DEÜ FMD 24(70), 111-131, 2022

Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi
Dokuz Eylul University Faculty of Engineering Journal of Science and Engineering

Basılı/Printed ISSN: 1302-9304. Elektronik/Online ISSN: 2547-958X

Bağlam-Duyarlı Rol-Tabanlı Erişim Denetiminin Çoklu-Etkileşimli Nesnelerin İnternetinde Uygulanması

Application of Context-aware Role-based Access Control on Internet of Things Applications with Multiple Interactions

Emrah Tomur [1*]

[1]Ericsson Araştırma Laboratuvarı, İzmir, TÜRKİYE
*Sorumlu Yazar / Corresponding Author **: emrah.tomur@ericsson.com

Geliş Tarihi / Received: 16.05.2021 *Araştırma Makalesi/Research Article*
Kabul Tarihi / Accepted: 22.09.2021 *DOI:10.21205/deufmd.2022247012*
Atıf şekli/ How to cite: TOMUR, E.(2022).Bağlam-Duyarlı Rol-Tabanlı Erişim Denetiminin Çoklu-Etkileşimli Nesnelerin İnternetinde Uygulanması.DEUFMD, 24(70), 111-131.

Öz

Bu makalede, Nesnelerin İnterneti (Nİ) uygulamaları için rol-tabanlı, bağlam bilgisi kullanan, uyarlanabilir çoklu seviyeli kimlik doğrulaması uygulanan, dinamik bir erişim kontrol yöntemi önerisinde bulunulmaktadır. Literatürdeki mevcut çalışmalar, çok sayıda ve farklı türde nesnenin (bilgisayar, makine, kişi, süreç, servis vb.) yoğun etkileşimini içeren Nİ uygulamaları için anlık bağlam bilgisini dikkate almayan ve baştan tanımlanmış statik erişim politikaları uygulayan güvenlik çözümleri sunmaktadır. Bunlar, Nİ'deki karmaşık etkileşimden doğabilecek, konvansiyonel ağlarda görülmeyen yeni tür güvenlik zafiyetlerini önlemede yetersiz kalmaktadır. Bu nedenle Nİ uygulamaları için nesnelerin birbiriyle etkileşimini dikkate alarak dinamik ve uyarlanabilir erişim denetimi sunan bir güvenlik yöntemi geliştirilmesi önemlidir. Bu makalede sunulan yöntem, bir Nİ sistemindeki varlıkları ve aralarındaki etkileşimi bir bağlam mimarisi modeli ile biçimlendirip anlık bağlam bilgisini erişim denetiminde kullanmakta, aynı zamanda rol-tabanlı yaklaşım ile güvenlik politikalarının mümkün olduğunca sade yazılabilmesini sağlamaktadır. Böylece, Nİ uygulamalarındaki kompleks etkileşimden doğabilecek, baştan tahmin edilmesi zor, anlık yetkisiz kullanım istekleri, önceden tanımlanan karmaşık olmayan erişim denetimi politikaları kullanılarak engellenebilecektir. Bu çalışmada, önerilen yeni erişim denetimi yöntemi ile çoklu ve karmaşık etkileşimli Nİ cihazlarının yer aldığı bir uygulama senaryosunda sade güvenlik politika kuralları ile olası saldırıların mevcut yöntemlere göre daha basit bir şekilde engellenebileceği gösterilmiştir. Bunun dışında, (i) çevre, kişi, zaman ve sistem dahil tüm bağlam türlerini içeren ve diğer bağlam-duyarlı Nİ uygulamalarında da kullanılabilecek bir bağlam modeli sunulmuş, (ii) çoklu ve karmaşık etkileşimli, bağlam-duyarlı Nİ uygulamalarında ortaya çıkabilecek saldırı/tehdit vektörleri belirlenmiş ve (iii) geliştirilen bağlam-duyarlı rol-tabanlı erişim kontrolü yöntemi yeni nesil Nİ uygulamalarını temsil eden karmaşık bir senaryo altında doğrulanmıştır.

Anahtar Kelimeler: *Nesnelerin İnterneti, Güvenlik, Erişim Denetimi, Rol-tabanlı erişim denetimi, Bağlam-duyarlı güvenlik, Bağlam-duyarlı erişim denetimi.*

Abstract

In this work, a context-aware role-based access control method with adaptive multi-level authentication is proposed addressing security of IoT applications and results of a proof of concept

implementation is presented. Security solutions that do not take instantaneous context information into account for IoT applications and that import static access policies used in conventional networks is insufficient to prevent security weaknesses of IoT networks, which involve intensive interaction of a large number of different types of things (computer, machine, person, process, service, etc.). This paper aims to model the interaction between the "things" in an IoT system in a contextual architecture and then to use this instantaneous context information in a role-based access control scheme enabling the security policies to be written as plain as possible. It is considered that, in this way, difficult to predict unauthorized usage requests that may arise from the complex interaction in IoT applications may be prevented by using predefined, uncomplicated access control policies.In this study, it is shown that the proposed new access control method is able to prevent attacks in an application scenario involving multiple and complex interactive IoT devices using simple security policy rules compared to the existing methods. Furthermore, (i) a context model is presented that covers all context types, including environment, user, time and system, and can be used in other context-sensitive IoT applications; (ii) attack/threat vectors that may arise in multiple and complex interactive, context-sensitive IoT applications are identified and (iii) the context-sensitive role-based access control method is validated under a scenario representing next generation IoT application with complex interactions.

Keywords: *Internet of Things, Security, Access Control, Role-based Access Control, Context-Aware Security*

1. Giriş

Kablosuz algılayıcı ağlar ve makineler arası iletişim teknolojilerinin ardından Nesnelerin İnterneti (Nİ) uygulamaları gün geçtikçe artmakta ve yakın gelecekte Nİ'nin daha ileri seviyede ve karmaşıklığı yüksek senaryolarda kullanılacağı öngörülmektedir. Buna bağlı olarak Nİ'deki güvenlik problemlerine ve bunların çözümlerine ilişkin çalışmalar da gün geçtikçe hızlanmaktadır. Bu çalışmalar arasında bağlam-duyarlı ve rol-tabanlı erişim denetiminin yeni nesil Nİ sistemleri için kullanımını öneren yaklaşımlar çok sınırlı sayıdadır. Literatürdeki mevcut bağlam-duyarlı erişim kontrolü çözümleri genellikle akıllı ev ya da akıllı sınıf gibi tekil kullanım senaryolarına yöneliktir ve ayrıca Nİ ile önemli etkileşimleri olan sosyal ağlar, bulut bilişim ve kitlesel kaynakları (crowd-sourcing) dikkate almamaktadır. Çoklu etkileşimli Nİ senaryolarını hedefleyen çalışmalarda ise temel olarak iki eksiklik ön plana çıkmaktadır: (1) önerilen bağlam ve güvenlik modellerinin karmaşık bir yapıya sahip olması nedeniyle uygulanmasının ve kullanımının zor olması, (2) önerilen erişim denetiminin yalnızca normal kullanım senaryosunda ya da konvansiyonel güvenlik tehditleri altında geçerlenmesi/test edilmesi. Literatürdeki bu mevcut çalışmalarda varlıkların etkileşiminden doğan bağlam bilgisinin saldırı için kullanılabileceği durumlar dikkate alınmamıştır.

Bizim çalışmamızın kapsamına alınan Nİ uygulamaları, birkaç cihazdan/sensörden toplanan verinin bilgilendirme/ölçme maksadıyla kullanıldığı akıllı ev/sınıf gibi tekil kullanımlı, basit etkileşimli uygulamalar değil; bilgisayar, makine, kişi, süreç, servis gibi farklı nitelikte varlığın bulut altyapısı, kitlesel kaynaklar ve sosyal platformlar üzerinden karmaşık ve çoklu etkileşimini içeren Nİ uygulamalarıdır. [1], makalemizin kapsamındaki Nİ modelini "collective computing" (müşterek bilişim) olarak tanımlamaktadır. [2] tarafından ortaya konulan ve üçüncü nesil bilişim olarak bilinen yaygın bilişim kavramının (ubiquitous computing), inch-foot-yard ölçeğindeki akıllı saat, akıllı telefon, PDA gibi cihazlar ile onlara sahip olan kişi arasında (1-many) bir etkileşimi tanımladığı bilinmektedir. Ancak, [1]'in müşterek bilişim olarak tanımladığı ve dördüncü nesil bilişim olarak da adlandırılan kavram ise, farklı bireylerin/cihazların birbirleriyle muhtemel (many-many) etkileşimini kapsamaktadır. Buna göre, geleceğin ileri düzey Nİ uygulamaları, ancak farklı ölçekteki ve mobilitedeki cihazın/varlığın sorunsuz entegrasyonu için kullanılan limitsiz hesaplama

ve saklama yeteneğine sahip bulut bilişim (cloud computing), bilgiye ulaşmak için kalabalığın/toplumun yardımını almaya yarayan kitlesel kaynaklar (crowd sourcing) ve fiziksel dünya ile dijital dünyanın etkileşimine dayanan siber fiziksel sistemlerin bütünleşik kullanımıyla gerçekleşebilecektir. Dolayısıyla [2]'de önerilen yaygın bilişim fenomeniyle modellenmesi mümkün değildir. Müşterek bilişim yaklaşımına göre geleceğin Nİ uygulamalarında kişilerin sağlık durumlarının takibi, üzerlerinde ve bulundukları her mekânda yer alan cihazlardan/sensörlerden toplanan bilgiler ile gerçek ya da sanal ortamda yaptıkları konuşma ya da yazışmalardan (kitlesel kaynak) veri analizi ile çıkarılan bilgilerin bulut bilişim alt yapısı üzerinden mevcut sağlık kayıtları da kullanılarak bütünleşik analizi ile gerçekleştirilir. Yaygın bilişimde ise sağlık takibine yönelik bir Nİ uygulamasında hastanın anlık sağlık değişiklikleri yalnızca hastaların üzerine yerleştirilen akıllı nabız ölçer gibi cihazlar ile kontrol edilir.

Bu çalışmanın ana motivasyonu çoklu ve karmaşık etkileşimli Nİ cihazlarının yer aldığı uygulama senaryoları için sade güvenlik politika kuralları ile olası saldırıların mevcut yöntemlere göre daha basit bir şekilde engellenebilmesini sağlayan yeni bir erişim denetimi yöntemi geliştirilmesidir. Bu çalışmayla literatüre yapılan katkılar ise şunlardır: (i) çevre, kişi, zaman ve sistem dahil tüm bağlam türlerini içeren ve diğer bağlam-duyarlı Nİ uygulamalarında da kullanılabilecek özgün bir bağlam modelinin oluşturulması (ii) çoklu ve karmaşık etkileşimli, bağlam-duyarlı Nİ uygulamalarında ortaya çıkabilecek saldırı/tehdit vektörlerinin belirlenmesi ve (iii) bu saldırıları önleyen özgün bir bağlam-duyarlı rol-tabanlı erişim kontrolü yöntemi geliştirilmesi, uygulamaya geçirilmesi ve yeni nesil Nİ uygulamalarını temsil eden karmaşık bir senaryo altında doğrulanması.

