstri 4.0, birçok çağdaş otomasyon sistemini, veri alışverişlerini ve üretim teknolojilerini içeren kolektif bir terimdir. Endüstri 4.0 konsepti ilk olarak Almanya'da düzenlenen Hannover Sanayi Fuarı'nda duyurulmuştur [1]. Endüstri 4.0 ile birlikte, endüstri sistemleri içeren sayısız unsurun geleceğin akıllı fabrikalarını ve imalat organizasyonlarını oluşturmak için internet iletişim teknolojileriyle etkileşime girdiği yeni bir devrim gerçekleşmektedir. Endüstri 4.0, akıllı siber-fiziksel sistemler ile kurulan akıllı fabrikaların bir vizyonudur. Üretimin hızlandırılması, verimliliğin artırılması ve insan gücünün azaltılarak otonom sistemlerin devreye alınması bu devrimin temel hedefleri arasında yer almaktadır. Üretim ve imalat alanında internetin öncülüğünde yüksek teknolojinin kullanımını hedefleyen bu kavram, kendi kendini yapılandırma, kendi kendini izleme ve kendi kendini iyileştirme gibi özerk özelliklere sahip akıllı sistemler tarafından üretilen üretim ekosistemlerinin oluşmasını sağlayacaktır. Ancak, bulut tabanlı tasarım ve üretim sistemleri, Nesnelerin İnterneti (IoT) ve Sosyal Ürün Geliştirme gibi ilgili teknolojiler, sayısız yeni değer yaratma fırsatı getirmeyi vaat eden yeniliklerden etkilenmektedir. Bununla birlikte, söz konusu İnternet teknolojileri, Endüstri 4.0 teknolojilerinin uygulayıcılarını kendine özgü benzersiz güvenlik ve gizlilik zorluklarıyla birlikte geleneksel siber güvenlik ve veri gizliliği sorunlarıyla karşı karşıya getirmiştir.

Endüstriyel Nesnelerin İnterneti aydınlık bir geleceğe sahip olabilir. Ancak, siber güvenlik ve veri gizliliği sorunları, Endüstriyel IoT teknolojilerinin uygulayıcıları için büyük engeller oluşturmaktadır. Verimlilik, sürat, işlerlik gibi insan hayatına önemli katkılar sağlamakla birlikte, söz konusu siber güvenlik açıklıkları uygun şekilde değerlendirilmezse, Endüstri 4.0'ın gerçek potansiyeline asla ulaşılamayabilir.

2. ENDÜSTRİ 4.0

Endüstri 4.0'daki temel amaç, kendini yönetebilen üretim aşamalarının olduğu akıllı fabrikaların hayata geçirilmesidir [2]. Akıllı fabrikalar olarak ifade edilen kavramı ise birbirleriyle haberleşebilen, sensörler yardımıyla ortamı algılayan gelişmiş yapay zeka ile donatılmış robotların veri analizi yapması ve üretim sürecini yönetmesi olarak ifade etmek mümkündür.

Endüstri 4.0'ın tarihsel gelişim süreci Şekil 1'de özetlenmiştir. Bu kapsamda, Endüstriyel anlamda ilk olarak 18. yüzyılda buhar makinaları ile başlayan ve üretimin artırılması yönünde olan Birinci Sanayi Devrimini (Endüstri 1.0), 20. yüzyılın başında seri üretime geçiş olarak ortaya çıkan ve elektrik enerjisinden faydalanmanın önünü açan İkinci Endüstri Devrimi (Endüstri 2.0) takip etmiştir. Bilgi teknolojilerinin gelişmesi ve üretim aşamalarında kullanılması ise Üçüncü Sanayi Devrimini (Endüstri 3.0) ortaya çıkarmıştır. Bu süreçleri müteakip 21. yüzyılın başında Endüstri 4.0 terimi ortaya atılmıştır [3].

Şekil 1. *Endüstri 4.0'ın Tarihsel Gelişimi*

Endüstri 4.0, sistemlerin uyumlu ve verimli çalışması amacıyla geleneksel sanayi üretiminin yerine bilgisayarlaşmanın ön planda olduğu, Şekil 2'de betimlenen dokuz bileşen üzerine inşa edilmiş bir yaklaşımdır. Bu bileşenler, Özerk Robotlar, Simülasyon Teknolojileri, Yatay ve Dikey Sistem Entegrasyonu, Endüstriyel Nesnelerin İnterneti, Siber Güvenlik, Bulut Bilişim, Eklemeli Üretim, Artırılmış Gerçeklik, Büyük Veridir.

Şekil 2. *Endüstri 4.0 Bileşenleri*

Endüstri 4.0 devrimi nesnelerin interneti, internetin hizmetleri ve siber fiziksel sistemlerden oluşan bir yapıdır. Aynı zamanda bu yapı, akıllı fabrika sisteminin oluşmasında büyük rol oynamaktadır. Bu devrim, üretim ortamında her bir verinin toplanmasına ve iyi bir şekilde izlenip analiz edilmesine olanak sağlayarak daha verimli iş modelleri ortaya çıkartmıştır [4]. Bu kavram doğrultusunda ortaya çıkan bileşenlerden çalışmanın devam eden bölümünde açıklanmıştır. Bu bileşenler Endüstri 4.0'ın ayırt edici unsurları olup, hepsi sanayi devrimi süresince getirdiği faydaların yanı sıra siber güvenlik problemlerine de yol açmıştır.

A. ÖZERK ROBOTLAR

Endüstri 4.0'ın önemli unsurlarından biri güvenlik, esneklik, çok yönlülük ve işbirliğine odaklanarak görevleri akıllıca tamamlayabilen robotların desteklediği otonom üretim yöntemleridir [5]. Üretim süreçlerinde robotların kullanımı yeni olmamakla birlikte robotlar da yaşanan gelişmelere ayak uydurmak zorunda kalmıştır. Robotlar, üretimde kullanılan tüm malzemeler, sistemler, cihazlar vb. unsurlarla etkileşim içinde çalışarak üretimde verimlilik ve artış sağlamaktadır. Geleneksel üretim yöntemleriyle karşılaşılan problemler robotlar sayesinde en aza indirilmektedir [6, 7]. Bu aşamada sensör teknolojilerinin kullanılması da büyük önem taşır.

Robotik teknolojiler endüstri 4.0 ile birlikte hızla gelişmesine karşın bu gelişim siber güvenlik açıklıklarının test edilmesi ve analizi açısından aynı hızla ilerlemediği ve endüstriyel sistemlerde güvenlik kullanılabilirliğin önünde tutulması nedenleriyle yeterli seviyeye beklendiğinden daha yavaş gelmektedir.

B. SİMÜLASYON TEKNOLOJİLERİ

Simülasyon, gerçek dünyada var olan fiziksel sisteme ait verilerin sanal bir ortama taşınmasıyla gerçek sisteme ait özelliklerin izlenmesine altyapı oluşturan bir modelleme tekniğidir [8]. Simülasyon, zaman içinde bir sistemin veya gerçek dünyadaki bir işlemin taklit edilmesi olarak da tanımlanır. Bir sistemin yapay tarihini ve gözlemini kullanarak gerçek sistemin temsilinin operasyonel özellikleri üzerinde çıkarımlar çizer [9].

Dijital üretimin başarılı bir şekilde uygulanması için simülasyon yöntemleri üretimin değişmez bir parçasıdır. Daha önce, üreticiler bir sürecin verimli ve etkili bir şekilde çalışıp çalışmadığını test etmek için deneme yanılma yöntemini kullanmaktaydı [6]. Simülasyon ve modelleme teknikleri sayesinde sanal ortamda test edilen üretim süreci, gerçek dünyada daha verimli ve az hata ile gerçekleşmektedir. Simülasyon modellemesi, maliyet ve geliştirme döngülerini azaltmaya ve ürün kalitesini artırmaya yardımcı olur [9].

C. YATAY VE DİKEY SİSTEM ENTEGRASYONU

Yatay Entegrasyon, üretim ve planlama sürecindeki her bir adımın kendi arasında, ayrıca farklı işletmelerin üretim ve planlama süreçlerindeki adımlar arasında kesintisiz bir akışı ifade etmektedir. Bu entegrasyon ham madde tedarikinden tasarıma, üretime, pazarlamaya, sevkiyata kadar her noktayı kapsamakta, bütünleşik ve uçtan-uca sistemler kurmaktadır.

