Bursa Uludağ Üniversitesi Mühendislik Fakültesi Dergisi, Cilt 27, Sayı 2, 2022 ARAŞTIRMA

DOI: 10.17482/uumfd.1068960

NESNELERİN İNTERNETİ GÜVENLİĞİ: EV AĞI GÜVENLİK İNCELEMESİ VE DEĞERLENDİRMESİ

Murat Osman KANDIR [*]
Esra Nergis YOLAÇAN [**]
Şahin IŞIK [**]

Alınma: 06.02.2022; düzeltme: 24.06.2022; kabul: 10.08.2022

Öz: Evrensel Tak ve Çalıştır (Universal Plug and Play, UPnP) ve IoT iletişim protokolleri sayesinde cihazların birbirleriyle ve ağ ile bağlantıları çok daha kolay ve hızlı yapılabildiğinden ev ağındaki bağlantı sayısı da artmıştır. Akıllı televizyonlar ve temizlik robotları gibi akıllı cihazlar, yaşam konforumuzu artırmakta ve ev ağı üzerinden tüm dünyaya bağlantı sağlar hale gelmiştir. Bu nedenle, ev ağının internete bağlı olduğu gerçeği ağdaki akıllı cihazların güvenlik durumlarının sorgulanması ihtiyacını ortaya çıkarmıştır. Bu çalışmada, ev ağı içerisindeki popüler cihazların güvenlik seviyelerinin analiz edilmesi sağlanmıştır. Ev Ağı içerisinde UPnP zafiyetine sahip cihazların varlığını tespit etmek için Python yazılım dili kullanılarak uygulama geliştirilmiştir. Geliştirilen uygulama kullanılarak ev ağı içerisindeki 15 adet cihazdan 3 adet cihazın UPnP açıklığına sahip olduğu görülmüştür. Bir senaryo içerisinde UpNP açıklığı kullanılarak saldırı uygulaması gerçekleştirilmiştir. Bu çalışma ile evdeki ağ ve iletişim yöntemleri güvenliğinin yanında her bir IoT cihazın güvenliğinin sağlanmasının gerekliliği ayrıntılı olarak sunulmuştur.

Anahtar Kelimeler: Evrensel Tak ve Çalıştır, UPnP, IoT, Güvenlik Açığı Tarama, Ağ Güvenliği, Nesnelerin İnterneti

Security of the Internet of Things: Home Network Security Review and Evaluation

Abstract: As a result of Universal Plug-and-Play (UPnP) and Internet of Things (IoT) communication protocols, the number of connections in home networks has expanded, as devices can be connected to each other and to the network more easily and quickly. Over the home network, smart devices such as smart televisions and cleaning robots boost our living comfort and connect us to the entire globe. The fact that the home network is connected to the Internet has therefore revealed the necessity to question the security status of networked smart devices. This study provides an analysis of the security levels of popular home network devices. Using the Python programming language, a program has been developed to detect the presence of UPnP-vulnerable devices on a home network. Using the built application, it was discovered that three out of fifteen network devices support UPnP. In a scenario, an attack was built via the UpNP vulnerability. In this study, the necessity of guaranteeing the security of each IoT device, as well as the security of the home's network and communication techniques, is discussed in depth.

Keywords: Universal Plug and Play, UPnP, IoT, Vulnerability Scan, Network Security, Internet of Things

[*] Eskişehir Osmangazi Üniversitesi Fen Bilimleri Enstitüsü 26040, Odunpazarı, Eskişehir, Türkiye
İletişim Yazarı: Murat Osman KANDIR (503020211007@ogrenci.ogu.edu.tr)

1. GİRİŞ

Kendi IP adresleri ve sensörleri olan cihazların, birbirleriyle bir ağ vasıtasıyla haberleşmeleri, sahip oldukları bilgileri paylaşmaları ve bu bilgileri analiz ederek birbirleriyle etkileşim içerisinde oldukları ortam Nesnelerin interneti olarak tanımlanmaktadır. Bu ortamda bulunan akıllı cihazlar ise birer nesnedir. Ev kilit ve güvenlik sitemleri, aydınlatma ve görüntüleme sistemleri, ısıtma, havalandırma ve iklimlendirme sistemleri, duman ve zararlı gaz ölçüm sistemleri, akıllı mutfak ve pişirme sistemleri gibi sistemleri IoT içerisinde tanımlamak mümkündür. Ev içerisinde mevcut olan IoT cihazlarını düşünürsek; buzdolabı, çamaşır makinesi, bulaşık makinesi, fırın, perde ve panjurlar, ev temizlik robotları ilk aklımıza gelenlerdir.

Günlük olarak ev içerisinde kullanılan IoT cihazları küçük ve zararsız olarak gözükmektedir. IoT cihazları, asıl amaçları olan işlevlerinin yanında ek olarak internete erişim yetenekleri kazandırılan klasik cihazlardır. Bu cihazların üretim amaçları klasik iş ihtiyaçlarıdır. Birçok klasik cihaz üzerine bir ağ kartı eklenerek internet üzerinden kontrol edilebilir ve iletişim kurulabilir duruma gelmektedir. Bu cihazlar için güvenlik kavramı hem fiziksel cihaz güvenliğini hem de ağ güvenliğini kapsamaktadır. Çalışmanın ana amacı, ev ağına sızacak bir saldırgan tarafından IoT cihazlarına yapılacak saldırılara karşı güvenlik durumunun sorgulanmasıdır.

Ev ağına bağlı tüm bilişim cihazlarının (akıllı televizyon, ev temizlik robotu, oyun konsolu, akıllı mutfak aletleri, kablosuz tekrarlayıcı, ip kamera, bebek izleme kamerası, masaüstü ve dizüstü bilgisayarlar, tablet ve akıllı telefonlar, vb.) ağ içerisinde kurdukları iletişimlerinin güvenli olması ve muhtemel ağ içerisine sızmış bir siber saldırgan tarafından istismar edilmelerine izin vermemek için gerekli ortamın yaratılmasına yönelik zayıflık taramalarının yapılması gerekmektedir. Bu cihazların büyük bir çoğunluğu özel güvenlik yazılımlarını çalıştırmaya uygun değildir. Son günlerde hızla kullanımı yaygınlaşan ev temizlik robotlarını örnek olarak incelenirse; asıl amacı ev zemininin süpürülmesi ve silinmesi hedefli üretilmiş olması nedeniyle iş odaklı çalışmaktadırlar. Bu cihazlar ev ağı içerisinde bir ip numarasına sahip olarak iletişim kurmakta ve akıllı cihazlardaki uygulamalar ile yönetilmektedirler. Eğer siber saldırganlar tarafından ele geçirilirlerse ev içerisindeki tüm eşya yerleşimini ortaya çıkartan ev haritası bilgisi çalınabilecektir.