2. Literatür Taraması

Literatürde bağlam-duyarlı erişim denetimi çözümü öneren çeşitli çalışmalar olup bunlardan [3], [4], [5], [6] ile [7]'de dahil olmak üzere, neredeyse tüm çalışmalar yaygın bilişim kategorisinde yer alan tekil uygulamalı senaryolara yönelik olarak geliştirilmiştir. Bunlar makalemizin kapsamına giren karmaşık etkileşimli müşterek bilişim kategorisindeki Nİ sistemleri için uygun değildir. Müşterek bilişim kategorisine giren yeni nesil Nİ uygulamaları için bağlam-duyarlı erişim denetimi öneren yegâne çalışma [8] olup burada da rol-tabanlı yaklaşımın kullanılmamasından kaynaklanan iyileştirmeye açık bölümler vardır. Bugüne kadar rol-tabanlı ve bağlam-duyarlı erişim denetimin Nİ uygulamaları için birlikte kullanımını öneren yegâne çalışma [9] olup önerilen yöntem aynı yazarın tez çalışması olan [10]'da daha kapsamlı anlatılmıştır. Bu makalede sunulan çalışmanın [9]/[10]'a göre en önemli iki farkı şu şekildedir: (i) diğer çalışmada operasyon tabanlı ismi verilen ve rol tabanlı ile nitelik tabanlı yaklaşımların birleştirilmesinden oluşan bir yaklaşımın kullanımı önerilmektedir. Bizim çalışmamızda ise mevcut Nİ geliştirme ortamlarında halihazırda bulunan rol tabanlı ve bağlam duyarlı araç setlerinin doğrudan kullanımına imkân veren bir yöntem kullanılmaktadır. (ii) Diğer çalışmada ele alınan senaryo gelecekteki çok elemanlı ve karmaşık etkileşimli Nİ uygulamalarını yeterli biçimde kapsamayan basit bir çerçevede ele alınmıştır.

Literatürde önerilen bağlam duyarlı çalışmaların derlendiği bir makale olan [11]'deki çözümler bulut ve sis ağlarına yöneliktir. [12]'de Nİ için bağlam durumuna duyarlı bir çözüm sunulmuştur. Nİ'ye yönelik bir diğer yöntemin sunulduğu [13]'te ise saldırı/tehdit modelleri ile jenerik güvenlik gereksinimlerini ele almıştır. Bu çalışmaya göre Nİ uygulamalarındaki cihazların heterojen olmasının güvenlik üzerindeki etkisi büyüktür ve Nİ'de güvenliğin tam anlamıyla sağlanabilmesi için yalnızca kriptografik algoritmaların doğrudan uygulanması yeterli olmayıp, uçtan uca güvenli iletişimi sağlayan özgün hafif (lightweight) güvenlik protokollerinin de geliştirilmesi gerekmektedir. Ayrıca Nİ uygulamalarında kimlik doğrulama, yetki ve erişim kontrolünün önemi vurgulanmış, mahremiyetin korunmasının tasarım prensibi olarak benimsenmesi gerektiği söylenmiştir. Nİ'ne yönelik saldırılar; hizmet reddi (Denial of Service: DoS), fiziksel zarar verme, haberleşme linkini dinleyerek bilgi elde etme, cihaz ele geçirme (node capturing) ve Nİ sisteminin tümünü ele geçirme olarak 5 başlıkta incelemiştir. [13]'te, Nİ uygulamalarının erişim denetiminde bağlam bilgisi kullanımı umut

veren yaklaşım olarak değerlendirilerek geleceğin Nİ senaryolarında daha granüler ve dinamik erişim denetimi için bağlam-tabanlı yöntemlerden yararlanılması önerilmiştir. Ayrıca yine bu çalışmada Nİ mimarileri merkezi (centralized), iş birliği-temelli (collaborative), birbirine bağlı nesnelerin intraneti (connected intranet of things) ve dağıtık (distributed) olarak dört ana kategoriye ayrılmış ve erişim kontrolünde tamamen dağıtık yapılar yerine merkezi ve iş birliği-temelli Nİ mimarilerinin daha kullanışlı olduğu belirtilmiştir. Bu çalışma kapsamında ele alınan Nİ uygulamaları tüm bileşenlerin birbirleriyle etkileşimine olanak tanıyan ancak bu etkileşim için merkezi bileşen ya da altyapıların (bulut vb.) kullanıldığı mimarilerdir. Nİ uygulamaları için alternatif mimarileri elen alan çalışmalardan bir diğeri olan [14]'te ayrık/dağıtık mimariler yerine çok çeşitli Nİ bileşenleri ve uygulamalarının etkileşimine olanak tanıması, dolayısıyla ortaya çıkan zengin bağlam bilgisinin hem fonksiyonellik hem de güvenlikte kullanımına imkân vermesi nedeniyle merkezi/bulut-tabanlı mimari kullanımının Nİ uygulamaları için daha uygun olduğundan bahsedilmektedir.

Nİ güvenliği konusunda güncel akademik literatürü tarayan ve bu bağlamda geleceğe projeksiyon yapan üç önemli çalışma [15], [16] ve [17]'dir. [16]'da Nİ güvenliği konusunda literatürdeki çalışmalar mahremiyet (privacy), güven (trust), uygulama (enforcement), orta katman (middleware) ve mobil kategorileri altında özetlenmiştir. Ayrıca, Nİ'deki güvenlik gereksinimleri kimlik doğrulama, gizlilik ve erişim kontrolü bağlamında incelenmiş, mevcut çalışmaların sunduğu farklı çözümlerden bahsedilmiş, bunların neredeyse tamamına yakınının kablosuz algılayıcı ağlar için geliştirilen yöntemlerin Nİ'ne uyarlanması şeklinde olduğu belirtilerek Nİ'deki varlık çeşitliliği ve bunların birbiriyle farklı bağlamlardaki etkileşiminin Nİ'ne özgü çözümler geliştirilmesi zorunluluğunu doğurduğu sonucuna varılmıştır. Nİ erişim denetimi özelinde ise yalnızca kişilerin değil kaynak, servis ve cihazların da çoklu etkileşimde olduğu Nİ dünyasında erişim izinlerinin nasıl güvence altına alınacağının, bu kapsamda varlıkların kimlik doğrulamasının nasıl yapılacağının ve merkezi, ayrık, yarı ayrık mimarilerden hangisinin bu kapsamda daha uygun olacağının çalışılması gereken konular olduğu vurgulanmıştır.

[17], Nİ güvenlik gereksinimlerini ağ güvenliği, kimlik yönetimi, mahremiyet, güven ve dayanıklılık olmak üzere beş ana kategoride ele almıştır. Bu genel güvenlik gereksinimleri dışında Nİ sistemlerine özgü anonimlik, takma ad kullanımı (pseudonimity), ilişkilendirilemezlik (unlinkability) gibi güvenlik gereksinimlerinden de bahsedilmiştir. Anonimlik bir kullanıcının veri veya eylem kaynağı olarak tanımlanamaz olması şeklinde açıklanırken takma ad kullanımı kullanıcının eylemlerinin kendi kimliği yerine rastgele bir tanımlayıcı ad ile bağlantılanmasıdır. İlişkilendirilemezlik ise kullanıcının belirli eylemlerinin birbirileriyle ilişkilendirilerek profilinin oluşturulmasının engellenmesidir. Ayrıca bu çalışmada, Nİ uygulamalarında erişim denetimi için kabiliyet-tabanlı (CBAC: Capability-Based Access Control) ve rol-tabanlı (RBAC: Role-Based Access Control) yöntemlerin tek başlarına ve statik şekilde kullanımının yetersiz kaldığını ifade edilmiş, bu yöntemlerin bizim çalışmamızda yapıldığı üzere bağlam bilgisi ile birlikte kullanılması önerilmiştir.

Literatürde, öznitelik tabanlı erişim denetim sistemi (ABAC: Attribute Based Access ontrol) ile rol tabanlı erişim denetim sistemlerinin, birleştirilerek kullanımını öngören çalışmalar da mevcuttur. Bunlardan ilki olan [18]'de, kullanıcılar rollere atanmıştır ve rollerin ilişkili izinleri bulunmaktadır. Ayrıca subjeler ve objeler için öznitelik tanımlanmıştır. Kullanıcıdan gelen istekler obje ve subje özniteliği kullanılarak izin filtreleme birimi olarak adlandırılan bir modülden geçirilerek sınırlandırılmıştır. Bu çalışmada öznitelik bilgisi filtreler yardımı ile kullanılarak rol sayısının çok artması sorununa çözüm getirilmiş, fakat rol-izin sayısı sorununa değinilmemiş ve çevresel bağlam bilgisi olarak adlandırılan zaman, lokasyon gibi değişkenler erişim denetiminde kullanılmamıştır. [19]'da ise bir önceki çalışmadan farklı olarak objeler özniteliklerine göre gruplanarak rol-izin sayısının çok artması sorununa çözüm getirilmeye çalışılmıştır.

Nİ sistemlerinin güvenlik gereksinimleri konusunda yapılan en güncel çalışmalardan biri olan [15]'te bu konu öncekilere benzer biçimde mahremiyet, güven, kimlik doğrulama ve erişim denetimi olarak kategorize edilmiştir. Burada, Nİ için erişim kontrolü literatüründe bugüne kadar yapılan çalışmalar, kullandıkları yaklaşıma göre erişim kontrol listesi, rol-tabanlı, kimlik-tabanlı, bağlam-duyarlı ve güven-tabanlı olarak beş

kategoride gruplandırılmıştır. Buna göre Nİ uygulamalarında bağlam-duyarlı ve rol-tabanlı erişim denetimi yaklaşımlarının bugüne kadar hep ayrı ayrı kullanıldığı görülmekte, ayrıca bağlam-duyarlı yaklaşım kullanan az sayıda çalışmada dikkate alınan bağlam bilgisinin konum, hareket ya da uzaklık gibi tekil ve basit bağlamları ifade ettiği anlaşılmaktadır.

Bilişim uygulamalarında bağlam bilgisi kullanımı ilk kez [2]'de öngörülse de bağlam-duyarlı bilişim kavramının bir çalışmada açıkça ilk kullanımı [20]'de yapılmıştır. Bundan sonra bağlam-duyarlı bilişim konusunda yapılan çalışmalarda farklı bağlam tanımları kullanılsa da bunların arasında yaygın kabul görmüş olan ve bu proje kapsamında kullanılacak bağlam kavramıyla da uyumlu olan tanım [21]'de ortaya konmuştur. Buna göre bağlam (context), bir varlığın (entity) durumunu karakterize etmek için kullanılabilecek herhangi bir bilgidir. Varlık ise kullanıcıların ve bilişim uygulamalarının kendileri de dahil olmak üzere etkileşim içinde oldukları kişi, yer veya herhangi bir nesne olabilir. Nİ uygulamalarında bağlam bilgisinin kullanımına yönelik kapsamlı bir literatür taraması teorik/akademik perspektiften [22]'de, uygulama/market perspektifinden ise [23]'de verilmiştir. [22]'de bağlam-duyarlı Nİ uygulamalarında güvenlik konusundan bahsedilmiş, bağlam bilgisi kullanan söz konusu Nİ uygulamalarının gizlilik ve güvenliğinin sağlanmasına yönelik zorluklardan söz edilmiş ancak Nİ'de güvenlik sağlamak amacıyla bağlam-bilgisinin kullanımına ilişkin bir atıfta bulunulmamıştır.

Bağlam bilgisinin güvenlik sağlamak amacıyla, özellikle erişim denetiminde kullanımını öneren çalışmalar mevcuttur:[3], [4], [5], [6], [7], [24] [25]. Bunlardan bir kısmı bizim çalışmamızda olduğu gibi bağlam-duyarlı ve rol-tabanlı yaklaşımların birlikte kullanımını da önermektedir. Ancak bu çalışmaların hiç birisi makalemiz kapsamında adreslenen Nİ sistemlerine yönelik olarak geliştirilmemiş olup ya farklı alanlar (mobil uygulama vb.) için ya da Nİ'nin bir önceki versiyonu sayılabilecek çoklu varlık etkileşimi içermeyen senaryolar için tasarlanmıştır.

[7]'de bağlam bilgisinin güvenliğinin sağlanmasının önemli olduğu vurgulanarak bağlam gizliliği, bütünlüğü ve kullanılabilirliği (availability) üzerinde durulmuştur. Bağlam bilgisinin, güvenliği arttırmak için kullanılabileceğinden [3], [4] ve [5]'deki çalışmalara atıfta bulunularak bahsedilmiştir. Ancak bu çalışmada belirli bir yöntem ya da yaklaşım önerisinde bulunulmamıştır.