Dikey Entegrasyon süreçler arasında değil, tüm süreçlerde kullanılan teknolojik altyapıda kesintisiz bir iletişim ve akış sağlamak anlamına gelmektedir. Örneğin üretim alanındaki sensörler, vanalar, motorlar, kumanda panelleri, üretim yönetimi sistemleri, kurumsal kaynak planlama yazılımları, iş zekâsı uygulamaları gibi birimlerin entegrasyonu bu kapsamda ele alınmaktadır [3]. Endüstri 4.0'ın getirdiği bu sistem entegrasyonları ile üretim süreçlerinde yaşanan hatalara çözüm getirmek kolaylaşmakta, verimlilik artmakta ve istenen değişikliklere cevap verilmesi kolaylaşmaktadır.

D. ENDÜSTRİYEL NESNELERİN İNTERNETİ

Nesnelerin interneti (IoT), bir ağ tarafından algılanan veya kontrol edilen nesneleri kapsayan, fiziksel gerçek dünya ve bilgisayar tabanlı sistemler arasındaki entegrasyonu destekleyen ve üretimde gelişmiş üretkenlik sunan bir kavramdır [2]. Endüstriyel Nesnelerin İnterneti (IIoT) ise nesnelerin internetinin endüstriyel sektöre uygulanmasına ilişkin genel bir kavram olarak ortaya çıkmıştır. Endüstriyel süreç verimliliğine daha fazla odaklanan Endüstri 4.0'ın genelleştirilmesidir. Beyaz eşyalar, otomobiller, kameralar, endüstriyel cihazlar, aydınlatma sistemleri, klimalar vb. milyarlarca nesnenin birbiri ile etkileşim içinde olması olarak ifade edilen bu kavram Endüstri 4.0 ile yakın bir ilişki içindedir. IoT ile

mevcut endüstriyel kontrol sistemlerinin birlikte kullanılması birçok avantajı beraberinde getirmiştir. Bu avantajlardan bazıları;

- IoT yeteneğine sahip akıllı üretim makinaları ağ üzerinden birbirleri ile otomatik iletişim kurarak üretimi kontrol eder ve operatör katkısını en az düzeye indirir,
- Mekanik ve elektriksel arızalar önceden tahmin edilerek arıza nedeniyle üretimin kesintiye uğrayacağı süreleri azaltılabilir,
- Fabrikanın üretimi için ham madde eksikliği hızla tespit edilerek giderilir,
- Fabrika yöneticileri üretim ve arızalarla ilgili bilgileri dünyanın herhangi bir yerinden gerçek zamanlı olarak alabilir,
- Bu bilgiler dağıtım kanalları ve müşteriler ile paylaşılabilir [10].

Nesnelerin interneti ile tüm cihazlar birbirleri ile etkileşim halinde yoğun bir bilgi alışverişi gerçekleştirmektedir. Bu durumda en değerli varlık olan bilginin korunma ihtiyacı ise kaçınılmazdır.

Günümüzde bilgisayarlar ve cep telefonlarının yanı sıra çevremizdeki birçok cihaz internete bağlı duruma gelmiştir. Yapılan istatistiklere göre; dünya çapında 2020 yılında 8,74 olan IoT cihazlarının sayısının, neredeyse üç katına çıkarak 2030 yılında dünya çapında internete bağlı cihaz sayısının 30 milyar civarı olacağı tahmin edilmektedir [2, 11]. Cisco'ya göre ise 2030'da 500 milyar cihazın internete bağlanması beklenmektedir [12].

E. BULUT BİLİŞİM

Bulut teknolojisi, herhangi bir kurulum gerektirmeyen, web tabanlı uygulamalarla operasyonel kolaylık sağlayan en basit çevrimiçi depolama hizmetidir [13]. Ulusal Standartlar ve Teknoloji Enstitüsü'nün (NIST) tavsiyelerine göre, ideal bir bulutun beş özelliği olmalıdır: isteğe bağlı kendi kendine hizmet, geniş ağ erişimi, ortak kaynak havuzu, çabukluk ve esneklik, ölçülebilir hizmet [9].

Bulut bilişim teknolojisi ile büyük verilerin internet üzerinde depolanması ve kolaylıkla bu verilere erişilmesi mümkün kılınmıştır. Kullanıcılar, istenildiği takdirde uygulama gereksinimlerine bağlı olarak kaynakları kullanır [14]. Böylelikle şirketlerin Endüstri 4.0 üretim süreci boyunca karşılaşacakları veri alışverişi ihtiyacı bulut teknolojisi üzerinden gerçekleşebilmektedir. Fakat bulut sistemlerinde depolanan veriler ve verilerin paylaşılması sistemlerin güvenlik sorunlarına maruz kalmasını artıracağı anlamına da gelmektedir [15].

F. KATKI ÜRETİMİ

Katkı üretimi, endüstride 3 boyutlu baskı yönteminin kullanılması olarak tanımlanabilir. Diğer bir ifadeyle bilgisayar kontrolü altındaki dijital bir veri formundan üç boyutlu bir nesne üretme teknolojisidir. Bu üretim şekliyle plastik, silikon, gıda, cam ve diğer bazı materyaller yazdırabilir ve bunlar hava araçlarında, mücevherat, moda, tıp ve dişçilik, otomotiv yedek parçaları ve diğer endüstrilerde kullanılabilir [16]. Dünyanın önde gelen Google, Motorola ve Apple gibi çeşitli şirketleri, akıllı telefon faaliyetlerini hızlandırmak için 3D baskı faaliyetlerine yatırım yapmaktadır [17].

Geleneksel üretime kıyasla avantajı, ürünlerin tasarım ve geliştirilmesindeki kabiliyetleridir [18]. Ayrıca materyal oluşturulurken malzeme katman katman eklendiğinden daha az israf vardır. Katmanlı üretim olarak da ifade edilen bu teknoloji ile daha kısa sürede, az maliyetle ve kolay bir şekilde ürün tasarımı yapılmaktadır. Katkı üretimi ile müşteriler için maliyet ve zaman azaltılırken aynı zamanda müşterilere veya son kullanıcılara daha fazla değer sunan küçük özelleştirilmiş ürün grupları üretilmektedir [6].

G. ARTTIRILMIŞ GERÇEKLİK

Artırılmış gerçeklik (İngilizce: Augmented reality; AR), gerçek dünyadaki nesnelerin dijital ortamda oluşturulup canlı ve gerçek zamanlı olarak görülebilmesini sağlayan bir teknolojidir. Artırılmış

gerçeklikle insan duyusuna hitap edecek ve hislerini harekete geçirecek girdiler bilgisayar tarafından düzenlenerek zenginleştirilir ve ortaya çıkan yeni gerçeklik kullanıcının algısına sunulur.

AR, Avrupa Birliğine göre endüstri 4.0 gibi kavramların gelişimini kontrol eden esas teknolojilerden biridir [19]. Bu sistemler Endüstri 4.0 için hala bebeklik döneminde olmasına rağmen gelecekte şirketler, çalışanların çalışma prosedürlerini iyileştirmek ve gerçek zamanlı bilgi sağlamak için artırılmış gerçekliği kullanacaktır. Ayrıca üreticiler, bakım prosedürlerini geliştirmek ve uzmanların yerinde bulunma maliyetlerini düşürmek için artırılmış gerçeklik tabanlı sistemlere yönelmektedir [6]. Örnek verilecek olursa işçiler, onarılması gereken gerçek sisteme baktıklarında belirli bir parçanın nasıl değiştirileceği konusunda onarım talimatları alabilirler. Bu bilgiler, artırılmış gerçeklik gözlükleri gibi cihazlar kullanılarak doğrudan çalışanların görüş alanında görüntülenebilir [20]. Bu durum her ne kadar avantaj gibi gözükse de, AR destekli görevlerin hata oranları ve tamamlanma sürelerinin artışı uygulamaların karmaşıklığı ve doğasına bağlı olduğu için uygun görev seçilimi önem arz etmektir [19].

