Orclever Proceedings of Research and Development
https://doi.org/10.56038/oprd.v5i1.599
OR CLEVER Science & Research Group

Konferans Bildirisi

5G Ağlarda Güvenlik Teknolojilerinin Perspektifinde IoT Uygulamalarının İncelenmesi

Yaşar Serdar Fidaner[1], Asuman Savaşçıhabeş[2]

[1]Nuh Naci Yazgan Üniversitesi, https://orcid.org/0009-0003-4903-2644, sefidaner@gmail.com
[2]Nuh Naci Yazgan Üniversitesi, https://orcid.org/0000-0002-7621-1906 ahabes@nny.edu.tr
[1]* Sorumlu Yazar: Yaşar Serdar Fidaner, sefidaner@gmail.com

Received 02 November 2024
Received in revised form 23 December 2024
In final form 25 December 2024

4th International Conference on Design, Research and Development (RDCONF 2024)
December 19 - 20, 2024

Reference: Fidaner, Y. S., & Savaşçıhabeş, A. (2024). Examining IoT applications in the perspective of security technologies in 5G networks. Orclever Proceedings of Research and Development, 5(1), 527-548.

Özet

5G teknolojisi, dijital dönüşümün itici gücü olarak haberleşme altyapısında devrim yaratırken, güvenlik tehditlerini de beraberinde getirmektedir. Yüksek hızlı veri iletimi ve düşük gecikme avantajları sunan bu teknoloji, karmaşık dalga formları ve geniş bant iletişim kanallarıyla kötü niyetli aktörler için yeni saldırı yüzeyleri oluşturmuştur. Artan cihaz bağlantıları ve ağ karmaşıklığı, bireylerin ve kurumların mahremiyetini tehdit eden siber saldırılara karşı daha güçlü güvenlik çözümlerine olan ihtiyacı ortaya koymaktadır. Genel olarak 5G, bağlantıyı ve performansı artırarak çeşitli sektörlerde ilerlemelere öncülük etmektedir. 5G güvenlik mimarisi, bu teknolojinin ortaya koyduğu benzersiz zorlukları ele almak için çeşitli gelişmiş kavramlar ve teknikler sunar. Bu çalışmada 5G güvenliğinin ayrılmaz bir parçası olan temel kavramlar ve koruma tekniklerinin yanısıra, modern ağların artan karmaşıklığını ve ölçeğini ele alarak güvenli ve dayanıklı bir iletişim ortamı sağlayan teknolojinin güvenlik çerçevesi incelenmiştir.

Anahtar: 5G, ağ, gizlilik, güvenlik mimarisi, Ağ dilimleme, uçtan uca güvenlik.

Orclever Proceedings of Research and Development
https://doi.org/10.56038/oprd.v5i1.599
OR CLEVER Science & Research Group

Conference Article

Examining IoT Applications in the Perspective of Security Technologies in 5G Networks

Abstract

While 5G technology revolutionizes the communication infrastructure as the driving force of digital transformation, it also brings security threats. Offering the advantages of high-speed data transmission and low latency, this technology has created new attack surfaces for malicious actors with complex waveforms and wide-band communication channels. Increasing device connections and network complexity reveal the need for stronger security solutions against cyberattacks that threaten the privacy of individuals and institutions. Overall, 5G is also leading to advances in various sectors by improving connectivity and performance. The 5G security architecture offers a variety of advanced concepts and techniques to address the unique challenges posed by this technology. This study examines the basic concepts and protection techniques that are integral to 5G security, as well as the security framework of the technology that addresses the increasing complexity and scale of modern networks and provides a secure and resilient communication environment.

Keywords: *5G, network, privacy, security architecture, network slicing, End to End security.*

https://doi.org/10.56038/oprd.v5i1.599

1. Giriş

İletişim ağı genişlemeye devam ettikçe giderek daha heterojen hale gelmektedir. Sensörlerden, IoT(nesnelerin interneti, internet of things) istemcilerine ve sunucularına kadar çeşitli cihazların ağa bağlı tutulmasıyla oluşan ekosistem, oldukça dağıtılmış durumdadır ve network sistemi birçok genişbant cihazı ve cihaz mobilitesi ağdaki dinamik değişimleri desteklemektedir[1]. Dolayısıyla, bu ağ sistemi güvenlik saldırılarına karşı savunmasız hale gelmektedir. Bu açıdan bakıldığında 5G ağlarında güvenli iletişim için en etkili yöntemler incelenmiş ve bu konuda çeşitli yaklaşımlar analiz edilerek bu çalışmada en yüksek doğruluktaki yöntemler belirtilmiştir. Bu inceleme çalışmasında ayrıca gelişen güvenlik tehditleri karşısında 5G ağlarının güvenliğini optimize etmeye çalışanlar için güvenlik mekanizmalarının karşılaştırması da yer almaktadır.

LİTERATÜR ARAŞTIRMASI

Beşinci nesil mobil ağ teknolojisi olan 5G, önceki nesillere kıyasla önemli ölçüde daha hızlı indirmeler, kesintisiz akış ve genel olarak daha iyi kullanıcı deneyimi sunar. Daha düşük gecikme avantajının yanısıra artan sayıda IoT cihazını ve akıllı teknolojiyi destekleyebilmektedir. Bu teknoloji, daha istikrarlı ve güvenlilir bağlantılar sağlayarak bağlantı kesintileri gibi sorunları azaltır.

5G ağları benzeri görülmemiş hızlar, artan kapasite ve çeşitli cihazların sorunsuz entegrasyonunu vaat ederken, aynı zamanda karmaşık güvenlik riskleri ve zorlukları da beraberinde getirmektedir. Bu yeni nesil mobil ağlar yalnızca saldırı ortamını genişletmekle kalmaz, aynı zamanda sıkı koruma önlemleri gerektiren otonom araçlar ve kritik altyapı gibi karmaşık kullanım durumlarını da içerebilmektedir. Bu konuda yapılan çeşitli araştırmalar göstermektedir ki, 5G için tasarlanmış çeşitli güvenlik mekanizmalarını değerlendirerek, bunların etkinliğini ve dayanıklılığını değerlendirmek için karşılaştırmalı bir çerçeve oluşturarak bu zorlukların ele alınması önemli bir güvenlik tehdidini önleyebilir. Bunu yaparak, mevcut güvenlik stratejilerindeki güçlü ve zayıf yönleri belirlemeyi, gelişen dijital ortamda ortaya çıkan tehditlere karşı korumaları optimize etmeye yönelik metodolojiler ortaya konulmuştur.

5G ağlarının yeni kablosuz erişim teknolojileriyle desteklenmesi, enerji ve bant genişliği kısıtlamaları sorununu çözebilecek hafif güvenlik tekniklerini gerektiren kablosuz erişim teknolojilerini gerektirmektedir[1].