[4]'de jenerik rol-tabanlı erişim kontrolü yöntemine "Context Toolkit" adı verilen bağlam mimarisi modeli eklemlenerek yer, zaman, vb. çevresel/fiziksel bağlam bilgilerini kullanan "çevresel rol" kavramı eklenmiştir. Çevresel rollerin güvenlik politikası oluşturmada kullanımı ile daha spesifik ve detaylı bir erişim kontrol modeli oluşturulmuştur. Bu modelin implementasyonunda basit bir akıllı ev senaryosu kullanılmıştır. Ayrıca, bu çalışmada bağlam bilgisinin erişim izni talep edildikten sonra değişmesi durumunda modelin vereceği tepkiden bahsedilmemiştir. [5]'de ise genelleştirilmiş rol-tabanlı erişim yöntemi (GRBAC: Generalized Role-based Access Control), bağlam-duyarlı güvenlik politikalarının yazılmasında sadelik ve kolay anlaşılabilirliği nedeniyle XML (Extensible Markup Language) dili ve haberleşme linki güvenliği için SSL (Secure Sockets Layer) kullanılmıştır. Her iki çalışma da tekil etkileşimli basit uygulama senaryosu içeren sistemlere yönelik olması, çoklu seviyeli dinamik güvenlik politikalarının oluşturulmasına imkân vermemesi ve saldırı/tehdit unsurlarının göz önünde bulundurulmaması nedeniyle burada önerilen yöntemden farklılık göstermektedir. Ayrıca çevresel bağlam bilgisinin rol olarak sisteme tanımlanması, rol sayısının artmasına, böylece rol patlaması problemine yol açacaktır. Bu çalışmada önerilen yöntemde (rol × subje) olan yazılması gereken güvenlik politikası kural sayısının ise, bu çalışmada (rol × subje × $2^{\text{çevresel roller}}$) olacağı belirtilmiştir.

[3]'de Cerberus adı verilen, bağlam bilgisini kullanan bir erişim kontrol yöntemi ve kimlik doğrulama mekanizması geliştirilmiştir. Tasarlanan güvenlik servisinde kimlik doğrulama için çoklu seviyeli bir güvenlik modeli öngörülmüş olup, her bir kişi/uygulama/kaynak bir güven değeri ile ilişkilendirilmiş ve bu değer erişim denetiminde kullanılmıştır. Diğer çalışmalardan farklı olarak, bizim çalışmamızda olduğu gibi, güvenlik politikalarının yazılmasında, erişim kontrol sorgularında ve bağlam bilgi mimarisinde birinci derece mantık (first-order predicate logic) ve boole cebiri (boolean algebra) kullanılmıştır. Ayrıca sistem dinamik olarak bağlam bilgisini kontrol etmekte,

erişim için gerekli olan bağlam bilgisinin değişmesi halinde erişimi iptal etmektedir. Bu çalışmada rol-tabanlı erişim kontrolü kullanılmamıştır ve sistem çok etkileşimli Nİ uygulamalarına yönelik değil, yaygın bilişim uygulamaları için tasarlanmıştır. Ayrıca, önerilen erişim denetimi normal kullanım senaryosunda test edilmiş fakat uygulama tarafından yararlanılan bağlam bilgisinin saldırı için kullanılabileceği durumlar dikkate alınmamıştır.

[6]'da erişim kararlarını vermek için bağlam bilgisi kullanımını öneren rol-tabanlı CA-RBAC (Context-aware Role-based Access Model) yöntemi sunulmuştur. CA-RBAC'de erişim isteğinde bulunan subjeler farklı bağlamlar için yaratılan ve erişim izinleri bağlam bilgisi göz önünde bulundurularak oluşturulan rollere dinamik olarak atanmaktadır. Dolayısıyla her bağlam için ayrı bir rol yaratılması gerekmekte olup bu durum fazla sayıda varlık etkileşimi içeren Nİ senaryolarında çok fazla sayıda rolün oluşturulmasına yol açacağından uygun olmayacaktır. Bizim çalışmamızda önerilen yöntemde bağlama göre yeni rol yaratmak yerine rollerin ilgili erişim izinleri aktif veya pasif hale getirilmektedir. Böylece çok fazla sayıda rol yaratılmasına ihtiyaç duyulmamaktadır. CA-RBAC yönteminde erişimin daha granüler düzeyde denetlenebilmesini sağlamak amacıyla aynı role sahip subjelerin, objelere/kaynaklara erişiminde bağlam bilgisi kullanımı öngörülmüştür. Böylelikle, bir objeye aynı role sahip kişilerden, sadece ilişkili bağlam bilgisini sağlayan kişi veya kişilerin erişimine olanak tanınmıştır. Bu da obje ile izini ayrı birer modül olarak düşünüp objelere bağlam bilgisi tanımlamak yoluyla gerçekleştirilmiştir.

[24], rol-tabanlı ve bağlam-duyarlı erişim denetiminin birlikte kullanıldığı güncel çalışmalardan biri olup Android başta olmak üzere mobil işletim sistemleri için uygulamaların kullanıcı verileri ve diğer uygulamalara erişimini CA-ARBAC ismi verilen yöntem ile kontrol etmeyi amaçlamaktadır. Bu çalışmada, erişim isteğinde bulunan subje olarak mobil uygulamalar ele alınmış ve bunlar kullanıcı tarafından belirlenen ve erişim izinleri bağlama göre etkin kılınan rollere atanmıştır. Tanımlanmış rollerin erişim izinleri, ilgili role atanmış bir uygulama (subje) tarafından kullanılmak istendiğinde bağlam bilgisi kontrol edilmekte ve önceden oluşturulmuş rol-izin-bağlam kural setine göre erişim izni verilip verilmeyeceği belirlenmektedir. Roller, uygulamalar ve izinler arasında çoklu eşleştirme yapılması mümkündür. [24]'teki erişim denetimi yöntemi farklı senaryolar için prototip olarak uygulanmıştır.

[25]'in benzer çalışmalardan en önemli farkı, bağlam bilgisinin yalnızca rollerin ilişkilendirildiği izinlerin yönetiminde değil, kullanıcılara farklı güvenlik seviyelerin atanmasında kullanılmasıdır. Kullanıcıya atanan güvenlik seviyesine göre kimlik doğrulaması esnasında farklı yöntemler kullanılarak sağlanan güvenliğin duruma göre artırılması öngörülmektedir. Böylece, bağlam bilgisi hem erişim denetimi esnasında hem de hemen öncesinde uygulanması gereken kimlik doğrulaması sırasında kullanılmaktadır. Güvenlik hassasiyeti yüksek kaynaklara ve uygulamalara erişimde uygulanan doğrulama yönteminin duruma göre değiştirilmesine imkân tanıyan bu yaklaşım kullanılabilirliği (usability) azaltmadan güvenlik seviyesinde artış sağlamaktadır. Daha önce kablosuz yerel alan ağlarının güvenliği konusunda [26]'da kullandığımız bu uyarlanabilir çok seviyeli güvenlik yaklaşımı, bu çalışmanın Nİ güvenlik politikalarında sadelik hedefiyle uyumlu olması ve Nİ sistemlerine kolaylıkla uyarlanabilmesi nedeniyle bu makalede sunulan yöntemde de kullanılmıştır.

Literatürde, yeni nesil Nİ sistemleri için bağlam-duyarlı erişim denetimine yönelik özgün bir yöntem önerisinde bulunan çalışma az sayıda çalışmadan biri de [8]'dir. ConUCON (Context-aware Usage Control Model) adı verilen bu yöntemde, zaman ve mekân gibi çevresel değişkenler, sistemin ve donanımın durumu, nabız, vücut sıcaklığı gibi geniş bir yelpazeye sahip bağlam bilgisinin, Nesnelerin Ağı (WoT: Web of Things) olarak adlandırılan ve varlık sayısının çok olduğu ve farklı türdeki varlıklar arasındaki iletişimin bilinen Web protokolleriyle sağlandığı Nİ uygulamalarında erişim denetimi için kullanılması öngörülmüştür.

ConUCON, subje, obje, bunların özellikleri (attributes), haklar (rights), yetkiler (authorizations), zorunluluklar (obligations) ve şartlar (conditions) olarak isimlendirilen bileşenlerden oluşan bir güvenlik modeli olan UCON üzerine inşa edilmiştir. ConUCON bu bileşenlere ek olarak erişim denetiminde subje

bağlam bilgisi ve obje bağlam bilgisinin de kullanımını önermiştir. Ancak, rol-tabanlı bir yaklaşım kullanılmaması her subjenin her objeye erişiminin ayrı ayrı denetlenmesi zorunluluğunu doğurmaktadır. Dolayısıyla erişim isteğinde bulunacak her bir subje ve kendisine erişilmek istenen her bir obje için bağlam bilgisinin kontrol edilmesi gerekmektedir. Bu da hem sayıca hem de nitelik açısından çok farklı nesneler (insan, servis, makine, bilgisayar) içeren geleceğin Nİ sistemlerinde erişim denetiminde bağlam bilgisi kullanımını sadelik ve kolay anlaşılabilirlikten uzaklaştırmış, hesaplama karmaşıklığı yüksek bir hale getirmiştir. Ayrıca, bu çalışmada kullanılan bağlam modellemesi ve dili de sadelikten oldukça uzaktır. Bu nedenle, içerdiği bileşenlerin sayısının, türünün ve etkileşiminin fazla olduğu Nİ uygulamalarında ortaya çıkacak bağlam bilgisinin çokluğu, hem sade erişim denetimi politikaları yazılmasına imkân tanımayacak hem de hesaplama karmaşıklığına bağlı olarak performansı olumsuz etkileyecektir.

Çalışmamızda önerilen erişim denetimi yöntemi ile belirli bir senaryoda güvenlik politikası tarafından kontrol edilmesi gereken erişim sayısının büyüklük derecesinin (order of magnitude) "*Subje sayısı × Rol sayısı*" seviyesinde tutulması sağlanmaktadır. Literatürde rol-tabanlı erişim denetimi kullanılmayan benzer yöntemlerde bu sayı "*Subje sayısı × Obje sayısı × Erişim hakkı sayısı × Bağlam sayısı*" düzeyindeyken rol-tabanlı erişim denetimi kullananlarda "*Rol sayısı × Erişim izni sayısı × Bağlam sayısı*" seviyesindedir. Ayrıca, rol-tabanlı yaklaşım kullanan benzer çalışmalara göre ihtiyaç duyulan rol sayısı bağlam sayısından bağımsız hale getirilerek "*Rol sayısı × Bağlam sayısı*" seviyesinden "Rol sayısı" seviyesine getirilmiştir.

Önerdiğimiz yaklaşımın literatürdeki çalışmalar ile karşılaştırması Tablo 1'de yer almaktadır.

