

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

**ÖZNİTELİK TEMELLİ ERİŞİM KONTROL(ABAC) MODELİNİN NESNELERİN
İNTERNETİNE UYGUNLUĞUNUN ARAŞTIRILMASI VE GEREKLİ
GENİŞLETMELERİN YAPILMASI**

DOKTORA TEZİ
Melike BURAKGAZİ BİLGİN

Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof.Dr. Ali Aydın SELÇUK

EKİM 2024

ÖZET

Doktora Tezi

ÖZNİTELİK TEMELLİ ERİŞİM KONTROL(ABAC) MODELİNİN NESNELERİN İNTERNETİNE UYGUNLUĞUNUN ARAŞTIRILMASI VE GEREKLİ GENİŞLETMELERİN YAPILMASI

Melike BURAKGAZİ BİLGİN

TOBB Ekonomi ve Teknoloji Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof.Dr. Ali Aydın SELÇUK

Tarih: EKİM 2024

Nesnelerin İnterneti (IoT), çok sayıda cihazın birbirleriyle iletişim kurduğu, birbirine bağlı bir ortamdır ve bu durum mahremiyet ve güvenlik sorunları oluşturmaktadır. Kullanıcıların IoT teknolojisini günlük yaşamlarında tam olarak benimsemeleri için bu ekosisteminin temel ağ, sistem ve güvenlik gereksinimlerini karşılaması kritik öneme sahiptir.

IoT uygulamaları, sensörler, kullanıcılar ve diğer bağlı cihazlar gibi çeşitli kaynaklardan hassas bilgiler toplayabilir. IoT cihazları giderek günlük rutinlerimize entegre oldukça önemli güvenlik ve mahremiyet endişelerini beraberinde getirir. Zayıf kimlik bilgileri, yetersiz kimlik doğrulama protokolleri ve yetersiz mahremiyet koruma IoT sistemleri içindeki başlıca zafiyetlerdir. Bu sorunların ele alınması, kullanıcı ve sistem güvenliğini artırmak ve IoT teknolojilerinin daha geniş bir şekilde benimsenmesini sağlamak açısından önemlidir.

Bu tez, IoT güvenliği bağlamında kullanıcı kimlik doğrulama, erişim kontrolü ve mahremiyet gibi kritik konuları, özellikle akıllı ev ortamlarına odaklanarak incelemektedir. Yetkisiz erişimi önlemek ve kişisel verilerin mahremiyetini sağlamak için detaylı ve dinamik bir erişim kontrolü esastır. Bu bağlamda, Öznitelik Tabanlı Erişim Kontrolü(ABAC) modeli uygun bir yaklaşım olarak ortaya çıkmaktadır. Bu tez, ABAC modelini üç aşamada genişletmektedir. İlk aşamada, genişletilmiş ABAC modeli, kullanıcı kimlik doğrulama sırasında elde edilen biyometrik eşleşme puanına (AMS) dayalı olarak kimlik doğrulama güvence seviyesini belirlemek için yenilikçi bir yöntem sunmaktadır. Bu puan, önceden tanımlanmış eşiklerle karşılaştırılarak, kullanıcının rolü ve kimlik doğrulama güvence seviyesi temelinde ince ayar yapılmış erişim kontrol kararları alınmasına olanak tanır.

İkinci aşamada, ABAC modeli Kimlik Doğrulama Yeteneğine Sahip ABAC modeli olarak genişletilmiştir(AeABAC). Erişim kararı verme sürecini geliştirmek için performans ölçütleri modele entegre edilmektedir. Yanlış Eşleşme Oranı (FMR) hesaplanarak ve Erişim Karar Belirsizliği Skoru (ADUS) tanımlanarak, AeABAC modeli, geniş biyometrik kimlik doğrulama cihazları ve algoritmaları yelpazesi arasında etkili normalizasyon sağlamaktadır. Cihaz işlevselliği, kritik, önemli ve temel kritiklik seviyelerine göre kategorize edilerek buna göre erişim kararları alınır. Bu yaklaşım, özellikle biyometrik kimlik doğrulamanın yaygın olduğu akıllı evlerde, IoT ortamlarında erişimi kontrol etmek için daha esnek ve ölçeklenebilir bir yöntem sunmaktadır. İlk iki aşama, akıllı ev ekosistemlerinde sistemden kullanıcıya güven oluşturmaya odaklanmaktadır.