Özellikle klasik cihazların ağ kartı eklenerek ev ağına dahil edildiği durumlarda yazılım güvenliği ilk amaç olmamaktadır. Nesnelerin İnterneti kapsamında ağa dahil olmuş akıllı cihazların farklı üreticiler tarafından üretilmiş olmaları ve farklı özelliklere sahip olmaları nedeniyle bir standartları bulunmamaktadır. Bu yüzden kablosuz ağlara bağlanmalarında kullandıkları iletişim yöntemlerinde yazılımdan veya donanımdan kaynaklanan açıklar bulunabilmektedir. Türkçe karşılığı "donanım yazılımı" olan firmware'lerin yeterli güncellenmemesi de siber saldırılara karşı hassasiyet yaratmaktadır. Literatür araştırması yapıldığında genelde yeni geliştirilen IoT cihazlarına donanım tabanlı siber saldırılar ile ilgili testlerin gerçekleştirildiği görülmektedir. Bu tür siber saldırılar için cihaza fiziksel erişim sağlama zorunluluğu nedeniyle kolayca yapılabilecek siber saldırılar olmayacağı açıktır. Özellikle süratle gelişen ve büyüyen internet üzerinden yönetilen ve erişilen IoT cihazlarının ağ üzerinden istismar edilmeleri daha olası gözüktüğünden çalışma bu yönde gerçekleştirilmiştir.

Ağ güvenliği söz konusu olduğunda, ağda bir cihazın siber saldırgan tarafından ele geçirilmesi ağ güvenliğinin tamamını tehlikeye atacaktır. Ele geçirilen cihaz, tüm ağın güvenliği için sorun yaratacaktır. Bu yüzden ağa bağlı her cihazın güvenliği önem taşımaktadır. Ağa bağlı cihazların farklı üreticiler tarafından üretilmiş olması ve hem donanım hem de yazılım olarak standartlarının henüz oluşmaması güvenliklerinin sağlanması kapsamında zorlukları beraberinde

getirmektedir. Ev ağında kullanılan tüm cihazların muhtemel siber saldırılara karşı açıklık taramalarını yapmak için güvenilir, açık kaynak kodlu, modüler ve geliştirilmeye açık bir uygulama ihtiyacı bulunmaktadır. Kablosuz olarak bağlandıkları ev ağında sahip oldukları ip numaraları üzerinden açıklık taramalarının yapılıp, açık haberleşme portlarının tespit edilmesi sonrasında, bu haberleşme portlarının istismara uygunluk durumlarının incelenebileceği bir uygulama ihtiyacı görülmektedir.

Ev ağı içerisinde ip numarasına sahip tüm cihazlar tespit edilip bu cihazlara farklı bir erişim olup olmadığı kontrol edilmektedir. Ev ağına erişim sağlayan tüm cihazların açık haberleşme portlarını tespit ettikten sonra bu haberleşme portlarının zayıflık kontrollerini yapılmaktadır. IoT cihazlarına özel haberleşme portlarının taramaları yapılabilmektedir. Ev ağında mevcut IoT cihazlarına karşı sızma testleri oluşturulmuştur. Bugüne kadar ağ için zayıflık tarama testleri yapabilecek yazılımların geliştirilmiş olduğu görülmektedir. Özgün hedef geliştirilmeye ve yeni özellikler eklenmeye açık IoT cihazlarına özel sızma testleri yapabilen bir zayıflık arama modülüne sahip bir uygulama gerçekleştirilmiştir.

Ev ağındaki cihazların kontrolü için piyasadaki mevcut uygulamalar zararlı yazılım içerme ihtimalleri nedeniyle kullanılmaktan kaçınılmaktadır. Gerçekleştirilen uygulama test yazılımı ile ev ağındaki iletişimi ve iletişim içerisindeki paketleri dinleme ve sonrasında analiz ederek ağ içerisindeki cihazlar tespit edilebilmektedir. Bu cihazların arasında ev ağına sızmış yabancı bir cihaz olup olmadığının kontrolü yapılabilmektedir. Ev ağına bağlı tüm cihazların hangi portlarının açık olduğunun tespiti yapılmaktadır. Tespit edilen açık portlarda çalışan yazılımların sürümleri ve güncellik durumları kontrol edilebilmektedir. Güvenlik şirketleri tarafından yayımlanan "Bilişim cihazlarının zayıf noktalarını istismar etmek için oluşturulan kötücül kodlar" (exploit) ile ilgili bilgilerden de faydalanılarak belirli protokoller ile ilgili zayıflık testi yapılabilmektedir.

2. LİTERATÜR TARAMASI

IOT cihazlarının güvenlik problemleri, endüstriyel otomasyon sistemlerinin geniş alan ağına irtibatları sağlanınca dikkat çekmeye başlamıştır. SCADA (Supervisory Control And Data Acquisition) sistemler olarak da adlandırılan ve uzaktan komuta kontrol edilebilen sistemler olan IoT cihazlarının endüstriyel alanda kullanımları güvenlik sorunlarını da beraberinde getirmiştir. Endüstriyel IoT alanında yapılan çalışmada Antrobus ve diğ. (2019) IIoT (Industrial Internet of Thing), cihazlarının haberleşme protokolleri incelenerek muhtemel haberleşme protokollerine yapılabilecek saldırıların tespit edilmesi için bir uygulama geliştirilmiştir. PIVoT (Producing awareness of the Industrial-Vulnerable of Things) olarak adlandırılan bu uygulama endüstriyel IoT cihazlarının bağlı olduğu ağı tarayarak açıklık tespiti yapmaktadır. Yazılımın başarısı farklı bir güvenlik yazılımı ile karşılaştırılmıştır.

Yu ve diğ. (2020) endüstri alanından ev ortamına geçen IoT cihazlarının önce yapısal özelliklerini incelemişlerdir. Yapısal mimarilerini inceledikten sonra güvenlik sorunlarına odaklanarak bu alanda yapılan çalışmaları değerlendirmişlerdir. Değerlendirmelerini güvenlik analiz araçları, tarama, tespit ve zayıflık giderme alanlarına ayırmak suretiyle yapmışlardır.