Tablo 1. Literatürdeki Benzer Çalışmalar ile Karşılaştırma

	Önerilen Yöntem	[4], [5]	[3]	[6]	[8]	[25]	[29]	[24]
Bağlam-duyarlı erişim denetimi	✓	✓	✓	✓	✓	✓		✓
rol-tabanlı erişim denetimi	✓	✓		✓		✓		✓
dinamik erişim denetimi	✓		✓	✓	✓	✓		✓
yeni nesil karmaşık Nİ senaryolarında doğrulama	✓				✓		✓	
uyarlanabilir çok seviyeli güvenlik	✓		✓			✓		
basit bağlam modellemesi	✓	✓	✓	✓				
sade erişim politikaları	✓	✓	✓					✓
az sayıda role ihtiyacı	✓							✓
aktif tehdit modellemesi	✓						✓	

3. Kavramsal Yöntem

Bu çalışmanın temel hedefi, Nesnelerin İnterneti uygulamalarında güvenlik sağlamak için kullanılacak rol-tabanlı ve bağlam-duyarlı kavramsal bir erişim denetimi yönteminin ortaya konulmasıdır. Bu yöntemin, çok farklı sayı ve çeşitte varlıktan oluşan, varlıklar arasında karmaşık ve çoklu bir etkileşimin olduğu Nİ senaryolarında ortaya çıkması muhtemel güvenlik zafiyetlerine yönelik saldırıları, çoklu seviyeli kimlik doğrulama kullanılan, dinamik ve sade erişim denetimi politikalarıyla engelleyebilmesi amaçlanmaktadır. Bu amaçların karşılanabilmesi için kullanılan yöntemler aşağıda sıralanmıştır:

1) Nİ uygulamalarında ortaya çıkabilecek farklı bağlam çeşitlerini kapsayan ve bunların basit bir şekilde ifade edilebilmesini sağlayan bir bağlam modelinin oluşturulması

2) Geliştirilen erişim denetimi yönteminin koruma sağlayacağı kapsamı örnekleyen bir uygulama senaryosunun geliştirilmesi

3) Çoklu ve karmaşık etkileşimli Nİ uygulamaları için güvenlik gereksinimlerinin, bağlam bilgisi kullanımı kaynaklı zafiyetlerin ve bunlara yönelik saldırı/tehdit vektörlerinin belirlenmesi

4) Nİ'ye yönelik saldırıları önleyebilecek bağlam-duyarlı, rol-tabanlı ve dinamik güvenlik politikalarının yazılmasına imkân tanıyan bir erişim denetimi yönteminin geliştirilmesi

5) Geliştirilen erişim denetimi yönteminin örnek senaryo altında doğrulanması

3.1. Bağlam Modeli

Literatürde bağlam bilgisinin modellenmesinde iki temel yaklaşım bulunmaktadır. Bunların ilki [8]'deki gibi farklı türdeki bağlam bilgilerini ayrı ayrı modelleyen geometrik temelli yaklaşım olup bu yaklaşımın bağlam modellemesinde sağladığı esneklik ve ayrıntılandırabilme özelliğine karşın hesaplama karmaşıklığı yüksektir. Diğer yaklaşım ise birinci derece mantık ve boole cebirinin kullanılması sayesinde çok sayıda varlığın etkileşiminden doğan bağlamın sade biçimde ifade edilebilmesine imkân tanıyan ve [23]'da kullanılan yöntemdir. Bu çalışmada ikinci türdeki bağlam modelleme yaklaşımı kullanılacak olup temel yaklaşım aşağıda verilmiştir.

Tanım (Bağlam Bilgisi): Nİ uygulamalarında yer alan her türlü varlığın (bilgisayar, makine, uygulama, kişi, süreç, servis, vb.) durumunu açıklamak için kullanılan her türlü bilgidir. *Bağlam Bilgisi* tanımlaması *Bağlam Adı (Bağlam Nitelikleri)* şeklinde yapılacaktır. Örnek: *Konum (Enlem, Boylam); Zaman (Yıl, Ay, Gün, Saat); Sağlık Durumu (Nabız, Tansiyon);*

Tanım (Bağlam Politikası): Dinamik erişim izni denetimine girdi olacak bağlam durumunu ifade etmek için kullanılacak *Bağlam İfadesi* ve güvenlik politikasına göre uygulanacak *Eylem* (İzin Ver/Engelle) olmak üzere iki bileşenden oluşur: *Bağlam Politikası (Bağlam İfadesi, Eylem)*.

Tanım (Bağlam İfadesi): Bağlam Bilgisine ait niteliklerin (attribute) herhangi bir andaki sayısal değerlerinin birinci derece mantık ($\forall$, $\exists$, $\Rightarrow$, ϵ, $\neg$, $\wedge$, $\vee$), boole cebiri ve karşılaştırma operatörleri ($>$, $\geq$, $<$, $\leq$, $=$, $\neq$) ile tanımlanmasıdır: *Bağlam İfadesi (Bağlam Adı, Mantıksal/Cebirsel İfade, Nitelik Değeri)*.

BP, tanımlı tüm Bağlam Politikalarını içeren küme, *Bİ* ise tüm Bağlam İfadelerini içeren kümedir. Buna göre, $BP_m \epsilon BP$ *ve* $Bİ_m \epsilon Bİ$ olmak üzere $BP_m = (Bİ_m, Eylem)$ olarak tanımlanır. Arabanın eve yakın olması durumunda mobil cihaz ile kapının otomatik olarak açılmasını öngören izne bağlı örnek bağlam politikası: *((|Araba konum-Ev konum|<= 5 m), kapıyı aç)*

Tanım (Birleşik Bağlam Politikası): Dinamik erişim izni denetiminde birden fazla bağlam politikasının mantık operatörleri '$\wedge$'(ve), '$\vee$'(veya) ve '$\neg$'(değil) ile birleştirilerek kullanılmasıdır. *BBP*; farklı Bağlam İfadelerinin birleşiminden oluşan birleşik bağlam politikası kümesini göstermektedir:

$(BBP_k \epsilon BBP, Bİ_m \epsilon Bİ$ olmak üzere $BBP_k = (Bİ_1 \wedge Bİ_2 \wedge \ldots \wedge Bİ_m)$ ya da $BBP_k = (Bİ_1 \vee Bİ_2 \vee \ldots \vee Bİ_m)$ ya da $BBP_k = (\neg Bİ_1)$

Örneğin, okul servisi eve yakınsa ve zaman okul saati ise mobil cihaz ile ev kapısının açılmasını engelleyecek bir erişim kontrol politikası düşünüldüğünde, istenilen bağlam bilgilerini kontrol edecek birleşik bağlam politikası aşağıdaki gibi olacaktır:

(((|Servis konum-Ev konum|<= 5 m) $\wedge$ (Saat, "arasında", 08:00-15:00), engelle)

3.2 Uygulama Senaryosu

Literatürdeki çalışmaların çoğu kapsam olarak basit akıllı ev/ofis senaryolarını almış ve geliştirilen yöntemler söz konusu çoklu etkileşimden doğabilecek güvenlik açıklarına yönelik tehdit senaryoları altında test edilmemiştir. Hatta çoğu zaman bu senaryolar herhangi bir saldırganın olmadığı, saldırı vektörünün tanımlanmadığı durumlar için ve yalnızca uygulamaların önceden planlanan erişim kurallarına göre kontrol edilip edilememesine göre test edilmiştir. Bu kapsamda, çalışmamızın literatürdeki diğer çalışmalardan önemli bir diğer farkı da önerilen yöntemin yeni nesil Nİ uygulamaları ile uyumlu farklı nitelikteki varlıkların çoklu ve karmaşık etkileşimini içeren bir senaryo ile test edilmesidir. Aşağıda verilen bu senaryo ile yakın gelecekte yaygınlaşması beklenen Nİ uygulamalarındaki varlıkların çeşitliliği, etkileşimin kompleksliği ve bu durumdan doğan güvenlik zafiyetlerinin mevcut yöntemlerle neden önlenemeyeceği ile geliştirilecek yöntemin buna nasıl bir çözüm sağlayacağına ilişkin proje hipotezi örnek ile açıklanmaya çalışılmıştır. Söz konusu uygulama senaryosu aşağıda verilmiştir.

- Sağlık, ev ve araçtan oluşan üç farklı Nİ uygulama alanı bütünleşik bir senaryo altında kapsanmaktadır.
- Birisi giyilebilir sensörler üzerinden anlık ölçülen veriler, birisi bulut üzerinde duran hastane kayıtları ve diğeri kitlesel kaynaklardan çıkarılan veriler olmak üzere üçü sağlık veri kaynağı, biri bulut üzerinden trafik/navigasyon veri kaynağı, ikisi sadece subje (akıllı kilitle kontrol edilen kapı ve akıllı IP kamera) ikisi de hem subje hem de obje (Nİ sağlık uygulaması ve Nİ ev uygulaması) olan toplam sekiz adet objeye yapılan erişim denetlenecektir.
- Dördü Nİ uygulaması (sağlık, ev, araç, spor) olan altısı ise kullanıcı (anne, baba, kız çocuk, erkek çocuk, yakın arkadaş, yakın akraba) olan toplam on adet subjenin yukarıdaki objelere erişimi denetlenecektir.
- Ev ve araç Nİ uygulamaları trafik yoğunluğu, çocukların servisinin anlık lokasyonu, vb. bilgilere trafik/navigasyon bulut servisi üzerinden erişebilmektedir.
- Evde yaşayan kullanıcılara ilişkin kritik sağlık bilgileri (i) giyilebilir sensörler ve (ii) hastanede yapılan kontrollere ilişkin kayıtlar aracılığıyla bulut üzerinden anlık ve tarihsel olarak Nİ sağlık uygulaması tarafından gözlenmektedir.
- Kullanıcılara ilişkin sağlıklı yaşamla ilgili bazı bilgiler (günlük yürüme mesafesi, harcanan kalori, vb.) giyilebilir sensörler aracılığıyla anlık ve tarihsel olarak Nİ spor uygulaması tarafından gözlenmektedir.
- Kullanıcılar sağlık durumlarıyla ilgili bazı bilgileri arkadaşları ya da sağlık uzmanlarından bilgi almak amacıyla kitlesel kaynaklar (forumlar, sosyal ağlar, vb.) aracılığıyla paylaşmaktadır. (Örneğin bir süredir sırt ağrısı şikâyeti olan birisinin bunun hangi hastalığın belirtisi olduğu ya da hangi doktora gitmesi gerektiği konusunda sosyal ağlarda ya da forumlarda bağlantılarına sorduğu sorular, verilen cevaplar, yapılan yorumlar)
- Evin içinde bazı bölümler ve kapı girişi, akıllı IP kamera sistemiyle sürekli biçimde izlenmektedir. Kamera görüntüleri anlık olarak yetkilendirilmiş kullanıcılar tarafından ve yalnızca aşağıdaki koşullar çerçevesinde izlenebilmektedir.
  - Anne ve baba her koşulda her zaman ve süre sınırı olmaksızın kamera görüntülerini izleyebilir.
  - Yakın arkadaş ve yakın akraba yalnızca acil durumlarda ve belirlenmiş süre boyunca görüntüleri izleyebilir.
  - Akıllı ev uygulaması kamera görüntülerine güvenlik ve bağlam bilgisi oluşturma (içerde/dışarda kimsenin olup olmadığı, acil bir durum olup olmadığı, vb.) maksadıyla sınırlı (kısa süreli, düşük çözünürlükle, vb.) biçimde erişebilir.
- Evin kapısı belirlenmiş kullanıcılar ya da Nİ uygulamaları tarafından aşağıdaki koşullar ile açılabilmektedir.
  - Anne ve baba her koşulda biyometrik kimlik doğrulama ile kapının akıllı kilidini hem evin içindeyken hem de dışındayken açabilir.
  - Çocuklar biyometrik kimlik doğrulama ile kapının akıllı kilidini evin dışındayken her koşulda, evin içindeyken ise yalnızca ebeveynlerden biri evin içindeyse ya da acil durumda açabilir.

