NESNELERİN İNTERNETİ VE GÜVENLİK

Mustafa Şirin - Ebu Yusuf Güven - Melike Başer - Muhammed Ali Aydın

Öz

Geleneksel nesnelerin internete bağlanan formlarının üretilmesi ve birbiri ile iletişim kurmasını ifade eden Nesnelerin İnterneti (Internet of Things - IoT) birçok ürün ve hizmeti insanlığa sunmaktadır. Yaygın olarak kullanılan kısıtlı kaynaklarla hizmet veren bağlı cihazlar geleneksel siber güvenlik yöntemleri uygulanmadığı için birçok gizlilik ve güvenlik riskini beraberinde getirmektedir. Bu çalışma kapsamında Nesnelerin İnterneti cihazları tanımlanmış olup, mevcut riskler ve tehdit vektörleri açıklanmış, IoT cihazlarının siber güvenlik testleri ve değerlendirmesi konusu cihazın yazılım, donanım, haberleşme ve yasal regülasyonlar & standartlar başlıkları altında açıklanmıştır. Son olarak Güvenli IoT cihazlarının tanımlanması için açık tartışmalar ve konular anlatılmıştır.

Anahtar Kelimeler: Nesnelerin İnterneti, Siber Güvenlik, Yazılım Güvenliği, Donanım Güvenliği, Standartlar

1. Giriş

Nesnelerin İnterneti (IoT), günümüzde en yaygın kullanılan teknolojilerden biridir ve genellikle verileri algılayan, yakalayan, dağıtan ve analiz eden akıllı sistemler ve hizmetler sağlayan heterojen bileşenlerden oluşan birbirleri ile bağlantılı bir ağ olarak tanımlanır. IoT ekosistemini kapsayan nesnelere, veri toplayan ve ileten sensörler, akıllı saatler, akıllı buzdolapları, duman dedektörleri, radyo frekansı tanımlama (RFID), kalp atışı monitörleri, ivmeölçerler, akıllı telefonlar vb. örnek olarak verilebilir. IoT sistemlerinde birbirine bağlı nesnelerin sayısı her geçen gün artmaktadır. IoT, sosyal, ticari ve ekonomik yönler dahil olmak üzere çeşitli şekillerde yaşamlarımız üzerinde önemli bir etkiye sahiptir. IoT, akıllı evler, akıllı şehirler, ulaşım, lojistik, akıllı sağlık, perakende, tarım ve iş dünyasının yanı sıra akıllı ölçüm, uzaktan kumanda dahil olmak üzere hayatımızın çeşitli alanlarında büyük ölçekli teknolojik ilerlemeler ve katma değerli hizmetler sağlar.

IoT cihazlarına yönelik çok sayıda siber saldırı ve tehdit, IoT'nin genişlemesine meydan okuyan sorunlar olarak görülmektedir. IoT ağındaki en temel ihtiyaç, tüm sistemleri, uygulamaları ve bağlı cihazları korumaktır. IoT ağlarının devasa boyutu, cihaz yönetimi, veri yönetimi, bilgi işlem, güvenlik ve gizlilik gibi çeşitli alanlarda yeni zorlukları da beraberinde getirmektedir. IoT ekosistemi büyüdükçe, potansiyel tehditler de artarak devam etmektedir. Tipik olarak IoT sistemleri, algılama katmanı (perception/sensing layer), ağ oluşturma ve veri iletişim katmanı (networking and data communication layer), ara yazılım veya destek katmanı (middleware or support layer) ve uygulama katmanı (application layer) dahil olmak üzere birkaç katman üzerinde çalışır. Bu katmanların her biri, bir IoT uygulamasında gerçekleştirilecek bir dizi görev ve ilgili teknolojilere sahiptir ve her katman gerçekleştirdiği göreve ve sahip olduğu teknolojiye göre bir dizi güvenlik riski taşır. Örneğin, hizmet reddi (DoS) saldırıları, kimlik sahtekarlığı saldırısı (spoofing attacks), karıştırma (jamming), gizli dinleme (eavesdropping), veri kurcalama (data tampering), ortadaki adam saldırıları (man in the middle) ve zararlı yazılımlar (malwares) vb. en yaygın IoT saldırılarıdır. Güvenlik sorunlarının doğasına bağlı olarak kimlik doğrulama, erişim kontrolü, tehdit ve risk tahmini, kötü amaçlı yazılım analizi, anormallik veya izinsiz giriş tespiti ve önleme gibi potansiyel IoT güvenlik çözümleri yararlı olabilmektedir. Güvenlik tehditleri ve saldırılarındaki gelişmiş yöntemler ve güvenlik olaylarındaki karmaşıklık nedeniyle, bunlarla başa çıkmak için kullanılan geleneksel teknikler yeterli olmamaktadır. Bu nedenle, yeni nesil IoT sistemini korumak için bu güvenlik endişelerini giderebilecek modern teknolojilere dayalı akıllı bir güvenlik sistemine ihtiyaç duyulmaktadır.

Çalışma kapsamında ilk olarak Kavramsal Çerçeve altında Nesnelerin İnterneti kavramı ve Nesnelerin İnterneti İletişim Protokolleri açıklanmıştır. Nesnelerin İnterneti Siber Tehdit ve Saldırı Vektörleri altında Varsayılan Parola ve Konfigürasyon, Güvenli Haberleşme, Uzaktan Kontrol Güvenliği, Yazılım Güvenliği ve Yazılım Güncellemesi anlatılmıştır. Nesnelerin İnternetinde Donanım Güvenliği altında donanım güvenliği ve saldırıları açıklanmış, Donanım Güvenlik Modülü ve Güvenli Haberleşme Modülleri anlatılmıştır. Son olarak IoT Kullanım Alanları ve Nesnelerin İnterneti Güvenlik Regülasyon ve Standartları açıklanmıştır.

2. Kavramsal Çerçeve

2.1. Nesnelerin İnterneti

Nesnelerin İnterneti (IoT) algılama, iletişim ve hizmet süreçlerini birleştiren genellikle kısıtlı kaynaklar (işlem gücü, hafıza ve pil ömrü) ile hizmet veren cihazlara verilen isimdir. Yaygın olarak Nesnelerin İnterneti yalnızca cihazları değil geleneksel bilgi teknolojileri (BT) cihazlarıyla birlikte oluşan donanım, yazılım ve haberleşme katmanlarından oluşan ekosistemi ifade için de kullanılmaktadır. Bu ekosistem cihaz sensörleri/donanımı, cihaz yazılımı, cihaz iletişim altyapısı, mobil uygulama, web servis, web uygulama sunucu / bulut bilişim altyapısını kapsamaktadır.

IoT cihazları mikrodenetleyici ya da basit mikroişlemci ile çalışan düşük hafızalı ve pil ya da enerji altyapısına bağlı cihazlardan oluşabilir. Genellikle mikrodenetleyici ile tasarlanmış cihazlar bir ya da birkaç özel iş için geliştirilmiş güncelleme ihtiyacı duyulmayan cihazlardır. Mikroişlemci ile çalışan IoT cihazları ise üzerinde temel işletim sistemi ve uygulama katmanı yazılımları bulunan genellikle uzaktan ya da manuel güncelleme mekanizması olan cihazlardır. IoT cihazlarında kullanılan farklı işletim sistemleri bulunmasına karşın genellikle linux kernel üzerine özelleştirilmiş / sadeleştirilmiş işletim sistemleri tercih edilmiştir. Bu iki tür işlem birimine sahip cihazların güvenli bir bağlantı altyapısı kurmak için çoğunlukla donanımsal gerçeklenmiş düşük güç tüketen iletişim modüller tercih edilmektedir.

Üretici firmaların hızlı ürün geliştirme döngüleri, bilinçsiz kullanıcılar ve yetersiz hukuki düzenlemeler gibi sebepler yüzünden geçtiğimiz on yılda birçok IoT cihazını konu alan siber saldırı gerçekleşmiştir. Artan farkındalık ve oluşturulan yasal düzenlemeler ve uygulamaya alınan güvenlik standartları IoT cihazlarının güvenliğini artırmaktadır. IoT cihazları ile ilgili endişeler arasında; kişisel verilerin sızdırılması, yetkisiz erişim, kimlik doğrulama, haberleşme trafiğinin güvenliği, uzaktan güncelleme işlemleri öne çıkmaktadır.

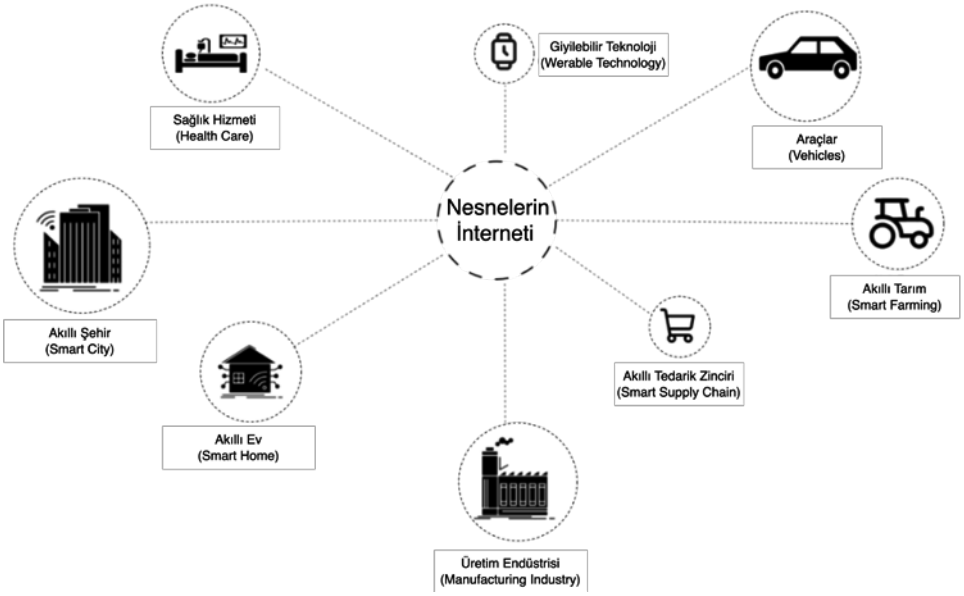
IoT cihazının güvenliğinin sağlanması için temel aşama cihaz donanımı üzerinde başlamaktadır. Özellikle fiziksel güvenliği sağlanamayan IoT cihazlarının saldırgan eline geçmesi halinde bile içindeki bilgileri muhafaza edebilecek altyapıya sahip olması gerekmektedir. IoT cihazları genellikle taşınabilir

veya çalınma ihtimali olan cihazlar olması dolayısıyla kurcalamaya karşı güvenli olması temel güvenlik aşamasıdır.

IoT sisteminin önemli bir başka bileşeni de iletişim altyapısı ve haberleşme protokolleridir. IoT cihazlarından oluşan ağ, bulut hizmetlerine erişim için erişim noktası ile internetin bir parçası olmaktadır. Özellikle güvenlik cihazları ve yazılımları bulunmayan işletme ve son kullanıcı cihazları için tüm internet altyapısından gelen saldırıların hedefi haline getirmektedir. Ayrıca IoT'nin yaygın kullanılan kablosuz hizmetlerde iletişim altyapısı erişim mesafesi içerisinde sinyali dinleme ve yanıltma saldırılarına da maruz kalabilmektedir. Kablosuz Ağı protokollerinden IEEE 802.15.4 standardını temel alan IoT süreçlerinin ihtiyaçlarına göre Bluetooth, ZigBee, PLC, WiFi, 4G ve 5G de iletişim protokolleri ile hizmet verebilmektedir.

2.2. IoT Kullanım Alanları

Nesnelerin İnterneti (IoT), bu nesnelerin veri toplamasını ve değiş tokuş etmesini sağlayan elektronik, yazılım, sensörler ve ağ bağlantısı ile gömülü fiziksel nesneler, cihazlar, araçlar, binalar ve diğer farklı öğelerin ağı olarak tanımlanabilir. IoT, canlı varlıklar, nesneler ve makinelerle etkileşim kurmanın bir yolunu sunmaktadır. IoT, sensörler yardımıyla çalışır ve internete bağlanır. İnsandan insana veya insandan bilgisayara etkileşim olmadan bir ağ üzerinden veri aktarma yeteneğine sahiptir. IoT, çevre ile ilgili bilgileri, nesnelerin koşullarını, yazılım sistemlerini ve makineleri insanların paylaşımına sunar. Teknolojinin gelişmesi ve IoT ekosisteminin genişlemesi ile dünyamız her açıdan akıllı hale gelmektedir. Akıllı şehirler, akıllı evler ve akıllı binalar inşa edilmekte, ayrıca ulaşım, atık yönetimi, sulama tesisi, tarım vb. Şekil 1'de görülen farklı hizmetler hayatımıza girmektedir. Bu yazıda IoT kavramını tüm kullanıldığı alanlarda genel başlıklar halinde inceleyeceğiz.