Fiziksel Katman Güvenliğinde, WBPLSec (fiziksel katman güvenliği) adı verilen yeni bir fiziksel katman

https://doi.org/10.56038/oprd.v5i1.599

güvenlik tekniği önerilmektedir[2]. Bu teknik, daha yüksek katmanlı şifreleme protokollerine güvenmeden iletişim sistemi güvenliğini iyileştirmeyi amaçlar. WBPLSec, artan sıkıştırma enerjisinin güvenliği artırması ancak filigran çıkarımını da düşürmesi nedeniyle güvenlik ve iletişim güvenilirliği arasında bir ödünleşim olarak karşımıza çıkmaktadır. iJAM'den farklı olarak, WBPLSec tam oranlı bir protokoldür ve daha iyi iletişim güvenilirliği sunar. WBPLSec, DSSS(Direct Sequence Spread Spectrum) veya OFDM(Orthogonal Frequency Division Multiplexing) gibi yayılı spektrum teknikleri kullanılarak uygulanabilir ve bu da bu güvenlik tekniğini çeşitli iletişim sistemleri için uygun hale getirir. WBPLSec'in bağımsız yapısı ve şifrelemeye kıyasla daha düşük enerji tüketimi nedeniyle düşük güçlü sensör ağlarında ve 5G cihazlarında güvenliği dağıtmak için değerli bir teknik olduğu bilinmektedir[2]. 5G-WLAN güvenliğinde WiFi, LiFi ve 5G ağları arasındaki iletişim için güvenlik hususları ayrıca önem arz etmektedir. Bu açıdan farklı protokol katmanlarındaki birlikte çalışabilirliği incelenmeli ve mimari model için güvenlik zorlukları ve hususları dikkate alınmalıdır. 5G ağları tam olarak uygulanıp test edildikten sonra gelecekteki güvenlik zorlukları ve potansiyel çözümler ele alınabilecektir. IoT güvenliği açısından incelendiğinde, mobil bulut robotları için dağıtılmış bir güvenlik platformu literatürde yer almaktadır. Platform, robotlardan, Yerel Robot Denetleyicilerinden (LRC'ler) ve bir IoT anormallik tespit modülünden oluşmaktadır[2]. LRC'ler, robot verilerini mobil ağlara iletmeden önce izler ve analiz ederler. IoT anormallik tespit modülü, anormallikleri tespit etmek ve yeni saldırıları etiketlemek için doğrusal ve öğrenme algoritmalarını kullanır. Platform, kötü amaçlı robotları tespit edebilir ve diğer MVNO(mobile virtual network operator) operatörleri bunları engellemeleri için bilgilendirebilir, böylece daha önce tespit edilen kötü amaçlı robotlar için işlem yükü azaltılır[2].

Mobil operatörlerin maliyet yapısını, zaman verimliliğini ve pazara sunma hızını iyileştirmeleri için bir Telekomünikasyon Ağı Hizmeti (TaaS) modeli önerilmektedir. Tüm bulut katmanları için tehditleri bir MVNO perspektifinden ele alınmakta ve mobil operatörlerin dağıtım ve güvenlik endişelerine göre hizmetlerini nasıl ödünleşebileceğini ve birleştireceklerini anlamalarına yardımcı olmak için bir bulut güvenlik modeli önerilmektedir. Ayrıca MVNO saldırı profilleri ve NFV'ye özgü tehditler gözden geçirilmekte ve azaltma mekanizmalarını uygulanmaktadır. 5G teknolojileri için güvenliğin önemini literatürde sıkça incelenen bir konudur[3-7] ve MEC ve bulut bilişim ortamlarındaki tehditleri azaltmak için kontrol önlemleri önerilmektedir[8].

https://doi.org/10.56038/oprd.v5i1.599

5G teknolojisi için mevcut güvenlik mekanizmaları veri koruması, ağ bütünlüğü ve kullanıcı gizliliğiyle ilgili bir dizi endişeyi gidermek amacı taşır. Bu mekanizmalar, 5G'nin gelişmiş yetenekleri ve karmaşıklıklarının ortaya koyduğu benzersiz zorluklarla başa çıkmak için tasarlanmış olup yeni tehditler ortaya çıktıkça ve teknoloji ilerledikçe sürekli olarak gelişmektedir. Amaç, kullanıcıları ve verileri çeşitli güvenlik tehditlerinden korurken modern bağlantının taleplerini karşılayabilen dayanıklı ve güvenli bir 5G ağ ortamı oluşturmaktır.

5G ağlarıyla ilişkili güvenlik zorlukları, gelişmiş veri hızları, artan ağ karmaşıklığı ve bağlı cihazların yaygınlaşması gibi gelişmiş özellikleriyle yakından bağlantılıdır. Bu faktörlerin her birinin güvenlik endişelerine nasıl katkıda bulunduğu incelendiğinde karşımıza çıkan faktörler şunlardır:

Gelişmiş veri hızları: 5G ağlarındaki veri aktarım hızlarındaki ve bant genişliğindeki çarpıcı artış, veri gizliliği ve bütünlüğüyle ilgili güvenlik açıkları ortaya çıkarır. Yüksek hızlı veri iletimi, saldırganların büyük miktarda hassas bilgiye hızlı bir şekilde erişip bunları sızdırabilmeleri nedeniyle veri ihlalleri veya müdahale gibi saldırıların etkisini artırabilir. Güçlü şifreleme protokolleri ve gelişmiş saldırı tespit sistemleri, aktarım sırasında verileri korumak ve yüksek hızlı iletişimlerin veri güvenliğini tehlikeye atmamasını sağlamak için çok önemlidir.

Artan Ağ Karmaşıklığı: 5G ağları, fiziksel altyapı, sanallaştırılmış ağ işlevleri ve ağ dilimlemesinin bir karışımını içeren karmaşık mimarileriyle karakterize edilir. Bu karmaşıklık, olası saldırı vektörlerinin sayısını artırır ve her bileşeni etkili bir şekilde yönetmeyi ve güvenliğini sağlamayı zorlaştırır. Bu karmaşıklığı yönetmek için kapsamlı ve uyarlanabilir güvenlik stratejileri gereklidir. Bu, 5G ağ ortamının dinamik ve çok yönlü doğasını ele almak için güçlü erişim kontrolleri, sürekli izleme ve otomatik tehdit algılama sistemleri uygulamayı içerir.

Bağlı Cihazların Yaygınlaşması: Akıllı telefonlardan IoT cihazlarına kadar 5G üzerinden bağlanan çok sayıda cihaz, saldırı yüzeyini önemli ölçüde genişletir. Her cihaz potansiyel olarak kötü niyetli aktörler için bir giriş noktası olabilir ve bu kadar çeşitli ve potansiyel olarak savunmasız uç noktaların güvenliğini yönetmek büyük bir zorluktur. nYetkisiz erişime karşı koruma sağlamak için etkili cihaz yönetimi ve kimlik doğrulama mekanizmaları esastır. Ek olarak, cihazların ağa güvenli bir şekilde entegre edilmesini ve bir segmentteki olası ihlallerin tüm sistemi tehlikeye atmamasını sağlamak için uçtan uca güvenlik protokolleri ve sağlam ağ segmentasyonu gereklidir.

https://doi.org/10.56038/oprd.v5i1.599

Bununla beraber 5G teknolojisi için mevcut güvenlik mekanizmaları, veri koruması, ağ bütünlüğü ve kullanıcı gizliliğiyle ilgili bir dizi endişeyi ele alır. Bu mekanizmalar, 5G'nin gelişmiş yetenekleri ve karmaşıklıklarının ortaya koyduğu benzersiz zorluklarla başa çıkmak için tasarlanmıştır. İşte 5G ağlarında uygulanan temel güvenlik mekanizmalarından bazıları şunlardır[9]:

Gelişmiş Veri Şifreleme: 5G ağları, aktarım sırasında verileri korumak için gelişmiş şifreleme protokolleri kullanır[10]. Bu, gizliliği ve bütünlüğü sağlamak için kullanıcı verilerinin ve sinyal verilerinin şifrelenmesini içerir. 5G, Gelişmiş Şifreleme Standardı (AES) gibi güncellenmiş algoritmalar ve 5G'nin yüksek hızlı veri gereksinimleri için uyarlanmış yeni şifreleme teknikleri kullanır.

Karşılıklı Kimlik Doğrulama ve Yetkilendirme: 5G ağları, hem kullanıcıların hem de ağ varlıklarının (örneğin, baz istasyonları ve çekirdek ağ öğeleri) kimliklerini doğrulamak için karşılıklı kimlik doğrulama mekanizmaları kullanır[11]. Bu, yetkisiz erişimi önler ve her iki tarafın da meşru olmasını sağlar.Gelişmiş Kimlik Doğrulama Protokolleri arasında yer alan 5G AKA (Kimlik Doğrulama ve Anahtar Anlaşması) ve USIM (Evrensel Abone Kimlik Modülü) tabanlı kimlik doğrulama gibi teknikler, çeşitli saldırı türlerine karşı sağlam koruma sağlar.