- Akıllı kapı kilidi dışarıdan, mobil ya da giyilebilir cihazlar ile yakın mesafe iletişim teknolojileriyle (bluetooth, NFC) aşağıdaki koşullar altında açılabilir.
  - Çocukların okul servisi eve 10 m mesafeden daha yakınsa çocukların sahip olduğu giyilebilir ya da mobil cihazlar akıllı kapı kilidine yaklaştırıldığında kapı açılır.
  - Ebeveyn arabası eve 10 m mesafeden daha yakınsa ebeveynlerin sahip olduğu giyilebilir ya da mobil cihazlar akıllı kapı kilidine yaklaştırıldığında kapı açılır.
- Nİ ev uygulaması sağlık görevlilerinin acil durumda eve girip müdahale edebilmesi için evin kapısını otomatik olarak yalnızca aşağıdaki alt koşullara göre açabilir:
  - sağlık uygulaması tarafından bildirilen ya da konfirme edilen VEYA yakın arkadaş/akraba tarafından kamera görüntüleri ile konfirme edilen bir acil durum varsa VE
  - evde acil durumda olan kişiden başka kimse yoksa VE
  - bir sağlık aracı (ambulans) eve 10 m mesafeden daha yakınsa

- Nİ sağlık uygulaması, Nİ ev uygulamasına acil durum bildirimini yalnızca aşağıdaki durumlarda gönderir ya da gelen sorguyu onaylar:
  - giyilebilir sensörlerden gelen veriye göre yerde hareketsiz yatan biri varsa VE
    - bulut üzerinden alınan sağlık verilerine göre kişinin yüksek riski varsa VEYA
    - kitlesel kaynaklardan alınan verilere göre yüksek risk varsa (örneğin son zamanlarda yaptığı paylaşımlarda göğüs ağrısı ya da sırt ağrısından bahsediyorsa)
- Nİ ev uygulaması, sağlık uygulamasına yalnızca aşağıdaki koşullarda acil durum sorgusu göndermek için erişebilir:
  - kamera görüntülerine (ya da evdeki diğer sensörlerden gelen verilere) göre evde hareketsiz yatan birisi varsa
- Ni sağlık uygulaması hem giyilebilir sensörler hem de bulut üzerinden sağlık verilerine her zaman erişebilir.
- Ni sağlık uygulaması kitlesel kaynaklar üzerinden sağlık verilerine yalnızca acil durumda kısa süreli erişebilir.
- Nİ spor uygulaması sağlık verilerine yalnızca giyilebilir sensörler üzerinden ve kullanıcı spor yaparken erişebilir.

3.3 Güvenlik Zafiyetleri ve Tehdit Modeli

Bu çalışmanın literatürdeki benzer yaklaşımlara göre önemli bir farkı, özellikle bağlam kullanımındaki zafiyetlerden yararlanmaya yönelik saldırıların da engellenebilmesidir. Bu kapsamda hedeflenen uygulama alanı kapsamındaki zafiyet ve tehditlere ilişkin öngörüler şu şekildedir: Ele alınan örnek senaryoya göre evin akıllı kilit ile kontrol edilen kapısı aile üyeleri tarafından biyometrik kimlik doğrulaması ya da yakın mesafe iletişim teknolojileri (NFC, vb.) aracığıyla mobil/giyilebilir cihazlar ile belirli koşullar sağlandığında açılabilmektedir. Buna göre, ÇOCUK rolüne sahip bir subjenin kapıyı mobil cihazı ile açabilmesi için erişim isteği yapıldığında çocukların okul servisiyle eve döndüğünü gösteren bağlamın (servisin evin yakınında olması) gerçekleşmesi gerekmektedir. Böylece kapı açma yetkisi olan mobil cihazı bulan ya da çalan başka birinin akıllı kilidi açarak eve girmesi engellenebilir. Mobil cihazı ele geçiren kişinin erişim denetiminde servisin konum bilgisinin kullanıldığını öğrenerek/tahmin ederek servis şoförü ile kötü niyetli bir anlaşma yapıp kapıyı açmaya çalışırken servis aracının evin yakınında olmasını sağlaması ya da bağlam bilgisinin bütünlüğünü (integrity) bozması durumunda servis aracının lokasyonunu erişim denetiminde kullanan bağlam-duyarlı yaklaşım başarısız olacaktır. Literatürdeki bağlam-duyarlı erişim denetimi yöntemlerinin hiçbiri bağlam bilgisinin kötü niyetli kullanımından kaynaklanabilecek bu tür saldırıları dikkate almamış ve geliştirdikleri yöntemlerin bunlara karşı dayanıklılığını test etmemişlerdir. Bu çalışmanın en önemli özgün katkılarından biri, varlıkların etkileşiminden doğan bağlam bilgisinin kullanımı ile ortaya çıkabilecek güvenlik zafiyetlerinin araştırılması

ve bunlar kullanılarak yapılabilecek saldırıların engellenebilmesini sağlayacak özelliklerin yönteme eklenmesidir. Bunun için geliştirilen erişim denetim yönteminde çoklu seviyeli kimlik doğrulama ve çapraz bağlam kontrolü (bulut/kitle kaynak) uygulanmaktadır. Örneğin, yukarıdaki saldırı senaryosunda okul servisinin lokasyonu ile birlikte kapı açma erişim talebinin yapıldığı saatin çocukların okulda (ebeveynlerin işte) olması gereken bir saat olup olmadığının çapraz kontrolü bulut üzerinden ebeveyn/çocuk takviminden kontrol edilir. Böylece servis lokasyonuna ilişkin bağlam bilgisinin saldırı amacıyla kullanılması, bu makaledeki yaklaşım ile engellenir. Ayrıca, kapı kilidinin açılmasında daha yüksek güvenlikli kimlik doğrulamanın (biyometrik) bağlam bağımsız, düşük seviyeli doğrulamanın (sahip olunan mobil cihaz) bağlam ile birlikte kullanılması, önerdiğimiz yöntemdeki çoklu seviyeli kimlik doğrulama yaklaşımına bir örnek olup bu sayede takvimlerine göre beklenmeyen bir saatte eve gelen çocuk ve ebeveynin biyometrik doğrulama ile her durumda eve girebilmesini sağlayacak, çapraz bağlam kontrolüyle artırılan güvenlik seviyesinin kullanılabilirliği azaltmasının önüne geçecektir.

Bağlam bilgisinin kötü niyetli kullanımından doğabilecek saldırıların bu makalede sunulan yöntem ile engellenebileceğine ilişkin bir başka örnek de şu şekildedir: Yukarıdaki senaryoda kamera ya da sensörler ile evde hareketsiz yatan birinin tespit edildiği ve evde başka kimsenin olmadığı acil durumlarda Ev Nİ uygulamasının kapı kilidini acil sağlık personeli geldiğinde otomatik olarak açabilmesine ilişkin erişim kural seti oluşturulmuştur. Burada acil durum oluştuğuna ilişkin gerçek olmayan bağlam bilgisi saldırganlar tarafından oluşturularak evin kapısının açılması sağlanabilir. Bunu engellemek için acil durumun oluştuğuna ilişkin bağlamın gerçekleşebilmesi için sensörlerden gelen hareketsiz yatan biri olduğu bilgisi ile bulut üzerindeki sağlık verilerinin ya da sosyal ağlardaki yazışmalardan çıkarılan verilerin yüksek risk göstermesine ilişkin bilginin birlikte kullanılması hedeflenmektedir. Ancak aniden ortaya çıkan ve bulut/kitle kaynak verilerinde risk görünmeyen gerçek acil durumlarda kapı açılmayacak ve dolayısıyla kişinin hayatı tehlikeye girebileceğinden TANIDIK rolüne sahip kişilere kamera görüntülerine geçici erişim izni verilerek acil durumu konfirme etmelerinin istenmesi, böylece çapraz bağlam kontrolü ile mevcut bağlam ve erişim sağlanacak kaynağın kritikliğine göre kimlik doğrulama yöntemini değiştiren dinamik çoklu seviyeli doğrulamayla hem bağlamın kötü niyetli kullanımından doğan güvenlik risklerinin azaltılması hem de kullanılabilirliğin sağlanması hedeflenmektedir. Literatürdeki mevcut çalışmalarda bu tür saldırı senaryoları ele alınmamış, saldırıları bertaraf edebilecek özellikler erişim denetimi yaklaşımlarına dahil edilmemiştir. Bizim çalışmamızda ise Nesnelerin İnterneti uygulamalarında bağlam bilgisini taklit ederek (context spoofing), geçersiz hale getirerek (context invalidation) ya da bozarak (malicous change of context) yapılabilecek saldırılar da çapraz bağlam kontrolü, çoklu seviyeli kimlik doğrulama gibi yöntemlerle engellenebilmektedir.

3.4 Erişim Denetimi Yöntemi

Yukarıda örnekleri verilen güvenlik zafiyetlerinin engellenebilmesi amacıyla kullanılacak olan erişim denetimi yöntemine ilişkin tanımlar aşağıda verilmektedir:

Tanım (*S*: Subje ve *O*: Obje): Subjeler belirli bir obje üzerinde sınırları belirlenmiş erişim haklarına sahip olan varlıklar, objeler ise erişilen, kullanılan varlıklar olarak tanımlanabilir. Bu çalışma kapsamında subjeler sistemdeki kaynakları kullanmak için erişim talebinde bulunan varlıklar (kişi, uygulama, servis, vb.) olabilirken, objeler bir Nİ uygulamasında yer alan her türlü kaynak (uygulama, veri kaynağı, servis, cihaz, vb.) olabilir. *S* ve *O* sırasıyla subje ve obje kümelerini tanımlamaktadır.

Tanım (*R*: Roller): Benzer erişim yetkilerine gereksinim duyan subjelerin kategorize edildiği ve tanımlı erişim izinlerine sahip gruplardır. *R* roller kümesini tanımlamaktadır.

Tanım (*İ*: İzinler): Bir role atanmış subjenin belirli bir objeye erişip erişemeyeceğini ve belirli bir eylemi gerçekleştirip gerçekleştiremeyeceğine ilişkin erişim haklarını tanımlamaktadır. *İ* izinler kümesini ifade etmektedir.

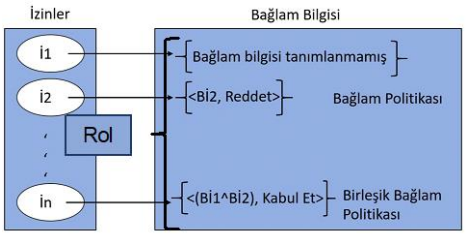
Tanım (*SRA*: Subje-Rol Ataması): Subjeler ve bunların atandığı roller *SRA*: Subje-Rol Ataması listesinde tutulmaktadır. Listenin elemanları (S_i, R_j) şeklinde 2'lilerden oluşmaktadır ve S_i, Subje ve R_j, Roller kümesinin elemanıdır: $S_i \in S$, $R_i \in R$ Sistemdeki her bir subjenin en az bir rolü olması zorunludur. Bir subjenin birden fazla rolü olabileceği gibi, bir rol birden fazla subje

tarafından sahip olunabilmektedir: $SRA \subseteq S \; X \; R$. Subje-Rol Ataması en başta yapılır ve daha sonra bağlam bilgisine göre değişmez.

Tanım **(***RİA:* Rol-İzin Ataması): Her rol için o role atanmış izinlerin tutulduğu listedir. Listenin elemanları (R_m, $İ_k$) şeklinde 2'lilerden oluşmaktadır ve R_m, Roller ve $İ_k$, İzinler kümesinin elemanıdır: $R_m \in R$, $I_k \in İ$. Roller ve izinler arasında çoklu ilişki bulunmaktadır; bir izin birden fazla rol içerisinde yer alabilir ve bir rol birden fazla izine sahip olabilir: $RİA \subseteq R \; X \; İ$.

Tanım (Aktif İzin): Bir role atanan tüm izinler rol için her zaman aktif değildir. Bir subje yalnızca aktif izinleri kullanabilir. Bir subje tarafından kullanılmak istenen iznin belirli bir rol için o anda aktif olup olmadığı izinle ilişkili bağlam politikası ya da birleşik bağlam politikası tarafından belirlenir.

Rollere atanmış bazı izinler bağlam bilgisini kullanmamaktadır ve dolayısıyla bu izinler sürekli olarak aktif kalmaktadır. Belirli bir subjeden gelen erişim isteği, eğer ait olduğu rolün *RİA* listesinde bir bağlam bilgisi ile ilişkilendirilmemiş bir izin kullanımı gerektiriyorsa erişime doğrudan izin verilir. Buna, statik erişim izni kullanımı denilmektedir. Dinamik erişim izni kullanımında ise rollere atanmış erişim izinlerin ilgili role üye bir subje tarafından kullanımı talep edildiğinde izinle ilişkilendirilmiş önceden tanımlı bir bağlam kısıtı olup olmadığı kontrol edilir ve ancak mevcut bağlam durumunun buradaki bağlam kısıtını karşılaması halinde erişim izni aktif hale getirilerek subjenin kullanımına sunulur. Dolayısıyla, bir subje atanmış olduğu rol için tanımlanmış belirli bir erişim iznini kullanmak istediğinde talebin yapıldığı andaki durumun oluşturduğu bağlam bilgisine göre söz konusu izni kullanabilir veya kullanamaz. Bu çerçevede, çalışmamızda önerdiğimiz erişim denetimi yöntemi bağlam-duyarlı ve dinamik yapıya sahip olmaktadır.