Endüstriyel sistemlerde AR teknolojilerinin kullanılması cihaz kullanılabilirliğini, maliyet ve üretim gibi faktörleri arttırıp kaza riskleri gibi olası kötü durumların ihtimallerini azalması açısından çok verimli bir teknolojidir. Ancak, siber güvenlik açıklıkları çoğunlukla belirsizdir. Bu nedenle de, saldırıya açık bir platform olmasından ötürü risk barındırmaktır. Örneğin kritik bir cihazın onarımı sırasında teknisyenin kullandığı AR cihaza, tamir edilecek cihazın teknik bilgileri, çizimleri ve arızalı olan parçanın bilgisi yansıtılmaktadır. Olası bir araya girme saldırısı ile istenmeyen üçüncü taraflara bir yönlendirme yapılması sonucu bakım onarım işlemi büyük bir faciaya dönüşebilir.

H. BÜYÜK VERİ

Karmaşık yapıdaki çok fazla verinin işlenmesi ve analiz edilmesi çalışmalarının tümünü büyük veri olarak ifade edebiliriz. Büyük verinin asıl amacı eldeki karmaşık verilerin analiz edilerek değerli bilgilerin ortaya çıkarılmasıdır. Akıllı sensörlerden, akıllı cihazlardan, kayıt dosyalarından, video ve ses cihazlarından gelen büyük, çeşitli, yapılandırılmış veya yapılandırılmamış veriler büyük verilerin kaynağıdır [21]. Alman Hükümeti tarafından dördüncü sanayi devriminin yakıtının büyük veri olacağı öngörülmektedir [22].

Endüstri 4.0'ın getirdiği dijitalleşme süreci ile cihaz sayısında ciddi bir artış meydana gelmiş, bu cihazlar tarafından üretilen verilerin hacimsel boyutları artmış ve bu verilerin güvenli bir şekilde depolanması ve işlenmesi ile ilgili problemler ortaya çıkmıştır [23]. Geleneksel veritabanı teknolojisi, büyük veri toplama işlemini, depolamayı, yönetimi ve analizinin tamamlanmasında güçlük çekmektedir. Yönetim açısından, imalat şirketlerinin büyük miktardaki ürün verileri, operasyonel veriler, değer zinciri verileri ve harici veriler gibi yapılandırılmamış verileri içeren çok çeşitli verileri yönetmesi gerekir [14]. İşletmeler, üretim kalitesi ve hizmetinin optimizasyonu, enerji tüketiminin azaltılması ve üretim sürecindeki verimliliklerin iyileştirilmesi söz konusu olduğunda çok faydalı olabileceğini düşündüğü için, gelen verileri göz ardı edemez [6].

Bankacılık, sanayi, sağlık vb. alanlarda sıklıkla kullanılan bu teknoloji iş hayatında doğru kararlar alınmasına ve risk yönetiminin düzgün bir şekilde yapılmasına olanak sağlamaktadır. Ancak bu tür kritik sistemlere ilişkin önemli kararlar verilirken yararlanılan büyük verinin gizliliği, bütünlüğü gibi temel siber güvenlik özelliklerinin korunması ve kullanılmadan önce teyit edilmesi, karaların doğruluğunda oldukça önemlidir.

I. SİBER GÜVENLİK

Endüstri 4.0 ile birlikte gelen dijitalleşme ile daha fazla cihaz birbiriyle birleşik çalışmakta ve sürekli haberleşmektedir. Diğer sanayi devrimlerinden farklı olarak Endüstri 4.0 yeni üretim yöntemleri sunmakla birlikte toplumsal yaşam, ekonomi, eğitim, iletişim, kamu hizmetleri vb. birçok alanda da değişim dalgası başlatmış ve tüm bu alanlarda siber güvenlik sorunlarını da beraberinde getirmiştir. Uluslararası Telekomünikasyon Birliği (ITU) tarafından siber güvenlik; siber ortamı, kuruluşu ve kullanıcının varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları,

güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvenceler ve teknolojilerin bütünü olarak tanımlanmıştır [24].

Endüstri 4.0 korunması gereken değerli veriler içermektedir. Bu sistemler üzerinde işlenen ve saklanan veriler güvenlik açısından kritik öneme sahiptir ve bu nedenle bilgi güvenliğinin gizlilik boyutu ön plana çıkmaktadır. Gizlilik bileşeninde var olan bu zafiyetler, hasım/rakip tarafa büyük zararlar vermek isteyen ve herhangi bir ahlaki değere bağlı olmayan siber saldırganların odağı haline gelmektedir. Üretim işlemleri bir siber saldırı ile durdurulabilir ve bu durum şirketlerin mali kayıplar yaşamasına neden olmaktadır. Günümüzde, kritik altyapılara ve stratejik endüstriyel sektörlere yönelik siber saldırılar daha sık ve gelişmiş bir şekilde yapılmaktadır [25].

Haziran 2010'da İran'ın nükleer tesislerine yönelik gerçekleştirilen Stuxnet saldırısı da endüstriyel kontrol sistemlerinin, korunuyor olsalar dahi saldırıya uğrayabileceğinin anlaşılması açısında önemli bir yer teşkil etmektedir. Diğer önemli bir örnek ise ABD'de meydana gelen geniş çaplı DDoS (Dağıtık Hizmet Dışı Bırakma) saldırısıdır. Saldırı IoT cihazlar aracılığıyla yapılmış en büyük siber saldırılardan biri olmuştur. 21 Ekim 2016'da Alan Adı Sistemi sağlayıcısı Dyn tarafından işletilen sistemleri hedef alan saldırının, Mirai kötü amaçlı yazılımından etkilenmiş yazıcılar, IP kameralar, ev ağ geçitleri ve bebek izleme monitörleri gibi internete bağlı çok sayıda cihazdan oluşan bir botnet aracılığıyla gerçekleştirildiği ifade edilmiştir [26].

Endüstri 4.0 alanında yaşanan siber güvenlik olayları oldukça fazladır. Sonuç olarak siber savaşa karşı alınması gereken önlemler şirketlere mali açıdan yük getirecek olsa da, siber saldırıların potansiyel olumsuz etkileri göz önüne alındığında saldırı gerçekleşmesi durumunda şirketlerin kayıplarının daha fazla olacağı açıkça görülmektedir [17]. Bu eksikliklerden dolayı çalışmada siber güvenlik ve endüstri 4.0 ana teması odak noktası olarak ele alınmıştır.

Çalışmanın devam eden bölümlerinde, sırasıyla 3. bölümde Endüstri 4.0'ın siber güvenlik bileşenine değinen benzer çalışmalara yer verilmiştir. 4. bölümde çalışmanın odak noktası olan Endüstri 4.0 ve Siber Güvenlik konusu incelenmiştir. 5. bölüm olan sonuç bölümüyle çalışma tamamlanmıştır.

3. İLGİLİ ÇALIŞMALAR

Bu bölümde Endüstri 4.0'ın siber güvenlik bileşeni konusunda yapılan benzer önemli çalışmalar incelenmiştir. Marianna ve arkadaşları Endüstri 4.0 kapsamında siber güvenliğin oynadığı rolün incelenmesi hususunda sistematik bir literatür taraması gerçekleştirmişlerdir. Çalışmada, siber güvenlik ve Endüstri 4.0, siber güvenlik sorunlarından etkilenen endüstriyel varlıkların incelenmesi, Endüstri 4.0 senaryolarıyla ilgili olarak alınabilecek sistem güvenlik açıklarının, siber tehditlerin, risklerin ve önlemlerin tanımlanması ve siber güvenlik konularını kapsayan kılavuz ilkelerin ve daha yapısal çözümlerin belirlenmesi konuları üzerinde durulmuştur. Ayrıca, analiz edilen makalelerde siber güvenliğin bilgi teknolojileri ile sağlanmaya çalışıldığı, yönetimsel bakış açısının bu hususta bir destek sunmadığı görülmüştür [27].

Nikos ve Angelos 2017 yılında yayınladıkları makalede, Endüstri 4.0'da çalışan siber güvenlik uzmanlarının karşılaştıkları siber güvenlik zorluklarına değinmekte olup nesnelerin interneti ve siber güvenlik hakkında bilgi vermektedir. Ayrıca etkili siber güvenlik için öneriler sunulmuştur [7]. Miklos ve Lajos, akıllı şehirler ve Endüstri 4.0 projelerinin başarılı bir şekilde uygulanmasının gereklilikleri üzerinde bir inceleme yapmış olup teknolojik bileşenlerin yanı sıra bilgi teknolojileri güvenliğine ilişkin yeniliklerin, projelerin planlanması ve uygulanması gerektiğinde bahsedilmiştir [28].