Ağ Dilimleme Güvenliği: Ağ dilimleme, aynı fiziksel altyapı içinde izole sanal ağların oluşturulmasına olanak tanır. Her dilimin kendi güvenlik politikaları olabilir; bu da olası ihlalleri sınırlamaya ve bir dilimin sorunlarının diğerlerini etkilememesini sağlamaya yardımcı olur. Dilimlere Özgü Güvenlik Önlemleri arasında yer alan, Farklı ağ dilimleri, düşük gecikmeli veya yüksek güvenilirlikli dilimler gibi destekledikleri hizmet veya uygulama türüne göre belirli güvenlik önlemleriyle uyarlanabilir.

Güvenli Arayüzler ve API'ler-Arayüz Koruması: Güvenlik önlemleri, farklı ağ bileşenleri arasındaki ve ağ ile harici varlıklar arasındaki arayüzleri korumak için uygulanır. Bu, iletişim için güvenli protokoller ve API'ler kullanmayı içerir. Bu arayüzleri yetkisiz erişim veya manipülasyondan korumak için sıkı erişim kontrolleri ve izleme uygulanır.

Ağ İşlevi Sanallaştırma (NFV) ve Yazılım Tanımlı Ağ (SDN) Güvenliği: Sanallaştırılmış ağ işlevleri, güvenli önyükleme mekanizmaları, izolasyon teknikleri ve düzenli güncellemeler dahil olmak üzere sanallaştırmaya özgü güvenlik önlemleriyle korunur. SDN, ağ kaynaklarının dinamik olarak yönetilmesine yardımcı olur ve güvenliği, SDN denetleyicilerini korumayı ve kontrol ile veri düzlemleri arasında güvenli iletişimi sağlamayı içerir.

https://doi.org/10.56038/oprd.v5i1.599

Kullanıcı Gizliliği Koruması-Veri Anonimleştirme: Kullanıcı kimliklerini ve kişisel verileri korumak için takma adlandırma ve anonimleştirme gibi teknikler kullanılır. Gelişmiş Gizlilik Protokolleri ile 5G, ifşa edilebilecek veya izlenebilecek kullanıcı bilgisi miktarını sınırlamak için yeni gizlilik mekanizmaları içerir.

İzinsiz Giriş Tespiti ve Önleme Sistemleri (IDPS): IDPS'ler, ağ trafiğini sürekli olarak izlemek ve olası güvenlik tehditlerini gösterebilecek şüpheli etkinlikleri veya anormallikleri tespit etmek için gerçek zamanlı izleme yapılarak kullanılır. Gelişmiş IDPS, tespit edilen tehditleri azaltmak ve olası hasarı azaltmak için otomatik yanıtlar sağlayabilmektedir.

Güvenlik Güvencesi ve Testi: Güvenlik Denetimleri Güvenlik mekanizmalarının etkili ve güncel olduğundan emin olmak için düzenli güvenlik denetimleri ve değerlendirmeleri yapılır. Devam eden penetrasyon testi, ağ altyapısındaki ve uygulamalardaki güvenlik açıklarını belirlemeye ve gidermeye yardımcı olur.

Bu mekanizmalar, yeni tehditler ortaya çıktıkça ve teknoloji ilerledikçe sürekli olarak gelişmektedir. Öncelikli olarak amaç, kullanıcıları ve verileri çeşitli güvenlik tehditlerinden korurken modern bağlantının taleplerini karşılayabilen dayanıklı ve güvenli bir 5G ağ ortamı oluşturmaktır.

5G GÜVENLİK MİMARİSİNE GENEL BAKIŞ

Yüksek veri hızına sahip heterojen ağlarda çeşitli sektörlerden (akıllı ev, akıllı şehirler, otonom araçlar, teletıp..vb) yeni uygulamaları destekleyen 5G ağları, yüksek hizmet kalitesi (QoS) ve denetim kalitesi (QoE) sağlarken güvenlik mimarisi önem kazanmaktadır. Bu aşamada 5G güvenlik mimarisinin temel alanları ağ erişim güvenliği ile kullanıcı ve uygulama etki alanları güveliği olarak karşımıza çıkmaktadır.

Ağ Erişim Güvenliği

3GPP (3rd Generation Partnership Project) erişim ağları ve 3GPP olmayan erişim ağları dahil olmak üzere bir UE(kullanıcı ekipmanı)'nın ağ üzerinden güvenli bir şekilde kimlik doğrulamasını ve hizmetlere erişmesini sağlayan bir dizi güvenlik parametresine olan bu yapı tüm radio ara yüzlerindeki saldırılara karşı koruma sağlar[7].

Ağ Etki Alanı ve Kullanıcı Etki Alanı Güvenliği

Kullanıcı düzlemi (UP) ve kontrol düzlemi (CP) ağ düğüm verilerinin güvenli şekilde değiş tokuş edilmesini sağlayan ağ etki alanı güvenliği ile kullanıcının mobil ekipmana (ME) erişimini güvenli tutan özelliklerdir[7].

Uygulama Etki Alanı Güvenliği

Kullanıcı etki alanında ve uygulama sağlayıcı etki alanında yer alan uygulamaların güvenli bir biçimde mesaj iletimi ve alımı yapmasını sağlayan güvenlik özellikleridir.

https://doi.org/10.56038/oprd.v5i1.599

Güvenliğin Yapılandırılması

Bir UE'de güvenlik ayarlarının yapılandırılması ve kullanıcının kimlik doğrulama olmadan evrensel abone kimlik modülüne erişim izni verilmesi veya verilememesini sağlayan bir dizi özelliktir.

5G çekirdek ağ ile birlikte (CN) 5G radyo erişim ağının (RAN) 128 bit uzunluğunda anahtarlara sahip erişim tabakası (AS) ve erişim dışı tabaka(NAS) koruması için şifreleme ve koruma algoritmalarının kullanımına izin verilir ve network arayüzleri ise 256 bit uzunluğundaki anahtarların taşşınmasını desteklemektedir. Ayrıca gizlilik ve gizlilik için gereksinimler ile bütünlük koruması, mimarinin farklı bileşenlerinde veri şifreleme ve son kullanıcı gizliliği özellikle önem taşımaktadır. Ayrıca 5G ağında gizli baz istasyonları ile başlatılan gizli dinleme özelliği ile UE kimliğini 5G ağına bildirmeden tanımlamaya imkan sağlayan geçici UE kimliği ile güvenlik sağlanmaktadır[7].

5G VARYANTLARININ GÜVENLİĞİ İLE İLGİLİ SPESİFİKASYONLAR

5G ağları için güvenlik özellikleri, öncelikle farklı 5G varyantları arasında güvenliğin çeşitli yönlerini özetleyen 3. Nesil Ortaklık Projesi (3GPP) tarafından tanımlanır. Özellikler, 5G sisteminin farklı bileşenleri ve işlevleri için çeşitli güvenlik gereksinimlerini ele alır. 3GPP TS 33.501, 5G sistemindeki güvenlik için birincil teknik özelliktir. 5G ağları için güvenlik mimarisini, ilkelerini ve mekanizmalarını özetler. Bu belge, kimlik doğrulama, şifreleme ve bütünlük koruması gibi güvenlik yönleri hakkında ayrıntılar içerir.

5G NSA, gelişmiş performans için eklenen 5G Yeni Radyo (NR) ile mevcut 4G LTE altyapısını kullanır ve belirli kontrol düzlemi işlevleri ve güvenlik için 4G LTE güvenilirdir. NSA, 4G LTE'den birçok güvenlik özelliğini devralır, ancak özellikle yeni 5G NR arayüzleri ve prosedürleriyle ilgili olarak ek 5G güvenlik önlemlerini de entegre eder. 5G SA, mevcut 4G altyapısına bağlı olmayan tamamen 5G tabanlı bir ağdır. Yeni güvenlik mekanizmaları ve mimari öğeler sunar.