Şekil 1. İzinler ve Bağlam Bilgisi İlişkisi

Yukarıda anlatılan erişim izinlerinin bağlama göre kullanımına ilişkin bir örnek Şekil 1'de verilmiştir. Buna göre, $İ_1$ izni herhangi bir bağlam bilgisine ihtiyaç duymaması sebebi ile sürekli aktif bir izindir, yani ilgili role üye bir subjeden bu izin ile ilgili bir erişim isteği geldiği her durumda izin verilir. $İ_2$ ise tek bir bağlam politikasına bağlıdır. Bağlam İfadesi izin talebinin geldiği anda geçerli ise erişim izini verilmeyecek, geçerli değil ise izin verilecektir. $İ_n$ izni için birleşik bağlam politikası tanımlanmış olduğundan her iki Bağlam İfadesinin de doğru olduğu durumda erişim izni verilecek, diğer durumlarda reddedilecektir.

Yukarıdaki açıklamalar ışığında, bu çalışmada önerdiğimiz Nesnelerin İnterneti kapsamında uygulanana bağlam-duyarlı rol-tabanlı erişim denetimi yönteminde bir subjenin bir objeye erişim sağlaması için aşağıdaki koşulların her birinin gerçekleşmesi gerekmektedir.

- Subje en az bir role atanmış olmalıdır.
- Subjenin atandığı rollerden biri, kullanmak istediği izine sahip olmalıdır.
- Kullanım talep edilen izin ile ilişkilendirilmiş bağlam bilgisi varsa o anki bağlam durumunu sağlamalıdır.

Yukarıda sözel olarak anlatılan erişim denetimi yöntemine ilişkin formal modeli oluşturabilmek için aşağıda verilen tanımların da yapılması gerekmektedir.

Tanım**:** $AtanmışSubjeler(r:Rol) \rightarrow 2^S$ Bir *r* rolüne atanmış subje setini ifade eder.

$AtanmışSubjeler(r) = \{s \in S \mid (s, r) \in SRA\}$

Tanım**:** $Atanmışİzinler(r:Rol) \rightarrow 2^İ$ Bir *r* rolüne atanmış izin setini ifade eder.

$Atanmışİzinler(r) = \{i \in İ \mid (r, i) \in RİA\}$

Tanım**:** *İzin Bağlam Ataması*: *İBA*, izinler ve ilgili oldukları bağlam politikaları arasındaki eşleme listesini ifade eder.

$İBA$, $İ_i \in İ$, $R_i \in R$ ve $BP_i \in BP$ olmak üzere $<İ_i, R_i, BP_i>$ üçlemesinden oluşmaktadır.

Tanım**:** $AtanmışBağlamlar (i: İzin, r: Rol) \rightarrow BP$ Bir *r* rolünün sahip olduğu *i* iznine atanmış bağlam politikasını ifade eder. Buna göre $AtanmışBağlamlar (i, r) = \{bp \in BP \mid (i, r, bp) \in İBA$

Tanım**:** *BağlamDurumu = {1, 0}* Bir bağlam politikası kuralının muhtemel sonuç setini ifade eder. Bir bağlam politikası kuralı o anki bağlam durumuna göre geçerli ya da geçersiz olabilir. Eğer geçerliyse *BağlamDurumu 1*, değilse *0* olur.

Tanım**:** *Bağlam Durumu Eşlemesi*: *BDE*, bağlam politikası kuralları ve onların durumu arasındaki eşleme listesini ifade eder. *BDE*, $BP_i \in BP$ ve *BD* $\in$ *BağlamDurumu* olmak üzere $<BP_i, BD>$ ikilemesinden oluşmaktadır.

Tanım**:** *AktifBağlamPolitikası={bp* $\in$ *BP* | *(bp, 1)* $\in$ *BDE} ve İnaktifBağlamPolitikası ={bp* $\in$ *BP* | *(bp, 0)* $\in$ *BDE}*

Yukarıdaki tanımlar çerçevesinde, bu makalede önerdiğimiz rol-tabanlı bağlam-duyarlı erişim denetimi modeli, bir Nİ uygulaması kapsamında *s* subjesinin *o* objesine erişim isteğini aşağıdaki ifadenin doğruluğuna göre değerlendirecektir:

(∀s:S) (∀i: İ): erişim izni var (s,i)⇒

(∃r: R) (∃i: İ): [s ϵ AtanmışSubjeler(r) ∧ i ϵ Atanmışİzinler(r)] ∧ [(AtanmışBağlamlar(i,r) = 0) V (AtanmışBağlamlar(i,r) ϵ AktifBağlamPolitikası)] ∧ ¬ [(∃r' : Rol) : (r' ≠ r) ∧ s ϵ AtanmışSubjeler(r') ∧ i ϵ Atanmışİzinler(r') ∧ AtanmışBağlamlar (i,r') ϵ İnaktifBağlampolitikası()]

Bu erişim denetimi modelindeki tanıma göre *"İ:izin (permission)",* obje ve obje üzerindeki erişim eylemini "*H:hak (right)*" bütünleşik olarak kapsamaktadır (örneğin *kapı:obje*, *açmak:hak*, *izin: kapıyı açmak*). Önerdiğimiz erişim denetimi modeli Şekil 2'de verilmiş olup ilgili akış diyagramı da Şekil 3'te verilmiştir.

Önerilen erişim denetimi modeline alternatif yaklaşım olarak ise Şekil 4'te gösterilen "hak" ve "obje"lerin bütünleşik değil bağlam-duyarlı erişim denetiminde ayrı ayrı ele alındığı yaklaşım kullanılabilir. Bu ikinci yaklaşım daha detaylı bir denetim kontrolü sağlasa da erişim politikalarında yazılması gereken güvenlik politikaları yönünden daha karmaşık bir yapı gerektireceği için yalnızca granülaritesi yüksek erişim denetimi gerektiği durumlarda kullanılması önerilmektedir. Bu yaklaşımda izinler objeler üzerinde belirli operasyonları gerçekleştirme hakkı olarak tanımlanmalıdır. Örneğin, 'açmak' izin, 'klima', 'TV' vb. bağlı bulunduğu objeler olarak düşünülebilir.

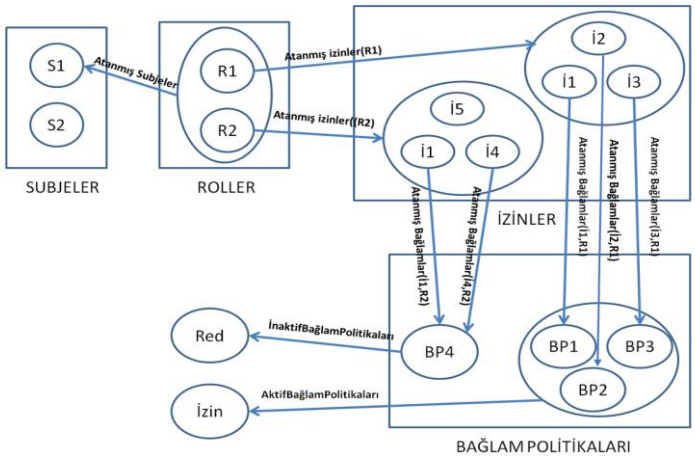
3.5 Yöntemin Uygulanması

Bu makalede önerilen erişim denetim yöntemi, çalışmamızın kapsamına giren çoklu ve karmaşık etkileşimli yeni Nesil Nİ uygulamalarını temsil eden örnek senaryo için uygulandığında ilgili Subje-Rol ve Rol-İzin atamalarının yapılmasıyla Tablo 2'de verilen güvenlik politikası kural seti ortaya çıkmaktadır. Bu kural seti ile örnek senaryo için yukarıda tanımlanan tüm erişim gereksinimlerinin kontrolü güvenli bir biçimde sağlanabilmektedir.

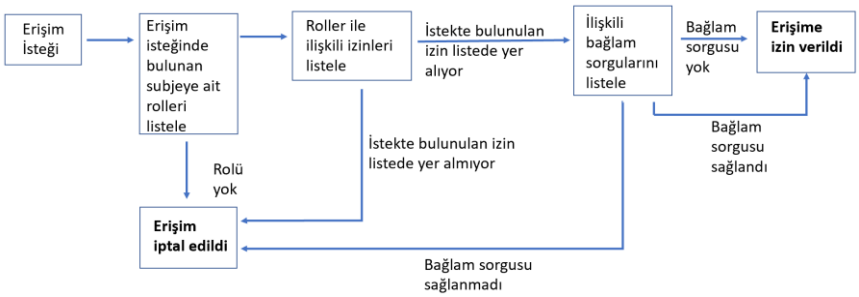
4. Bulgular ve Tartışma

Bu çalışmada önerdiğimiz bağlam-duyarlı erişim denetimi yöntemi, [8]'deki yönteme göre güvenlik politikasındaki kural sayısını azaltmaktadır. Önceki kısımda verilen örnek senaryoda 8 obje, 10 subje, 4 erişim hakkı (kamera izleme, kapı açma, uygulamaya erişim, veri okuma) ve 8 farklı bağlam bulunmaktadır (evin içinde/dışında olma, evde birinin olması, hareketsiz yatan birinin olması, sağlık riskinin yüksek olması, acil durum olması, ambulansın eve yakın olması, okul servisinin eve yakın olması, ebeveyn aracının eve yakın olması). Bu senaryoya, [8] tarafından geliştirilen ConUCON yöntemi uygulandığında, ilgili makalede verilen güvenlik politikası tanımına göre, en az 8 × 10 × 4 × 8 = 2650 adet farklı erişim isteğini denetleyebilecek karmaşıklıkta bir kural seti yazılmalıdır (S: subje sayısı, O: obje sayısı, E: erişim hakkı sayısı, OnContext: bağlam sayısı). Adı geçen yöntemde belirtilen, *zorunluluklar: PreOb* ve *OnOb*, *kısıtlar:StateConstraint*, *güncellemeler:Update* gibi daha esnek ve detaylı kural yazılmasını sağlayan ekstra bileşenlerin kullanılması durumunda hesaplama karmaşıklığı daha da artmaktadır. $UP \subseteq E \times O \times R \times PreOb \times OnOb \times StateConstraint \times PreContext \times OnContext \times Update$

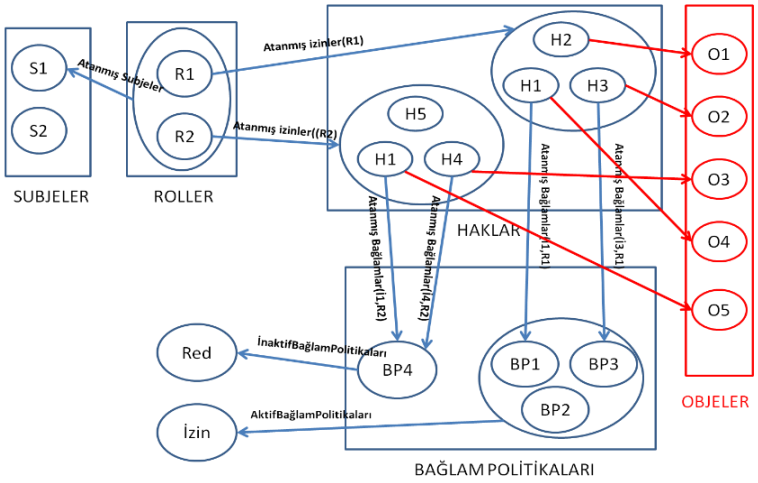
Önerdiğimiz yöntemde subjelerin tanımlanmış rollere atanması ve rollere atanan izinlerin bağlama göre aktive edilmesi ile güvenlik politikası tarafından kontrol edilmesi gereken erişim sayısının büyüklük derecesi azaltılabilmektedir. Bu durumda denetlenmesi gereken tüm erişim istekleri, bağlama göre aktif/pasif hale getirilen erişim izinleri içeren gerekli rol setinin (*R*) oluşturulması ve erişim talebinde bulunan subje setinin (*S*) bu rol setine atanması ile denetlenebilecek, dolayısıyla, kontrol altında tutulması gereken erişim kuralı sayısının büyüklük derecesinin *R* × *S* seviyesinde tutulması sağlanabilecektir.