Filipinler'de yapılan çalışmada Intal Tayag ve diğ. (2020) bulut tabanlı IoT cihazı olan IP kameranın güvenlik ihtiyaçlarına dikkat çekilmiştir. Teknoloji marketlerde satılan bir IP kameranın güvenlik açıkları incelenmiştir. IP tarama ve Port tarama uygulamaları ile açıklık taraması yapılmış ve cihaza yetkisiz erişim sağlanmıştır.

Ev ağı içerisinde süratle kullanımı yaygınlaşan robot süpürgelerin güvenilirliklerinin sorgulandığı çalışmada Olsson ve Larsson Forsberg (2019) açıklık arama uygulamaları ve sızma

testlerini barındıran Kali Linux sürümü kullanılarak Çin üretimi bir robot süpürge çeşitli testlere tabi tutulmuştur. Yapılan sızma testlerinde başarıya ulaşılarak robot süpürgeye yetkisiz erişim sağlanmıştır. Bu tür saldırılara karşı yapılması gereken güncellemelerin gerekliliği konusu tartışmaya açılmıştır. Akıllı televizyonlar, internet kameraları ve yazıcıların güvenlik açıkları üzerine yapılan çalışmada Williams ve diğ. (2017) bu IoT cihazları Sızma Testi yapan bir yazılım ile test edilmiş ve sonuçları değerlendirilmiştir. Ortaya çıkan zayıflıklar orta, yüksek ve en yüksek olarak sınıflandırılmıştır. Hemen hemen her evde kullanılan bu IoT cihazlarının güvenlik olarak geliştirilmeye ihtiyaçları olduğu sonucuna varılmıştır.

Upadhyay ve diğ. (2019) IoT cihazlarının donanım ve yazılım kısıtlarından kaynaklanan güvenlik sorunlarını incelemiş ve bu alanda kullanılabilecek siber saldırı çeşitlerini değerlendirmiştir. Siber saldırı türlerinin incelendiği çalışmada bu saldırılara karşı IoT cihazlarının durumları da ele alınmıştır. Bu alanda genel bir yaklaşıma sahip olan çalışma IoT güvenlik ihtiyaçlarına karşı kısıtlı yazılım ve donanım imkanlarına odaklanmıştır.

IoT cihazları ile yapılan farklı bir çalışma Mehic ve diğ. (2019) özelliği gösteren bu makalede; Xiaomi Akıllı Ev Sistemi 30 gün boyunca izlenmiş ve sonuçlar analiz edilmiştir. Akıllı ev sistemindeki duyargaların ağ trafikleri kaydedilmiş ve ağı kullanım miktarları analiz edilmiştir. Ayrıca IoT cihazlarının güvenlik açıklarını tespit maksatlı yapacakları bir sonraki çalışmalarına temel teşkil edecek şekilde veri toplamışlardır.

Patel ve Shah (2020) yaptığı çalışmada IoT cihazları ile ilgili bir simülasyon ortamı yaratmış ve bu ortamda çeşitli simülasyon uygulamaları ile cihazlar arasındaki ağ trafiğini dinleyerek protokolleri incelemiştir. Ağ trafiğini dinleyerek ücretsiz ve ticari yazılımlar kullanarak paketleri incelemiş ve haberleşme protokollerindeki güvenlik zafiyetlerini incelemişlerdir.

Diğer bir çalışmada Meidan ve diğ. (2020) IoT cihazlarının, saldırganların hedefi olarak değil saldırganların aracı olarak kullanılması incelenmiştir. Çalışmada akıllı lambalardan internet kameralarına birçok cihaz incelenmiştir. Siber saldırganlar tarafından ele geçirilip belli hedeflere Dağıtık Hizmet Engelleme Saldırısı (Distributed Denial-of-Service (DDoS)) yapan bir zombi ağının parçası olarak kullanılan cihazların bu tür saldırılara karşı içerdikleri zafiyetler incelenerek alınabilecek önlemler değerlendirilmiştir. Deepak (2020) ise DDoS saldırılarının hedefi olma konusunda IoT cihazlarını incelemiştir. Ücretsiz bir ağ güvenlik tarama uygulaması olan Nmap'i kullanarak ağı tarayıp açıklık bulunan IoT cihazlarının uçtan zayıflık analizini yapan bir uygulama geliştiren Geeta Yadav ve arkadaşları uygulamayı IoT-PEN Yadav ve diğ. (2020) olarak isimlendirmişlerdir. Saldırı tespit sistemlerinin yapay zekâ ile desteklenerek IoT cihazlarının mevcut olduğu ağlardaki uygulanmasını inceleyen çalışmada Malhotra ve diğ. (2021) çeşitli Makine Öğrenmesi algoritmaları karşılaştırılmıştır.

Norveç'te yapılan bir çalışmada Amro (2020) IoT cihazlarının zafiyet taraması alanında Sistematik Literatür Taraması yapılmıştır. Bir diğer çalışmada Huang ve diğ. (2021) yönlendiriciler IoT olarak değerlendirilmiş ve bu cihazlara yönelik Kablosuz Ağ Zafiyet taraması yapmak için bir uygulama geliştirilmiştir. Shodan isimli web üzerinden IoT cihazlarının açıklık taramasını yapan bir web sitesinin sağladığı bilgileri kullanarak IoT cihazlarının güvenliği üzerine yapılan çalışmada Raghuvanshi ve diğ. (2020) IoT cihazlarının %60'ının istismara açık olduğu görülmüştür. ZigBee, Bluetooth vb. kablosuz erişim modellerinin açıklıkları üzerinden IoT güvenliği konulu çalışmada McDaid ve diğ. (2021) saldırı çeşitleri tanımlanmış ve Radyo frekans aralığını tarayan bir cihaz kullanılarak IoT cihazlarının haberleşmesi takip edilmiştir. Raspberry Pi kartı ile oluşturulmuş IoT güvenlik

sistemi Shreenidhi ve diğ. (2021) bir internet kamerasına bağlanmış ve bu sisteme çeşitli siber saldırı yöntemleri uygulanarak saldırı tespit sisteminin bu saldırıları raporlaması sağlanmıştır.

IoT cihazlarının dahil olduğu ağlarda mevcut olan açıklıklar üzerine yapılan bir başka çalışmada Kayas ve diğ. (2020) sıkça kullanılan UPnP hizmetine odaklanılmış ve bu hizmet tarafından kullanılan protokollerin zafiyetleri incelenmiştir. Söz konusu çalışmada UPnP destekli cihazların maruz kaldıkları saldırılar ve saldırılara karşı alınabilecek önlemler değerlendirilmiştir.