Kullanıcı Ekipmanı (UE) ile ağ arasında gelişmiş karşılıklı kimlik doğrulama için iyileştirilmiş AKA prosedürleri. - Hem kontrol hem de kullanıcı düzlemlerinde sinyal ve kullanıcı verilerini güvence altına almak için gelişmiş algoritmalardır.

Farklı ağ dilimlerinin izolasyonunu ve güvenliğini sağlayan mekanizmalar, dilim başına özelleştirilmiş güvenlik politikalarına izin verir.

B. Anahtar güvenlik bileşenleri

https://doi.org/10.56038/oprd.v5i1.599

Kimlik Doğrulama: 5G-AKA (Kimlik Doğrulama ve Anahtar Anlaşması) Karşılıklı kimlik doğrulama ve anahtar değişimi için geliştirilmiş mekanizmalar içeren, 4G LTE'de kullanılan AKA prosedürünün geliştirilmiş bir sürümüdür. EAP-AKA (Genişletilebilir Kimlik Doğrulama Protokolü) ise 3GPP olmayan erişim ağları gibi bazı senaryolarda kimlik doğrulama için kullanılan bir uzantıdır.

Şifrelerme-Algoritma Desteği: 5G, değişen anahtar uzunluklarına sahip AES (Gelişmiş Şifreleme Standardı) dahil olmak üzere gelişmiş şifreleme algoritmalarını destekler. Kullanıcı verileri ve sinyal mesajları için güçlü koruma sağlar.

Şifreleme Anahtarları: Hem kullanıcı düzlemi (veri) hem de kontrol düzlemi (sinyal) dahil olmak üzere ağ üzerinden iletilen verileri korumak için dinamik anahtar yönetimi sağlar.

Bütünlük Koruması-Sinyal Bütünlüğü: UE ile ağ arasında değiştirilen sinyal mesajlarının bütünlüğünü sağlayarak kurcalamayı ve yetkisiz değişiklikleri önler.

Kullanıcı Veri Bütünlüğü: Ağ üzerinden iletilen kullanıcı verilerinin yetkisiz değişikliklere veya bozulmasına karşı koruma.

Ağ Dilimleme-İzolasyon: Farklı ağ dilimlerini izole etmek için mekanizmalar sağlar ve bir dilimin güvenliğinin diğerlerini etkilememesini sağlar.

Özelleştirilmiş Güvenlik: Her ağ dilimi, desteklediği hizmetlerin özel gereksinimlerine göre uyarlanmış kendi güvenlik politikalarına sahip olabilir.

Güvenli Arayüzler-API Güvenliği: Ağ işlevleri arasındaki iletişim için kullanılan arayüzlerin ve API'lerin yetkisiz erişime ve olası saldırılara karşı güvence altına alınmasını sağlar.

SEPP (Güvenlik Kenarı Koruma Proxy'si): Farklı operatörlerin ağları arasındaki sinyal trafiğini koruyarak operatörler arası güvenli iletişimi garanti eder[12].

NESNELERİN İNTERNETİ (İOT)

Nesnelerin İnterneti (IoT - Internet of Things), fiziksel nesnelerin internet aracılığıyla birbirleriyle ve diğer sistemlerle iletişim kurmasına olanak tanıyan bir ağdır. Bu ağ, genellikle sensörler, yazılım, işlemciler ve diğer teknolojileri barındıran cihazlardan oluşur. IoT, günlük yaşamdan endüstriyel uygulamalara kadar geniş bir yelpazede kullanılır ve cihazların daha akıllı, daha otonom ve daha verimli hale gelmesine yardımcı olur.

IoT'nin Bilimsel Temeli ve Bileşenleri

"IoT, çeşitli cihazların sensörler aracılığıyla topladığı verilerin internet üzerinden bulut sunucularına aktarılması ve bu verilerin işlenip kullanıcılara anlamlı bilgiler olarak

https://doi.org/10.56038/oprd.v5i1.599

sunulması ile çalışır. Bu sistem, nesnelerin birbirleriyle iletişim kurabilmesini ve insan müdahalesine ihtiyaç duymadan otomatik olarak veri işlemelerini mümkün kılar[13].

Sensörler ve Aktüatörler:

IoT'nin temel bileşenlerinden biri sensörlerdir. Sensörler, fiziksel çevredeki sıcaklık, nem, basınç gibi verileri toplar. Aktüatörler ise topladıkları bu veriler ışığında hareket eden mekanizmalardır. Örneğin, bir sıcaklık sensörü odanın sıcaklığını ölçer ve aktüatörler bu sıcaklığa göre ısıtma sistemini açar veya kapatır.

TABLO1. 5G GÜVENLİĞİ İLE İLGİLİ TEMEL GEREKSİNİMLER[7]

Gereksinimler	**Açıklama**
Abonelik Kimlik Doğrulaması	Hizmet veren ağ, UE ve ağ arasındaki kimlik doğrulama ve anahtar sürecinde Abonelik Kalıcı Tanımlayıcını(SUPI) doğrular.
Ağ Kimlik doğrulaması	UE, örtük anahtar kimlik doğrulaması aracılığıyla hizmet veren ağ tanımlayıcısının kimliğini doğrular.
UE Yetkilendirmesi	Hizmet veren ağ, abonelik profili aracılığıyla UE'yi (SUPI tarafından) yetkilendirir.
Home Network tarafından ağ yetkilendirmesi sunma	Bir hizmet ağına bağlı olan UE, home network tarafından da yetkilendirilir.
Erişim Ağı Yetkilendirilmesi	Erişim şebekesi, UE'ye hizmet sunmadan önce hizmet veren şebeke tarafından yetkilendirilmelidir.

Bağlantı (Connectivity): IoT cihazları, toplanan verileri birbirlerine ve merkezi sistemlere iletmek için kablolu veya kablosuz ağları kullanır. En yaygın kullanılan kablosuz iletişim protokolleri arasında Wi-Fi, Bluetooth, Zigbee, ve daha düşük enerji tüketen LoRa ve NB-IoT (Dar Bant IoT) yer alır.

Veri İşleme (Data Processing): Toplanan verilerin işlenmesi, IoT'nin ana amaçlarından biridir. Bu işlem yerel olarak cihazın içinde (edge computing) veya bulut tabanlı bir sistemde gerçekleştirilebilir. Veri işleme, ham veriyi anlamlı bilgilere dönüştürmeyi sağlar. Bu bilgiler daha sonra bir karar mekanizması için kullanılır.

Kullanıcı Arayüzü (User Interface): IoT sistemleri, kullanıcıların cihazlarla etkileşime girmesi için bir arayüze ihtiyaç duyar. Bu arayüzler genellikle mobil uygulamalar, web siteleri veya belirli kontrol panelleri şeklinde olabilir.

IoT'nin Bilimsel İlkeleri ve Teknolojileri

https://doi.org/10.56038/oprd.v5i1.599

Kablosuz İletişim Teknolojileri: IoT'nin ana bilimsel ilkesi, cihazlar arasındaki kesintisiz veri alışverişidir. Bunu sağlamak için çeşitli kablosuz iletişim teknolojileri kullanılır. Wi-Fi ve Bluetooth gibi kısa mesafeli teknolojilerden, 5G ve LoRa gibi daha geniş alan kapsama alanına sahip olan teknolojilere kadar birçok farklı iletişim standardı IoT'ye entegre edilebilir.
Bulut Bilişim (Cloud Computing): IoT cihazlarından elde edilen veriler, genellikle merkezi bir sistemde depolanır ve analiz edilir. Bulut bilişim, bu verilerin depolanması, işlenmesi ve analiz edilmesi için güçlü bir altyapı sunar. Böylece IoT cihazlarının sınırlı işlem gücü ve depolama kapasitesi aşılmış olur.

Edge Bilişim (Edge Computing): IoT cihazlarının veriyi yerel olarak işlemeye başlamasıyla, merkezi sistemlerdeki yük azaltılmış olur. Edge bilişim, verinin cihazın bulunduğu yerde işlenmesine olanak tanır. Örneğin, bir güvenlik kamerası, sürekli olarak buluta veri göndermek yerine, belirli kritik durumlarda (örneğin, hareket algılandığında) veri göndermeyi seçebilir.