Şekil 2. Önerilen Erişim Denetimi Modeli



Şekil 3. Erişim Denetimi Modeli Akış Diyagramı



Şekil 4. Alternatif Erişim Denetimi Modeli

Tablo 2. Örnek Senaryo için Erişim Denetimi Kural Seti

ROL-Subje	ROL-İzin	BAĞLAM	KİMLİK DOĞRULAMA	ERİŞİM İZNİ
EBEVEYN • Anne • Baba	Evin kapısındaki akıllı kilidi açma	_	biyometrik	VAR
		ebeveyn arabası eve yakınsa	giyilebilir/ mobil cihaz	VAR
		ebeveyn arabası eve yakınsa VE zaman iş saatiyse	giyilebilir/ mobil cihaz	YOK
	Kamera görüntüsünü izleme	_	biyometrik	VAR
ÇOCUK • Kız • Erkek	Evin kapısındaki akıllı kilidi açma	çocuk evin dışındaysa	biyometrik	VAR
		çocuk evin içindeyse VE (Ebeveyn evin içindeyse VEYA acil bir durumsa)	biyometrik	VAR
		okul servisi eve yakınsa	giyilebilir/ mobil cihaz	VAR
		okul servisi eve yakınsa VE zaman okul saatiyse	giyilebilir/ mobil cihaz	YOK
TANIDIK • Akraba • Arkadaş	kamera görüntüsünü 5 dakika süreyle izleme	acil bir durum varsa	parola	VAR
GÜNLÜK Nİ Uyg. • Nİ Ev • Nİ Araç	trafik/navigasyon bulut servisine erişim	_	parola	VAR
YAŞAM Nİ Uyg. • Nİ Sağlık • Nİ Spor	giyilebilir sensörler üzerinden spor (mesafe, hız, vb.) ve sağlık bilgilerine (nabız, vb.) bilgilerine erişim	_	parola	VAR

	giyilebilir sensörler üzerinden sağlık bilgilerine (nabız, vb.) erişim	erişim isteği Nİ Spor'dan geliyorsa ve kullanıcı o anda spor yapmıyorsa	parola	YOK
Nİ Sağlık	bulut üzerinden sağlık verilerine erişim	_	parola	VAR
	kitlesel kaynaklar üzerinden sağlık verilerine erişim	acil bir durum varsa	parola	VAR
	Nİ Ev uygulamasına acil durum bildirimi için erişim	hareketsiz yatan biri varsa VE sağlık verilerine göre yüksek risk varsa	parola	VAR
Nİ Ev	kamera görüntüsünü 640x480 çözünürlükle 5 dakika süreyle izleme	_	parola	VAR
	Nİ Sağlık uygulamasına erişim	evde hareketsiz yatan birisi varsa	parola	VAR
	evin kapısındaki akıllı kilidi açma	acil bir durum varsa VE evde başkası yoksa VE bir sağlık aracı eve yakınsa	parola	VAR

Bizim yöntemimizin [6] tarafından yaygın bilişim uygulamaları için geliştirilen ve basit etkileşimli Nİ senaryoları için de kullanılabilecek CA-RBAC yöntemine göre sağladığı avantaj ise yaratılması gereken rol sayısının daha az olmasıdır. CA-RBAC'de erişim isteğinde bulunan subjeler farklı bağlamlar için yaratılan rollere dinamik olarak atanmaktadır. Bizim yaklaşımımızda ise her bağlam için ayrı bir rol yaratılmasına gerek kalmadan bağlama göre rolün ilgili izninin aktif veya pasif hale getirilmesi planlanmaktadır. Tablo 3 ve Tablo 4'te, diğer yöntemde belirli bir subje için ancak üç farklı rol ile erişim kontrolü yapılabilen bir senaryoda, bizim yöntemimizin kullanılması durumunda tek rolün yeterli olabileceği gösterilmektedir.

Fazladan rol yaratımı ihtiyacı dışında CA-RBAC'teki bir başka problem de önerilen yöntemdeki "context-based object binding" özelliğinin neden olduğu kural yazma karmaşıklığıdır. Buna göre bağlam bilgisi ile yalnızca bir rolün kullanabileceği erişim izinleri (rol → hak- obje) değil objelerin kullanabildiği

Tablo 3. Önerdiğimiz yöntemde 5 erişim izni, 3 bağlam olan senaryoda bir subje için gerekli rol sayısı=1

Rol	**İzin**	**Bağlam**
R1	İ1	B1
	İ2	her durumda
	İ3	B2
	İ4	her durumda
	İ5	B3

Tablo 4. [6] CA-RBAC'da 5 erişim izni, 3 bağlam olan senaryoda bir subje için gerekli rol sayısı=3

Bağlam	Rol	İzin
B1	R1	İ1
		İ2
		İ4
B2	R2	İ2
		İ3
		İ4
B3	R3	İ2
		İ4
		İ5

veri kaynakları ve servisleri de (obje → servis-kaynak) kontrol edilebilmekte, böylece erişim denetiminde bağlama göre daha ayrıntılı bir kontrol yapılabilmektedir. Örneğin yukarıdaki örnek senaryoda Nİ Ev uygulamasının Nİ Sağlık uygulamasına erişimini düzenleyen bir kural bulunmaktadır. CA-RBAC'te bu kural yazılırken Nİ Ev'in Nİ Sağlık'a hangi bağlamda erişeceğinin belirtilmesi yeterli olmamakta, bu kuralda obje konumunda olan Nİ Sağlık'ın veri kaynaklarına (giyilebilir sensörler) ya da veri servislerine (bulut sağlık servisi) erişimini bağlam-duyarlı şekilde düzenleyen bilgilerin de aynı kurala yazılması gerekmekte, dolayısıyla erişim kuralları uzun ve karmaşık olabilmektedir. Bu çalışmada önerdiğimiz yöntemde erişim denetiminde bağlama göre ayrıntılandırma yapılmasını sağlayan bu özelliğin belirtilen karmaşıklığı yaratmadan uygulanması mümkündür. Bunun için tek bir uzun kuralda hem rollerin objelere hem de objelerin servislere/kaynaklara erişimini bağlam-duyarlı şekilde düzenlemek yerine, subjelerin duruma göre obje olarak da kullanılmasıyla birden fazla basit kural yazarak aynı düzenleme yapılabilir. Bu yaklaşımın bir örneği yukarıda tanımlanan kural setinde ayrı ayrı yazılan Nİ Ev (Subje) -Ni Sağlık (Obje) ve Ni Sağlık (Subje)-Bulut sağlık verileri (Obje) kurallarında görülebilmektedir.

Rol tabanlı erişim denetimi yöntemlerinde dikkat edilmesi gereken önemli hususlardan bir diğeri de güvenlik politikası ile uygulaması arasındaki uygunluktur (policy-implementation conformance). Erişim politikalarının yönetiminde RBAC kullanan modellerin uygulanmasında subje-rol ve rol-izin atamalarındaki olası çakışmaların (conflict) dikkatli bir biçimde yönetilmesi gerekmektedir [27]. Söz konusu çakışmalar güvenlik politikasının üç temel zorunluluğu olan *önkoşul (prerequisite), kardinalite (cardinality)* ve *görevler ayrılığı (SoD: Separation of Duties)* kurallarına aykırı uygulamalar yapılması ile ortaya çıkar. Örneğin bir kullanıcı ya *Çocuk* ya da *Ebeveyn* rolüne atanabilir, her iki rolde de yer alamaz (*statik görevler ayrılığı)*. Benzer şekilde, bir Nİ uygulaması verdiği servise göre *GÜNLÜK Nİ Uygulaması* ya da *YAŞAM Nİ Uygulaması* rollerine atanabilir ancak aynı anda yalnızca bu rollerden birinde aktif olabilir *(dinamik görevler ayrılığı)*. Erişim politikasının implementasyonunda eğer bu olası çakışmalar kontrol edilmez ve engellenmezse, örneğin bir çocuğun, evin içindeyken, ebeveyni evde yokken ve acil bir durum değilken kapıyı güvenlik politikasına aykırı şekilde açması mümkün olabilir. Bu tür politika ve rol-izin çakışmalarının önlenmesi için literatürde önerilen çözümlerden biri sonlu model kontrolü (finite model checking) yapılmasıdır [28]. Bu yaklaşımda SPIN aracıyla güvenlik politikası, izin verilen ve engellenen sistem davranışları olarak ifade edilir, Lineer Zamansal Mantık (LTL) ile politika kısıtları tanımlanır ve SPIN'in modelleme dili olan PROMELA ile uygulamaya geçirilir. LTL ifadeleri ve PROMELA kodu karşılaştırılarak politika ile uygulama arasında çakışma olup olmadığu kontrol edilir. Bizim önerdiğimiz yöntemde çakışma yönetimi için benzer bir yaklaşım izlenmesi öngörülmüştür.

5. Sonuç ve Öneriler

Yukarıda ayrıntıları verilen bağlam-duyarlı rol-tabanlı erişim denetimi yönteminin hayata geçirilmesi için JAVA programlama dili kullanılarak bir ön prototip uygulaması yapılmıştır. Bu prototip uygulamanın temel bileşenlerini gösteren Sistem Mimarisi Şekil 5'te verilmiştir. Bu mimarinin bileşenleri aşağıda açıklanmakta, akış şeması Şekil 6'da gösterilmektedir.

Politika Uygulama Birimi-PUB: Subjeden gelen erişim isteği ilk olarak bu birim tarafından karşılanarak, değerlendirilmek üzere Politika Karar Birimine iletilir. Politika Karar Biriminden gelen cevap yine PUB aracılığı ile subjeye iletilir.

Politika Karar Birimi-PKB: PUB'dan gelen istek doğrultusunda, erişim izni verilmesi için gerekli kontrolleri yapmak üzere ilişkili çevre birimlerini (SRV: Subje Rol Veritabanı, RİV: Rol İzin Veritabanı, BV: Bağlam Veritabanı) sorgulayarak sonucu PUB'a iletir.

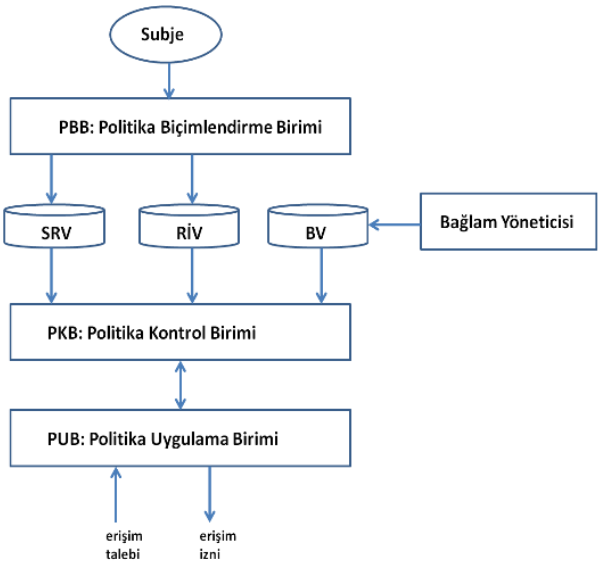
Politika Biçimlendirme Birimi-PBB: Erişim politikaları PBB arayüzü ile sistem yöneticisi tarafından oluşturulmaktadır.