IoT cihazlarının güvenlik problemleri üzerine birçok çalışma yapılmaktadır. IoT cihazlarının güvenlik problemlerine yönelik çalışmalar ilk endüstriyel alanda kullanılan cihazlara yönelik olarak yapıldığı görülmektedir. Daha sonrasında IoT cihazlarının ev ortamlarında kullanımları yaygınlaştıkça inceleme ve çalışmalar bu alanlara yönelmiştir. Bu çalışmaların bazılarında ücretsiz veya ticari güvenlik yazılımları kullanılmıştır. Hazır zayıflık tarama uygulamalarının tarama sonuçları üzerinden yapılan çalışmalarda saldırı tekniklerine odaklanılmıştır. Yapılan çalışmalarda kablosuz ağların sahip olduğu zayıflıkların yanında ev ağındaki cihazların yazılım ve donanım kısıtlarından kaynaklanan güvenlik açıklıkları incelenmiştir. Henüz yeni teknoloji olduğu değerlendirilen IoT cihazlarının güvenlik açısından geliştirilmeye muhtaç oldukları sonuçlarına varılmıştır. Özellikle farklı üreticiler tarafından üretilen ve farklı haberleşme protokolleri kullanan cihazların güvenlik standartlarını sağlamadıkları yapılan çoğu çalışmada varılan sonuçlar arasında belirtilmiştir.

Literatürde gerçekleştirilen çalışmalarda varılan ortak sonuç IoT cihazlarının bağlı oldukları ağda zayıflık yarattıklarıdır. Bu cihazların, siber saldırganlar tarafından ağa yetkisiz erişim sağlamak için kullanılabilme tehdidi altında oldukları görülmektedir. Bu nedenle zayıflıklarının önceden tespit edilip donanım ve yazılımlarında gerekli güncellemelerin ve iyileştirmelerin yapılması için zayıflık taramalarının yapılması gerekmektedir.

Özellikle siber saldırganlar tarafından ele geçirilerek hedef seçilen kurbanlara karşı yapılan saldırılarda kullanılan zombi ağların içerisine dahil edilen IoT cihazları olduğu görülmektedir. Bu kapsamda yapılan çalışmalarda genel olarak IoT cihazlarının kolay kullanım özelliklerinden kaynaklanan ve kolayca istismar edilmeye açık olan bazı protokollerin kullanıldığı görülmektedir.

3. METODOLOJİ

Ev ağında bulunan IoT cihazların güvenliğinin sağlanması ve güvenlik açıklarının tespitinin yapılması için öncelikle IoT cihazları için risk yaratan faktörler incelenmiştir. Geçmişte yapılan çalışmalar dikkate alındığında IoT cihazlarının istismar edilme riskleri kadar olası bir siber saldırıda saldırgan tarafından kullanılabilme riskine de sahip oldukları görülmüştür. Bu nedenle, çalışmada UPnP açıklıklarını kullanan saldırılar üzerine odaklanılmıştır.

3.1. UPnP Açıklıklarını Kullanan Saldırılar

Simple Service Discovery Protokolü (SSDP), Evrensel Tak ve Çalıştır (UPnP) keşif protokolünün temelini oluşturmaktadır. Protokol, ev veya küçük ofis ortamlarında kullanılmak üzere tasarlanmıştır. SSDP hizmeti düzenli olarak ev ağı içerisindeki UPnP özelliğine sahip cihazları tespit etmeye çalışmaktadır. Ev ağında bulunan UPnP cihazları ise SSDP protokolü ile gönderdiği bilgileri ile ağ içerisindeki varlığını bildirmektedir. SSDP, User Datagram Protocol (UDP) tabanlı çalışmaktadır. UDP 1900 portunu kullanan SSDP kimlik doğrulama içermediğinden oldukça hızlı veri iletimi sağlamaktadır. Ancak UDP ile kurulan iletişimlerde kimlik doğrulama olmadığından bazı zafiyetler ortaya çıkmaktadır. Siber saldırganlar da bu zafiyetleri kullanarak çeşitli saldırılar gerçekleştirmektedirler

Dağıtılmış Hizmet Reddi (DDoS) saldırıları, web üzerinden hizmet sunan ağ kaynaklarının cevap verebileceğinden fazla istekle karşılaşması sonucunda istekleri karşılayamayıp çalışamaz duruma gelmesini sağlayan siber saldırı tekniğidir. Ağ içerisindeki UPnP destekli cihazların varlığını ağdaki diğer cihazlara bildirmek için kullanılan SSDP protokolünün bu özelliğini kullanan siber saldırganlar tarafından yansıma tabanlı DDoS saldırısı şu şekilde gerçekleştirilir:

- Siber saldırgan saldırıda kullanacağı UPnP özelliği aktif cihazları tespit eder,
- Kurban olarak belirlenmiş cihazın IP adresini kullanarak UDP aketleri oluşturur,
- Oluşturduğu UDP paketlerini ağ içerisinde UPnP aktif cihazlara gönderir,
- Her cihaz kendisine gelen sorgu paketine çok fazla veri içeren paketler ile cevap verir,
- Saldırıda zombi bilgisayarlardan oluşan ağ (BOTNET) kullanılarak sorgu paketleri artırılmaktadır,
- Kurban olarak belirlenen cihaz tüm bu cevapların hedefi olur.

UPnP özelliği aktif olan cihazlar hedef olarak belirlenen kurbanın hizmetlerinin aksamasına neden olacak saldırıda saldırganın amacına hizmet etmiş olmaktadırlar.

3.2. Kullanılan Yöntem ve Teknikler

IoT cihazlarının, kolay kullanımını sağlayan UPnP özelliğinin, siber saldırganlar tarafından kullanıldığı örnek siber saldırılar olduğu görülmüştür. IoT cihazlarının istismar edilerek DDoS olarak adlandırılan siber saldırıda kullanılan bir zombi ağın üyesi olmasına engel olmak için açıklıkların tespitini sağlayan uygulamayı geliştirmek için protokoller üzerinde araştırma yapılmıştır.

Söz konusu protokollerin incelenmesi kapsamında, IoT cihazlarının bazılarında çalışır halde bulunan UPnP protokoller kümesi üzerine odaklanılmıştır. UPnP, bilgisayar sistemleri başta olmak üzere her türlü IoT cihazının birbiriyle iletişimini sağlamaktadır. UPnP, içerisinde IP, UDP, HTTP, SSDP, SOAP gibi farklı OSI katmanlarındaki protokolleri kullanmaktadır. UPnP özelliğine sahip cihazlar bir ağa otomatik olarak dahil olabilmekte, bir IP adresi alabilmekte ve ağ üzerindeki diğer cihazlara otomatik olarak bağlanabilmektedir.