Makine Öğrenmesi ve Yapay Zeka (AI): IoT cihazlarından elde edilen büyük miktardaki veri, makine öğrenmesi algoritmaları ile analiz edilir ve bu verilerden anlamlı çıkarımlar yapılır. Örneğin, bir üretim hattındaki sensörlerden gelen veriler, makine öğrenmesi algoritmaları ile analiz edilerek, arıza oluşmadan önce önleyici bakım yapılması sağlanabilir.
Gelecekte, 5G teknolojisi ile birlikte IoT cihazlarının bağlantı hızları ve kapasitesi önemli ölçüde artacaktır. Bu, daha fazla cihazın anlık veri iletimini mümkün kılacak ve akıllı şehirler, otonom araçlar ve endüstriyel otomasyon gibi alanlarda daha geniş uygulama alanları yaratacaktır."[14].

5G VE IOT UYGULAMALARINDA YENI NESIL GÜVENLIK TEHDITLERI

5G'nin getirdiği yüksek hız, düşük gecikme süresi ve geniş bağlantı kapasitesi sayesinde IoT cihazlarının yaygınlaşmasıyla daha kritik hale gelmiştir. IoT (Nesnelerin İnterneti) cihazlarının sayısındaki bu büyük artış, siber güvenlik tehditlerinin de genişlemesine neden olmuştur.
DDoS (Distributed Denial of Service) Saldırıları
5G ağları, düşük gecikme süresi ve yüksek kapasiteyle aynı anda milyarlarca cihazın bağlanmasına olanak tanır. Bu geniş cihaz ekosistemi, DDoS saldırıları için büyük bir potansiyel tehlike yaratır. IoT cihazları genellikle düşük güvenlik seviyelerine sahip

https://doi.org/10.56038/oprd.v5i1.599

olduğundan, kötü niyetli aktörler bu cihazları ele geçirip bir botnet oluşturabilir ve bu botnet'leri DDoS saldırıları başlatmak için kullanabilir. Saldırganlar, aynı anda çok sayıda cihazı hedefe yönlendirerek, hizmet kesintilerine ve büyük çaplı ağ çöküşlerine neden olabilir. Örneğin, Mirai botnet saldırısı, IoT cihazlarını ele geçirerek internet hizmet sağlayıcılarını ve büyük web sitelerini etkileyen devasa bir DDoS saldırısı düzenlemiştir.

5G'nin düşük gecikme süresi, IoT cihazlarının daha hızlı yanıt vermesini sağlarken, aynı zamanda dağıtık hizmet reddi (DDoS) saldırılarını daha güçlü hale getirebilir. Bu saldırılar, 5G'nin bant genişliğini kullanarak IoT cihazlarını aşırı yükleyebilir ve hizmet kesintilerine neden olabilir.[15].
Neden Tehlikelidir?
Milyarlarca Bağlı Cihaz: 5G'nin sağladığı yüksek kapasite, daha fazla IoT cihazını birbirine bağladığından, saldırı yüzeyi genişlemiştir.
Zayıf Güvenlik: Birçok IoT cihazı güvenlik protokollerinden yoksundur, bu da DDoS saldırılarının başarı oranını artırır.
Kesinti ve Finansal Kayıplar: DDoS saldırıları, ağ hizmetlerini kesintiye uğratarak önemli iş ve veri kayıplarına yol açabilir.
Botnet Saldırıları
5G, IoT cihazlarının sürekli bağlantıda kalmasını sağladığı için, saldırganlar bu cihazları kolayca ele geçirip bir botnet ağı kurabilir. Botnet'ler, çeşitli IoT cihazlarını kontrol eden büyük ağlardır ve saldırganlar tarafından spam gönderimi, veri hırsızlığı veya daha geniş çaplı DDoS saldırıları gibi siber suç faaliyetlerinde kullanılabilir. Özellikle zayıf güvenlik önlemleri olan akıllı cihazlar (akıllı ev sistemleri, güvenlik kameraları, sağlık cihazları vb.) bu tip saldırılara karşı savunmasızdır. Örneğin bir saldırgan, evde kullanılan IoT cihazlarının (akıllı termostatlar, güvenlik kameraları, akıllı buzdolapları) kontrolünü ele geçirip, bu cihazları bir botnet'e ekleyerek geniş çaplı saldırılar düzenleyebilir.

Man-in-the-Middle (MitM) Saldırıları
IoT cihazları, 5G ağları üzerinden veri iletişimi yaparken MitM saldırıları riski altındadır. Bu saldırı türünde, bir saldırgan iki cihaz arasındaki veri akışını gizlice izleyip manipüle edebilir. IoT cihazları, verileri genellikle şifrelemeden gönderdikleri için, saldırganlar bu

https://doi.org/10.56038/oprd.v5i1.599

verilere kolayca erişebilir. Özellikle hassas veriler (sağlık bilgileri, finansal veriler, güvenlik sistemleri bilgileri) bu tür saldırılar sonucunda çalınabilir veya değiştirilebilir.

Neden Tehlikelidir?

Zayıf Şifreleme: Birçok IoT cihazı, veri aktarımı sırasında yeterli şifreleme kullanmaz, bu da saldırganların iletişim kanallarına sızmasını kolaylaştırır.
Kritik Verilerin Çalınması: MitM saldırıları, IoT cihazları arasında geçen hassas bilgilerin çalınmasına yol açabilir.
Yetersiz Güncelleme ve Güvenlik Yamaları
IoT cihazlarının büyük bir kısmı, güvenlik güncellemelerini ve yamalarını düzenli olarak alamaz. 5G'nin IoT ağlarını genişletmesiyle birlikte, bu cihazların birçoğu güncel güvenlik önlemlerinden yoksun kalabilir. Yazılım açıkları, IoT cihazlarının uzun süre savunmasız kalmasına neden olabilir ve bu da saldırganların cihazlara sızmasını kolaylaştırır.
Örneğin bir ev güvenlik kamerası veya sağlık izleme cihazı, güncelleme almadığında eski ve savunmasız yazılımlara sahip olabilir. Saldırganlar bu güvenlik açıklarını kullanarak cihazın kontrolünü ele geçirebilir.
Yan Kanal Saldırıları
Yan kanal saldırıları, IoT cihazlarının donanımsal zayıflıklarından yararlanarak gerçekleştirilir. 5G bağlantısıyla bu cihazların sayısındaki artış, yan kanal saldırılarına olanak tanır. Bu saldırı türünde, cihazın güç tüketimi, elektromanyetik yayılımı gibi fiziksel yan etkiler izlenerek gizli bilgilere erişim sağlanır. IoT cihazları genellikle düşük maliyetli donanımlarla üretildiği için bu tür saldırılara karşı savunmasız olabilir.
Veri Gizliliği İhlalleri
5G'nin sağladığı geniş bant bağlantısı, IoT cihazlarının sürekli veri iletimi yapmasına olanak tanır. Bu, özellikle kullanıcı gizliliği açısından büyük bir tehdit oluşturabilir. IoT cihazları, kullanıcının özel bilgilerini (lokasyon verisi, sağlık bilgileri, ev içi aktiviteler vb.) sürekli olarak toplar ve iletir. Eğer bu veriler şifrelenmez veya güvenli bir şekilde saklanmazsa, saldırganlar tarafından ele geçirilebilir ve kullanıcıların mahremiyetini ihlal edebilir.
Örneğin Bir akıllı ev cihazı (akıllı hoparlör, termostat vb.), kullanıcının evde olup olmadığını, evdeki aktiviteleri sürekli olarak izleyip bu bilgileri paylaşabilir. Saldırganlar bu verilere sızarak kullanıcının özel hayatını izleyebilir veya kötü amaçlı kullanabilir.

https://doi.org/10.56038/oprd.v5i1.599

Zararlı Yazılım (Malware) ve Ransomware Tehditleri

IoT cihazları, genellikle sınırlı güvenlik önlemlerine sahip olduğundan, kötü amaçlı yazılımlar bu cihazlara kolayca bulaşabilir. 5G ile daha geniş çapta bağlı cihaz ekosistemi, kötü niyetli yazılım geliştirenler için yeni fırsatlar yaratır. Özellikle fidye yazılımları (ransomware) IoT cihazlarına bulaştırılarak, cihazın veya verinin kilitlenmesine ve kullanıcının fidye ödemeye zorlanmasına neden olabilir. Örneğin Bir sağlık izleme cihazı veya endüstriyel IoT cihazı, fidye yazılımı ile hedeflenebilir ve kritik verilere erişim durdurulabilir. Kullanıcıdan veya şirketteki IT ekibinden cihazı geri almak için fidye talep edilebilir.