İnternet Güvenliği Merkezi (Internet Security Center-CIS) ile SANS Enstitüsü tarafından yapılan çalışmada, kritik siber güvenlik saldırılarının önlenmesine yönelik yapılabilecek kontroller, Tablo 1'de görüldüğü üzere 20 kategori 3 ana başlık altında belirlenmiştir [29].

Tablo 1. *Yapılabilecek kontroller listesi[29]*

Basit Kontroller	Temel Kontroller	İdari Kontroller
• Donanımların envanteri ve kontrolü • Yazılımların envanteri ve kontrolü • Devamlı olarak güvenlik açığı değerlendirilmesi. • Yetkilendirme kontrolü • Bilgisayarların, iş istasyonlarının, mobil cihazların ve sunucuların donanımı ve yazılımı için yapılandırma ayarlarının güvenliğinin kontrolü. • Günlük kayıtların bakımı, izlenmesi ve analizi	• Web tarayıcı ve e-posta güvenliği • Kötü amaçlı yazılım koruması • Protokollerin, hizmetlerin ve ağ bağlantı noktalarının kontrolü • Veri kurtarma ve yedekleme • Ağ cihazları için güvenli yapılandırma • Çevresel Güvenlik • Veri koruma • Kontrollü ve güvenli erişim. • Kablosuz erişim kontrolü • Kullanıcı hesaplarının izlenmesi ve kontrolü	• Güvenlik farkındalığı eğitimi uygulanması • Yazılım güvenliği • Etkinlik yönetimi • Sızma (Penetrasyon) testleri

4. ENDÜSTRİ 4.0 VE SİBER GÜVENLİK

Endüstri 4.0'a geçiş ile her gün milyonlarca yeni cihaz birbirine bağlanmakta, siber korsanlar için ise birbirine bağlı cihaz sayısının artışı siber saldırı imkânlarının artması anlamına gelmektedir. Bu sebeple Endüstri 4.0 ve siber güvenlik kavramları ayrı düşünülemez. Siber güvenlik konusunun bu denli önemli olmasının bir diğer nedeni ise, alınan güvenlik tedbirlerine karşı sürekli olarak yeni saldırı vektörlerinin geliştirilmesidir. Geliştirilen güvenlik stratejilerinin devamlı olarak güncellenmesi ve denetlenmesi ise yeni saldırı tehditlerine karşı büyük ölçüde koruma sağlamanın en önemli adımını oluşturmaktadır. Yeni stratejiler geliştirilmediği ve önlemler alınmadığı takdirde kurum/kuruluş ve şirketler için yıkıcı sonuçların ortaya çıkması kaçınılmaz bir gerçektir.

Fikri mülkiyet hırsızlığı başta olmak üzere verilerin değiştirilmesi, çalınması, üretim süreçlerinde aksamalar yaşanması Endüstri 4.0'ı bekleyen önemli tehditler arasında yer almakta olup bu tehditler firmalarda itibar kayıpları yaşama endişesini artırmıştır. Endüstri 4.0 modelini kullanmak isteyen endüstriyel kuruluşlar bu şekilde veri ve itibar kaybı yaşamamak adına bu duruma yol açabilecek faaliyetlere karşı önlem almaları gerekmektedir. Akıllı cihazlarda yaşanacak bilgi güvenliği ihlallerinin önüne geçmek için, üretim aşamasında güvenlik kriterlerinin artırılmasının yanı sıra farkındalık olgusu geliştirilmesi de gerekmektedir.

Son 10 yılda yapılan çalışmalar, Endüstri 4.0 kapsamında siber güvenlik standartları için kontrollerin etkinliğinin değerlendirilmesi adına ortak bir anlayış oluşturulmasına yardımcı olmuştur. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) ve Avrupa Siber Güvenlik Organizasyonu (ESCO) mevcut standartları, prosedürleri, uygulamaları ve yönergeleri toplamıştır [30]. Endüstriyel iletişim ağları - ağlar ve sistemler için BT güvenliği kapsamında gerçekleştirilen spesifikasyonlar ve standartlardan ilki ISA/EAC (International Organization for Standardization/International Electrotechnical Commission)) 62443'dir. 2016 yılında yayınlanmış olan bu standartın hedef sistemi Endüstriyel Otomasyon ve Kontrol sistemlerinin güvenliği, erişebilirliği, gizliliği, bütünlüğü ve elektronik güvenliğidir. Diğer bir önemli standart ise IACS (International Association of Classification Societies- Uluslararası Klas Kuruluşları Birliği) Siber Güvenlik Sertifika Çerçevesi (ICCF)'dir. 2018 yılında yayınlanan bu çerçeve (framework) ise kendi kendine uygunluk beyanı, bağımsız uygunluk değerlendirilmesi, ürün siber dayanıklılık sertifikasyonu ve tam-siber dayanıklılık sertifikasyonu şemalarının içerildiği üç farklı değerlendirmeyi önermektedir. Bunlar Uygunluk değerlendirmesi, siber dayanıklılık testi ve geliştirme sürecinin değerlendirilmesidir. Hedef sistem Endüstriyel Otomasyon ve Kontrol Sistemleridir [31].

Web güvenliği konusunda önemli çalışmalar yapan OWASP (Open Web Application Security Project - Açık Web Uygulaması Güvenlik Projesi) tarafından yayınlanan nesnelerin interneti projesi de Endüstri 4.0'da siber güvenlik alanında yapılan önemli çalışmalardandır. Bu çalışma, üreticilerin, geliştiricilerin ve tüketicilerin Nesnelerin İnterneti ile ilgili güvenlik sorunlarını daha iyi anlamalarına yardımcı olmak ve kullanıcıların, IoT teknolojilerini oluştururken, dağıtırken veya değerlendirirken daha iyi güvenlik kararları almalarını sağlamak ve kullanıcılara yardımcı olmak için tasarlanmıştır. 2018 yılında

yayınlanan raporda IoT cihazlarında yer alan güvenlik zafiyetleri 10 başlık altında kritiklik seviyelerine göre belirtilmiştir. Rapora göre, IoT cihazlardaki en kritik zafiyetin zayıf ve tahmin edilebilir parolalar olduğu sistemlere yetkisiz erişimlerin bu parolaların kolayca tahmin edilmesi ve sistemdeki arka kapılar kullanılarak gerçekleştirildiği ifade edilmiştir. Cihazda ihtiyaç duyulmayan, güvensiz ağ servislerinin çalışıyor olması (özellikle internete açık olması) bilginin gizlilik, bütünlük ve erişilebilirliğini tehlikeye atan önemli zafiyet unsurları arasında yer almaktadır. Yaygın problemler arasında yer alan bir diğer unsur kimlik doğrulama, yetkilendirme, sistem ara yüzündeki giriş ve çıkışların filtrelenmesidir. Cihaz ve sistemlerin güvenli ve zamanında güncellenmemesi, cihaz ve sistemlerin tehlikeye girmesine izin verebilecek kullanımdan kalkmış, güvensiz yazılım bileşenleri ve kütüphanelerinin kullanılması da siber korsanlar tarafından sistemlerin hedef haline gelmesine neden olmaktadır. Kullanıcıların sistemlerde saklanan kişisel bilgileri, gizliliğin sağlanmasında sorun yaratmaktadır. Ekosistem içindeki hassas verinin depolama, transfer veya işlenme süreçlerinde erişim kontrolü ve şifreleme eksikliği varsa güvenlik problemleri yaşanabilmektedir. Cihaz yönetimi eksikliğinin beraberinde getirdiği güvenlik problemlerinin yanı sıra, varsayılan ayarlar ve şifrelerle gönderilen cihaz ve sistemler kullanıcılar tarafından güvenlik önlemleri alınmadığı takdirde her zaman risk altındadır. Fiziksel güvenlik üzerinde sıkılaştırma yapmanın zor olması sebebiyle oluşan eksikliklerin sistemler için risk ortamı oluşturduğundan bahsedilen raporda, ayrıca bu durumun en düşük kritiklik seviyesinde olduğu da belirtilmiştir [32].