Üçüncü ve son aşamada, kullanıcının mahremiyetinin korunmasına yönelik sorunlara etkili çözümler üretilmesine odaklanılmıştır. Kimlik doğrulama ve yetkilendirme süreçleri, sistem güvenliğini sağlamaktadır (sistemden kullanıcıya güven); ancak bu aşamadan sonra, sistemlerin istenen işlevi yerine getirebilmesi için kullanıcıların hassas verilerine ihtiyaç duyulmaktadır. Bu noktada kullanıcılar, mahremiyetlerinin korunmasına öncelik vermek isterler (kullanıcıdan sisteme güven). Bu tezde, kullanıcıların veri mahremiyetine olan güvenlerini artırmak amacıyla, AeABAC modeline Risk Tabanlı mahremiyet Yaklaşımı entegre edilerek RBP-AeABAC modeli önerilmiştir. Önerilen yaklaşım, akıllı ev ortamında mahremiyet profillerini tanımlayarak veri ifşa olasılığını ve potansiyel zararları (ifşa etkisi) değerlendiren bir mahremiyet riski analizi sunmaktadır. Bu sayede, veri toplama ve ifşa süreçlerinde şeffaf ve güvenilir bir koruma sağlanarak kullanıcı mahremiyetini güvence altına alınmaktadır. Model, kullanıcı mahremiyetini gözeterek veri ifşasının olasılığı ve etkisini değerlendirip, kullanıcıların bilinçli kararlar alabilmesine olanak tanır. Kullanıcı tanımlı mahremiyet profilleriyle özelleştirilen bu yaklaşım, bireysel mahremiyet ihtiyaçlarına yönelik korumalar sunmaktadır. Modelin uygulanabilirliği çeşitli kullanım senaryolarıyla gösterilmiştir.

Bu tez kapsamında genişletilen ABAC modeli sadece akıllı evlerdeki IoT cihazlarının güvenliğini güçlendirmekle kalmayıp, aynı zamanda mahremiyet risklerini yönetmek için kapsamlı bir çerçeve oluşturmaktadır. Biyometrik kimlik doğrulama, performans metriklerine dayalı erişim kontrolü ve mahremiyet risk değerlendirmelerini birleştirerek, bu tez, IoT ortamlarında kullanıcılar ve sistem arasındaki iki yönlü güveni artıran yenilikçi bir çözüm sunmaktadır. **Anahtar**

Kelimeler: ABAC, Akıllı evler, IoT, mahremiyet, Erişim kontrolleri

ABSTRACT

Doctor of Philosophy

**EXPLORING THE ADAPTABILITY OF THE ATTRIBUTE BASED ACCESS CONTROL
MODEL TO THE INTERNET OF THINGS AND MAKING NECESSARY EXTENSIONS**

Melike BURAKGAZİ BİLGİN

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Department of Computer Science

Supervisor: Prof.Dr. Ali Aydın SELÇUK

Date: OCTOBER 2024

The Internet of Things (IoT) is an interconnected environment where numerous devices communicate with each other, which poses privacy and security challenges. For users to fully adopt IoT technology in their daily lives, it is crucial that this ecosystem meets fundamental network, system, and security requirements.

IoT applications can collect sensitive information from a variety of sources, including sensors, users, and other connected devices. As IoT devices increasingly integrate into our daily routines, the absence of strong authentication and access control mechanisms raises significant security and privacy concerns. Weak credentials and insufficient authentication protocols remain key vulnerabilities within IoT systems, making it crucial to address these issues to enhance user trust and facilitate broader adoption of IoT technologies.

This thesis explores critical aspects of user authentication, access control, and privacy within the context of IoT security, focusing particularly on smart home environments. To ensure the privacy of personal data and prevent unauthorized access, detailed and dynamic access control is essential. In this regard, the attribute-based access control (ABAC) model proves to be a suitable approach. This thesis extends Attribute-Based Access Control (AeABAC) model in three stages.