Sonuç olarak 5G'nin sunduğu yüksek kapasite ve hız avantajları, IoT uygulamalarının genişlemesini sağlarken, bu cihazların güvenlik tehditlerine açık olmasını da beraberinde getiriyor. DDoS, botnet saldırıları, MitM saldırıları gibi yeni nesil tehditler, IoT cihazlarının güvenliğini riske atıyor. Bu nedenle, IoT ekosisteminde güvenliği artırmak için ileri seviye kimlik doğrulama, şifreleme teknikleri ve düzenli güvenlik güncellemeleri kritik öneme sahiptir.

IoT EKOSISTEMINDE GÜVENLIĞI ARTIRMAK İÇİN KULLANILABİLECEK TEKNİKLER

Gelişmiş Kimlik Doğrulama ve Yetkilendirme

IoT cihazlarının kimliklerinin doğrulanması ve ağa yetkili olarak erişim sağlamaları, güvenliğin ilk adımıdır. Gelişmiş kimlik doğrulama ve yetkilendirme teknikleri, yetkisiz erişimlerin önlenmesine yardımcı olur.

IoT cihazlarının kimlik doğrulama süreçleri, sahte cihazların ağa sızmasını ve güvenlik açıklarını kullanmasını engeller. Bu da ağ güvenliğini önemli ölçüde artırır.

5G AKA (Authentication and Key Agreement): Bu, 5G ağlarında kimlik doğrulama ve anahtar yönetimini sağlayan gelişmiş bir mekanizmadır. Hem IoT cihazının kimliğini doğrular hem de ağ bileşenlerinin güvenliğini sağlar. Bu sayede sahte cihazların veya yetkisiz erişimlerin önüne geçilir.

EAP-AKA (Extensible Authentication Protocol): 5G'ye özel olmayan ağlarda kullanılabilen bu kimlik doğrulama protokolü, IoT cihazlarının güvenliğini sağlamak için farklı kimlik doğrulama yöntemleri sunar.

Uçtan Uca Şifreleme (End-to-End Encryption)

IoT cihazları tarafından üretilen ve iletilen verilerin güvenli bir şekilde korunması için uçtan uca şifreleme hayati bir öneme sahiptir. Bu sayede, veriler cihazdan sunucuya veya

https://doi.org/10.56038/oprd.v5i1.599

diğer cihazlara iletilirken herhangi bir üçüncü tarafın verileri okuması veya değiştirmesi engellenir.
IoT cihazları çoğu zaman hassas veriler (sağlık bilgileri, finansal veriler vb.) ilettiği için bu verilerin şifrelenmesi, saldırganların veri çalmasını veya manipüle etmesini önlemek açısından önemlidir.

AES (Advanced Encryption Standard): 5G ağlarında kullanılan AES, IoT cihazları arasında iletilen verilerin güçlü bir şekilde şifrelenmesini sağlar. Verinin hem cihaz içinde hem de cihazlar arasında iletilirken korunmasına olanak tanır.
TLS (Transport Layer Security): IoT cihazları ve sunucuları arasındaki iletişimin güvenliğini sağlamak için kullanılır. Verilerin aktarımı sırasında şifreleme yaparak gizliliği ve bütünlüğü sağlar.

Ağ Dilimleme (Network Slicing)
5G ağlarındaki ağ dilimleme, aynı fiziksel altyapıyı paylaşan ancak birbirinden bağımsız sanal ağların oluşturulmasına olanak tanır. IoT cihazları için özel dilimlerin oluşturulması, bu cihazların diğer ağlardaki olası tehditlerden izole edilmesini sağlar.
Bu, IoT cihazlarının birbirlerinden izole edilmesini ve bir dilimde meydana gelen bir güvenlik ihlalinin diğer dilimleri etkilemesini önler.
IoT için Özel Ağ Dilimleri: IoT cihazları için oluşturulan dilimler, bu cihazların güvenlik ihtiyaçlarına göre özelleştirilmiş güvenlik politikalarına sahip olabilir. Örneğin, sağlık uygulamaları için yüksek güvenlikli bir dilim, enerji sektöründeki cihazlar için ise düşük gecikmeli ve yüksek güvenilirlikli bir dilim oluşturulabilir.
IoT Cihazları İçin Güvenli Yazılım Güncellemeleri
IoT cihazları, zaman içinde güvenlik yamaları ve yazılım güncellemeleri almalıdır. Ancak bu süreç genellikle güvenlik tehditlerine karşı savunmasız olabilir. Güvenli yazılım güncellemeleri, IoT cihazlarının güvenlik açıklarını kapatmanın yanı sıra, yeni tehditlere karşı dayanıklı olmasını sağlar.
Cihazların güncel güvenlik yamalarını almaması, eski yazılımlar üzerindeki zayıf noktaların saldırganlar
tarafından suistimal edilmesine yol açabilir. Güvenli güncelleme süreçleri, bu riskleri en aza indirir.

https://doi.org/10.56038/oprd.v5i1.599

OTA (Over-the-Air) Güncellemeler: OTA (Over-the- Air) yazılım güncellemeleri, IoT cihazları için güvenlik yamalarının ve yeni özelliklerin hızlıca uygulanmasına olanak tanır. Güncellemeler şifrelenir ve cihazın yetkili bir kaynaktan geldiğini doğrulamak için dijital imza ile doğrulanır[16].
İmza Tabanlı Güncellemeler: Yazılım güncellemeleri, cihaz üreticileri tarafından imzalanarak güvenilirlik doğrulanır. Bu, yalnızca yetkili yazılımların cihazda çalışmasını sağlar.

IoT için Anomali Tespit Sistemleri
IoT cihazlarından gelen veri ve trafik hareketlerinin sürekli izlenmesi, güvenlik açıklarını tespit etmek için önemlidir. Anomali tespit sistemleri, IoT cihazlarında şüpheli davranışları ve olası saldırıları tespit ederek hızlı müdahale sağlar.
Anomali tespiti, özellikle geniş çaplı IoT ağlarında güvenlik açıklarını gerçek zamanlı olarak tespit etmek ve saldırganların izinsiz girişlerini engellemek için kritik bir araçtır.

Makine Öğrenimi Tabanlı Anomali Tespiti: IoT cihazlarından gelen veri akışlarını öğrenen sistemler, normal trafik davranışlarını analiz eder ve anormal aktiviteleri tespit eder. Bu sayede olası siber saldırılara erken müdahale edilebilir.
Gerçek Zamanlı İzleme: IoT cihazlarının sürekli izlenmesi, anormal trafik veya cihaz davranışlarının hızlıca tespit edilmesini sağlar. Böylece, saldırılar cihazlara veya ağa zarar vermeden önce engellenebilir.
Fiziksel Katman Güvenliği
IoT cihazları çoğunlukla düşük güçlü ve sınırlı donanım kaynaklarına sahip olduğundan, saldırganlar bu cihazların donanımlarına yönelik fiziksel saldırılar gerçekleştirebilir. Fiziksel katman güvenliği, IoT cihazlarının donanımsal saldırılara karşı korunmasını sağlar.
IoT cihazlarının fiziksel güvenliği, özellikle akıllı şehirler, sağlık sistemleri ve endüstriyel otomasyon gibi kritik uygulamalarda güvenliğin sağlanması için önemlidir.