Endüstri 4.0'ın temel odak noktalarından biri de akıllı fabrikalardır. Akıllı fabrikalara yapılan saldırılar ise üretim, müşteriler, üreticiler ve ürünler üzerinde geniş çaplı zararlara sebep olmaktadır. Endüstri 4.0 için uzun değerli zincirler imalatta en büyük güvenlik kaygısı arasındadır. Endüstri 4.0 ile üretimde artan dijitalleşme benimsenirken, bu zorluğu kabul eden bir güvenlik yaklaşımının olmaması, gizliliğin, bütünlüğün ve üretim verilerinin kullanılabilirliğinin risk altında olduğu anlamına gelir. 4. Sanayi devrimi fırsatlar ve zorluklar anlamına gelmekle birlikte, bu devrim ile sunulan fırsatlardan uzun vadeli faydalar elde etmek maksadıyla, imalat şirketleri akıllı fabrikalar için etkin ve verimli bir güvenlik yönetim sistemi belirlemek zorundadır [33]. Sadece dijital alanda değil, aynı zamanda fiziksel dünyada da, saldırıların üretime, müşterilere, üreticilere ve ürünlere yönelik etkileri daha geniş ve potansiyel olarak daha önemli bir şekilde büyüyebilir. Endüstriyel kontrol sistemlerinde kullanılan cihazların kapalı ağlarda konumlandırılması sebebiyle üreticiler, cihaz düzeyinde bir güvenlik önlemi alma gereği duymamışlardır. Dördüncü sanayi devrimi sürecine girilmesi itibariyle geleneksel güvenlik önlemleri bu cihazlar için yetersiz kalmıştır. Kritik altyapılarda kullanılan cihazların/sistemlerin güvenliğini artırmak için derinlemesine savunma yöntemleri geliştirilerek, bilgi varlığının üzerine çoklu kontrol ve denetim yöntemleri uygulanmalıdır [34]. Bu tür uygulamalarla saldırganların aşması gereken engellerin sayısı artırılmaktadır.

Endüstri 4.0 ile üretimin, yapay zeka kullanılarak farklı bir boyuta taşınması ve makinelerin akıllı bir şekilde programlanıp birbirleri ile iletişim halinde olması siber güvenlik problemlerine zemin hazırlamıştır. Bununla birlikte yapay zekanın farklı bir kullanım alanı olan, yapay zeka yöntemlerinin kullanılarak siber güvenlik ürünlerinin geliştirilmesi fikri son yıllarda popülaritesini artırmıştır. Birçok firma bu alanda çalışmalar yaparak ticari ürünler geliştirmiştir. Burada yapay zekânın güvenlik için bir risk faktörü mü yoksa bir çözüm yolumu olduğu fikri doğmaktadır. Yapay zekanın kötü niyetli saldırganlar tarafından bir araç olarak kullanılmasının önüne geçilemeyeceği düşünülürse sistemlerin yapay zeka uygulamaları kullanılarak yapılan saldırılara karşı korunaklı olması gerekmektedir.

Bilginin önemine ve değerine odaklanan Bilgi Teknolojileri (BT) dallarının yanı sıra Endüstri 4.0'da asıl amaç güvenlikten önce üretim ve yönetme süreçleri olmuştur. Genel olarak, Bilgi Teknolojileri sistemlerinin Operasyon Teknolojisi (OT) sistemleriyle entegrasyonu, Endüstri 4.0'ın başarısı için çok önemlidir. Endüstri 4.0'da siber güvenlik ile ilgili karşılaşılan önemli engellerden biri, herhangi bir Endüstri 4.0 kuruluşunun paydaşları arasında entegrasyon ve işbirliği yapılamamasıdır. Endüstri 4.0 ortamları, birçok farklı konu uzmanları ile birçok disipline yayılmış çeşitli teknolojilerden oluşmaktadır. Üretim tarafında Operasyonel Teknoloji ve bu teknolojileri yöneten bir kesim varken, benzer şekilde, Bilgi Teknolojileri tarafında, sunucular ve yazılımlar gibi geleneksel BT ve BT varlıklarıyla çalışan sistem yöneticileri mevcuttur. Bu kapsamda, OT varlıklarını güvence altına alırken bir kontrol mühendisi çoğunlukla "görev güvencesi (mission assurance)" ile, bir BT sistem yöneticisi ise "bilgi

güvencesi" ile ilgilenmektedir. Sonuçta, OT ile BT ortak dilde anlaşamadıkları için her alanda olduğu gibi güvenlik alanında da öncelikler farklılaşmaktadır.

Endüstriyel sistemlerde nihayetinde izole ağ yapısından çıkarak, öncelikle intranet ve müteakiben internete bağlı oldukları için önceden belirlenmiş olan güvenlik standartlarına ve bunlar ile alakalı stratejilere sahip olmaları gerekmektedir. Üretim siber güvenliği, giderek artan dijital cihazlar tarafından yürütülen yeni üretim sistemlerinin ortaya çıkmasından önce bile önemli boşluklara sahipti. Çünkü kritik öneme sahip işlerin gerçekleştirildiği Endüstri 4.0'da öncelikli hedef sistemin her zaman kullanılabilir durumda olmasıdır. Bilgi teknolojilerinde ise sistemin gizliliği ön planda olup, erişiminin bir süreliğine kesilmesi ihmal edilebilir. Bilişim sistemlerinde siber güvenlik ve bilgi güvencesi üç geleneksel merkezi dayanak etrafında dönmektedir: gizlilik, bütünlük ve erişilebilirliktir. BT sistemlerinde bilgi güvenliği unsurları Gizlilik, Bütünlük ve Erişilebilirlik (Kullanılabilirlik) olarak sıralanırken, endüstriyel kontrol sistemlerinde Erişilebilirlik, Bütünlük ve Gizlilik olarak sıralanmaktadır (Şekil 3). Buradan anlaşılacağı üzere, endüstriyel kontrol sistemleri güvenlik önceliğinden ziyade her zaman sistemlerin sürekliliğini esas alan bir yaklaşım benimsemektedir [35]. Endüstriyel kontrol sistemlerini kullanan şirketler ise birkaç saniyelik dahi olsa erişilebilirliği kaybetmeyi göze alamazlar. Gizlilik unsurunun ihmal edildiği bu tür sistemlerde bilgi varlıklarının kaybı şirketler için sorunlar yaratabilmektedir. Bu nedenle, geleneksel siber güvenlik tedbirlerinin, mevcut durumlarıyla endüstriyel kontrol sistemlerine aktarılması mümkün olmayacak, kullanıldıkları endüstri sektörüne göre özelleştirilmesi ihtiyacı ortaya çıkacaktır. Örneğin, bir siber saldırı meydana geldiğinde, etkilenen klasik kurumsal bilişim teknoloji sistemleri geçici olarak devre dışı bırakılabilir ve saldırı sonrası sistemler tekrar aktif edilebilmektedir. Ancak bu yaklaşım, erişilebilirliğin temel bir gereklilik olduğu endüstriyel kontrol sistemlerinde uygulanamaz [36].

***Şekil 3**. Endüstri 4.0'da Bilgi Güvenliği Unsurları*

Gelişmiş dijital üretimin siber-fiziksel güvenliği için gereklilikler, geleneksel BT sistemlerinin güvenliğinden çeşitli yönleriyle farklılık gösterir. BT siber güvenliği, merkezi sunuculara odaklanırken, çevre birimlerine önem vermeyen bir katmanlı savunmaya dayalı güvenlik mimarisini benimser. Ancak, Nesnelerin İnternet'inin benimsenmesi ve yaygınlaşmasıyla bu teori geçerliliğini kaybetmeye başlamıştır [37]. Özellikle dijital imalatta, uzak imalat ekipmanını merkezi tasarım bilgisayarı kadar korumamız gerekir. Artan tehditler, endüstriyel kontrol sistemlerinin kötü niyetli siber izinsiz girişlerin hedefi haline geldiğini göstermektedir [38].