In the first stage, the model introduces an innovative method for determining the authentication assurance level based on the biometric match score (AMS) obtained during user authentication. This score is compared to predefined thresholds, allowing for fine-grained access control decisions based on the user's role and authentication assurance level.

In the second stage, performance metrics are integrated into the ABAC model to enhance decision-making. By calculating the False Match Rate (FMR) and defining an Access Decision Uncertainty Score (ADUS), the AeABAC model enables effective normalization across a wide range of biometric authentication devices and algorithms. It categorizes device functionality by criticality level and makes access decisions accordingly. This approach demonstrates a more flexible and scalable method for controlling access in IoT environments, particularly in smart homes where biometric authentication is common. The first two stages focus on establishing system-to-user trust in smart home ecosystems.

In the third and final phase, the focus is on developing effective solutions to issues related to the protection of user privacy. Authentication and authorization processes ensure system security (system-to-user trust); however, after this stage, systems require users' sensitive data to perform the desired functions. At this point, users want to prioritize the protection of their privacy (user-to-system trust). In this thesis, to enhance users' trust in data privacy, a Risk-Based Privacy Approach is integrated into the AeABAC model, resulting in the proposed RBP-AeABAC model. This approach offers a privacy risk analysis that assesses the likelihood of data disclosure and potential harms (disclosure impact) by defining privacy profiles in the smart home environment. This way, transparent and reliable protection is provided in data collection and disclosure processes, ensuring user privacy. The model allows for an evaluation of the likelihood and impact of data disclosure while considering user privacy, enabling users to make informed decisions. This user-defined privacy profile approach offers protections tailored to individual privacy needs. The model's applicability is demonstrated through various use-case scenarios.

The proposed extensions of the ABAC model in this thesis not only enhance the security of IoT devices in smart homes but also offer a comprehensive framework for managing privacy risks. By integrating biometric authentication, performance metric-based access control, and privacy risk assessments, this thesis presents an innovative solution that fosters bidirectional trust between users and systems in IoT environments. Future research will investigate the model's scalability and its applicability in larger IoT ecosystems.

Keywords: ABAC, Smart homes, IoT, Privacy, Access controls

TEŞEKKÜR

Çalışmalarım boyunca değerli yardımları ve katkılarıyla beni yönlendiren, yoluma ışık tutan kıymetli hocam Prof. Dr. Osman ABUL'a sabrı ve değerli destekleri için en içten teşekkürlerimi sunarım. Değerli hocam Prof. Dr. Ali Aydın SELÇUK'a bu zorlu süreçteki kıymetli desteği, rehberliği, bana olan inancı ve katkıları için minnettarım. Tez izleme komitemde yer alan saygıdeğer hocam Prof. Dr. Kemal BIÇAKÇI'ya destekleri ve yol gösterici katkıları için şükranlarımı sunarım ,

TOBB Ekonomi ve Teknoloji Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyelerine, kıymetli tecrübelerinden faydalanma imkânı sundukları için teşekkür ederim.

Bana ilmin ve eğitimin önemini aşılayan, her daim kendimi geliştirmem için beni yüreklendiren, maddi ve manevi destekleriyle varlıklarını yanımda hissettiren, haklarını asla ödeyemeyeceğim canım babam Suphi ve annem Sülbiye BURAKGAZİ'ye; her zaman yanımda olan, bu süreçte beni sabır ve anlayışla destekleyen, bana olan inancıyla beni daima motive eden, yolumda karşıma çıkan engelleri aşmamı kolaylaştıran sevgili eşim Akif Sinan BİLGİN'e; birlikte geçireceğimiz zamandan fedakârlık ederek bana çalışmam için uygun ortamı anlayışla sağlayan, varlıklarıyla hayatımıza neşe katan canım kızlarım Ayşe Ceren ve Defne Betül'e; ve her daim yanımda olan, beni sevgi ve şefkatleriyle kuşatan ve beni her zaman cesaretlendirip bana yol gösteren sevgili ablalarım Evren, Hatice, Ayşe Serap ve Betül'e ve abim Ahmet Zübeyir'e ve eniştem(abim) Erhan'a sonsuz teşekkürlerimi sunarım.