Şekil 1. IoT Kullanım Alanları

2.2.1. Akıllı Şehir (Smart City)

Son yıllarda, kentsel alanların nüfusu hızla artmaktadır. Birçok şehir, yaşam kalitesini artırmak ve vatandaşlara daha iyi hizmet sunmak için akıllı şehirler konseptine yönelik kendi stratejilerini geliştirmeye başlamıştır. Akıllı şehirlerin altyapısı akıllı ulaşım, akıllı otopark, akıllı trafik sistemi, akıllı tarım ve akıllı evler gibi çeşitli uygulamalarda insanlara fayda sağlamak için birçok cihaz ve birbirine bağlı sistemler içerir.

Bir akıllı şehir birkaç bileşenden oluşur. Akıllı şehir uygulamalarının tipik olarak kendileriyle ilişkili dört yönü vardır: veri toplama, iletim/alma, depolama ve analiz. Verilerin toplanması uygulamaya bağlıdır ve çeşitli alanlarda sensör gelişimi için bir itici güç olmuştur. İkinci kısım, veri alışverişidir, veri toplama birimlerinden depolama ve analiz için buluta veri iletimini içerir. Bu görev birkaç şekilde gerçekleşmektedir. Birçok akıllı şehir girişimi şehir çapında Wi-Fi ağlarına sahiptir, 4G ve 5G teknolojileri ve ayrıca verileri yerel düzeyde veya küresel düzeyde iletebilen çeşitli yerel ağ türleri kullanılmaktadır. Üçüncü aşama bulutta depolamadır, veriler dördüncü aşama olan veri analizi için kullanılabilir hale getirilerek düzenlenir. Veri Analizi, karar vermeye rehberlik etmek için toplanan verilerden istatistiklerin çıkarılmasını ifade eder. Daha karmaşık karar verme için, bulutun kullanılabilirliği yalnızca hete-

rojen veri toplama/depolama ve işlemeye değil, aynı zamanda gerçek zamanlı olarak makine ve Derin Öğrenme algoritmalarının yanı sıra istatistiksel yöntemlerin kullanımı yoluyla analiz de kullanılır.

Akıllı şehir hizmetleri, bir şehrin nüfusunu sürdüren faaliyetleri kapsar, bunlar su temini, atık yönetimi, çevresel kontrol ve izleme gibi belediye görevlerini içerir. Şehirde kullanılan suyun kalitesi hakkında sürekli güncelleme sağlamak ve sızıntıları tespit etmek için su kalitesi sensörleri kullanılabilir (Rojek ve diğerleri, 2019). Akıllı şehir girişimlerinin popüler bileşenlerinden biri atık yönetimidir ve Barselona'daki oluklardan sensörlerle donatılmış ve buluta bağlı çöp kutularına kadar daha önce bahsedilen akıllı şehir girişimlerinin birçoğunun bir parçası olmuştur. İlgili makamlar bunları boşaltma ihtiyacının yanı sıra maliyeti azaltma amacıyla en iyi rotayı belirlemek için yapay zekayı da kullanmaktadır (Pardini ve diğerleri, 2019). Sensörler aynı zamanda bir şehirdeki çevre koşullarını izlemek, kirlilik seviyelerini belirlemek (Dutta ve diğerleri, 2017) ve yakıt maliyetlerinden tasarruf etmek amacıyla vatandaşları bir sonraki boş park yerine yönlendirmek için kullanılabilir (Al-Turjman, 2019).

2.2.2. Akıllı Ev (Smart Home)

Akıllı Şehirlerin ana bileşenlerinden biri, şehir sakinlerinin yaşamının merkezi olduğu için Akıllı Ev'dir. Akıllı Evler, bir kişinin evinin her yerine kurulan ve ev ve içinde oturanlar hakkında bilgi sağlayan algılama birimlerinin kullanımını içerir. Bu sensörler, ortam sensörleri, hareket izleyicileri ve güç/enerji tüketimi gibi kullanıcı etkinliği monitörlerini içerebilir.

2.2.3. Akıllı Tarım (Smart Farming/Agriculture)

Gıda güvenliği, Birleşmiş Milletler'in 2030 Sürdürülebilir Kalkınma hedeflerinin en önemli parçalarından biridir. Artan dünya nüfusu, kötüleşen iklim değişikliğinin dünyadaki gıda merkezlerinde düzensiz hava koşullarına yol açması, gıda üretiminin sürdürülebilir olmasını sağlama yarışı ve su gibi azalan kaynakların verimli bir şekilde kullanılması, dünyadaki ülkeler için yüksek bir öncelik olmuştur. Akıllı tarım, karar vermede yardımcı olmak ve hastalıkları, haşereleri vb. önlemek için çeşitli parametreleri ölçmek üzere bitkilere ve tarlalara gömülü sensörlerin kullanılmasıdır (Koubaa ve diğerleri, 2020). Akıllı tarım paradigmasının bir parçası, hedeflenen ölçümleri sağlamak için bitkilere yerleştirilen sensörleri içeren ve dolayısıyla hedeflenen bakım mekaniz-

malarının konuşlandırılmasına izin veren hassas tarımdır. Gelecekte gıda güvenliği için hassas tarım gerekli olacaktır (O'Grady ve diğerleri, 2019) ve bu nedenle sürdürülebilir gıda üretimi mücadelesinin önemli bir parçasıdır. Yapay zekanın tarım için IoT'deki başlıca uygulamaları, mahsul izleme, hastalık tespiti, veriye dayalı mahsul bakımı ve karar vermedir.

2.2.4. Sağlık Hizmeti / Akıllı Sağlık (Health Care / Smart Health)

Akıllı Sağlık, sağlık hizmetlerinin mevcudiyetini ve kalitesini iyileştirmeyi hedeflemektedir. Artan nüfus ve artan sağlık hizmetleri maliyetleri ile bu alan, araştırmacıların yanı sıra sağlık hizmeti sağlayıcılarının yoğun odak noktası olmuştur. Akıllı sağlık, teletıp hizmetleri (Andreão ve diğerleri, 2018) ve Yapay Zeka kullanılarak doktorlara gelişmiş tanı yardımı (Keane ve diğerleri, 2018) aracılığıyla sağlık hizmetlerinin mümkün olduğu kadar çok kişiye sunulmasını amaçlamaktadır. İnsanların sağlığı hakkında gerçek zamanlı verileri (EKG'ler, sıcaklık, vücut oksijen doygunluğu ve diğer biyosensörler) yakalayabilen ve aynı zamanda günlük aktiviteyi kaydeden ve atalet sensörlerini kullanarak anormal hareketleri tespit edebilen cep telefonlarının ve sağlık izleyicilerinin her yerde bulunmasıyla (Trencher ve diğerleri, 2019) daha iyi sağlık hizmetlerinin sunulması ve verileri işleyerek analizinin yapılması için bulut yeteneklerinden yararlanmak mümkündür.

2.2.5. Akıllı Ulaşım (Smart Transport)

Birçok şehir merkezi trafik sorunlarından muzdariptir, buna toplu taşıma için sıkışıklık, kirlilik, zamanlama ve maliyet düşürme sorunları dahildir. Yeni Bilgi ve İletişim Teknolojilerinin hızla gelişmesi ve uygulanması, Araç-Altyapı-Yaya iletişimini olağan hale getirmiştir. Araçtan Araca (V2V), Araçtan Altyapıya (V2I), Araçtan Yayaya (V2P) veya Yayadan Altyapıya (P2I) olsun, bu tür teknolojiler akıllı ulaşım sistemlerinin tasarımını mümkün kılmaktadır. GPS cihazının arabalarda ve sürücülerin cep telefonlarında ortak olmasıyla, birçok yaklaşım, sürücü davranışını ve trafik modellerini izlemek için GPS verilerini kullanır (Wang ve diğerleri, 2016). Bu gerçek zamanlı veriler, Waze ve Google Haritalar gibi uygulamalarda rota haritalama ve toplu taşımada yolculuk planlaması için kullanılmaktadır.

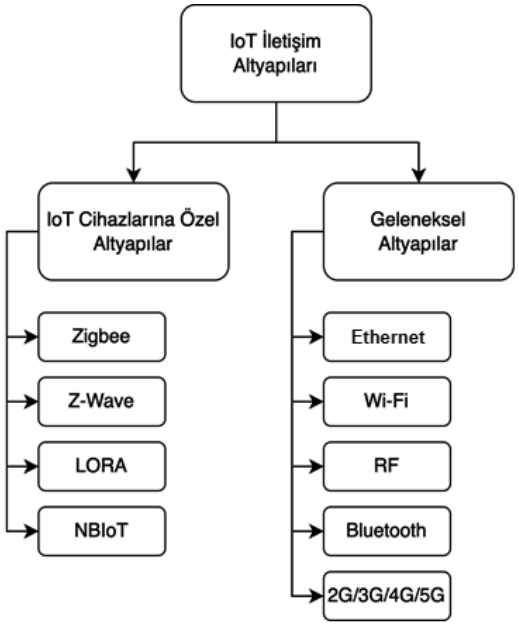
2.2.6. Akıllı Endüstri (Smart Industry)

Dünyanın dört bir yanındaki endüstriler, maliyetleri düşürürken sürekli olarak daha verimli olma ve üretkenliği artırma peşinde koşuyor. Endüstri 4.0 paradigması, tüm aracı görevlilerinin sorunsuz bir şekilde entegre olduğu ve birbirleriyle etkileşimli çalıştığı bağlantılı bir fabrika vizyonunu gerektirir. Bu vizyon ise Nesnelerin İnterneti (IoT) sayesinde mümkün olmaktadır (Haverkort ve diğerleri, 2017). Üretim ve üretim süreçlerinde, işçileri ve makineleri entegre eden siber fiziksel sistemlerde IoT kullanımı, sektöre daha hızlı ve daha iyi yenilik, üretim şemalarının (kaynaklar ve süreçler) optimizasyonu, daha iyi ürün kalitesi ve gelişmiş güvenlik gibi çeşitli faydalar sağlamıştır. Bununla birlikte, bir dizi heterojen cihaz ve makine ile çalışmanın kendi zorlukları vardır ve Akıllı Endüstri, IoT uygulamalarında kullanım için yapılandırma, bağlantı ve hızlı uygulama konusunda esnekliğe sahip siber fiziksel sistemler gerektirir (Koca ve İsa, 2023, Tao ve diğerleri, 2017). Yapay Zeka, Endüstri 4.0 hizmetlerinin geliştirilmesini ve dağıtımını teşvik etmek için IoT ile entegre edilmiştir. Fabrikadaki makinelere ve diğer süreçlere yerleştirilen sensörlerle, bu kaynaklardan gelen veriler, otomasyonu artırmak, iş zekası operasyonlarını gerçekleştirmek ve daha fazlası için yapay zeka tekniklerini kullanma fırsatı sunar. Araştırmacılar, Yapay Zekayı Akıllı Endüstri'de IoT'ye entegre ederek izleme/arıza tespiti (makine sağlığı) ve üretim yönetimi gibi alanlarda geliştirme yapmışlardır (Trakadas ve diğerleri, 2020).