UPnP, farklı protokolleri birlikte kullanarak çalışmaktadır. Temelinde İnternet Protokol'ünü (IP) kullanan UPnP, iletim katmanında UDP kullanmaktadır. UDP 1900 portu üzerinden diğer cihazlarla iletişime geçmektedir. Ağdaki diğer cihazları bulmak için SSDP kullanmaktadır. UDP üzerinden gönderdiği HTTP paketini 239.255.255.250 çoklu-yayın (multicast) adresine göndererek karşı taraftan cevap beklemektedir. Karşı tarafta bu isteğe içerisinde kendisine ait tanımlayıcı bilgilerini, üretici bilgileri, ilgili web servis tanımlarının olduğu XML dosyasının adresi gibi bilgiler olan HTTP paketini göndermektedir.

Siber saldırgan bu bilgileri alarak çeşitli saldırılarda kullanabilmektedir. UPnP özelliği barındıran cihazların çok büyük kısmında uzaktan komut çalıştırma (remote code execution) zafiyeti bulunmaktadır. Bu zafiyet istismar edilerek, hedef sisteme gönderilen UDP paketlerindeki belli parametrelere belli değerler atanarak, hedef sistemde önbellek taşmasına (buffer overflow) neden olmaktadır. Bellek taşması sağlandıktan sonra, belleğe istenen kod parçası yüklenerek hedef sistem ele geçirilmektedir.

Ev ağının güvenliğinin sağlanması projesi kapsamında söz konusu UPnP zafiyetine sahip cihazların varlığı kapsamında 3 aşamalı ve modüler bir uygulama yapılmıştır. Uygulamanın gerçekleştirilmesi kapsamında programlama dili olarak Python kullanılmıştır. Ağ güvenlik yazılımlarında kullanılmak için oluşturulmuş "scapy" kütüphanesi ve gerek duyulan diğer python kütüphaneleri kullanılmıştır.

3.3. Kullanılan Araçlar

Yazılım geliştirme aşamasında Windows 10 işletim sistemi kurulu dizüstü bilgisayar kullanılmıştır. Yapılan çalışmada ağ uygulamaları geliştirme kapsamında geniş ve kullanışlı kütüphanelere sahip olması nedeniyle Python programlama dili tercih edilmiştir.

Test yapılacak ortamın oluşturulması kapsamında, Şekil-1. de görülen ev ağı test ortamı olarak seçilmiştir. VMG3312-B10B model ZyXEL marka VDSL modem tarafından oluşturulan ev ağı içerisinde 2 adet masaüstü bilgisayar, 2 adet dizüstü bilgisayar, 1 adet Xiaomi Mipad4 tablet bilgisayar, 1 adet Digitürk uydu alıcısı, 1 adet uydu alıcı modülü,1 adet kindle elektronik kitap okuyucu, 4 adet akıllı cep telefonu, 1 adet Viomi V3 marka temizlik robotu, 1 adet PS4 Oyun Konsolu ve 1 adet Samsung Q70 Serisi akıllı televizyon bulunmaktadır.

Şekil 1:
Test Ortamı

3.4. Analiz Yöntemleri

Gerçekleştirilen çalışma üç aşama içermektedir; bu kapsamda, öncelikle ev ağındaki cihazların tespit edilmesi için bir Ağ Tarama modülü oluşturulmuştur. Ağ tarama modülü basit ve hızlı ağ taraması yaparak ağa bağlı cihazların tespit edilmesi maksatlı kullanılmaktadır. Ağa bağlı cihazların IP adresleri ve MAC adreslerini tespit etmektedir. Özelliği basit ve kötücül kod içermeyen projeye ait olmasıdır.

İkinci aşamada ağ içerisinde UPnP zafiyetine sahip cihazları tespit etmek için UPnP Tespit Modülü (UPnPTespit.py) oluşturulmuştur. Bu modül ise Simple Service Discovery Protokol'ünü (SSDP) kullanarak ev ağı içerisinde çoklu-yayın adresine sorgulama mesajı göndererek hangi cihazlarda UPnP zafiyeti olduğunu tespit etmektedir. UPnP zafiyetine sahip olan cihazların modül içerisinde yapılan sorguya verdikleri cevap paketleri ile cihazların tespitleri yapılmaktadır.

Üçüncü aşamada ise ağ içerisinde UPnP zafiyetine sahip olan cihazlar ile ilgili olarak daha kapsamlı bilgi almak ve bu cihazların sahip oldukları bilgilerin sunulduğu XML formatlı

dosyalara ulaşarak bu dosyaların içeriğinin okunmasını sağlayan UPnP Bilgi Toplama Modülü (UPnPBilgiToplama.py) geliştirilmiştir. Bu modül sayesinde UPnP özelliği açık olan cihazların sahip oldukları hizmetlerin, her türlü üretici bilgilerinin, yazılım versiyonlarının ve sundukları diğer bilgilere ulaşım sağlanabilmektedir. Bu bilgiler incelenerek siber saldırganlar tarafından istismar edilebilecek açıkların varlığı kontrol edilebilmektedir.

4. BULGULAR VE DEĞERLENDİRMELER

UPnP protokolünün ağ içerisinde kullanımına yönelik olması nedeniyle modüller şeklinde yapılmıştır.

4.1. Uygulama Sonucunda Elde Edilen Bulgular

Ev ağı içerisinde VMG3312-B10B model ZyXEL marka VDSL modemi hem internete bağlantı sağlamakta hem de kablolu ve kablosuz ev ağının oluşturulmasında kullanılmaktadır. Test ortamını oluşturan nesnelerden; 2 adet masaüstü bilgisayar, 1 adet Digitürk uydu alıcısı, 1 adet uydu alıcı modülü ev ağına kablo ile bağlanmaktadır. Diğer cihazlar ise Wi-Fi ile ev ağına bağlantı sağlamaktadır.

```
========== RESTART: C:\Users\mkandir\De
Available devices in the network:
IP                  MAC
192.168.1.1         5c:6a:80:ac:f6:34
192.168.1.33        cc:d3:c1:6c:fe:5f
192.168.1.37        2c:f0:5d:8e:54:6b
192.168.1.34        64:90:c1:6e:37:c9
192.168.1.45        32:2d:92:c0:4e:2c
192.168.1.50        d0:53:49:15:a7:a4
192.168.1.40        bc:7f:a4:25:5f:17
192.168.1.55        b8:bc:5b:de:cd:33
192.168.1.57        60:45:cb:8a:33:a5
192.168.1.53        9a:da:c4:44:78:18
192.168.1.51        e8:9e:b4:ed:8c:ab
192.168.1.43        a4:6b:b6:ee:04:26
192.168.1.58        0c:1d:af:53:f0:05
192.168.1.52        f0:a2:25:84:1a:2d
192.168.1.47        0c:2f:b0:fc:0b:42
```