İÇİNDEKİLER

	<u>Sayfa</u>
ÖZET	iv
ABSTRACT	vi
TEŞEKKÜR	viii
İÇİNDEKİLER	ix
ŞEKİL LİSTESİ	xi
ÇİZELGE LİSTESİ	xii
KISALTMALAR	xiii
1. GİRİŞ	1
1.1 Tezin Amacı	3
1.2 Tezin Literatüre Kattıkları	6
1.3 Tezin Düzeni	8
2. ABAC MODELİNİN KİMLİK BİLGİSİ İLE DESTEKLENEREK IOT İÇİN GENİŞLETİLMESİ	11
2.1 Erişim Kontrol Modelleri	11
2.2 Öznitelik Temelli Erişim Kontrolü (ABAC)	13
2.2.1 Genişletilebilir erişim kontrol işaretleme dili (XACML)	14
2.3 Nesnelerin İnternetinde Erişim Kontrol İhtiyaçları ve ABAC	17
2.4 Literatür Taraması	19
2.5 Kimlik Bilgisi ile Desteklenmiş Öznitelik Tabanlı Erişim Kontrol Modeli- nin Genişletilmesi	22
2.6 Kullanıcı Kimlik Doğrulaması ve Yetkilendirme	27
3. AKILLI EVLERDE KİMLİK DOĞRULAMA ÖZELLİKLİ ABAC (Ae- ABAC)	31
3.1 AeABAC Modeli	31
3.2 Kullanıcı Kimlik Doğrulamasının Güvence Düzeyi	33
3.2.1 1. Senaryo	34
3.2.2 2. Senaryo	35
3.2.3 3. Senaryo	37
3.3 Akıllı Evler için AeABAC Modeli	40
3.3.1 Tanımlar	40
3.3.2 Öznitelikler	42
3.3.3 Örnekler	44
3.3.4 İşlevsellik Temelli Erişim Kararları	46
3.3.5 Uygulanabilirlik	48

3.4 Örnek Akıllı Ev Senaryoları ve XACML Uygulaması	50
3.5 AeABAC Modelinin Literatür Karşılaştırması	51
3.6 Mevcut IoT Çerçevelerine Modelimizi Uyarlama Çalışmaları	55
3.6.1 Azure IoT	55
3.6.2 ThingsBoard	56
4. RİSK TABANLI MAHREMİYET YAKLAŞIMI İLE AeABAC (RBP-AeABAC)	
MODELİ	59
4.1 Literatür Taraması	61
4.2 Akıllı Ev Ekosisteminde Mahremiyet	64
4.2.1 Kullanıcıların perspektifinden mahremiyet	64
4.2.2 Üreticilerin perspektifinden mahremiyet	67
4.2.3 Mahremiyet normları	69
4.2.4 Mahremiyet politikaları	71
4.2.5 RBP-AeABAC Modeli	73
4.3 Akıllı Evlerde Kullanıcı Mahremiyet Risk Değerlendirmesi	75
4.3.1 İfşa Etkisi	76
4.3.2 İfşa Olasılığı	80
4.3.3 Mahremiyet Profilleri	84
4.3.4 Birden Fazla Alternatif Cihazla Karar Alma	88
4.4 Uygulama ve Kullanım Senaryoları	89
4.4.1 Senaryo I	89
4.4.2 Senaryo II	91
4.4.3 Senaryo I için XACML Uygulaması	92
4.4.4 Akıllı ev ortamına yeni bir cihaz eklenmesi	94
5. SONUÇ VE ÖNERİLER	97
KAYNAKLAR	99
EKLER	106
ÖZGEÇMİŞ	119