2.3. Nesnelerin İnterneti İletişim Protokolleri

IoT cihazlarını dijital diğer ürünlerden ayıran en temel özelliği bulut sunucuları veya diğer IoT cihazları ile bağlantı kurabilmesidir. IoT iletişiminde bağlantının güvenliği, cihaz ile Bulut, cihaz ile erişim noktası, cihaz ile mobil uygulamalar, cihaz ile başka bir cihaz ve erişim noktası ile Bulut sunucuları arasındaki güvenliğin sağlanmasıyla mümkündür. İletişim kalite, kapasite ve kapsama alanı gibi sorunları yanında gizlilik ve güvenlik sorunları da geleneksel cihazlarda olduğu gibi IoT cihazlarında da devam etmektedir. Ancak IoT cihazları kaynak kısıtları nedeniyle geleneksel sistemlerde kullanılan güvenli iletişim protokollerine desteği bulunmayabilir. Düşük güç tüketimini destekleyen ve IoT cihazlarının internete ya da merkezi bir düğüme veri iletmesine yetecek kapasitede IoT cihazlarına özgü Zigbee, Z-Wave, Lora ve NBIoT altyapı protokolleri geliştirilmiştir. Bunun yanında geleneksel sistemlerde de yaygın olarak kullanılan RF ve Bluetooth gibi düşük güç gerektiren protokoller de IoT cihazlarında ve geleneksel cihazlarda sıklıkla tercih edilmektedir. Güç tüketimi

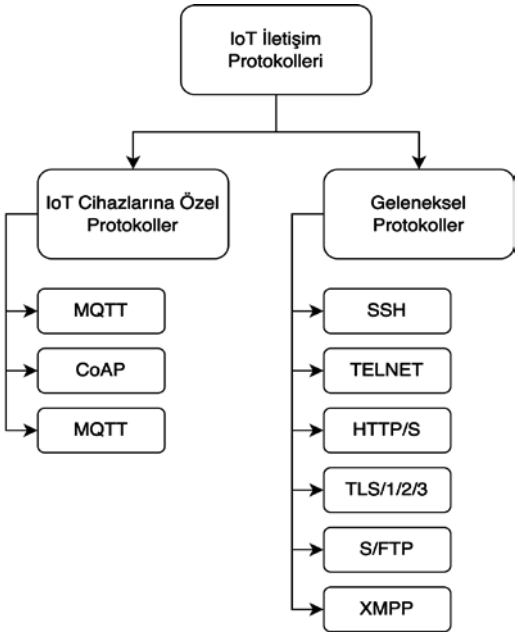
ve iletişim kapasitesi daha yüksek IoT cihazları için geleneksel altyapılardan Ethernet Wi-Fi ve GSM farklı jenerasyonları hizmet verebilmektedir. IoT cihazları iletişim altyapıları Şekil 2'de geleneksel ve IoT cihazlarına özgü protokoller olarak ayrıştırılmıştır.



Şekil 2. IoT İletişim Altyapıları

IoT cihazları için farklı iletişim altyapıları üzerinde uyarlanabilen düşük kaynak gerektiren ve düşük güç tüketen MQTT ve CoAP (Bormann, 2012) gibi IoT cihazlarına özgü iletişim protokolleri geliştirilmiştir. Geleneksel güvenli protokolleri kullanmak isteyen üreticiler ise kaynak kısıtları olan IoT cihazlarına HSM (Hardware Security Module - Donanımsal Güvenlik Modülü) gibi yeni güvenli iletişim donanımları ekleyerek iletişim güvenliğini sağlamaya çalışmaktadırlar. Kimlik doğrulama, ağ katmanında güvenli iletişim sağlamak için en yaygın güvenlik yöntemidir. IoT cihazlarına erişim sağlamak için, kimlik doğrulama ve yetkilendirme prosedürleri ihtiyacı ortaya çıkmaktadır. IoT cihazlarında MQTT, CoAP, Zigbee ve Z-Wave gibi altyapılar ve protokoller kimlik doğrulamayı desteklemektedir (Hassan, 2019). IoT cihazlarında telemetri, geliştirici kontrolleri, cihaz eşleştirme ve haberleşme için gerekli kimlik doğrulama araçlarını sağlamış olsa bile, trafiğin dinlenmesi riskleri devam etmektedir. Ayrıca, güvenli olmayan ağ hizmetleri (herkese açık ya da yayıncısı bi-

linmeyen Wi-Fi ağları gibi), kötü aktörün (kötücül ikiz - Evil Twin gibi) veya saldırganın ağı keşfetmesine (zayıf şifreleme neticesinde ağa dahil olma ya da pasif dinleme) saldırılarına sebep olabilir. IoT cihazlarında kullanılan ve geleneksel sistemlerle de kullanılan iletişim protokolleri Şekil 3'te gösterilmiştir.



Şekil 3. IoT İletişim Protokolleri

2.4. Donanımsal İletişim Protokolleri

Yazılım uygulamalarında veritabanlarıyla, çeşitli sunucularla ve uygulamaların kendi arasında iletişim için kullandığı birçok protokol bulunmaktadır. Bu protokoller ile belirli kurallar dizisine bağlı olarak haberleşme işlemi gerçekleştirerek kullanıcının uygulamayı verimli bir şekilde kullanmasını sağlamaktadır. Yazılım uygulamalarında olduğu gibi donanımlar da haberleşme işlemleri için bazı haberleşme protokollerini kullanır. Bu donanım haberleşme protokolleri ile donanımlar kendi aralarında ya da dışarıdaki bir cihazla iletişim kurabilirler. Örneğin bir mikrodenetleyici bir sensörle veya bir mikrodenetleyici başka bir mikrodenetleyici ile iletişim kurabilmektedir. Bu özelliği ile donanım haberleşme protokolleri cihazlar arasındaki iletişimin düzenlenmesinde büyük rol oynar. IoT cihazlarının donanımlarının haberleşmesinde genellikle UART, SPI, JTAG, SWD, I2C gibi protokoller görülmektedir.

2.4.1. UART

Açılımı Universal Asynchronous Receiver/Transmitter şeklinde olan UART, gömülü sistem uygulamaları, mikrodenetleyiciler ve bilgisayar sistemlerinde sıklıkla kullanılan bir donanım haberleşme protokolüdür. Açılımından da anlaşılacağı üzere asenkron iletişim için kullanılır. Tx (verici) ve Rx (alıcı) olmak üzere iki ucu bulunduğundan iletişim için yalnızca iki kablo kullanır. Asenkron kavramı verici cihazdan alıcı uca giden çıkış bitlerini senkronize edecek saat (clock) sinyali olmadığı anlamına gelmektedir. Yapılandırılabilir hızda veri iletişimi sağlayan UART bir seri iletişim protokolüdür. UART iletişiminin özelliği olan bu hız baud hızı olarak adlandırılır. Baud hızı, verinin bir iletişim kanalına aktarılma hızını ifade eder. Bir başka ifadeyle saniye başına aktarılacak maksimum bit sayısıdır. Genellikle baud hızı 9600, 19200, 38400, 57600, 115200 olarak kullanılırken farklı konfigürasyonlar ile daha yüksek hızlarda da kullanılabilir. İletişim halindeki verici ve alıcı cihazların baud hızlarının aynı olması gerekmektedir. I2C ve SPI protokolleri ile karşılaştırıldığında, yalnızca iki kabloyla full-duplex asenkron iletim gerçekleştirebilmesi ile daha fazla kaynak tasarrufu sağlayan UART, uzun mesafeli iletim konusunda da iyidir. (Li ve diğerleri, 2022; Peňa, Legaspi, 2020)

2.4.2. SPI

SPI (Serial Peripheral Interface) master-slave tabanlı seri haberleşmeye izin veren senkron bir haberleşme protokolüdür. Veri alışverişi master ve slave cihazlar arasında gerçekleşmektedir. Saat (clock) sinyali kullanılan bu protokolde master cihaz saat sinyalini üretir. Master ve slave'ler arasında iletilen veriler master tarafından üretilen saat sinyaliyle senkronize edilir. Hem çipler arasında hem de çip içi düşük/orta hızlarda veri iletişimi için en yaygın protokollerden birisi olan SPI, bir mikrodenetleyici ile harici EEPROM'lar, DAC'ler, ADC'ler vb. gibi çevre birimleriyle iletişim kurmak için kullanılır. (Anand ve diğerleri, 2014)

I2C protokolüne göre daha yüksek hızlarda saat frekanslarını destekleyen SPI haberleşmesi 4 uçtan oluşur:

- CS: slave seçmek için kullanılan sinyaldir. Birden fazla slave olduğu durumda master'dan her bir slave için ayrı bir CS sinyali gerekir.
- SCLK: Seri saat sinyalidir. Veri yolu boyunca gerçekleşen iletimleri senkronize eder.

- MOSI: verileri master'dan slave'e iletir.
- MISO: verileri slave'den master'a iletir. (Dhaker, 2018)

2.4.3. JTAG

Eski dönemlerde birden fazla giriş-çıkış yolu olan bir kartı veya entegreyi test etmek için test yatağı gibi ek işlemler hazırlamak gerekmekteydi. Giriş-çıkış pinlerinin artması ve Bilyalı Izgara Dizisi (Ball Grid Array - BGA) paketlemenin yaygınlaşmasıyla daha zor hale gelen test işlemleri için entegreler arasındaki donanım ara bağlantılarını test edebilecek yeni bir test çözümüne ihtiyaç duyulmuştur. Bir IEEE standardı olan JTAG (Joint Test Action Group), normal işlemler esnasında devre aktivitesini gözlemleme, değiştirme ve entegre ara bağlantılarını test etme mantığıyla bu soruna bir çözüm olmuştur. Geniş bir kullanım alanına sahip olan JTAG, yarı iletken cihazlarda ve baskı devre kartlarında programlama, hata ayıklama, test ve doğrulama uygulamaları için kullanılmaktadır. JTAG, çip üzerinde test fonksiyonlarına erişim sağlayan Test Erişim Noktalarından (Test Access Points - TAP) oluşmaktadır. Standarda göre minimum 3 giriş ve 1 çıkış olmak üzere 4 porttan oluşması zorunludur. Bu portlar; TDI, TDO, TCK ve TMS şeklindedir. TRST portu ise isteğe bağlı kullanılabilmektedir. Bu portlardan TDI test veri girişi pini, TDO test veri çıkış pini, TCK saat (clock) pini, TMS test modu seçme pini ve TRST test sıfırlama pinidir. Bellek kayıtları, donanım kesme noktalarının ayarlanması, kayıtların değiştirilmesi vb. gibi düşük düzeyde donanım erişimi olması ile JTAG, donanım güvenliği konusunda da dikkat çekmektedir. (Gallagher, 2020; Rajput & Maniatakos, 2019)

3. Nesnelerin İnterneti Siber Tehdit ve Saldırı Vektörleri

IoT cihazları düşük kaynak profilleri ve özelleşmiş çalışma alanlarıyla insan hayatını kolaylaştıran ve dijitalleştiren ürün ve hizmetleri temsil etmektedir. Bu cihazlar düşük maliyet amacıyla kısıtlı kaynaklarla tasarlandıkları için geleneksel cihazlarda alınan bir takım siber güvenlik önlemini uygulamak için uygun altyapıya sahip değillerdir. Bu nedenle geleneksel saldırı vektörlerinin çoğuna karşı zafiyetler içerir. Buna karşın bazı temel güvenlik aşamaları; kimlik doğrulama, yetkilendirme gibi güvenlik aşamaları cihaz kabiliyetleri dolayısıyla IoT cihazlarında bulunmamaktadır. Bu nedenle IoT cihazları geleneksel sistemlerden miras aldığı siber tehditlerin yanında kaynak kısıtlarından iletişim altyapısı ve iletişim protokollerinden kaynaklanan siber tehditlere de maruz kalmaktadır.

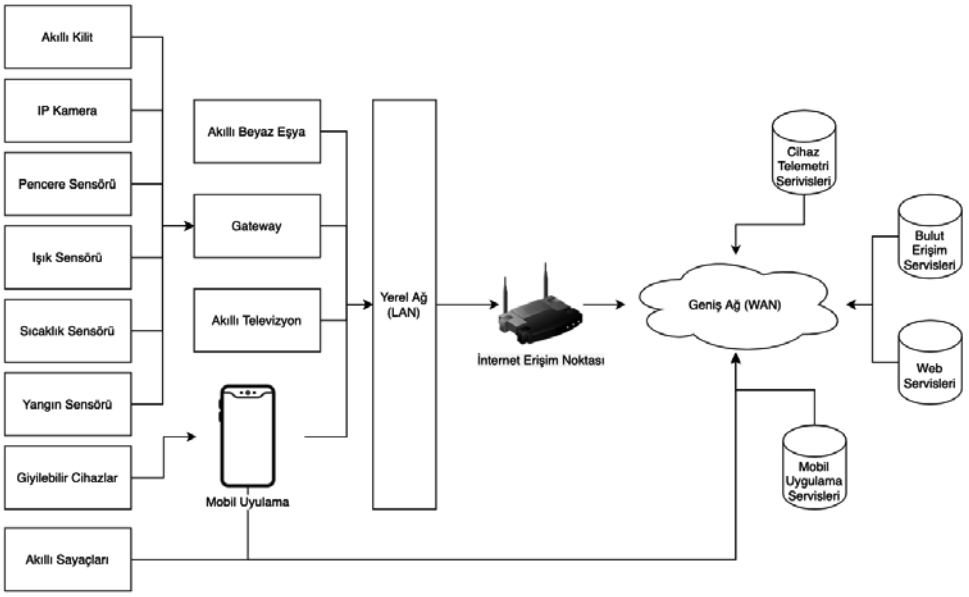
3.1. Varsayılan Parola ve Konfigürasyon

Fabrika çıkışı varsayılan kullanıcı bilgileri gibi birçok hatalı ve varsayılan güvensiz konfigürasyonlar, yetersiz kullanıcı güvenlik yapılandırması IoT cihazları için siber riskleri artırmaktadır. Üretici tarafından varsayılan parola ile üretilen IoT cihazlarının saldırganların, zararlı yazılımların ve botnetlerin birincil hedefi haline gelmiştir (Başer 2021). IoT cihazları gerçek hayatın bir parçası olarak üretildikleri için fiziksel güvenliğin yeterince sağlanmaması ve cihaz donanımındaki güvenlik açığından kaynaklanan saldırılar IoT cihazları için önemli bir atak vektörüdür. Cihaz üzerinde tutulan verilerin ve iletişim trafiğinin şifrelenmemesindeki temel engel, IoT cihazı bir ya da bir kaç sensör bulunduran cihazların basitliğinden ve işlem gücü yetersizliğinden kaynaklanmaktadır. Ayrıca, IoT cihazının karmaşıklaştırması ve işlem gücünün artırılması maliyet ve ürünün kullanılabilirliği açısından bir sorunlar oluşturabilmektedir. Ancak, kullanıcıların gizliliğini ve güvenliğini sağlamak için cihazlarda tüysiklet (ligth-weigt) şifreleme ve beyaz kutu (white-box) şifreleme yöntemleri uygulamak faydalı olabilir.