Bağlam Yöneticisi-BY**:** PK'nin erişim kararı verebilmesi için izin ile ilişkilendirilen bağlam bilgisinin anlık durumunun kontrol edilmesi gerekmektedir. Bağlam veritabanında farklı türdeki bağlam bilgilerinin anlık değerleri tutulmaktadır. Bağlam Yöneticisi, farklı sensörlerden ya da bağlam sağlayıcı servislerden gelen bağlam bilgisini veritabanına kaydeder ve günceller. Çalışmamızın ana kapsamının güvenlik uygulaması olması sebebi ile bağlam bilgileri veritabanına manuel olarak girilmektedir.

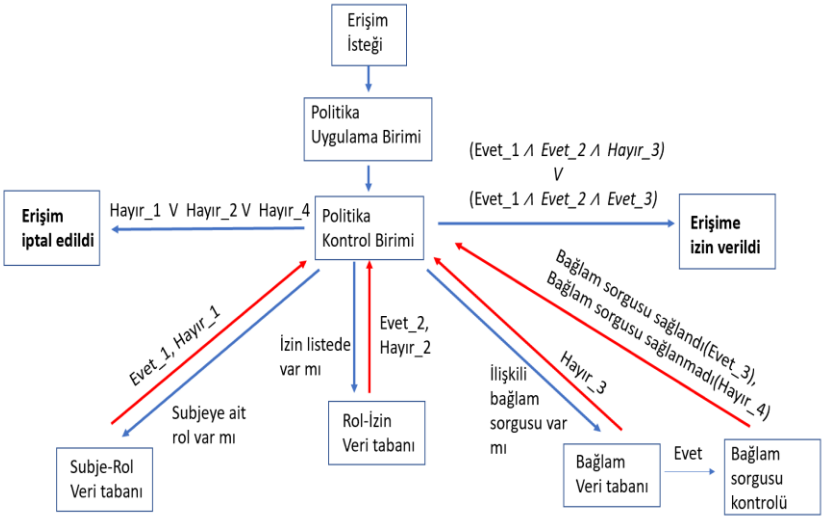
Prototip uygulama ile önerilen kavramsal yöntemin uygulamada çalıştığı gösterilmiş ve hem güvenlik hem de performans testleri yapılmıştır. Prototip uygulamanın performans başarım ölçümünde temel dört performans metriği kullanılmış olup bunlar (i) erişim isteğine cevap süresi, (ii) işlemci kullanım oranı, (iii) bellek kullanım miktarı ve (iv) saldırı senaryoları altında erişim isteğine cevap süresidir. Yukarıdaki örnek senaryo için prototip uygulama performans sonuçları yapılan 100 erişim talebinin ortalaması alınarak hesaplanmıştır. Buna göre, erişim isteğine cevap süresi 203 milisaniye, işlemci kullanım oranı %6, hafıza kullanım miktarı 9 MB ve saldırı altında cevap süresi 430 milisaniyedir.

Performans testleri dışında prototip uygulama üzerinde önceki bölümlerde belirlenen zafiyetleri ve tehdit vektörlerini sınayacak şekilde güvenlik testleri de gerçekleştirilmiştir. Güvenlik testlerinde uygulanan ana yöntem, Tablo 5'te verilenen saldırı türlerinin prototip uygulama üzerinde ayrı ayrı gerçeklenmesi ve her saldırı sonucunda yetkisiz kişilere erişim izni verilmediğinin, yetkili kişilere ise yetkileri ile uyumlu erişim izni verildiğinin gözlemlenmesidir. Güvenlik testlerinde kimlik doğrulaması için [29]'da önerilen çoklu seviyeli yaklaşım uygulanmıştır. Bu güvenlik testlerinin tamamı olumlu sonuçlanmış ve uygulamanın yetkili erişimlere izin verirken yetkisiz erişimleri başarıyla engellediği tespit edilmiştir.

Görüldüğü üzere, bu makalede bağlam duyarlı rol tabanlı erişim denetimi yöntemi ile çoklu ve karmaşık etkileşimli Nİ cihazlarının yer aldığı bir senaryosda sade güvenlik politika kuralları ile olası saldırıların mevcut yöntemlere göre daha az karmaşık kural setleriyle ve kabul edilebilir çalışma performansı ile engellenebilmektedir.



Şekil 5. Temel Sistem Mimarisi



Şekil 6. Sistem Mimarisi Akış Diyagramı

Tablo 5. Uygulanan Saldırı Türleri ve Güvenlik Testleri

Saldırı Türü	**Güvenlik Testi**	**Yöntemin Sınanan Özelliği**
Kimlik taklit etme	Yetkisiz kişinin yetkili mobil cihaz ile ev kapısını açmayı denemesi	Bağlam duyarlı erişim denetimi
Bağlam bilgisini değiştirme	Acil durum oluştuğuna dair sahte bağlam bilgisi oluşturularak ev kapısının açılmaya çalışılması	Çapraz bağlam kontrolü
Bağlam bilgisini geçersiz hale getirme	Servis konum bilgisini bozarak yetkili kişinin ev kapısını açmasının engellenmek istenmesi	Çoklu seviyeli kimlik doğrulama
Bağlam taklit etme	Yetkisiz kişilerin (mobil cihazı çalan & servis şoförü) kötü niyetli işbirliği ile erişim yetkisine sahip bağlam oluşturup kapıyı açma denemesi	Çapraz bağlam kontrolü ve çoklu kimlik doğrulamanın birlikte kullanımı

Kaynakça

[1] Abowd G.D. 2016. Beyond Weiser: From Ubiquitous to Collective Computing, Computer, 49 (1): 17-23.

[2] Weiser M. 1991. The Computer for the 21st Century, Scientific American, 265 (3): 78-89.

[3] Al-Muhtadi J., Ranganathan A., Campbell R., Mickunas M.D. 2003. Cerberus: A Context-aware Security Scheme for Smart Spaces, Proceedings of the 1st IEEE International Conference on Pervasive Computing and Communications, pp489-494, 23-26 March, Texas.

[4] Covington M.J., Long W., Srinivasan S., Dey A.K., Ahamad M., Abowd G.D. 2001. Securing Context-aware Applications Using Environmental Roles, SACMAT '01 Proceedings of the 6th ACM Symposium on Access Control Models and Technologies, pp10-20, 3-4 May, Chantilly.

[5] Covington M.J., Fogla P., Zhan Z., Ahamad M. 2002. A Context-aware Security Architecture for Emerging Applications, Proceedings of 18th Annual Computer Security Applications Conference, pp124-131, 9-13 December, New Orleans.

[6] Kulkarni D., Tripathi A. 2008. Context-aware Role-based Access Control in Pervasive Computing Systems, SACMAT '08 Proceedings of the 13th ACM Symposium on Access Control Models and Technologies, pp113-122, 11-13 June, Estes Park.

[7] Wrona K., Gomez L. 2005. Context-aware Security and Secure Context-awareness in Ubiquitous Computing Environments, XXI Autumn Meeting of Polish Information Society Conference Proceedings, pp255-265, 5-9 December, Katowise.

[8] Bai G., Yan L., Gu L., Guo Y., Chen X. 2014. Context-aware Usage Control for Web of Things, Security and Communication Networks, 7 (12): 2696-2712.

[9] Genç D., Tomur E., Erten Y.M. 2019. Context-aware Operation-based Access Control for Internet of Things Applications, International Symposium on Networks, Computers and Communications, pp235-256, 19-20 June, İstanbul.

[10] Genç D. 2018. Context Aware Role Based Access Control Model For Internet Of Things Applications, Yüksek Lisans Tezi, izmir Yüksek Teknoloji Enstitüsü.

[11] Kayes, A.S.M., Kalaria, R., Sarker, I.H., Islam, M., Watters, P.A., Ng, A., Hammoudeh, M., Badsha, S. and Kumara, I., 2020. A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues. Sensors, 20(9), p.2464.

[12] Dong, Y., Wan, K., Huang, X. and Yue, Y., 2018, May. Contexts-states-aware access control for internet of things. IEEE 22nd International Conference on Computer Supported Cooperative Work in Design pp. 666-671.

[13] Roman R., Zhou J., Lopez J. 2013. On the Features and Challenges of Security and Privacy in Distributed Internet of Things, Computer Networks, 57 (1): 2266-2279.

[14] Gubbi J., Buyya R., Marusic S., Palaniswami M. 2013. Internet of Things (IoT): A Vision Architectural Elements and Future Directions, Future Generation Computer Systems, 29 (1): 1645-1660.

[15] Sfar A.R., Natalizio E., Challal Y., Chtourou Z. 2017. A Roadmap for Security Challenges in Internet of Things, Digital Communications and Networks, 4 (2): 118-137.

[16] 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 (1): 146-164.

[17] Vasilomanolakis E., Daubert J., Luthra M., Gazis V., Wiesmaier A., Kikiras P. 2015. On the Security and Privacy of Internet of Things, Architectures and Systems, Proceedings of the 2015 International Workshop on Secure Internet of Things (SIoT), pp49-57, 21-25 September, Washington, D.C.

[18] Jin X., Sandhu R., Krishnan R. 2012. RABAC: Role-centric Attribute-based Access Control, International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, pp84-96, 17-19 October, St. Petersburg.

[19] Rajpoot Q.M., Jensen C.D., Krishnan R. 2015. Attributes Enhanced Role-based Access Control Model, 12th International Conference on Trust, Privacy and Security in Digital Business, pp342-357, 1-2 September, Valencia.

[20] Schilit B., Theimer M. 1994. Disseminating Active Map Information to Mobile Hosts, Network, IEEE, 8 (5): 22-32.

[21] Abowd, G.D., Dey A.K., Brown P.J., Davies N., Smith M., Steggles P. 1999. Towards a Better Understanding of Context and Context-awareness, Proceedings of the 1st International Symposium on Handheld and Ubiquitous Computing, pp304-307, 27-29 September, Karlsruhe.

[22] Perera C., Zaslavsky A., Christen P., Georgakopoulos D. 2013. Context-aware Computing for the Internet of Things: A Survey, IEEE Communications, Surveys and Tutorials, 16 (1): 414-454.

[23] Perera C., Liu C.H., Jayawardena S., Chen M. 2014. Context-aware Computing in the Internet of Things: A Survey on Internet of Things From Industrial Market Perspective, IEEE Access, 2 (1): 1660-1679.

[24] Abdella J., Özuysal M., Tomur E. 2016. CA-ARBAC: Privacy Preserving Using Context-aware Role-based Access Control on Android Permission System, Security and Communication Networks, 5977-5995.

[25] Trnka M., Cerny T. 2016. On Security Level Usage of Context-aware Role-based Access Control, SAC '16 Proceedings of the 31th Annual ACM Symposium on Applied Computing, pp1192-1195, 4-8 April, Pisa.

[26] Erten Y.M., Tomur E. 2004. A Layered Security Architecture for Corporate 802.11 Wireless Networks, IEEE Wireless Telecommunications Symposium, pp123-128, 14-15 May, Pomona.

[27] Cheng, X.R., Chen, X.Y. , Bin, Z., 2010. Research on RBAC policy conflict and its detection algorithm Computer Engineering, 36(18), pp.135-137.

[28] Moon CJ., Paik W., Kim YG., Kwon JH., 2005. The Conflict Detection Between Permission Assignment Constraints in Role-Based Access Control, Lecture Notes in Computer Science, vol 3822. Springer, pp.144-155, Berlin.

[29] Huang X., Craig P., Lin H., Yan Z. 2016. SecIoT: A Security Framework for the Internet of Things, Security and Communication Networks, 9 (16): 3083-3094.