ŞEKİL LİSTESİ

	<u>Sayfa</u>
Şekil 2.1: ABAC modeli	15
Şekil 2.2: OASIS XACML Akış Diyagramı	16
Şekil 2.3: Genişletilmiş ABAC Modeli	24
Şekil 2.4: Akıllı Evdeki Özniteliklerin Detayları	25
Şekil 3.1: HXKJ V4.3 Metrikleri [36].	36
Şekil 3.2: Senaryo I için FMR Değerleri	37
Şekil 3.3: MMFV 12.0 Metrikleri[36].	38
Şekil 3.4: Senaryo II için FMR değerleri	39
Şekil 3.5: HXKJ 3.02 Metrikleri [36].	41
Şekil 3.6: FMRs for the Scenario III	42
Şekil 3.7: Erişim karar kurallarının tablosal gösterimi	47
Şekil 3.8: Cihaz İşlevlerinin kritiklik seviyelerinin tablosal gösterimi	47
Şekil 3.9: AMS kullanıldığı durumda 5 farklı biyometrik cihaz için erişim kararlarının tablosal gösterimi	49
Şekil 3.10: Örnek Akıllı Ev Ortamı	50
Şekil 3.11: Kullanıcı, Kaynak ve Aksiyon Öznitelikleri	52
Şekil 3.12: Çevresel Öznitelikler	53
Şekil 3.13: Akıllı Ev ABAC Politikaları	53
Şekil 3.14: Azure Platform’unda Özel Tanımlanmış Roller	56
Şekil 3.15: Azure Platform’unda Tam Kimliği Doğrulanmış Rolünün Bazı Yetkileri	57
Şekil 4.1: AeABAC için Risk Tabanlı Mahremiyet Yaklaşımı (RBP-AeABAC)	75
Şekil 4.2: Kategorilerine Göre Akıllı Ev Ortamında Kullanılan Bilgiler.	78
Şekil EK 3.1: ThingsBoard Ortam Bileşenleri	116
Şekil EK 3.2: Yetişkin Rolü Yetkilendirme	116
Şekil EK 3.3: Eş Rolü Yetkilendirme	117
Şekil EK 3.4: Çocuk Rolü Yetkilendirme	117
Şekil EK 3.5: Akıllı Cihaz İşlevleri ve Kritiklik Seviyeleri	117
Şekil EK 3.6: Eş Rolü Gösterge Paneli	118
Şekil EK 3.7: Çocuk Rolü Gösterge Paneli	118
Şekil EK 3.8: Bebek Bakıcı Rolü Gösterge Paneli	118

ÇİZELGE LİSTESİ

	<u>Sayfa</u>
Çizelge 2.1: Nesnelerin Internetinde Erişim Kontrol Gereksinimleri Anketi	22
Çizelge 3.1: Erişim Kontrol Politikalarındaki Kural Sayısı	50
Çizelge 3.2: AeABAC Modelinin Literatür İçinde Konumlandırılması	55
Çizelge 4.1: Akıllı Ev Ortamı İçin Bilgi Kategorileri.	77
Çizelge 4.2: Veri Setindeki Bilgilerin İfşa Etkisi	80
Çizelge 4.3: Mahremiyet Kriterlerine Dayalı Cihaz Güvenlik Puanları	83
Çizelge 4.4: Çocuk Mahremiyet Profili için Mahremiyet Onay Kararları.	86
Çizelge 4.5: Bakıcı Mahremiyet Profili için Mahremiyet Onay Kararları.	86
Çizelge 4.6: Misafir Mahremiyet Profili için Mahremiyet Onay Kararları.	87
Çizelge 4.7: Genç Mahremiyet Profili için Mahremiyet Onay Kararları.	87
Çizelge 4.8: Eş Mahremiyet Profili için Mahremiyet Onay Kararları.	87