3.2. Güvenli Haberleşme

IoT cihazları kişisel ağ (PAN), yerel ağ (LAN) ve geniş ağlarda (WAN) hizmet veren çeşitli ürün ailelerinden oluşmaktadır. Doğrudan IoT cihazına olan tehdit vektörleri etki derecesi IoT cihazının bulunduğu ağın büyüklüğüyle orantılı olarak artmaktadır. Akıllı Sayaçların Şekil 4'te görüldüğü üzere doğrudan IP kamera gibi cihazların bir ev erişim noktası üzerinden yine internete eriştiği görülmektedir. Akıllı sayaçlar için doğrudan sağlanmış bir VPN ya da erişim için beyaz liste uygulaması gibi güvenlik yapılandırmaları olmadığı durumda keşfedilen cihazların güvenliğini sağlamak mümkün olmamaktadır. Özellikle akıllı sayaç gibi uzun pil ömrü gerektiren sistemlerde pil ömrünü tüketmeye dönük saldırılar da yapılmaktadır. IP kamera gibi cihazların ise yapılandırılabilir bir ağ geçici (gateway) veya modem üzerinden internete çıkması durumunda ağın kenarı (edge) üzerinde alınacak önlemlerin güvenlik sıkılaştırması için faydalı olacaktır. Aksi durumda doğrudan dışarıdan erişimi olan IoT cihazı ağdaki diğer IoT cihazlarının güvenliğini riske atmaktadır. Aynı gateway'e bağlı ve yalnızca güvenli ağlar için tasarlanmış IoT cihazları saldırgan ile aynı ağda bulunuyormuş gibi pasif dinleme, araya girme, veri manipülasyonu, pil tüketme ve cihazın fiziksel etki özelliklerine göre fiziksel zararlara sebep olabilmektedir. Dolaylı ya da ikincil tehdit vektörleri ise geleneksel ve diğer IoT cihazlarını etkiledikten sonra erişim yetkisi, izni veya erişime imkan

sağlayan bir zafiyet ile cihaza erişmesiyle oluşan tehditlerdir. Giyilebilir cihazlar Şekil 4'te görüldüğü üzere genellikle doğrudan PAN ağı üzerinden mobil platformu köprü olarak kullanarak internete erişmektedir. Bu senaryoda PAN ağı dinlenme mesafesine kadar pasif saldırılar, mobil cihaz ile eşleşmesi mekanizmaları, mobil cihazın güvenliği öne çıkmaktadır. Cihazın fiziksel güvenliği olmadığında PAN üzerinden gerçekleşen pasif ve aktif saldırılar cihaz ürün eşleşme mekanizmasına yapılan saldırılar gerçekleşebilmektedir. Üretici firmaların IoT ürünlerinin bağladığı kişisel ağı veya yerel ağı güvenli kabul ederek oluşturdukları sistemler cihazların ve tuttukları verilerin güvenliğini riske atmaktadır. IoT cihazı varsa donanımı üzerindeki komponentleriyle, çevre cihazlarıyla, diğer geleneksel ve IoT cihazlarıyla iletişimi güvenli olmalıdır. PAN, LAN veya WAN üzerinde konumlandırılan cihazların ağ özelliklerinden ve güvenlik cihazlarından (Firewall gibi) dolayı doğrudan saldırı yüzeyleri açık olmasa bile saldırganın aynı ağda bulunabileceği değerlendirilerek güvenlik önlemleri alınmalıdır. Ağ büyüklüğüne bakılmaksızın güvenli konfigürasyon ve şifreli haberleşme süreçleri tanımlanmalıdır.



Şekil 4. IoT cihazı topolojisi

3.3. Uzaktan Kontrol Güvenliği

IoT cihazları ürün ve hizmetin amaçlarına ve cihaz özelliklerine göre doğrudan mobil platform veya bilgisayar üzerinden kontrol edilebildiği gibi uzak sunucu ve bulut sistemleri üzerinden kontrol edilen versiyonları da bulunmaktadır. Tek bir adımda IoT cihazına erişilen senaryolarda cihazların eşleşmesi için konulan fiziksel erişim kontrolü (bir tuşa basmak, cihaz üzerinden uzaktan erişimi aktif hale getirmek) gibi aşamalar cihazların güvenliğini sağlamaktadır. Ancak erişim sağlandıktan ve cihaz uzaktan kontrolü aktif edildikten sonra saldırganın pasif dinlemesine, tekrarlama, manipülasyon ve araya girme gibi saldırılarına karşı güvenli olması gerekmektedir. Şekil 4'te görülen akıllı cihazlar ve giyilebilir eşyalar bu kapsamda değerlendirilebilir. IoT cihazının ürettiği veriyi doğrudan uzak sunucu ve bulut sistemleri üzerinde depolandıktan sonra son kullanıcıya erişilen web ya da mobil arayüzler ile hizmet veren sistemlerin doğrudan geniş ağa çıktıkları için geleneksel cihazlar tarafından da kullanılan güvenli TLS versiyonları ile haberleşmeleri gerekmektedir. Aksi halde cihazın ürettiği verilerin ağ üzerinden yapılabilecek manipülasyonlara ve yönlendirmeler karşı riskler içerebilir. Özellikle cihaz ve bulut arasındaki erişim kontrolü için kullanılan anahtarların, beyaz listelere eklenen IP ve MAC adreslerinin saldırgan tarafından ele geçirilmesi sunucu ve bulut sistemlerine yapılan saldırılarda kullanılmaktadır.

3.4. Yazılım Güvenliği

IoT Cihazlarında yazılım güvenliği IoT cihazı donanımı üzerinde yer alan firmware ve uygulama yazılımlarının güvenliğini kapsamaktadır. Cihaz ile doğrudan ilişkili olan mobil uygulama web uygulaması ve bulut servislerinin güvenliği de ayrıca ilişkili olan yazılım hizmetlerin güvenliği olarak değerlendirilebilir. Ancak ilişkili olan yazılım hizmetlerinin güvenliği geleneksel sistemlerin güvenliği çalışma kapsamında değerlendirilmemiştir.

IoT cihazları yazılım güvenlik açığı, birbirinde çok farklı donanım platformları ve özelleştirilmiş işletim sistemleri güvenlik risklerinin kontrolünü zorlaştırmaktadır. Donanımla uyumlu yazılım versiyonları zafiyetler içerebilmekte ve güncelleme için donanım yükseltmesi ihtiyaçları bulunabilmektedir. Bazı IoT cihazlarında uzaktan güncelleme mekanizmaların bulunmaması bulunsa bile kullanıcı kontrolünde güncellemenin aktif edilmesi zafiyetlerin devam etmesine neden olmaktadır. Yazılım güvenlik açıkları ve iyi yapılandırılmamış servis arayüzleri arka kapı sorununa yol açabilmektedir. Yazılım gü-

venlik açıkları ile saldırganlar, kurbanın cihazın kontrolünü ve cihazın üzerinde bulunan bilgileri ele geçirebilir. Saldırganlar tarafından cihazı kontrol etmek veya bir bot (uzaktan kontrollü bir robata) dönüştürmek için savunmasız bir IoT cihazına arka kapı yerleştirilebilir. IoT cihazlarının kaynak kısıtlamaları nedeniyle, makul miktarda hesaplama gücü gerektiren IDS veya antivirüs gibi güvenlik mekanizmaları IoT'de uygulanmadığı için son kullanıcılar tarafından fark edilmesi zordur. Bu gibi durumlarda cihaz komple sıfırlanmalı (eğer bu fonksiyon mevcut ise) ya da güncel firmware'i baştan yüklenmelidir. Ancak saldırganın cihazı ele geçirmesine sebep olan zafiyet devam ediyorsa kısa süre içinde tehditlerden tekrar etkilenmesi mümkündür.

Üreticiler ve hizmet sağlayıcılar tarafından IoT cihazına yönetim, servis hizmetleri veya test amacıyla kasıtlı olarak arka kapılar yerleştirilebilir. Bu arka kapılar saldırganlar tarafından keşfedilebilir ve kullanıcı verilerini çalmak için kullanılabilir. Özellikle tersine mühendislik teknikleri uygulayarak cihazın kaynak kodu inceleyebilir ve bu tür bir arka kapıyı keşfedebilir. Ancak üretici tarafından yerleştirildiği için bu tür bir arka kapının konuşlandırılması kolay ancak son kullanıcı ve regülatörler tarafından incelenmesi zordur. Devlet tarafından yayınlanan regülasyonlara ve güvenlik politikalarına uyulmasını zorunlu tutması ve takibi ile mümkündür.

3.5. Yazılım Güncellemesi

IoT cihazlarında doğrudan mikrodenetleyici ile tasarlanmış ve üretimde programlanan ve sonradan bir güncelleme süreci planlanmamış ürünler bulunmasına karşın linux kernel veya farklı temel işletim sistemleri üzerinde inşa edilmiş yazılım platformları da hizmet vermektedir. Bu tür IoT cihazlarında işletim sistemi ve üzerinde uygulamaların bulunduğu firmware olarak isimlendirilen yazılım bulunmaktadır. Geliştirilen yazılımların yeni özelliklerin eklenmesi, hata ve zafiyetlerin giderilmesi için yeni yazılımların güncellenmesi gerekmektedir. Bu nedenle, geliştiriciler ve cihaz üreticileri için değişen ürün ortamına uyum sağlamak için, yazılımı kablosuz olarak (Over The Air - OTA) güncellemektir. IoT cihazının yalnızca güvenilir kaynaklardan gelen kodu kabul ettiğini ve sunucudan cihaza geçiş sırasında kodun değiştirilmediğini doğrulamak için dijital imzalama yöntemleri kullanılmalıdır. Yazılım dağıtımları, TLS ile şifrelenmiş iletişim kanalları üzerinden gerçekleştirilmelidir. Güncellemeler, SSH, SFTP ve HTTPS güvenli gibi protokoller kullanılarak güvenli bir şekilde yapılmalıdır. IoT cihazlarına manuel fiziksel ya da uzaktan güncelleme aşamalarında kaynağı bilinmeyen yazılımların yüklenmesi ile alakalı

kontrol mekanizmaları eşleştirilmelidir. Halka açık forumlarda paylaşılan ek özellik ve yöntem vadeden değiştirilmiş firmware'lar ve uygulamalar cihazlara yüklenmemelidir.