WBPLSec (Wireless Physical Layer Security): Fiziksel katman güvenliği (WBPLSec), IoT cihazlarının donanımsal zayıflıklarından yararlanarak yapılan saldırılara karşı koruma sağlar. Bu yöntem, IoT cihazlarının daha düşük enerji tüketimi ile güvenli iletişim sağlamasına olanak tanır[17].
Veri Gizliliği ve Anonimleştirme Teknikleri

https://doi.org/10.56038/oprd.v5i1.599

IoT cihazları sürekli veri toplar ve bu verilerin birçoğu kullanıcıya ait hassas bilgileri içerir. Bu yüzden veri gizliliği IoT ekosisteminde önemli bir unsurdur. Verilerin güvenliğini sağlamak için anonimleştirme ve takma ad kullanımı gibi teknikler uygulanabilir. Kullanıcı gizliliği, IoT ağlarının genişlemesiyle daha da önem kazanmıştır. Bu teknikler, kullanıcıların özel bilgilerinin kötüye kullanılmasını engeller.

Takma Adlandırma (Pseudonymization): Kullanıcı verilerini gizlemek için gerçek kimlik bilgileri yerine takma adlar kullanılır. Bu, verilerin izinsiz kişiler tarafından ele geçirilse bile kullanılamaz hale gelmesini sağlar.
Veri Anonimleştirme: IoT cihazları tarafından toplanan verilerin anonim hale getirilmesi, kişisel bilgilerin ifşa edilmesini önler.
Güvenli Ağ Protokolleri
IoT cihazları arasındaki iletişim için kullanılan ağ protokollerinin güvenliğini sağlamak, IoT ekosisteminin korunması için önemlidir. Güvenli ağ protokolleri, veri aktarımı sırasında üçüncü tarafların bu verileri ele geçirmesini veya manipüle etmesini önler.

Güvenli ağ protokolleri, IoT cihazlarının birbirleriyle veya sunucularla güvenli bir şekilde iletişim kurmasını sağlar. Bu sayede veri gizliliği ve bütünlüğü korunur.

DTLS (Datagram Transport Layer Security): IoT cihazları arasındaki veri iletimini güvence altına almak için kullanılan bir güvenlik protokolüdür. Güvenli veri iletimi sağlarken IoT cihazlarının düşük enerji tüketimini destekler.
CoAP (Constrained Application Protocol) Güvenliği: CoAP, kısıtlı kaynaklara sahip IoT cihazları için tasarlanmış bir uygulama katmanı protokolüdür. DTLS ile birlikte çalışarak veri iletiminin güvenliğini sağlar.

Sonuç olarak, IoT ekosistemindeki güvenliği sağlamak, 5G'nin sağladığı avantajlar ve getirdiği geniş cihaz ekosistemi göz önüne alındığında oldukça önemli hale gelmiştir. Gelişmiş kimlik doğrulama, uçtan uca şifreleme, ağ dilimleme, güvenli yazılım güncellemeleri ve anomali tespiti gibi güvenlik teknikleri, IoT cihazlarının hem ağ içinde hem de cihazlar arası güvenliğini sağlayarak IoT ekosistemini daha dayanıklı hale getirebilir.

https://doi.org/10.56038/oprd.v5i1.599

2. 5G ve IoT Güvenlik Stratejileri: Kuantum Kriptografiden Otonom Sistemlere Yönelik Çözümler

5G ve IoT'de Post-Kuantum Kriptografi

Kuantum bilgisayarlar, mevcut şifreleme algoritmalarını kırma kapasitesine sahiptir ve bu durum, özellikle 5G ve IoT ağları gibi büyük veri akışlarının bulunduğu sistemler için ciddi bir tehdit oluşturur. Post-kuantum kriptografi, kuantum saldırılarına dayanıklı yeni algoritmalar geliştirerek, 5G altyapısında IoT cihazlarının güvenliğini artırmayı amaçlar. IoT cihazlarının düşük işlem gücü ve enerji gereksinimleri göz önüne alındığında, bu cihazlar için optimize edilmiş post-kuantum çözümleri kritik önemdedir.

Post-kuantum kriptografi algoritmaları, mevcut asimetrik kriptografik yöntemlerin yerine geçerek kuantum bilgisayarların kırabileceği RSA ve ECC gibi algoritmaların yerini almaktadır. Özellikle IoT cihazlarının düşük enerji ve işlem gücü gereksinimlerine uygun hale getirilmiş post- kuantum algoritmaların, güvenlik açısından hayati bir role sahip olması beklenmektedir[18].

Zero Trust Architecture (Sıfır Güven Mimarisi) ve IoT Güvenliği

Zero Trust mimarisi, tüm cihazların sürekli olarak kimlik doğrulamasına tabi tutulduğu bir güvenlik modeli sunar. IoT ağlarında cihazların sayısının ve çeşitliliğinin artması, bu mimarinin uygulanmasını gerekli kılmaktadır. IoT cihazları genellikle güvenlik açısından zayıf halkalar oluşturur ve bu cihazlar ağa bağlanmadan önce kimlik doğrulama süreçlerinden geçmelidir.

5G ve IoT Uygulamalarında MEC (Mobile Edge Computing) Güvenliği

MEC (Mobile Edge Computing), verilerin IoT cihazlarına daha yakın bir noktada işlenmesini sağlar ve bu sayede gecikme sürelerini minimize eder. Ancak, bu verilerin yerel sunuculara taşınması, yeni güvenlik açıkları yaratabilir. MEC altyapısında, IoT cihazlarının ve verilerin korunması için uçtan uca şifreleme, güvenli erişim protokolleri ve güçlü kimlik doğrulama yöntemleri gereklidir. Bu model, verilerin yalnızca güvenilir bölgelerde işlendiğinden emin olunmasını sağlayarak, IoT güvenliğini artırır.

Otonom Sistemler ve 5G IoT Güvenliği

Otonom sistemler, düşük gecikme süreleri ve yüksek bant genişliği gerektiren uygulamalardır. 5G'nin sağladığı bu avantajlar, otonom araçlar ve endüstriyel robotlar gibi sistemlerin geniş çaplı IoT ağlarına entegrasyonunu mümkün kılmaktadır. Ancak, bu tür sistemlerin güvenliğini sağlamak kritik öneme sahiptir. Otonom sistemlerde

https://doi.org/10.56038/oprd.v5i1.599

güvenlik ihlalleri ciddi fiziksel ve mali sonuçlar doğurabilir. Bu nedenle, uçtan uca güvenlik önlemleri bu sistemler için kaçınılmazdır.

Yasal Düzenlemeler ve IoT Güvenliği (GDPR, HIPAA)

IoT ağlarında veri güvenliği, kullanıcıların mahremiyetini koruma sorumluluğunu da beraberinde getirir. Avrupa'da GDPR ve ABD'de HIPAA gibi düzenlemeler, 5G ile IoT sistemlerinin veri güvenliğine uyum sağlamasını zorunlu kılmaktadır. Bu düzenlemeler, verilerin işlenmesi ve saklanması sırasında kişisel bilgilerin izinsiz erişimden korunmasını amaçlamaktadır.

GDPR ve HIPAA gibi düzenlemeler, IoT ağları üzerinde toplanan verilerin güvenli bir şekilde saklanması ve işlenmesi için gereklilikler sunar. Bu yasal çerçeveler, kişisel verilerin korunması ve ihlallerin önlenmesi açısından önemlidir[19].