Şekil 2:
Ağ Tarama Sonucu

UPnP, farklı protokolleri birlikte kullanarak çalışmaktadır. Temelinde IP kullanan UPnP, iletim katmanında UDP kullanmaktadır. UDP 1900 portu üzerinden diğer cihazlarla iletişime geçmektedir. Ağdaki diğer cihazları bulmak için SSDP kullanmaktadır. UDP üzerinden gönderdiği HTTP paketini 239:255.255.250 çoklu-yayın adresine göndererek karşı taraftan cevap beklemektedir. Eğer bir cihazda UPnP açıksa, bu isteğe 200 OK olarak cevap dönmekte ve döndüğü HTTP paketinin içerisinde kendisine ait UUID, üretici bilgileri, ilgili web servis tanımlarının olduğu XML uzantılı dosya yolu gibi bilgiler bulunmaktadır.

Python dili ile yazılmış Ağ Tarama Modülü ile evde oluşturulan test ağında tarama yapılarak ağa kablolu ve kablosuz olarak dahil olmuş Şekil-2. de görülen cihazların tespiti yapılmıştır. Sonrasında ağ içerisinde UPnP protokolü açık olan cihazların tespit edilmesi için SSDP protokolü ile çoklu-yayın adresine bir sorgu gönderilerek ev ağına bağlı olan cihazlardan cevap beklenmiştir.

Şekil 3:
SSDP ile yapılan çoklu-yayına verilen cevaplar

Ağda bulunan cihazlardan, Ağ protokolleri kümesi olan UPnP aktif olan akıllı cihazlar Şekil-3'te görülen bilgileri cevap olarak göndermişlerdir. Gelen bilgilerden hangi cihazların cevap verdiği tespit edilebilmektedir. Ağda yapılan sorgulara cevap geldiği için bu ağda UPnP zafiyetine sahip cihazlar olduğu anlaşılmıştır.

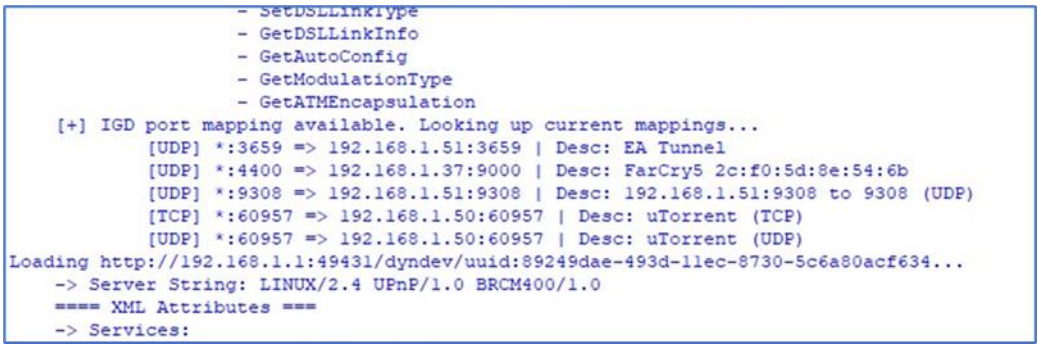
Şekil 4:
Ayrıntılı UPnP Sorgulama Sonucu

Ağ içerisinde SSDP ile yapılan sorgu sonucu UPnP özellikleri aktif cihazların olduğunun anlaşılması sonrasında UPnP Bilgi Toplama Modülü ile kapsamlı sorgulama yapılmıştır. Bir kısmı Şekil-4. de görülen bilgiler bu ayrıntılı sorgulama sonucunda elde edilmiştir.

Port forwarding (port yönlendirme) yöntemiyle ağdaki bir cihaza belirli bir port atamak ve internete doğrudan bağlanmasını sağlamak mümkün olmaktadır. Port forwarding, yerel ağ üzerindeki bir cihazla uzaktaki bir cihaz arasında doğrudan bir bağlantı kurmak gerektiği tüm durumlarda kullanılmaktadır. Bu durumlara:

- Evden uzaktayken ev ağı içerisindeki bir güvenlik kamerasına bağlanmak,
- Dışarıdan ev içerisindeki sunucuya bağlanmak,
- Eğer ev içerisinde bir sunucu işletiliyorsa dışarıdan bu sunucuya bağlanmak,
- Çok oyunculu bir oyunun sunucularına doğrudan bağlanmak gibi ihtiyaçlar örnek verilebilmektedir.

Bu şekilde port forwarding yapılmış olan porta, bağlantı şifresini bilen (veya kıran) herkes ulaşabilir. Açık bir port, ağdaki diğer cihazlara erişilerek zararlı yazılımlar yüklenmesine sebebiyet verebilecektir. UPnP Bilgi Toplama Modülü ile bu zafiyet taraması da yapılmıştır.



Şekil 5:
IGD Port Mapping Sorgulama Sonucu

Yapılan sorgulama sonucunda geçmişte açılmış olan portlar rahatlıkla tespit edilmiştir. Kullanımına devam edilmese bile portların istismara açık olarak tanımlanmış oldukları görülmüştür.

Ev ortamında yapılan testlerde; "Broadcom Corporation" üretimi olan VMG3312-B10B model ZyXEL marka VDSL modemin UPnP özelliğinin açık olduğu tespit edilmiştir. Ayrıca bir diğer IoT cihazı olan Samsung Q70 Series akıllı televizyonun da UPnP özelliğinin açık olduğu tespit edilmiştir. Yine ağa kablolu olarak bağlanan ve uydu alıcısı temelli olarak çalışan IPTV özellikli Korax marka cihaz da UPnP özelliğinin aktif olduğu görülmüştür. Her üç cihazla ilgili tüm bilgiler UPnP Bilgi Toplama Modülü ile ele geçirilmiştir. Bu cihazlar için gerekli zayıflık sömürü yazılımları (exploit) temin edildiğinde kolayca istismar edilebilecekleri sonucuna ulaşılmıştır.