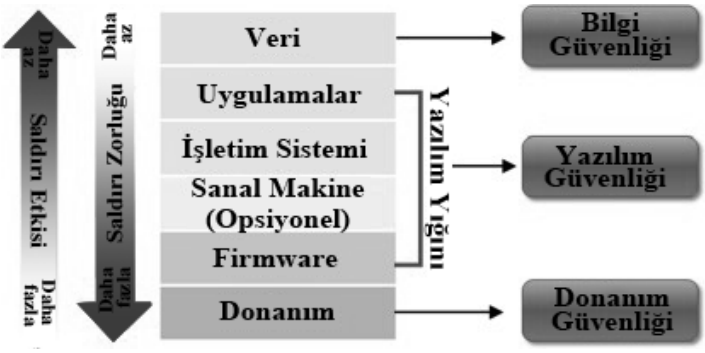
4. Nesnelerin İnternetinde Donanım Güvenliği

Nesnelerin İnterneti ekosistemini oluşturan ve gündelik hayatımızın da bir parçası hâline gelen cihazların çoğunun donanım tarafında gömülü sistemler olarak adlandırılan karmaşık bir sistemde, belirli ve kendisine tanımlanan işlevleri yerine getiren özel bilgisayarlar bulunmaktadır. Bu sistemler çalıştığı ürüne göre tanımlanan işlemleri yapmaktadır. Örneğin akıllı çamaşır makinesine ait donanım sadece makinenin çalışmasını sağlayacak özelliklere sahipken akıllı kahve makinesindeki donanım da uzaktan kahve hazırlamak, kahve makinesinin durumunu kontrol etmek gibi kahve makinesinin çalışması için gerekli işlevleri yerine getirmektedir. Sistemin işlevini bu şekilde yapacağı görevlere göre sınırlamak donanımın küçük, hızlı ve verimli olması anlamına gelmektedir. (Grau, 2015). Ancak bu durum cihazların verimli ve hızlı çalışması, küçük boyutta olmaları gibi cihazlar için avantaj sağlasa da güvenlik tarafında dezavantaj oluşturabilir. IoT cihazların boyut olarak küçük olması nedeniyle ekstra bir güvenlik modülü eklenememesi, cihazın donanımında kullanılan mikrodenetleyicilerin düşük hesaplama yeteneği dolayısıyla mevcut karmaşık güvenlik algoritmalarının uygun olmaması, IoT cihazların (özellikle kablosuz olarak çalışan sistemlerin enerji açısından verimli olması beklendiğinden) düşük güç tüketimi gibi özellikleri ile ekstra enerjiye ihtiyaç duyan güvenlik sistemlerinin uygulanamaması ve donanım tarafındaki güvenlik sorunlarına çok bakılmaması gibi durumlar güvenlik tarafındaki bu dezavantajların sebepleri olabilmektedir. (Koley & Ghosal, 2015).

IoT cihazlarının güvenliği bir bütün olarak ele alınmalı ve tüm sistem bileşenlerini kapsamalıdır. Saldırganlar cihaz yazılımına veya cihazın haberleşme yapısına saldırıda bulunabileceği gibi cihazın donanımına da saldırı düzenleyerek cihaz hakkında veya kullanıcısı hakkında bilgiler ele geçirebilir. Cihaz bir saldırganın eline geçtiği durumda cihazın yazılımı güvenli hale getirildiyse bile donanımı savunmasız kalabilir. Cihazın kutusunu açarak elektronik kartını inceleyen bir saldırgan donanım düzeyinde farklı saldırı yöntemleri kullanarak cihaza zarar verebilir. Bu kapsamda donanım güvenliği yapılabilecek bu türden saldırılara ve donanımın korunmasına odaklanır. Sistem güvenliğinin temelini oluşturan donanımlar sistemin kendisiyle yakın etkileşim içerisinde

olan diğer bileşenleri için bir güven çapası sağlar. (Bhunia & Tehranipoor, 2019).

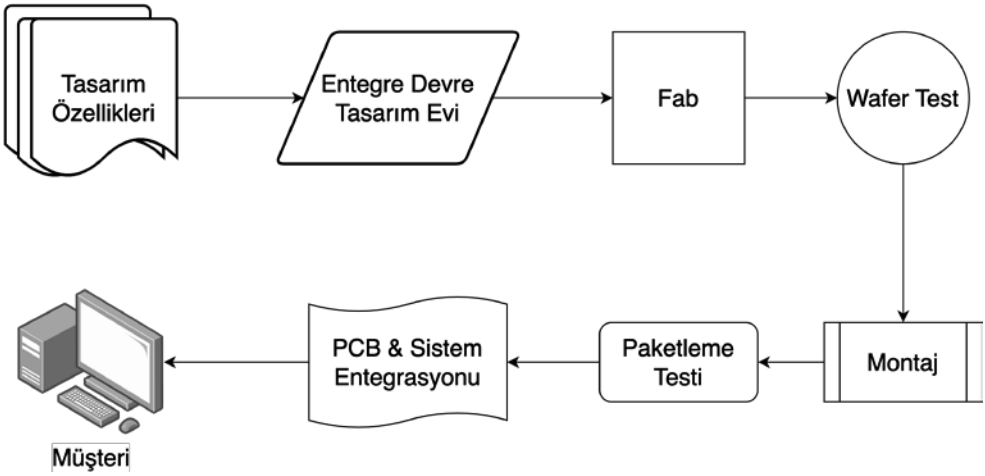
Modern bir bilgisayar sistemi Şekil 5'te gösterildiği bir birçok katmandan oluşan bir organizasyon olarak görülebilir. Burada bazı katmanlar birçok IoT uygulaması için fazla olsa da genel yapı donanım - yazılım - veri şeklinde özetlenebilir. Siber güvenlik sorunları bu sistemdeki tüm katmanları kapsamaktadır. Donanım güvenliği konusunda saldırıların zorluğu veya sorunlar diğer katmanlara göre az olsa da bu katmanda meydana gelen bir sorunun veya açığın sistem üzerindeki etkisi diğer katmanlara göre çok daha büyük olmaktadır. Özellikle geçmiş dönemlerde gündeme gelen Spectre ve Meltdown açıkları birçok bilgisayar sistemini etkilemiştir. (Bhunia & Tehranipoor, 2019).



Şekil 5. Saldırıların bir sistemin katmanları üzerindeki etkisi ve zorluk dereceleri (Bhunia & Tehranipoor, 2019).

Donanım güvenliği kapsamında yapılan çalışmalar ve saldırı örnekleri sadece kullanıcı düzeyinde kullanıcıya ait verilere erişmek üzerine değil aynı zamanda çip üreticisi firmanın fikri mülkiyetine (Intellectual Property - IP) yönelik de olabilir. Burada karşımıza donanım güveni kavramı çıkmaktadır. Donanım güveni sorunları bir entegrenin tasarım, üretim, test veya dağıtım aşamalarından birinde veya birkaçında entegrenin veya donanımın yaşam döngüsüne güvenilir olmayan varlıkların dahil edilmesinden kaynaklanır. Bu tip bir güvensizlik durumunda üretici firmanın fikri mülkiyeti olan tasarım bilgisi gibi önemli bilgiler saldırganın bir başka tarafın eline geçebilir. Bunun yanında bu üretim döngüsü içerisinde entegre tasarımına saldırgan kötü amaçlı bir tasarım ekleyebilir ve bu kötü amaçlı entegrenin kullanıldığı cihazın hatalı çalışmasına, dışarıya veri sızdırmasına vb. kötü senaryolara yol açabilir. Şekil 6'da bir entegrenin üretim yaşam döngüsü ve saldırıların olabileceği

aşamalar gösterilmektedir. (Bhunia & Tehranipoor, 2019; Jin,2015; Koley & Ghosal, 2015).



Şekil 6. Bir entegrenin yaşam döngüsü ve potansiyel saldırı noktaları (Bhunia & Tehranipoor, 2019).

Entegrelere tasarım aşamasında veya sonrasında saldırganlar tarafından eklenen ve kötü amaçlı çalışarak entegre devrenin veya donanımın arızalanmasına, dışarıya veri sızdırmasına ve bunlar gibi donanımın kötü amaçlı işler yapmasına neden olan devrelere Donanım Truva Atı (İng. Hardware Trojan) adı verilmektedir (Koley & Ghosal, 2015). Bir donanımın erken aşamalarında entegre devreye eklenen donanım truva atı tespit edilememesi halinde hem üretici firmaya hem de o donanımı kullanan kullanıcılara büyük zararlar verebilir.

Donanım güvenliği kapsamında gerçekleştirilebilecek saldırı çeşitlerini **Şekil 6**'yı inceleyerek saldırının olabileceği aşamalara göre yapabileceğimiz gibi bu konuda yapılan literatürdeki çalışmalar incelendiğinde farklı ana başlıklarda sınıflandırmalar da görülmektedir. Saldırı yapılacak yüzeye göre yapılan bir sınıflandırmada saldırılar 3 ana başlıkta toplanmıştır. Bu 3 ana başlıktaki saldırı yüzeyleri: Çip Seviyesinde Saldırılar, PCB Seviyesinde Saldırılar ve Sistem Seviyesinde Saldırılar şeklinde tanımlanmıştır. Burada çip seviyesindeki saldırılara donanım truva atı ve tersine mühendislik saldırıları, PCB düzeyinde yapılan saldırılara örnek olarak kurcalama saldırıları, tersine mühendislik saldırıları ve sistem düzeyi saldırılara fiziksel arayüz saldırıları örnek olarak verilebilir. (Bhunia & Tehranipoor, 2019). Farklı bir kaynakta, donanıma fiziksel erişim ve fiziksel erişimin donanım üzerindeki etkilerine (donanı-

ma verdiği zarar) göre bir sınıflandırma yapılmıştır. 3 ana başlıkta yapılan sınıflandırma: İnvaziv, Yarı İnvaziv ve İnvaziv Olmayan şeklinde tanımlanmıştır. İnvaziv saldırılara mikroproblama ve tersine mühendislik saldırıları, yarı invaziv saldırılara optik görüntüleme ve invaziv olmayan saldırılara yan kanal saldırıları örnek olarak verilebilir. (Skorobogatov, 2014). Yapılan sınıflandırma farklı noktalardan farklı isimlerle olsa da sınıflandırmaların içerdikleri saldırıların sistem etkileri benzerlik göstermektedir. Örneğin tersine mühendislik saldırıları hem invaziv saldırı sınıfına hem de çip seviyesi saldırı sınıfına girmektedir. (Bhunia & Tehranipoor, 2019; Skorobogatov, 2014).

Siber güvenlik konusunda kılavuz bir kaynak olarak ön plana çıkan OWASP'ın (Open Web Application Project) yayınladığı OWASP Nesnelerin İnterneti Projesinde nesnelerin interneti cihazları için saldırı yüzeyleri de tablo halinde verilmiştir. Hem saldırı yüzeyi hem de saldırı yüzeylerinde olabilecek güvenlik açıkları listelenen tabloda IoT donanım güvenliğini ilgilendirdiği düşünülen saldırı yüzeyleri: Cihaz Hafızası, Cihazın Fiziksel Arayüzleri, Lokal Veri Sızıntısı ve Donanım (Sensörler) şeklindedir. Burada:

- Cihaz Hafızası saldırı yüzeyi için Hassas veri (Okunabilir kullanıcı adları, Okunabilir parolalar, Şifreleme anahtarları, 3. parti kimlik bilgileri)
- Cihazın Fiziksel Arayüzleri saldırı yüzeyi için Firmware dışa çıkarma, Komut satırı arayüzü erişimi, Yetki yükseltme, Güvensiz duruma resetleme, Depolanan medyanın silinmesi, Kurcalamaya karşı koruma, Hata ayıklama portları, Cihaz ID/Seri numarası teşhiri
- Lokal Veri Sızıntısı saldırı yüzeyi için Şifrelenmemiş veri, Keşfedilen anahtarlarla şifrelenmiş veriler, Veri bütünlüğü kontrollerinin eksikliği, Statik aynı şifreleme/şifre çözme anahtarının kullanımı
- Donanım (Sensörler) saldırı yüzeyi için Sensör ortamının manipülasyonu, Kurcalama (fiziksel olarak), Zarar verme (fiziksel olarak)

güvenlik açıkları olarak verilmiştir ("IoT Attack Surface Areas Project", 2019).

Nesnelerin İnterneti ekosisteminde yer alan cihazların ürün yazılımını dışarı çıkarmak IoT sistemin güvenliğini analiz ederken önemli bir ilk adımdır. Cihaz yazılımının saldırganın veya rakip firmanın eline geçmesi istenmeyen bir durumdur. Cihaz yazılımı özel şifreleme anahtarları, kullanıcı verileri, üretici firmaya ait bilgiler içerebildiğinden güvenliğinin sağlanması önemlidir. Bir IoT cihazın yazılımı güncelleme esnasında ağ üzerinden elde edilebileceği gibi yazılım donanım üzerinde çalıştığından donanıma erişerek de elde edilebilir.