Endüstriyel üretim sistemlerinin en önemli hedefi, üretkenlik kaybı ve gelir kaybıyla sonuçlanan üretimde gereksiz gecikmeleri önlemek için kullanılabilirlik bileşenidir. Bu bileşen, siber fiziksel sistemlerin üretim sistemlerine yönelik hizmet reddi saldırılarına karşı korumayı içermektedir. Diğer bir temel hedef, fiziksel hasara veya insanlara zarar verebilecek herhangi bir sistem arızasını önlemektir. Bu amaca ulaşmak için IIoT sistemlerinin bütünlüğü korunmalıdır. Bu olgu, fark edilmeyen ürün kalitesi kaybına ve kaynakların artan kullanımına yol açabilecek sabotajlara karşı korumayı içermektedir. IoT tabanlı üretim sistemlerinin ve akıllı ürünlerin güçlü bağlanabilirliği, endüstriyel casusluğa ve

müşterilerin ve çalışanların gizliliğine karşı yeni güvenlik mekanizmaları geliştirilmesini gerektirmektedir. Bu nedenle, üretim sistemlerinin kod, veri ve konfigürasyonunun yanı sıra ürün taslaklarının gizliliği de önemli bir güvenlik gereksinimidir [39]. Çeşitli siber saldırılara maruz kalınan Endüstri 4.0 ortamında siber güvenlik politikasının oluşturulması için gerekli kavramların özet karşılaştırması Tablo 2'de verilmiştir [40].

Tablo 2. *Siber saldırıların uygulanma şekillerine göre sınıflandırılması [40]*

	Fiziksel- Trafik analizi	Fiziksel- Protokol Analizi	Fiziksel-Frekans Bozma	Siber-Bulanıklaştırma	Siber-Komut Enjekte Etmek	Siber-Durum Verisi Enjeksiyonu	Siber-Sürücü Çökertme	Fiziksel-Haberleşme Süresi	Siber- Geçici kod Enjeksiyonu	Siber- Hasım Komut Desteği	Siber-Yanlış Komut Yorumlama	Siber- Sistem Bileşen Uyarılarını	Siber-İşletim Sistemi Haberleşme	Siber- Fiziksel Bellek Okuma	Siber-Protokol Analizi	Fiziksel-Bellek Okuma (Silmekte	Siber-Veri Yolu Haberleşme	Siber-Zararlı Kod Yoketme	Siber-Bağlı Cihazları Enfekte
Aldatmak					X	X											X		X
Hile Karıştırmak									X							X		X	X
İnkar Etmek					X	X											X		
Bilgi İfşalamak	X	X		X						X				X	X		X		
Hizmet Reddi			X				X	X		X	X	X	X				X		
Ayrıcalık										X						X	X	X	X
Güvenilirlik										X	X	X	X			X	X	X	
Mahremiyet			X		X	X				X	X	X	X			X	X	X	
Sürdürülebilirlik												X				X		X	X
Kullanılabilirlik			X				X	X		X	X	X	X			X		X	
Bütünlük									X		X								
Gizlilik		X		X										X	X				
Kimlik Doğrulama										X	X					X	X		
Yetkilendirme										X	X					X	X		X
İnkar Edilemezlik					X	X						X					X		
Siber-Fiziksel Sistemde Fiziksel Reaksiyon																			
Siber-Fiziksel Sistemde Çevresel Çarpışmalar					X	X													
Zamanlama		X						X											
Azaltılmış Yaşam Süresi										X	X	X							
Onarılamaz Hasar					X	X				X	X	X							
Hasar Çevreşeme										X	X	X							
Çevre Hasarı					X	X						X							

Güvenlikle ilgili olarak ele alınması gereken diğer konular aşağıdaki gibi sıralanabilir [41];

- *Saldırı etkisi:* Endüstriyel sistemlerin kritik yapısı nedeniyle başarılı siber saldırıların etkisi normalden çok daha yüksektir. Bu durum, endüstriyel sistemleri saldırganlar için çok popüler hedefler haline getirmektedir.

- *Güvenli iletişim*: Sistemde, IIoT cihazları arasında güvenli iletişim kanallarının sağlanması esastır. Sınırlı esnekliklerinin yanı sıra, cihazların çeşitliliğini de göz önünde bulundurarak, yazılım özelleştirme açısından, iletişim için güçlü şifreleme yaklaşımları uygulanmalıdır.

- *Kimlik Doğrulama / Yetkilendirme*: Dikkatle ele alınması gereken bir diğer önemli konu, kullanılan kimlik doğrulama ve yetkilendirme mekanizmalarıdır. İnsan müdahalesi olmadan çalışan IIoT cihazları arasında gerekli güven katmanını sağlamak için makineden makineye güçlü kimlik doğrulama teknikleri kullanılmalıdır.

- *Hesap Verebilirlik*: Güvenlikle ilgili olaylardan kaynaklanabilecek olası zararların büyüklüğü, sorunun kaynağını tespit edebilmenin çok önemli olduğunu göstermektedir. Kullanıcılar ve sistemin düğümleri arasındaki etkileşimlerin kaydedilmesi önem arz etmektedir.

- *Güven Yönetimi*: Birden fazla IIoT cihazının, yedekli çalışma amacıyla aynı hizmeti vermesi yaygın olarak kullanılan bir yöntemdir. Tüm cihazların aynı şekilde çalışmadığı heterojen bir ortamda, işbirliği yapmak için hangi cihazın aktif olarak çalışacağını seçebilmek çok önemlidir.

IIoT cihazlarının, kontrol edilmesi ve hangi cihazlarla irtibat halinde olacağının sağlanması doğru bir güven yönetimi ile mümkün olacaktır. IoT cihazları batarya ile çalması sebebiyle sınırlı hesaplama gücüne, işlemeye ve depolama kapasitesine sahiptirler. Bu sebeple, kablolu sistemlerde kullanılan güvenlik algoritmalarının doğrudan kullanılmasına uygun değildir [42, 43]. Ayrıca, IoT sistemlerinde sınırlı kaynakların olması sebebiyle 6LoWPAN, MQTT, CoAP gibi düşük güç tüketimine yönelik çok çeşitli protokoller ortaya çıkmıştır [44]. Yeni geliştirilen protokoller ile beraber IoT cihazları mevcut protokollerin güvenlik açıklıkları ile birlikte yeni açıklıklara karşıda hassas hale gelmiştir. Bu sonuç ise IoT güvenliğinde standart güvenlik protokolleri geliştirilmesini zorlaştırmış ve IoT cihazlarını saldırganların gözdesi haline getirerek, saldırılara daha açık hale getirmektedir.

Yukarıda belirtilen Endüstri 4.0' da karşılaşılan zorluklar dikkate alınarak, bu kapsamda ilgili kurum/organizasyonlar tarafından yapılması gereken öneriler Tablo 3'te özetlenmiştir.

Tablo 3: *Endüstri 4.0'ın Siber Güvenlik Bileşeninde Karşılaşılan Zorluklar ve Alınması Gereken Önlemler*

KATE-GORİ	ZORLUKLAR	ÖNERİLER	İLGİLİ KURUM /ORGANİZASYON
KİŞİLER	1. Bilgi güvenliği farkındalığının eksikliği 2. Endüstri 4.0'ın farklı alanlarda (Ağ Güvenliği, OT/IT Güvenliği, vb.) kapsamlı uzmanlık gerektirmesi ve kalifiye personel eksikliği 3. Endüstri 4.0 çözümlerinin güvenli kullanımı için gereken yeni yetkinliklerden yoksun olunması 4. Endüstri 4.0'da siber güvenlik konusunda sınırlı eğitimlerin olması ve bu eğitimlerin pahalılığı	1. Farkındalığın artırılmasına yönelik çalışmalar yapılmalı 2. Şirketler ve kurumlar siber güvenlik eğitimlerine yatırım yapmalı 3. Okullar ve üniversitelerde ilgili programlar ve kurslar açılmalı	1. Akademi ve Ar-Ge Organları 2. Düzenleyiciler 3. Endüstri 4.0 Güvenlik Uzmanları
	1. Organizasyonların politika eksikliği ve siber güvenliğe yatırım yapılmaması 2. Çalışanların güvenlikle ilgili rollerinin ve sorumluluklarının açıkça tanımlanmaması 3. Siber güvenliğe sadece maliyet gözüyle bakılması	1. Şirketlerin güvenli bir Endüstri 4.0 ekosistemine geçişini desteklemek için finansman sağlanmalı 2. İnovasyon ve AR-GE faaliyetleri teşvik edilmeli 3. Endüstri 4.0 siber güvenliği için istikrarlı bir yasal ortam sağlanmalı	1. Endüstri 4.0 Operatörleri (Çözüm Sağlayıcılar ve İmalatçılar 2. Düzenleyiciler