3. Yorum ve Çıkarımlar

5G kablosuz ağlar, kullanılan çeşitli teknolojiler ve kullanım senaryolarıyla birlikte karmaşık bir ekosistem oluşturur ve bu durum, geliştirilmiş performans, esneklik ve kişiselleştirme gibi yeni fırsatlar sunar. Toplumların dijital dönüşümündeki rolü nedeniyle, bu ağların güvenilirliği ve güvenilirliği, kabul, dağıtım ve işletme süreçlerinde kritik öneme sahiptir. Güvenlik mimarisinin tüm güvenlik çerçevesindeki tek bir unsur olduğunu göz önünde bulundurarak, 5G güvenlik mimarisinin ana özelliklerini kısaca açıklanmıştır. Ağların güvenlik ve gizliliği hala gelişim aşamasında olduğundan, ele alınması gereken konular bu çalışmada açıklanmıştır. Böylece, 5G güvenlik prosedürleri ve mekanizmalarının gerekli iyileştirmelerini sağlamak amacıyla, karşılaşılacak zorlukları tanımlanıp çözüm önerileri geliştirilmelidir. Mevcut güvenlik sorunlarını çözmeyi hedefleyen teknolojilerin getirdiği yeni olasılıkları da göz önünde bulundurarak bu alanda devam eden çalışmalar önem arz etmektedir. 5G teknolojisi küresel bir altyapı haline geldikçe, kablosuz iletişimlerin dayanıklılığını, güvenilirliğini ve gizliliğini garanti altına almak için gecikmeyi en aza indirmeye ve sağlam güvenlik önlemleri uygulamaya odaklanmak esastır. Bu çalışmada, 5G güvenlik mekanizmaları üzerine bir dizi araştırma çalışması incelenmiş olup, 5G güvenlik protokollerini geliştirmek için en güvenilir yöntem olarak kablosuz fiziksel büyük tanımlama yapılması gerektiği sonucuna varılmıştır. Sonuç olarak fiziksel katman güvenliğinin teknik zorlukları ve uygulama durumları incelenerek fiziksel katman güvenliğinin mimari, teknoloji ve kullanılabilirlik açılarından geliştirilmesine yönelik öneriler sunulmaktadır.

https://doi.org/10.56038/oprd.v5i1.599

Sonuç olarak, 5G'nin sunduğu yüksek kapasite ve hız avantajları, IoT uygulamalarının genişlemesini sağlarken, bu cihazların güvenlik tehditlerine açık olmasını da beraberinde getiriyor. DDoS, botnet saldırıları, MitM saldırıları gibi yeni nesil tehditler, IoT cihazlarının güvenliğini riske atıyor. Bu nedenle, IoT ekosisteminde güvenliği artırmak için ileri seviye kimlik doğrulama, şifreleme teknikleri ve düzenli güvenlik güncellemeleri kritik öneme sahiptir. IoT ekosistemindeki güvenliği sağlamak, 5G'nin sağladığı avantajlar ve getirdiği geniş cihaz ekosistemi göz önüne alındığında oldukça önemli hale gelmiştir. Gelişmiş kimlik doğrulama, uçtan uca şifreleme, ağ dilimleme, güvenli yazılım güncellemeleri ve anomali tespiti gibi güvenlik teknikleri, IoT cihazlarının hem ağ içinde hem de cihazlar arası güvenliğini sağlayarak IoT ekosistemini daha dayanıklı hale getirebilir.

5G ve IoT ekosistemlerinin genişlemesi, beraberinde yeni nesil güvenlik tehditlerini getirmiştir. Bu çalışmada, DDoS ve MitM gibi klasik saldırıların yanı sıra, botnet saldırıları ve veri gizliliği ihlalleri gibi yeni tehditlerin ortaya çıktığı vurgulanmıştır. 5G altyapısında, post-kuantum kriptografi, uçtan uca şifreleme, gelişmiş kimlik doğrulama ve ağ dilimleme gibi güvenlik çözümleri, IoT cihazlarının güvenliğini sağlamada kritik öneme sahiptir. Ayrıca, MEC (Mobile Edge Computing) ve SDN/NFV gibi teknolojiler, IoT verilerinin daha güvenli ve verimli bir şekilde işlenmesine olanak tanır. Otonom sistemler gibi kritik uygulamalarda, gecikme süresinin düşük tutulması ve güvenlik açıklarının minimize edilmesi için uçtan uca güvenlik protokolleri uygulanmalıdır. Sonuç olarak, 5G ve IoT ağlarının güvenliği için yasal düzenlemeler (GDPR, HIPAA) de göz önünde bulundurulmalı ve bu teknolojiler için sürekli güncellenen güvenlik çözümleri geliştirilmelidir. Gelişmiş güvenlik stratejilerinin uygulanması, 5G ekosisteminin daha dayanıklı ve güvenilir olmasını sağlayacaktır.

Referanslar

[1] Mechanisms," *2023 6th International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, India, 2023, pp. 1-4,2023.

[2] T. Sachdeva, S. Kumar, M. Diwakar, P. Singh, N. K. Pandey and S. Choudhary, "Comparative Analysis of 5G Security

[3] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, M. Ylianttila, "A Comprehensive Guide to 5G Security", Wiley, 2018.

[4] N. Ben Henda, "Overview on the Security in 5G Phase 2," in Journal of ICT Standardization, vol. 8, no. 1, pp. 1-14, 2020.
[5] J. Cao et al., "A Survey on Security Aspects for 3GPP 5G Networks," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 170-195, 2020.
[6] S. Qin and C. Lao, "Computer Network Security Defense System in 5G Era," 2022 International Conference on Artificial Intelligence of Things and Crowdsensing (AIoTCs), Nicosia, Cyprus, pp. 169-174, 2022.
[7] J. Lee, H. Kim, C. Park, Y. Kim and J. -G. Park, "AI-based Network Security Enhancement for 5G Industrial Internet of Things Environments," 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, pp. 971-975, 2022.
[8] M. Pejanović-Djurišić and S. Kuklinski, "5G Security Landscape: Concept and Remaining Challenges," 2022 30th Telecommunications Forum (TELFOR), Belgrade, Serbia, pp. 1-4, 2022.
[9] S. Xia et al., "Research on the Physical Layer Security for Industrial 5G Private Networks," 2023 IEEE 11th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, pp. 816-819, 2023.
[10] W. You, M. Xu and D. Zhou, "Research on security protection technology for 5G cloud network," 2021 International Conference on Advanced Computing and Endogenous Security, Nanjing, China, pp. 01-11, 2022.
[11] M. Pejanović-Djurišić and S. Kuklinski, "Enabling end-to-end security of networks with 5G segment," 2023 31st Telecommunications Forum (TELFOR), Belgrade, Serbia, pp. 1-4, 2023.
[12] X. Zhang, J. Fei, H. Jiang and X. Huang, "Research on Power 5G Business Security Architecture and Protection Technologies," 2021 6th International Conference on Power and Renewable Energy (ICPRE), Shanghai, China, pp. 913-917, 2021.
[13] Z. Zou, T. Chen, J. Chen, Y. Hou and R. Yang, "Research on Network Security Risk and Security Countermeasures of 5G Technology in Power System Application," 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, pp. 102-105, 2021.
[14] Ashton, K. (2009), "That 'Internet of Things' Thing"
[15] Khan et al. (2021), "5G and IoT: A New Era of Connectivity"
[16] Liu, Y. et al. (2020), "A Survey of DDoS Attacks in IoT and 5G Networks"
[17] J. Cao, et al., "A Survey on Security Aspects for 3GPP 5G Networks," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 170- 195, 2020
[18] S. Xia, et al., "Research on the Physical Layer Security for Industrial 5G Private Networks," 2023 IEEE 11th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 2023

https://doi.org/10.56038/oprd.v5i1.599

[19] M. Pejanović-Djurišić ve S. Kuklinski, "5G Security Landscape: Concept and Remaining Challenges," 30th Telecommunications Forum (TELFOR), Belgrad, Sırbistan, 2022

[20] Ben Henda, N. (2020). "Overview on the Security in 5G Phase 2," Journal of ICT Standardization, 8(1), 1-14.