Böyle bir senaryoda donanıma yönelik saldırı donanım haberleşme protokolleri, hata ayıklama arayüzleri veya flash hafızanın okunması üzerinden yapılmaktadır. Bu tip bir saldırı genellikle cihazdan cihaza değişiklik gösterebilmektedir. (Vasile, Oswald, Oswald, 2019). Ürün üreticileri donanımlarını ve yazılımlarını tasarlarken farklı teknolojiler kullanabilmektedir. Örneğin donanım haberleşmesi tarafında UART, SPI ve JTAG gibi protokollerden biri veya birkaçı kullanılabilir. Aynı şekilde donanım üzerinde harici bir hafıza çipi bulunabileceği gibi hafıza tarafında mikrodenetleyiciden de faydalanılabilir. Donanım tarafında yapılacak ön çalışma ile öncelikle donanımın bileşenleri tanımlanmalı ve kullandığı haberleşme protokolü keşfedilmelidir. Bu işlemlerin ardından protokolün özelliklerine göre donanım üzerinden cihaz yazılımına erişim sağlanabilir. İnternette cihazların donanımını çevreleyen kutularının nasıl açılacağı ve elektronik kart üzerindeki bileşenlerin ne olduğunu tanımlayan birçok web sitesi mevcuttur. Örneğin ifixit.com web sitesini kullanarak elinizdeki bir cihazın (web sitesinde paylaşılmışsa) içinin nasıl açılacağını öğrenebilirsiniz. Buna ek olarak donanım güvenliği kapsamında, www.exploitee.rs web sayfasında belirli cihazlar için donanım üzerinden cihazın yazılımına veya işletim sistemine nasıl erişileceği adım adım yazmaktadır.

Donanım tarafında genellikle test işlemleri içim kullanılan JTAG, bellek dökümü ve kayıt manipülasyonu gibi donanıma düşük düzeyde erişim sağlama özelliği ile siber güvenlik konusunda dikkat çekmektedir. (Rajput & Maniatakos, 2019). Ayrıca üretim sırasında yazılım yüklemek için de kullanılabilen JTAG bazı durumlarda çip içerisindeki tüm belleğin okunması için de kullanılabilir. Bu şekilde bir cihazın JTAG ile belleğini okumak için bellek dökümünü alıp bilgisayara aktarabilen ara bir ekipmana ihtiyaç bulunmaktadır. Çoğu durumda üreticiler üretimden sonra cihazın hafızasının okunmasını veya yeniden programlanmasını engelleyebilirler. Fakat JTAG bağlantı noktalarının ve cihaz üzerindeki yetkisinin açık bırakıldığı durumda cihazın yazılımının çıkarılmasına ve cihaz yazılımı enjeksiyonu saldırılarına neden olabilir. (Vasile, Oswald, Oswald, 2019). JTAG arabiriminden faydalanarak yapılan saldırılar incelendiğinde bir araştırma ekibinin hedef donanımdaki EEPROM'da depolanan bilgileri ayıklamak ve çıkarmak için JTAG arabirimini kullanarak kolayca çıkardığı görülmüştür. (Rajput & Maniatakos, 2019).

JTAG haricinde donanım güvenliği tarafında firmware erişimi için sıklıkla kullanılan bir diğer yol UART protokolü üzerinden sızma gerçekleştirmektir. JTAG arabirimine ait pinleri donanım üzerinde bulmak ve hangi pinin ne pini olduğunu belirlemek çoğu durumda zor olabilmektedir. JTAG'in aksine UART

daha kolay keşfedilmesi, 2 pin bulundurduğu için pinlerin hızlıca belirlenebilmesi ve sık kullanılmasıyla donanım güvenliğinde dikkat çeken haberleşme protokollerinden birisidir. Donanım üreticileri, üretim sonrası bakım ve teknik servis gibi işlemler için cihaz yazılımına erişim sağlayan UART pinlerini açık bıraktığında saldırganların cihaz yazılımına erişmesine neden olabilmektedir. UART haberleşme için 2 pin (Tx ve Rx) gerektirdiğinden donanım üzerinden işletim sistemine erişim işlemini oldukça kolaylaştırmaktadır. Bu tip bir saldırıda saldırgan USB-UART dönüştürücü kullanarak bilgisayarına bağladığı donanıma seri port üzerinden erişebilmektedir. (Vasile, Oswald, Oswald, 2019) yaptığı çalışmada test ettikleri birçok IoT cihazın UART portlarının açık olduğunu ve bu portlar üzerinden root erişime sahip olunabileceğini (Örn. Şekil 7) göstermişlerdir.



Şekil 7. Bir donanım üzerinde bulunan UART ve JTAG arabirimleri (Vasile, Oswald, Oswald, 2019).

IoT donanımları basit bir kablosuz sensör veya kontrol ekipmanı olabileceği gibi kritik bilgi taşıyan cihazlar da olabilir. Örneğin kartla ödeme alan POS cihazları internete bağlanan ve kullanıcının kritik bilgileriyle işlem yapan cihazlardır. Kritik bilgi saklayan veya uzak sunucuya ileten cihazların daha güvenli olması için ilgili veriler saldırganın eline geçse dahi anlamlı olmasın diye şifrelenmekte ve veri güvenliği sağlanmaktadır. Bu tip uygulamalar donanım güvenliği konusunda hem araştırmacıların hem de saldırganların ilgisini çekmiştir. Şifreleme işlemi gerçekleştiren donanım bileşeni şifreleme anahtarını veya şifre çözme anahtarını (asimetrik şifreleme kullanılıyorsa) içerdiğinden donanım üzerinden bu anahtarın ele geçirilmesi durumunda şifreli olan bölümlerin şifreleri kolayca açılabilir duruma gelmektedir. Önceki paragraflarda anlatılan cihaz yazılımına erişmeye yönelik saldırılar ile cihaz donanımı içeri-

sindeki yazılıma erişen saldırgan açık halde tutulan şifreleme anahtarlarına erişim sağlayabilir. Bu çoğu durumda üretici tarafından gizlenen bir veri olduğu için cihaz yazılımına erişilerek şifreleme anahtarı elde edilemediği durumda mikrodenetleyicinin veya mikroişlemcinin doğrudan kendisi gözlem altına alınarak şifreleme konusunda bir saldırı yapılabilir. Bu tip saldırılara Yan Kanal Saldırıları adı verilmektedir. Yan Kanal Saldırıları donanımın dışarıya sızdırdığı istemsiz çıkışları inceler. Cihaz donanımlarında bulunan mikrodenetleyiciler veya mikroişlemciler çalışma esnasında gerçekleştirdikleri işlemlerle alakalı dışarıya istemsiz veri sızdırabilmektedirler. Bu veri sızıntısı işlemcinin harcadığı güç, işlem süresi veya etrafa yaydığı radyasyon şeklinde olabilir. Yan Kanal Saldırıları bu sızıntıları elde edip anlamlı veri çıkarmaya odaklanır. (Sadhu, Yanambaka, Abdelgawad, 2022).

Mikrodenetleyicilerde veya mikroişlemcilerde gerçekleşen mantıksal işlemler arasında harcadıkları güç veya gerçekleşme süreleri gibi farklar oluşabilmektedir. Örneğin RSA (Rivest-Shamir-Adleman) şifreleme algoritmasını çalıştıran bir donanımda çarpma işlemi ile kare alma işlemi arasında belirgin bir fark oluşabilmektedir. (Bhunia & Tehranipoor, 2019). Donanım üzerinden yakalanan bu tipte sızıntıların türüne göre Yan Kanal Saldırıları; Güç Analizi, Elektromanyetik Analiz, Zamanlama Analizi şeklinde isimlendirilirler. Güç analizi saldırılarında mikrodenetleyicinin veya mikroişlemcinin harcadığı güç ölçülüp analiz edilerek yapılan şifreleme işlemi veya anahtar hakkında bilgi edinmek amaçlanırken elektromanyetik analiz saldırılarında da mikrodenetleyici veya mikroişlemcinin etrafa yaydığı elektromanyetik sinyaller yakalanarak anahtar hakkında bilgi edinmek amacıyla incelenir. Zamanlama analizi saldırılarında ise donanım üzerinde yürütülen işlemlerin gerçekleşme süreleri analiz edilerek sistem hakkında (şifreleme anahtarı, parola gibi) bilgi edinmek amaçlanır. (Hu ve diğerleri, 2020). Örneğin zamanlama tarafında açık bulunan parola korumalı bir cihazın parola kontrol yapısının işlem süresi incelenerek parola elde edilebilmektedir. Girilen her yanlış giriş sonrası ölçülen süre analiz edilerek farklı işlem süresine sahip giriş üzerinden bu bilgiye erişilebilir. Bu durum sadece parola koruması olmasının sistemde tam güvenlik sağlamadığı anlamına da gelir.

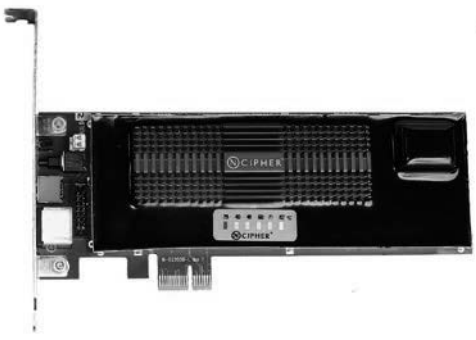
Donanım tarafında çıkacak bir açığın sistemlere büyük ölçüde zarar verebileceğine ilişkin en önemli örnek Meltdown ve Spectre açıklarıdır. Günümüzde kullanılan çoğu mikroişlemciyi hedef alan bu iki önemli açık, kullanıcının erişimi olmayan hafıza alanlarına erişimi mümkün kılarak gizli anahtar ve parola gibi hassas verilerin tehlikeye girmesine neden olabilmektedir. ("Meltdown' and 'Spectre' guidance", 2018). Gerçekleştirilen saldırılara bakıldığında ve gerçekleştirilebilecek saldırılar göz önüne alındığında bir IoT cihazı için

güvenliğin hem yazılım hem ağ hem de donanım tarafında sağlanması gerekir. Bütüncül bir koruma ile hem ürün üreticisine ait bilgiler hem de kullanıcıya ait bilgiler güven altına alınabilir.

Donanım tarafında kritik bilgilerin veya verilerin saldırganların eline geçmemesi adına üreticiler donanım tarafında farklı güvenlik tedbirleri alarak bu saldırıların gerçekleşmesini engellemeye veya saldırı olduğu durumda bile saldırganın önemli bilgileri ele geçirmesinin önüne geçmeye çalışmışlardır. Cihazın yazılımında güvenlik sıkılaştırmaları yapılarak donanım üzerinden veri sızıntısının engellenebileceği gibi bazı durumlarda ek donanımlar da kullanılarak güvenlik artırılabilmektedir. Bu konuda yapılan bazı güvenlik donanımlarına; Donanım Güvenlik Modülü (Hardware Security Module - HSM) ve Güvenilir Platform Modülü (Trusted Platform Module - TPM) örnek olarak verilebilir.

3.1 Donanım Güvenlik Modülü (Hardware Security Module - HSM)

Donanım Güvenlik Modülü, şifreleme anahtarları oluşturup verileri şifreleyen, şifrelediği verileri çözen ve dijital imzalar oluşturarak doğrulamasını yapan bir donanım aygıtıdır. Kimlik doğrulama ve tanımlama için güvenli bir yapı sağlayan bu modüller cihaz korumaları konusunda yaygın olarak kullanılmaktadır. Cihazın güvenliğini sağlamak için kriptografik işlemcisi ile donanım üzerinde farklı kriptografik algoritmaları gerçekleştirmektedir. Bu şekilde donanım üzerinde yapılabilecek kurcalamalara, veri manipülasyonlarına karşı koruma sağlamakta ve güçlü bir kimlik doğrulama mekanizması sunmaktadır. HSM'ler farklı büyüklük ve formlarda olabilmektedir. Şekil 8'de örnek bir HSM gösterilmiştir. (Mehrabi, Doche, Jolfaei, 2020; Cabrera-Gutiérrez ve diğerleri, 2022)

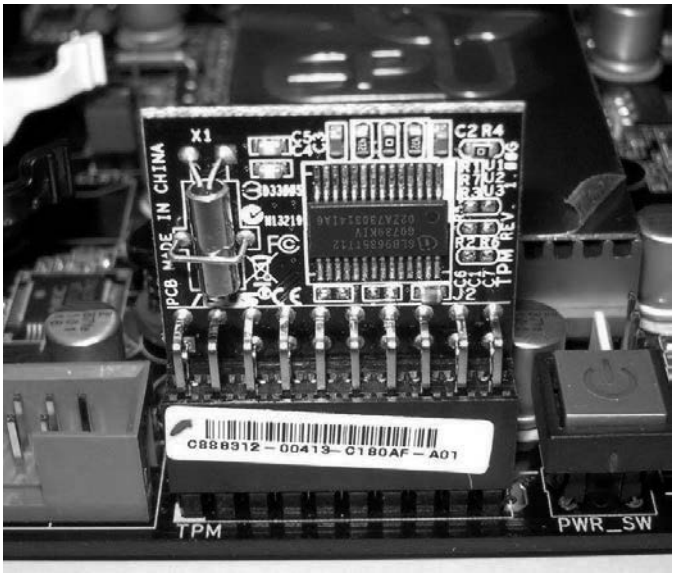


Şekil 8. nCipher nShield F3 Donanım Güvenlik Modülü ("Hardware security module," 2023)