SÜREÇLER	1. Endüstri 4.0'ın yaşam döngüsünde çok sayıda paydaş olması sebebi ile bir güvenlik olayı sonrasında sorumluluğun paylaştırılmasının zorluğu 2. Endüstri 4.0 cihaz üreticilerinin ürünlerde gerekli güvenlik işlevlerini yerine getirmemesi 3. Endüstri 4.0 çözümlerinin uzun ömrü ve uzun vadeli bakımları ile ilgili finansal taahhütlerin ağırlığı 4. Endüstri 4.0 güvenlik standartları ve kılavuzlarında önerilen önerilerin uygulanması için sistematik tariflerin eksikliği	1. Endüstri 4.0 operatörlerinin sorumluluklarının yasal yükümlülüklerinin açık bir şekilde belirtilmesi 2. Siber sigorta poliçelerinin potansiyelinin değerlendirilmesi 3. Endüstri 4.0 siber güvenlik gereksinimlerinin satın alma sırasındaki sözleşmelerde belirtilmesi 4. Endüstri 4.0 güvenliği için mevcut standartlar üzerinde analizler yapılması 5. Teknik standartların geliştirilmesinde fikir birliği sağlamak için Endüstri 4.0 aktörleri arasında diyalogların geliştirilmesi	1. Endüstri 4.0 Operatörleri (Çözüm Sağlayıcılar ve İmalatçılar 2. Düzenleyiciler
	1. Farklı ulusal yasama çerçevelerine tabi tedarik zinciri aktörlerinin sayıca fazlalığı 2. Tedarik zincirinin herhangi bir noktasında bir güvenlik ihlalinin nihai ürünün güvenliği üzerinde olumsuz etkisi	1. Tedarik zinciri risklerini tanımlamak için periyodik aralıklarla risk değerlendirmesi yapılmalı 2. Her tedarikçiye duyulan güven miktarı tanımlanarak devam eden ve ortaya çıkan tehdit ortamı izlenmeli 3. Ürünleri, tanınmış güvenlik standartlarına ve sertifikasyon programlarına uyan tedarikçiler ile çalışılmalı	1. Düzenleyiciler 2. Standardizasyon Topluluğu
TEKNOLOJİLER	1. Farklı üreticilerin cihazlarının ve platformlarının kullanılması durumunda, birlikte çalışabilirliğin sağlanması problemi 2. Platformlar, cihazlar ve protokoller arasında ortak bir güvenlik temeli sağlamanın zorluğu 3. Tüm unsurlar üzerinde birleştirici ortak bir siber güvenlik katmanının sağlanmasının getirdiği problem	1. Endüstri 4.0 bileşenleri için ortak bir protokol kullanımının teşvik edilmesi 2. İşbirliği ortakları ve tedarik zincirindeki şirketler arasında, üç siber güvenlik yönünü (insanlar, süreçler ve teknolojiler) de kapsayacak şekilde belirli güvenlik düzeylerinin belirlenmesi 3. Birlikte çalışabilirliğin testi için laboratuvar ve testbed ortamlarının oluşturulması	1. Düzenleyiciler 2. Standardizasyon Topluluğu 3. Endüstri 4.0 Operatörleri (Çözüm Sağlayıcılar ve İmalatçılar 4. Akademi ve Ar-Ge Organları 5. Endüstri 4.0 Güvenlik Uzmanları

5. SONUÇ

Endüstri 4.0 hala gelişmekte olan bir kavram olmasına rağmen, tüm dünyada ve özellikle Avrupa ülkelerinde varlığı oldukça hissedilmektedir. Yaşanan gelişmelerde bu devrimin durdurulamayacağını göstermektedir. Siber dünya ile olan etkileşim/bağlantı, bilişim teknoloji cihaz ve arayüz sayıları ne kadar fazlaysa, siber saldırılar için potansiyel saldırı yüzeyi o kadar büyük olmaktadır. Bu nedenle, bu riskleri teknik ve örgütsel düzeyde en aza indirmek için mutlaka gerekli tedbirler alınmalıdır. Bu tedbirlerden en önemlileri aşağıdaki gibi sıralanabilir;

- Çalışanların ve yöneticilerin, siber güvenlik farkındalığının arttırılmasına yönelik eğitim verilmesi,
- Güvenlik duvarı, sanal özel ağ kullanımı, saldırı önleme/tespit sistemleri, antivirüs yazılımları gibi teknik çözümlerin kullanılması,
- Bilişim teknoloji cihazları ve kullanıcılarının tüm aktivitelerinin kayıt edilmesi ve bunların sürekli olarak izlenmesi,

- Siber saldırıları üzerine çekerek, asıl sistemleri saldırganlardan uzak tutmak için "bal küpleri" kullanılması.
- Politika (Siber güvenlik uygulamalarının hayata geçirilmesi amacıyla, farklı kullanım durumları için çeşitli yönergeler hazırlanmalı ve uyarlanmalıdır.)

Endüstri 4.0 üretim sürecinin yukarıda belirtilen 9 bileşen üzerinde uyumlu bir şekilde çalışması ve üreticiye fayda sağlaması için siber güvenlik esas alınmalıdır. Siber güvenlik iş sürekliliğinin devamı için koruyucu bir mekanizma olarak düşünülmelidir. Endüstri 4.0 sürecine geçiş öncesinde ilgili siber güvenlik tehditlerinin tam olarak tespit edilip farkında olunması ve güvenlik çözümlerinin tüm bu sürece geçiş öncesinde ele alınması gerekmektedir.
Düzenli bakım ve sürekli yenilenen bir güvenlik planı uygulanarak tüm sistemler kontrol altında tutulmalıdır.

Siber güvenlik, Endüstri 4.0'ın kurumlar tarafından benimsenmesinin önündeki en büyük engellerden biri olmuştur. Endüstri 4.0'da siber güvenliği tek bir boyutta düşünmemek gerekir. Her sistemin risk değerlendirmesi yapılarak, sistemlere özel derinlemesine bir güvenlik yaklaşımı ortaya koyulmalıdır. Yalıtılmış ortamlarda başarılı olması amaçlanarak tasarlanan endüstriyel cihazlar, Endüstri 4.0 ile başlangıçta tasarlandıkları amaçlarının sınırlarının dışına çıkabilir ve daha önce var olmayan yeni tehditlerin ortaya çıkmasına neden olabilir. Bu sıkıntılı durumun aşılması adına, doğru bir varlık ve risk yönetimi bu yeni tehditlere karşı koruma sağlamak için bir basamak olacaktır.
Hayata geçirilecek siber güvenlik yazılım ve donanımlarının, mutlaka gerçekçi bir test yatağında önceden kontrol edilmesi gerekmektedir. Aynı süreç, gömülü yazılım ve güvenlik güncelleştirmeleri içinde uygulanması gerçek sistemler üzerinde yaşanacak aksaklıkların önüne geçilmesini sağlayacaktır. Kamu veya özel sektörlere ait kritik altyapılara gerçekleştirilen siber saldırıların sonuçlanması veya girişim aşamasında kalması durumlarında dahi elde edilen tecrübeler mutlaka ortak bir platformda belirli gizlilik ilkelerine uyarak paylaşılması gerekmektedir.

İmalat ve endüstrideki siber güvenlik bilinci ticari sistemler ve özellikle savunma sanayii kadar gelişmemiştir. Ancak endüstriyel casusluk ve bilgi ifşası başta olmak üzere gerçekleştirilecek siber saldırılar sonucunda çok ciddi maddi kayıplarla karşılaşılabilir. Bu nedenle, Endüstri 4.0 sürecinin getirdiği verimlilik, otomasyon, sürat, işlerlik gibi potansiyelleri etkin kullanabilmek için siber güvenlik boyutuna yeterli önem verilmelidir.

KAYNAKLAR

[1] H.S. Kang, , J. Y. Lee, S. Choi, H. Kim, J. H. Park, J. Y. Son & S. Do Noh, "Smart manufacturing: Past research, present findings, and future directions" *International journal of precision engineering and manufacturing-green technology* vol.3, no.1, pp. 111-128, 2016.