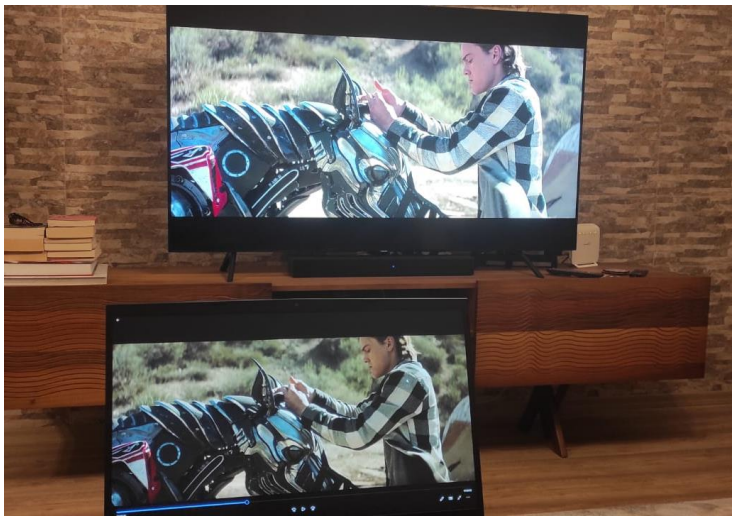
4.2. Saldırı Senaryosu ve Uygulaması

UPnp özelliği aktif olan Samsung Q70 Series akıllı televizyonun bir saldırgan tarafından uzaktan uygun programlar ile istismar edilerek o anki yayının kesilmesi ve saldırgan tarafından istenen görüntünün oynatılmasını içeren bir saldırı senaryosu hazırlanmış ve uygulanmıştır. Akıllı televizyondaki UPnP özelliğinin aktif olduğunu çalışmamızın uygulama sürecinde tespit etmiştik. DLNA (Digital Living Network Alliance) olarak adlandırılan ve dijital cihazların birbirleri ile iletişim kurmasını sağlamak amacıyla geliştirilen bir teknolojiyi de kullanarak UPnP özelliği açık olan akıllı televizyona erişim sağlanmış ve dizüstü bilgisayarımızdaki video aynı anda akıllı televizyonda oynatılmıştır.

Söz konusu senaryonun gerçekleştirilmesinde Şekil-6'da ara yüz görünümü verilmiş olan uygulama kullanılmıştır. Uygulama UPnP özelliği aktif olan cihazı tespit ederek uygun bağlantıyı sağlamış ve akıllı televizyon ile doğrudan kablolu bir bağlantı olmadan kablosuz olarak bağlanılan Ev Ağı içerisindeki bağlantı özelliklerini kullanarak akıllı televizyona erişim sağlamıştır.

Şekil 6:
DeviceOnline Free media streamer

Üreticiler tarafından tüketicilere kolay kullanım imkânı sağlamak için kullanılan UPnP özelliği kolayca istismar edilmiş ve akıllı televizyona izinsiz erişim sağlanmıştır. Şekil 7 de senaryonun uygulanma anı gösterilmiştir.



Şekil 7:
Saldırı Senaryosu Uygulaması

4.3. Sonuçların Değerlendirilmesi

Nesnelerin interneti kapsamındaki akıllı cihazların kullanımlarının kolaylaştırılması ve birbirlerine kolayca bağlanmalarını sağlayan teknolojilerden olan UPnP zafiyeti ev ağında incelendiğinde 3 adet cihazın bu açıklığa sahip olduğu görülmüştür. Bu cihazların marka ve modelleri göz önüne alındığında kurumsal firmalar olduğu görülmektedir. Dünyadaki teknoloji cihazlarına duyulan yoğun ihtiyaç düşünüldüğünde birçok firma tarafından bu tür akıllı cihazların üretildiği görülmektedir. Kurumsal firmalar tarafından bile göz ardı edilebilen güvenlik önlemlerinin diğer firmalar tarafından daha az dikkate alınabileceği öngörüsüyle bu tür yazılım açıklarıyla gelecekte çok daha fazla karşılaşılabileceği düşünülmektedir.

Üreticilerin daha fazla talep edilmesi için kolay kullanım sunan bu tür cihazlar üreterek istem dışı bir güvenlik problemi yarattıkları görülmüştür. İnternete bağlı nesnelerin hızla artması ve bir ağın en zayıf bileşeni kadar güvenli olabileceği kuralı göz önünde bulundurulduğunda bu tür zafiyetlerin ağ güvenliği için ciddi birer tehdit olduğu görülmektedir.

Yapılan test sonucunda tespit edilen UPnP zafiyetine sahip cihazların bu özellikleri iptal edilerek güvenlikleri sağlanmıştır. Ancak her geçen gün ağa yeni nesneler dahil olmaktadır. Ağ güvenlik tedbirleri kapsamında UPnP açıklık kontrolü adımının güvenlik kontrolleri listesine eklenmesinin bu zafiyetin önlenmesi bakımından önem taşıdığı sonucuna ulaşılmıştır.

Ağ içerisindeki cihazların tespiti için oluşturulan ilk modül olan Ağ Tarama Modülü yanında Ağ Port Tarama Modülü de oluşturulmalıdır. Ancak port tarama işleminin paket gönderme ve belli bir süre bekleme işlemleri nedeniyle uzun bir süre aldığı görülmektedir. Port tarama işleminin paralel programlama teknikleri kullanılarak yapılması ve belirlenen özel portların taranması yöntemleri ile hızlandırılarak gerçekleştirilmesi verimi artıracaktır.

5. SONUÇ

Literatürde IoT cihazları için yapılan güvenlik kontrol çalışmaları donanım ve yazılım olarak ayrılmıştır. Özellikle SCADA sistemlerin taşıdıkları öneme haiz olmak üzere çalışmalar bu alanlarda yoğunluk göstermektedir. Bu çalışma ise her ne kadar ev ağı içerisinde yapılmış olsa da akıllı cihazların bulunduğu ve erişim sağlanabilen her türlü ağ ortamı için geçerlilik taşımaktadır. Sıradan ve özel olarak hazırlanmamış bir ev ağında bulunabilecek akıllı cihazlar test edilmiştir. Yapılan test sonuçları, istatistiki olarak değerlendirildiğinde; bir ağ ortamı bulunan ve o ortama bağlı olan akıllı nesnelerin bir kısmında söz konusu olan ve kullanımı oldukça yaygın olan UPnP zafiyetinin olabileceği görülmüştür. UPnP protokolünün cihaz ilk kez ağa tanıtılırken aktif olması ve sonrasında kapatılması gerektiği yapılan testler sonucunda anlaşılmıştır.