3.2. Güvenilir Platform Modülü (Trusted Platform Module - TPM)

Trusted Computing Group (TCG) tarafından tanımlanan TPM'ler, HSM cihazlarının bir alt grubudur. Şifreli korunan verilerin (anahtarlar, sertifikalar, parolalar ve Platform Yapılandırma Kayıtları gibi TPM ile ilgili diğer veriler) güvenli bir şekilde depolanmasını ve Gerçek Rastgele Sayı Üreticileri (True Random Number Generators - TRNG), gizli/genel anahtar şifreleme, imza işlemlerini kullanarak TPM içinde anahtarların oluşturulmasını sağlayan bir donanım bileşenidir. TPM'ler yazılımın altına bir güvenlik katmanı eklemek için cihazı başlatmaktan sorumlu bir BIOS'u veya bir üretici yazılımını destekleyen bilgisayar sistemlerinde de kullanılır. Örneğin, bilgisayarın başlatılması sırasında üretici yazılımını, bağlı çevre birimleri, bellek ve diğer ilgili parametreleri kontrol eder. Kontrol ettiği parametreleri hashleyerek Platform Yapılandırma Kayıtlarında sakladığı değerlerle karşılaştırır. Bu karşılaştırma işleminin sonucunun doğruluğuna göre sistemin açılması veya engellenmesi sağlanır. Genel olarak bir TPM; geçici ve geçici olmayan bellekte anahtarların güvenli bir şekilde depolanması, sistemin mevcut donanım ve/veya yazılım durumunu saklamak için platform yapılandırma kayıtları (PCR'ler), kriptografik yardımcı işlemciler (örn. şifreleme/şifre çözme) ve bir gerçek rasgele sayı üreteci özelliklerine sahiptir. (Cabrera-Gutiérrez ve diğerleri, 2022; Hoeller, Toegl, 2018)

Günümüzde büyük bilgisayar üreticileri tarafından kişisel bilgisayarlara ve sunuculara da entegre edilmesi nedeniyle TPM'ler oldukça yaygındır. Microsoft Windows bilgisayarlarda TPM, Bitlocker sürücü şifrelemesi, diğer uygulamaların şifreleme işlemlerindeki anahtarların oluşturulması ve depolanması, işletim sistemi ve üretici yazılımlarının doğrulanmasını onaylamak için kullanılır. 2005 yılından beri bilgisayarların bir parçası haline gelen TPM'nin son sürümü olan TPM 2.0 2016 yılında yeni bilgisayarlar için standart haline gelmiştir. Şekil 9'da anakart üzerine montajlanmış bir TPM gösterilmektedir. ("TPM nedir?," 2023)



Şekil 9. Bir anakart üzerinde montajlanmış Güvenilir Platform Modülü ("Trusted Platform Module," 2023)

5. Nesnelerin İnterneti Güvenlik Regülasyon ve Standartları

IoT, genellikle çevreden bilgi toplayan, fiziksel dünya ile etkileşime giren ve ortak bir amaca ulaşmak için İnternet bağlantısını kullanan birbirine bağlı nesneler kavramı olarak kabul edilir (Damayanti, 2016). Nesnelerin İnterneti (IoT), tanımı konusunda fikir birliği yoktur. Sağlanan hizmetlere, amaçlara ve mimariye bağlı olarak tanım farklılık göstermektedir (Minerva ve diğerleri, 2015). Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE) (Logvinov ve diğerleri, 2016), Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) (Voas, 2016) ve Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) gibi çeşitli kuruluşlardan da farklı tanımlar bulunmaktadır (ETSI, 2010).

Günümüzde IoT cihazlarının sayısı sürekli olarak artmaktadır. Bu sistemler farklı alanlarda kullanılmakta ve giderek daha önemli hale gelmektedir. IoT cihazlarının yaygınlaşmasıyla birlikte potansiyel saldırılarda kullanılacak cihaz sayısı da artmaktadır (Pacheco ve diğerleri, 2017). Birbirine bağlı "nesne" lerin sayının 2025 yılına kadar 75 milyara çıkacağı tahmin ediliyor (Vega, 2020). Özel tüketiciler tarafından kullanılan bu cihazların çoğu, TV'ler, eğlence sistemleri, hoparlörler veya aydınlatma ve ısıtma sensörleri gibi Akıllı Ev cihazlarıdır (Liu, 2020). IoT cihazlarının yoğun bir şekilde benimsenmesinin bir sonucu olarak, yeni güvenlik endişeleri de ortaya çıkmaktadır. Geleneksel Bilgi

Teknolojisi (BT) güvenlik hedefleri, esas olarak sistemlerin ve mesajların gizliliğini, bütünlüğünü ve erişebilirliğini sağlamaktan oluşuyordu. Bununla birlikte, bu geleneksel önlemler, IoT cihazlarına uygulandığında, bilgi işlem güçlerinin genellikle uzun süreli işlemler için yetersiz olması nedeniyle bazı sınırlamalar gösterir. Ayrıca, IoT cihazlarının geniş ara bağlantıları nedeniyle ölçeklenebilirlik endişeleri de ortaya çıkmaktadır. IoT güvenliği, kritik öneme sahiptir: IoT için uygun geçerli güvenlik modelleri olmadan, kullanıcı güvenliği sağlanamaz. Bu nedenle öncelikle güven tesis edilmelidir (Sicari ve diğerleri, 2015).

Hükümetler, kurum ve kuruluşlar artan siber risklerini azaltmaya ve yalnızca tüketicileri değil, genel olarak toplumları ve ekonomileri korumaya çalışmakta ve buna bağlı olarak IoT ekosistemi için düzenleyici ortam hızla gelişmektedir. IoT ekosistemi genelinde gelişmiş güvenliği zorunlu ve sürdürülebilir kılmak için standart ve regülasyonlar oluşturulmakta ve yayınlanmaktadır. IoT Güvenlik Standartları, IoT cihazları, kullanıcı verileri ve ilgili sorunlar için güvenlik gereksinimlerini sağlamak üzere saygın ve geniş çapta kabul gören bir kuruluş tarafından yayınlanan IoT cihazlarının güvenliğine yönelik düzenleyici standartlardır. Dünya genelinde kabul görmüş tek bir IoT güvenlik standardı yoktur. Amerika, Avrupa kuruluş ve organizasyonlarının yayınlamış olduğu, dünya ülkelerinin temel IoT güvenlik standardı olarak kabul ettiği ve uyguladığı genel veya özel IoT alanlarında (örn: akıllı ev, akıllı araç vb.) standartlar mevcuttur. Bu bölümde, bu standartların, regülasyonların veya düzenlemelerin en yaygın olanları anlatılmıştır.

5.1. ETSI EN 303 645

Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI), tüketiciye yönelik bir ağa bağlı IoT cihazları için 65 güvenlik hükmü belirler. Standart, tüketiciye yönelik IoT cihazlarının geliştirilmesi ve üretilmesinde yer alan kuruluşlar, yani satıcılar içindir. Bu nedenle, nispeten eksiksiz bir gereksinim seti sağlamayı amaçlamaktadır.

ETSI'de geçen ifadeler cihazları belirli bir teknoloji veya protokolle kısıtlamaktan kaçınmak istediğini açıkça ortaya koyacak şekildedir. Örneğin, parolalarla ilgili yayınlanmış bir gereklilik, aygıtların parolalara dayanmayan bir kimlik doğrulama mekanizması kullanmasını engelleyebilir. Bu nedenle EN 303 645, "şifre" yerine "doğrulama değeri" terimini kullanır. Ne yazık ki, bazı durumlarda bu, hükümleri yeterince spesifik kılmamaktadır. Örneğin, aşağıdaki hükümde, hangi kriptografik algoritmanın kullanılması gerektiğine dair spesifik bir belirtme yapılmadığından yoruma açıktır:

Hüküm 5.1-3 Bir cihaza karşı kullanıcıların kimliğini doğrulamak için kullanılan kimlik doğrulama mekanizmalarında teknolojinin özelliklerine, riske ve kullanıma uygun en iyi kriptografi uygulaması kullanılacaktır.

Genel olarak, ETSI 303 645, satıcılara IoT cihazlarının güvenliğini sağlamak için önlemler sağlayan pratik, kullanılabilir bir kılavuzdur.

5.2. ENISA Baseline Security Recommendations for IoT (ENISA IoT için Temel Güvenlik Önerileri)

ENISA (Avrupa Birliği Siber Güvenlik Ajansı), üç ana kategoride önlemler sağlar:

- Politikalar,
- Organizasyonel, İnsan ve Süreç ölçütleri
- Teknik önlemler

Politikalarla ilgili önlemler, satıcıdaki geliştirme sürecini hedefler. Organizasyonel, Kişiler ve Süreç ölçümleri, satıcı ile tüketici arasındaki etkileşimi hedefler ve örneğin güvenlik açığı ifşasını kapsar. Son olarak, teknik önlemler, IoT cihazının nasıl davranması gerektiğine dair en somut önlemleri sağlar.

ENISA belgesinde tek bir nokta olarak yer alan önlemlerin birçoğu aslında birkaç gereklilikten oluşmaktadır. Örneğin:

GP-TM-18: Cihaz yazılımının/belleniminin, yapılandırmasının ve uygulamalarının Kablosuz (OTA) güncelleme yeteneğine sahip olduğundan, güncelleme sunucusunun güvenli olduğundan, güncelleme dosyasının güvenli bir bağlantı üzerinden iletildiğinden emin olun hassas veriler (örn. sabit kodlanmış kimlik bilgileri) içermediğini, yetkili bir güven kuruluşu tarafından imzalandığını ve kabul edilen şifreleme yöntemleri kullanılarak şifrelendiğini ve güncelleme paketinin dijital imzasının, imza sertifikasının ve imzalama sertifikası zincirinin, yetkili kişi tarafından doğrulanmış olduğunu güncelleme işlemi başlamadan önce emin olunuz.

Bu tek önlem en az sekiz gereksinimden oluşur. Bu da sınıflandırmayı ve değerlendirmeyi zorlaştırır. ENISA önlemleri, cihazların güvenliğinin nasıl sağlanacağı hakkında bilgi sağlamayı amaçlamaktadır. Çeşitli önlemler, cihazın belirli bir bölümünün güvenli olması gerektiğini belirtir. Örneğin:

GP-TM-35: Şifreleme anahtarları güvenli bir şekilde yönetilmelidir.

Bir cihazın güvenli olabilmesi için tüm alt bileşenlerinin güvenli olması gerektiği açıktır. Ancak, güvenli bileşenlerin nasıl geliştirileceğini bilmeyen satıcılar için, bir şeyin güvenli olması gerektiğini belirtmek yetersiz olabilir. Test edenler için, hangi düzeyde güvenlik talep edildiği veya sistemin ne tür bir saldırıya karşı güvenli olması gerektiği bile belirsiz olabilir. Bu önlemlerin çoğu yeterince spesifik olmadığı için çıkarılmıştır.

5.3. IoT Security Compliance Framework

IoT Güvenlik Vakfı, 233 gereksinimden oluşan IoT Güvenlik Uyumluluk Çerçevesini yayımlamıştır. Gereksinimler zorunlu veya tavsiye niteliğindedir ve güvenliği ihlal edilmiş bir aygıtın etkisine bağlı olarak belirli aygıt sınıfları için geçerlidir. Bir saldırının nispeten küçük etkilere neden olacağı cihazlar, Sınıf 0 olarak belirtilir ve bu tür cihazlar için daha az güvenlik önlemi uygulanır. Hassas verileri işleyen cihazlar, Sınıf 3 olarak belirtilir ve bunlar için çoğu güvenlik önlemi uygulanır. Pek çok cihaz hassas verileri bir şekilde işlediğinden, bu çerçevenin getirdiği güvenlik gereksinimleri oldukça katıdır. Çerçeve geniş bir kapsama sahiptir ve mobil uygulamalar, bulut hizmetleri, tedarik zinciri ve üretim süreci için güvenlik gereksinimlerini içerir.