[2] A. Soylu, "Endüstri 4.0 ve girişimcilikte yeni yaklaşımlar." *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* c.32, ss.43-57, 2018.

[3] A. Yıldız, "Endüstri 4.0 ve akıllı fabrikalar." *Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, c.22, s.2, s.s.546-556, 2018.

[4] M. ÖZKAN, A. L. Arzu ve S. Yavuz, "Uluslararası politik ekonomi açısından dördüncü sanayi-endüstri devrimi'nin etkileri ve Türkiye." *International Journal of Political Science and Urban Studies,* c.6, s.2, ss.1-30, 2018.

[5] M. A. K. Bahrin, M. F. Othman, N. H. N. Azli, & M. F. Talib, "Industry 4.0: A review on industrial automation and robotic." *Jurnal Teknologi*, vol.78, pp.6-13, 2016.

[6] A. Gilchrist, "The Technical and Business Innovators of the Industrial Internet," *Industry 4.0: the industrial internet of things*. Berkeley, CA, Apress, 2016 pp. 37, 58.

[7] G. Li, W. Zhu, H. Dong & Y. Ke, "Stiffness-oriented performance indices defined on two-dimensional manifold for 6-DOF industrial robot," *Robotics and Computer-Integrated Manufacturing*, vol.*68*, pp.1-9, 2021.

[8] S. ÇELEN, " Sanayi 4.0 ve simülasyon," *International Journal of 3D Printing Technologies and Digital Industry*, c.1, s.1, ss.9-26, 2017.

[9] V. Alcácer, C. Rodrigues, H. Carvalho, & V. Cruz-Machado, "Tracking the Maturity of Industry 4.0: The Perspective of a Real Scenario," *Research Square*, Preprint, 2021.

[10] L. Da Xu, W. He, & S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol.10, no.4, pp.2233-2243, 2014.

[11] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. (2021, 13 March). [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[12] Internet of Things. (2021, 13 March). [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf?dtid=osscdc000283.

[13] E. Oztemel, S. Gursev, "Literature review of Industry 4.0 and related technologies," *Journal of Intelligent Manufacturing*, *31*(1), 127-182, 2020

[14] K. Zhou, T. Liu, L. Zhou, "Industry 4.0: Towards future industrial opportunities and challenges," *12th International conference on fuzzy systems and knowledge discovery (FSKD)*, August 2015, pp. 2147-2152.

[15] N. Benias, & A. P. Markopoulos, "A review on the readiness level and cyber-security challenges in Industry 4.0," *South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, September 2017, pp.1-5.

[16] İ. Akben, "3 Boyutlu Yazıcılar ve Tedarik Zincirine Etkiler," *International Journal of Academic Value Studies (Javstudies)*, c.3, s.10, ss.20-35, 2017.

[17] G. Erboz, "How to define industry 4.0: main pillars of industry 4.0," *How to define industry 4.0: main pillars of industry 4.0 at Szent Istvan University, Gödöllő*, November 2017, pp.1-9.

[18] D. J. Horst, C. A. Duvoisin, & R. de Almeida Vieira, "Additive manufacturing at Industry 4.0: a review," *International journal of engineering and technical research*, vol.8, no.8, pp.3-8, 2018.

[19] T. Masood, J. Egger, J. "Augmented reality in support of Industry 4.0—Implementation challenges and success factors," *Robotics and Computer-Integrated Manufacturing*, vol.*58*, pp.181-195, 2019.

[20] M. Rüßmann, M. Lorenz, P. Gerbert, M. Waldner, J. Justus, P. Engel & M. Harnisch, "Industry 4.0: The future of productivity and growth in manufacturing industries," *Boston Consulting Group*, vol.9, no.1, pp.54-89, 2015.

[21] İ. İlhan, M. Karaköse, "Requirement Analysis for Cybersecurity Solutions in Industry 4.0 Platforms," *International Artificial Intelligence and Data Processing Symposium (IDAP)*, September 2019, pp. 1-7.

[22] S. Yin, O. Kaynak, "Big data for modern industry: challenges and trends [point of view]," *Proceedings of the IEEE*, vol.103, no.2, pp.143-146, 2015.

[23] Ö. Tuttokmağı, A. Kaygusuz, A. "Smart Grids and Industry 4.0," *International Conference on Artificial Intelligence and Data Processing (IDAP)* September 2018, pp.1-6.

[24] Definition of cybersecurity, (2021, 13 March), [Online]. Available: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[25] A. Corallo, M. Lazoi, M. Lezzi, " Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Computers in industry*, vol.114, pp.1-15, 2020.

[26] S. Ozawa, T. Ban, N. Hashimoto, J. Nakazato, J. Shimamura, J. "A study of IoT malware activities using association rule learning for darknet sensor data," *International Journal of Information Security*, vol.19, no.1, pp.83-92, 2020.

[27] M. Lezzi, M. Lazoi, A. Corallo, A. "Cybersecurity for Industry 4.0 in the current literature: A reference framework," *Computers in Industry*, vol.103, pp.97-110, 2018.

[28] M. Kiss, L. Muha, L. "The cybersecurity capability aspects of smart government and industry 4.0 programmes," *Interdisciplinary Description of Complex Systems: INDECS*, vol.16, no.3-A, pp.313-319, 2018.

[29] Addressing the SANS TOP 20 critical security controls for effective cyber defense. (2021, 13 March). *A trend Micro Whitepaper,* [Online]. Available: https://resources.trendmicro.com/rs/945-CXD-062/images/sans_top20_csc_trendmicro2016.pdf

[30] A. Corallo, M. Lazoi, M. Lezzi, M. " Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Computers in industry, 114*, 103165, 2020.

[32] OWASP Internet of Things. (2021, 13 March). [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[33] E. Casalicchio, G. Gualandi, G. " ASiMOV: A self-protecting control application for the smart factory," *Future Generation Computer Systems*, vol.115, pp.213-235, 2021.

[34] M. T. Rahman, M. S. Rahman, H. Wang, S. Tajik, W. Khalil, F.Farahmandi & M. Tehranipoor, "Defense-in-depth: A recipe for logic locking to prevail," *Integration*, vol.72, pp.39-57, 2020

[35] S. GÖNEN, "PLC ile Kontrol Edilen Mikro Tip Akıllı Şebeke Sistemlerde Bilgi Güvenliğinin Sağlanması," Doktora Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 2018.

[36] A. R. Sadeghi, C. Wachsmann, M. Waidner, "Security and privacy challenges in industrial internet of things," *52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, June 2015, pp. 1-6.

[37] M. Indri, A. Grau, M. Ruderman, "Guest editorial special section on recent trends and developments in industry 4.0 motivated robotic solutions," *IEEE Transactions on Industrial Informatics*, vol.14, no.4, pp.1677-1680, 2018.

[38] G. Culot, F. Fattori, M. Podrecca, M. Sartor, "Addressing industry 4.0 cybersecurity challenges," *IEEE Engineering Management Review*, vol.47, no.3, pp.79-86, 2019.

[39] H. Mouratidis, V. Diamantopoulou, "A security analysis method for industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol.14, no.9, pp.4093-4100, 2018.

[40] A. A. Süzen, “A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem,” *International Journal of Computer Network & Information Security*, vol.12, no.1, pp.1-12, 2020.

[41] A. Hassanzadeh, S. Modi, S. Mulchandani, “ Towards effective security control assignment in the Industrial Internet of Things,” *IEEE 2nd World Forum on Internet of Things (WF-IoT),* December 2015, pp.795-800.

[42] Z. S. M. Attarbashi, Y. Fazea, “Investigation on 6LoWPAN Data Security for Internet of Things,” *2nd International Conference on Computer and Information Sciences (ICCIS)*, October 2020, pp. 1-5.

[43] S. Chakraborty, A. Majumder, A. “6LoWPAN Security: Classification, Analysis and Open Research Issues,” *International Journal of Computational Intelligence & IoT*, vol.1, no.1, pp.8-12, 2019.

[44] S. Sharma, S. Kumar, “A Review on IoT: Protocols, Architecture, Technologies, Application and Research Challenges,” *10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, January 2020, pp. 559-564.