Çalışma ile gerçekleştirilen üç modül, gelecekte yapılacak çalışmalara temel teşkil edecektir. Açık kaynak ve temiz bir kodlama ile yapıldığı için zararlı yazılım içerme ihtimali olmayan modüller bu kapsamda güvenlik tehdidi içermemektedirler. Ayrıca kolayca farklı sorgulamalar ile farklı protokollerin testlerini yapacak şekilde geliştirmeye açık modüler bir çalışma gerçekleştirilmiştir.

Gelecek çalışmalarda farklı protokollerin ağ içerisinde test edilmesi, henüz tespit edilmemiş açıklık içeren protokollerin tespiti bakımından önem taşımaktadır. Endüstriyel ortamlarda IoT kullanımın çok yaygın olması nedeniyle bu tür sızma testi yazılımlarına dönüştürülebilecek yapıda açıklık tespit yazılımlarına ihtiyaç bulunmaktadır. SCADA sistemlerin kontrolleri oldukça önemlidir. Bu tür sistemlerin siber saldırganlar tarafından ele geçirilmesi ulusal güvenlik açısından da sorun teşkil etmektedir. Gelecekte SCADA sistemler için Sisteme Özel bu tür açıklık arama yazılımları geliştirilmesi önem arz etmektedir. Çalışma neticesinde, nesnelerin interneti kapsamında bir ev ağında mevcut cihazların zayıflık taramaları yapılarak durumları incelenmiş ve güvenlik ihtiyaçları değerlendirilmiştir.

ÇIKAR ÇATIŞMASI

Yazar bilinen herhangi bir çıkar çatışması veya herhangi bir kurum/kuruluş ya da kişi ile ortak çıkar bulunmadığını onaylamaktadır.

YAZAR KATKISI

Murat Osman KANDIR, Çalışmanın literatür araştırması, deneysel ve teorik araştırma, sistemin tasarımı ve programlama konularında,

Esra Nergis YOLAÇAN, makalenin oluşturulması, sistemin tasarımı ve sonuçların yorumlanması konularında,

Şahin IŞIK, makalenin oluşturulması, sistemin tasarımı ve sonuçların yorumlanması konularında katkı sağlamışlardır.

KAYNAKLAR

1. Amro, A., (2020) IoT Vulnerability Scanning: A State of the Art, *European Symposium on Research in Computer Security 2020 International Workshops, Cyber-Physical Systems, Sociedad Espanola de Cirugia Plastica Reparadora y Estetica, and Attacks and Defenses for Internet-of-Things, Guildford,* UK. doi: 10.1007/978-3-030-64330-0_6

2. Antrobus, R., Green, B., Freyy, S., ve Rashidz, A. (2019) The forgotten I in IIoT: A vulnerability scanner for industrial Internet of Things, *Living in the Internet of Things (IoT 2019).* doi: 10.1049/cp.2019.0126

3. Deepak K.R. Singh, (2020) Cyber Security and Internet of Things, *International Journal of Computer Techniques*, Volume 7 Issue 6

4. Huang, Y., Zhu, F., Liu, L., Meng, W., Hu, S., Ye, R. ve Lu, T. (2021) WNV-Detector: automated and scalable detection of wireless network vulnerabilities *EURASIP Journal on Wireless Communications and Networking*. doi: 10.1186/s13638-021-01978-4

5. Intal Tayag, M., Napalit, F. ve Napalit, A. (2020) IoT Security: Penetration Testing of White-label Cloud-based IoT Camera Compromising Personal Data Privacy, *International Journal of Computer Science & Information Technology (IJCSIT)* Vol 12, No 5. doi: 10.5121/ijcsit.2020.12503

6. Kayas, G., Hossain, M., Payton, J. ve Riazul Islam, S. M. (2020) An Overview of UPnP-based IoT Security: Threats, Vulnerabilities, and Prospective Solutions *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). doi: 10.1109/IEMCON51383.2020.9284885*

7. Malhotra, P., Singh, Y., Anand, P., Kumar Bangotra, D., Kumar Singh, P. ve Hong, W., (2021) Internet of Things: Evolution, Concerns and Security Challenges, *Sensors. doi: 10.3390/s21051809*

8. McDaid, A., Furey, E. ve Curran, K. (2021) Wireless Interference Analysis for Home IoT Security Vulnerability Detection, *International Journal of Wireless Networks and Broadband Technologies. doi: 10.4018/IJWNBT.2021070104*

9. Mehic, M., Selimovic, N. ve Komosny, D. (2019) About the Connectivity of Xiaomi Internet-of-Things Smart Home Devices *Conference: 2019 XXVII International Conference on Information, Communication and Automation Technologies (ICAT). doi: 10.1109/ICAT47117.2019.8939043*

10. Meidan, Y., Sachidananda, V., Peng, H., Sagron, R., Elovici, Y. ve Shabtai, A. (2020) A novel approach for detecting vulnerable IoT devices connected behind a home NAT *Computers & Security Volume 97. doi: 10.1016/j.cose.2020.101968*

11. Olsson, T. ve Larsson Forsberg, A. (2019) IoT Offensive Security Penetration Testing Hacking a Smart Robot Vacuum Cleaner, *Computer Science*

12. Patel, B. ve Shah, P. (2020) Simulation, modelling and packet sniffing facilities for IoT: A systematic analysis, *International Journal of Electrical and Computer Engineering (IJECE)* Vol. 10, No. 3

13. Raghuvanshi, A., Dr. Kumar Singh, U., Bulla, C., Dr. Saxena, M., ve Abadar, K. (2020) An Investigation on Detection of Vulnerabilities in Internet of Things, *European Journal of Molecular & Clinical Medicine* Volume 07, Issue 10

14. Shreenidhi H.S., Prabakar, S. ve P Ashish Kumar, (2021) Intrution detection system Using IoT device for safety and security, *2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, Amity University Dubai, UAE. doi: 10.1109/ICCIKE51210.2021.9410730

15. Upadhyay, S., Kumar, S. ve Dutta, S. (2019) Vulnerability scanning in IOT Devices, *Conference: ICICD 2018 At: University of Petroleum and Energy Studies*

16. Williams, R., McMahon, E., Samtani, S., Patton, M. ve Chen, H. (2017) Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach, *2017 IEEE International Conference on Intelligence and Security Informatics (ISI). doi: 10.1109/ISI.2017.8004904*

17. Yadav, G., Paul, K., Allakany, A. ve Okamura, K. (2020) IoT-PEN: An E2E Penetration Testing Framework for IoT, *Journal of Information Processing* Vol.28 633–642. doi: 10.2197/ipsjjip.28.633