5.4. OWASP ISVS

OWASP Nesnelerin İnterneti Güvenlik Doğrulama Standardı (ISVS), Nesnelerin İnterneti (IoT) uygulamaları için güvenlik gereksinimleri sağlar. Web uygulamaları ve web hizmetleri için güvenlik kontrollerinin doğrulanması için popülaritesi artan bir standart olan Uygulama Güvenliği Doğrulama Standardı'na (ASVS) göre modellenmiştir.

ISVS ağırlıklı olarak bir IoT uygulamasının teknik güvenlik yönlerini hedefleyen 34 doğrulama gereksiniminin bir listesinden oluşur. Mevcut haliyle, ASVS'nin bir parçası olarak ISVS, derinliği artan üç güvence düzeyi tanımlar. Bu, temelde bir IoT uygulamasının daha yüksek bir güvenlik düzeyi seçildiğinde daha fazla gereksinime göre doğrulandığı anlamına gelir. Seviye 1 gereksinimleri, minimum olarak kabul edilebilir. Bu seviyedeki gereksinimlerin doğrulanması genellikle kolaydır. Seviye 2, günümüzün güvenlik risklerinin çoğuna karşı savunma sağlayan gereksinimler sunar. Seviye 3, yüksek düzeyde güvence gerektiren ve önemli güvenlik doğrulaması gerektiren uygulamalar için ayrılmıştır. Bu tür uygulamalara örnek olarak askeri, sağlık, finansal veya kritik altyapılar verilebilir.

6. Sonuç ve Öneriler

Nesnelerin İnterneti sağladığı ürün ve hizmetlerle insan hayatını kolaylaştıran ve dijitalleştiren teknolojik atılımı ifade etmektedir. Ancak Nesnelerin İnterneti geliştiği zaman itibariyle siber tehditlerin ve siber saldırıların ve siber vandalizmin hızla arttığı ve yayıldığı bir döneme denk gelmiştir. Bireysel ve topluluk olarak gelişen siber saldırganlar artık ülkelerin desteklediği kalıcı tehdit aktörlerine dönüştüğü bir dönemde hızlı ve ucuz üretim amacıyla üretilmiş akıllı ürünler birçok siber tehditle karşı karşıyadır. Bu çalışma kapsamında Nesnelerin İnterneti kavramı ve altyapısı ve siber güvenliği hakkında temel bilgiler verilmiştir. Nesnelerin İnterneti cihazlarının güvenliği yazılım donanım, haberleşme ve yasal regülasyonlar için değerlendirilmiştir. IoT cihazları siber saldırılarına karşı korunmaya çalışan güvenlik önlemlerini ve protokolleri incelenmiştir. IoT cihazları için güvenlik çözümlerinden bazılarını açıklanmış ve bu ortam için etkili güvenlik önlemlerini tartışılmıştır.

Yapılan bu çalışma çerçevesinde görüldüğü üzere IoT cihazlarının güvenliği yalnızca cihazın yazılımın, haberleşmenin veya donanımının güvenliğini sağlamak ile mümkün olmadığını göstermektedir. Geliştirilen güvenli yazılım framework'leri, olası riskleri uzaktan kontrol ve güncelleme mekanizmaları, güvenli haberleşme protokolleri, güvenli donanım donanımlar güvenlik için temel seviye olarak belirlenmelidir. Güvenlik IoT ekosisteminde bulunan tüm düğümlerin güvenlik ve gizlilik ilkelerine uygun olarak üretilmesi ve hizmet vermesiyle mümkün olduğu görülmüştür. Teknoloji gelişimi geri dönülemez bir şekilde dijitalleşmeyi desteklediği sürece IoT cihazları hayatın bir parçası olmaya devam edecektir. Ancak mevcut tehditlerden çıkarılan dersler, hükümetlerin çıkardıkları regülasyonlar ve organizasyonların çıkarmış oldukları standartlar siber risklerin yönetilebildiği bir dijital dünya için ümit vermektedir.

Kaynaklar

Anand, N., Joseph, G., Oommen, S. S., & Dhanabal, R. (2014, January). Design and implementation of a high speed Serial Peripheral Interface. In 2014 International Conference on Advances in Electrical Engineering (ICAEE) (pp. 1-3). IEEE.

Al-Turjman, F., & Malekloo, A. (2019). Smart parking in IoT-enabled cities: A survey. *Sustainable Cities and Society*, *49*, 101608.

Andreão, R. V., Athayde, M., Boudy, J., Aguilar, P., de Araujo, I., & Andrade, R. (2018). Raspcare: a telemedicine platform for the treatment and monitoring of patients with chronic diseases. In *Assistive Technologies in Smart Cities*. London, UK: IntechOpen.

Başer, M., Güven, E. Y., & Aydın, M. A. (2021, September). SSH and Telnet Protocols Attack Analysis Using Honeypot Technique: Analysis of SSH AND TELNET Honeypot. In 2021 6th International Conference on Computer Science and Engineering (UBMK) (pp. 806-811). IEEE.

Bormann, C., Castellani, A. P., & Shelby, Z. (2012). Coap: An application protocol for billions of tiny internet nodes. *IEEE Internet Computing*, *16*(2), 62-67.

Cabrera-Gutiérrez, A. J., Castillo, E., Escobar-Molero, A., Álvarez-Bermejo, J. A., Morales, D. P., & Parrilla, L. (2022). Integration of Hardware Security Modules and Permissioned Blockchain in Industrial IoT Networks. IEEE Access, 10, 114331-114345.

Damayanti, N. Internet of Things: a vision, architectural elements, and future directions. *Internet of Things: a vision, architectural elements, and future directions*.

Dutta, J., Chowdhury, C., Roy, S., Middya, A. I., & Gazi, F. (2017, January). Towards smart city: sensing air quality in city based on opportunistic crowd-sensing. In *Proceedings of the 18th international conference on distributed computing and networking* (pp. 1-6).

Dhaker, P. (2018, Eylül). Introduction to SPI Interface. Analog Dialog. https://www.analog.com/en/analog-dialogue/articles/introduction-to-spi-interface.html, Erişim 4 Nisan 2023.

ETSI,2010 Machine-to-Machine communications (M2M) (2010), pp. 1-34

Gallagher, S. (2020, November 18). Introduction to JTAG and the Test Access Port (TAP). All About Circuits. https://www.allaboutcircuits.com/technical-articles/introduction-to-jtag-test-access-port-tap/, Erişim 4 Nisan 2023.

Hardware security module. (2023, 29 Mart). Wikipedia. https://en.wikipedia.org/wiki/Hardware_security_module, Erişim 5 Nisan 2023.

Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks*, *148*, 283-294.

Haverkort, B. R., & Zimmermann, A. (2017). Smart industry: How ICT will change the game!. *IEEE internet computing*, *21*(1), 8-10.

Hoeller, A., & Toegl, R. (2018, April). Trusted platform modules in cyber-physical systems: On the interference between security and dependability. In 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 136-144). IEEE.

Keane, P. A., & Topol, E. J. (2018). With an eye to AI and autonomous diagnosis. *NPJ Digital Medicine*, *1*(1), 40.

Koca M., Avcı İ., (2023). "Siber Güvenlik Yönetim Sistemi", Mühendislik Alanında Uluslararası Araştırmalar Sayfalar, Platanus Publishing, 163-183, ISBN: 978-625-6971-54-7, doi: 10.5281/zenodo.7744333.

Koubaa, A., Aldawood, A., Saeed, B., Hadid, A., Ahmed, M., Saad, A., ... & Alkanhal, M. (2020). Smart Palm: An IoT framework for red palm weevil early detection. *Agronomy*, *10*(7), 987.

Li, J., Yang, L., Feng, X., Xing, Y., Chen, Z., & Wan, P. (2022, December). UART Controller with FIFO Buffer Function Based on APB Bus. In 2022 IEEE 16th International Conference on Anti-counterfeiting, Security, and Identification (ASID) (pp. 1-4). IEEE.

Liu S., Internet of things (IoT) - Statistics & facts, (2020), Accessed: 2020-11-09. [Online]. Available: https://www.statista.com/topics/2637/internet-of-things/

Logvinov, O., Kraemer, B., Adams, C., Heiles, J., Stuebing, G., Nielsen, M., & Mancuso, B. (2016). Standard for an Architectural Framework for the Internet of Things (IOT) IEEE p2413. *IEEE-P2413 Working Group. Technical Report*.

Grau, A. (2015). Can you trust your fridge?. IEEE Spectrum, 52(3), 50-56.

Koley, S., & Ghosal, P. (2015, August). Addressing hardware security challenges in internet of things: Recent trends and possible solutions. In 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom) (pp. 517-520). IEEE.

Bhunia, S., & Tehranipoor, M. (2019). Introduction to hardware security. In Hardware Security (pp. 1-20). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-812477-2.00006-X.

Jin, Y. (2015). Introduction to hardware security. Electronics, 4(4), 763-784.

Skorobogatov, S. (2014, February 3). Tamper resistance and hardware security. Retrieved April 3, 2023, from https://www.cl.cam.ac.uk/~sps32/PartII_040213.pdf

IoT Attack Surface Areas Project. OWASP Internet of Things Project. (2019, November 1). Retrieved April 4, 2023, from https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Attack_Surface_Areas

Vasile, S., Oswald, D., & Oswald, T. (2019). Breaking all the things—A systematic survey of firmware extraction techniques for IoT devices. In Smart Card Research and Advanced Applications: 17th International Conference, CARDIS 2018, Montpellier, France, November 12–14, 2018, Revised Selected Papers 17 (pp. 171-185). Springer International Publishing.

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and Solutions Survey. Sensors, 22(19), 7433.

Hu, W., Chang, C. H., Sengupta, A., Bhunia, S., Kastner, R., & Li, H. (2020). An overview of hardware security and trust: Threats, countermeasures, and design tools. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 40(6), 1010-1038.

Meltdown' and 'Spectre' guidance. (2018, February 13). National Cyber Security Centre. https://www.ncsc.gov.uk/guidance/meltdown-and-spectre-guidance, Erişim 6 Nisan 2023.

Mehrabi, M. A., Doche, C., & Jolfaei, A. (2020). Elliptic curve cryptography point multiplication core for hardware security module. IEEE Transactions on Computers, 69(11), 1707-1718.

Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). *IEEE Internet Initiative*, *1*(1), 1-86.

Pardini, K., Rodrigues, J. J., Kozlov, S. A., Kumar, N., & Furtado, V. (2019). IoT-based solid waste management solutions: a survey. *Journal of Sensor and Actuator Networks*, *8*(1), 5.

Pacheco, J., Ibarra, D., Vijay, A., & Hariri, S. (2017, October). IoT security framework for smart water system. In *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1285-1292). IEEE.

Peňa, E., & Legaspi, M. G. (2020, Aralık). UART: A Hardware Communication Protocol Understanding Universal Asynchronous Receiver/Transmitter. AnalogDialog. https://www.analog.com/en/analog-dialogue/articles/uart-a-hardware-communication-protocol.html, Erişim 4 Nisan 2023.

Rajput, P. H. N., & Maniatakos, M. (2019, July). Jtag: A multifaceted tool for cyber security. In 2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS) (pp. 155-158). IEEE.

Rojek, I., & Studzinski, J. (2019). Detection and localization of water leaks in water nets supported by an ICT system with artificial intelligence methods as a way forward for smart cities. *Sustainability*, *11*(2), 518.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, 146-164.

Trusted Platform Module. (2023, 3 Nisan). Wikipedia. https://en.wikipedia.org/wiki/Trusted_Platform_Module, Erişim 5 Nisan 2023.

TPM nedir?. (n.d.). Microsoft Destek. https://support.microsoft.com/tr-tr/topic/tpm-nedir-705f241d-025d-4470-80c5-4feeb24fa1ee, Erişim 5 Nisan 2023.

Trakadas, P., Simoens, P., Gkonis, P., Sarakis, L., Angelopoulos, A., Ramallo-González, A. P., ... & Karkazis, P. (2020). An artificial intelligence-based collaboration approach in industrial iot manufacturing: Key concepts, architectural extensions and potential applications. *Sensors*, *20*(19), 5480.

O'Grady, M. J., Langton, D., & O'Hare, G. M. P. (2019). Edge computing: A tractable model for smart agriculture?. *Artificial Intelligence in Agriculture*, *3*, 42-51.

Wang, Y., Ram, S., Currim, F., Dantas, E., & Sabóia, L. A. (2016, September). A big data approach for smart transportation management on bus network. In *2016 IEEE international smart cities conference (ISC2)* (pp. 1-6). IEEE.

Vega, M. (2020). 's Internet of Things Statistics, Facts & Predictions.

Voas, J. (2016). Networks of 'things'. *NIST Special Publication*, *800*(183), 800-183.