KISALTMALAR

IoT	: Nesnelerin Interneti (Internet of Things)
ABAC	: Öznitelik Temelli Erişim Kontrolü (Attribute Based Access Control)
RBAC	: Rol Temelli Erişim Kontrolü (Role Based Access Control)
AeABAC	: Kimlik Doğrulama Yeteneğine Sahip ABAC (Authentication enabled Attribute Based Access Control)
PIP	: Politika Bilgi Noktası (Policy Information Point)
PAP	: (Policy Administrator Point)
PDP	: Politika Karar Noktası (Policy Decision Point)
PEP	: Politika Uygulama Noktası (Policy Enforcement Point)
XACML	: Genişletilebilir Erişim Kontrol İşaretleme Dili
EER	: Eşit Hata Oranı (EER)
ACC	: Maksimum Doğruluk (ACC)
AMS	: Kimlik Doğrulama Eşleşme Puanı (Authentication Matching Score)
FMR	: Yanlış Eşleşme Oranı (False Match Rate)
FNMR	: Yanlış Eşleşmeme Oranı (False Non Match Rate)
ADUS	: Erişim Kararı Belirsizlik Puanı (Access Decision Uncertainty Score)
ROC	: Alıcı Operatör Karakteristik Eğrisi (Receiver Operator Characteristic Curve)
TPR	: Gerçek Pozitif Oranı (True Positive Rate)
FPR	: Yanlış Pozitif Oranı (False Positive Rate)
AUROC	: ROC Eğrisi Altındaki Alan (Area Under ROC Curve)
DET	: Karar Hata Takası (Decision Error Tradeoff)
RBP-AeABAC	: AeABAC Modeli için Risk Tabanlı Mahremiyet Yaklaşımı (Risk-based Privacy Approach for AeABAC Model)

1. GİRİŞ

Geçmişte yalnızca cep telefonları, tabletler ve bilgisayarlar internete bağlıyken, günümüzde güvenlik kameraları, mikrodalga fırınlar, arabalar ve endüstriyel ekipmanlar da internete bağlanabilmektedir. Nesnelerin İnterneti (IoT), buzdolabı ve fırın gibi cihazlara CPU ve sensör ekleyerek, bu cihazların temel fonksiyonlarına ek olarak hesaplama kabiliyeti kazandırılması ve diğer cihazlarla iletişim kurabilmelerini içerir [67]. IoT, fiziksel işlevselliği olan cihazlar ile internete bağlı hesaplama yeteneğine sahip cihazlar arasında bir köprü kurarak, devasa bir ağa dönüşür. Güncel verilere göre, yaklaşık 17,08 milyar bağlı IoT cihazı bulunmakta ve bu sayının 2030 yılına kadar 29,42 milyara çıkması beklenmektedir [53].

IoT, siber-fiziksel sistemler olarak kabul edilir ve büyük ölçekli kritik altyapıları içeren enerji nakil ağları, içme suyu ve ulaşım gibi hayati hizmetlerin yanı sıra akıllı şehir uygulamaları ve endüstriyel nesnelerin interneti sistemleri gibi orta ve küçük ölçekli uygulamalarla hayatımıza girmektedir. Bu sistemlerin herhangi bir yanlış yapılandırılması ya da kötü niyetli erişim sağlanması durumunda, yalnızca dijital varlıklar değil, fiziksel dünya da büyük ölçüde etkilenebilir. Bu nedenle, IoT'nin güvenlik ve bilgi güvenliği unsurları büyük önem taşır [28].

Bu bağlamda, küçük ölçekli IoT uygulamaları olan akıllı ev teknolojileri, kullanıcılarına sürekli kolaylık sağlarken, yetkisiz erişim veya kötü niyetli kullanım gibi güvenlik tehditlerine açık hale gelmektedir. Literatürde, bu tehditlerin üstesinden gelmek için öznitelik tabanlı erişim kontrolü (ABAC) modeli en uygun yöntem olarak kabul edilmektedir.

Bu tezde, ilk olarak ABAC modelinin genişletilerek kimlik doğrulama aşamasındaki belirsizliklerin yetkilendirme politikalarına entegre edilmesi önerilmektedir. İlk olarak, biyometrik kimlik doğrulama sistemlerinden elde edilen Kimlik Doğrulama Güvence Seviyesi, kullanıcının erişim izinlerinin belirlenmesinde kullanılmaktadır. Kimlik doğ-

rulama eşleşme puanı (AMS), belirlenmiş eşik değerlerle karşılaştırılarak kullanıcı rolü ve güvence seviyesine göre ayrıntılı erişim kararları alınmaktadır.

İkinci olarak, Kimlik Doğrulama Yeteneğine Sahip ABAC (AeABAC) olarak genişletilen modelde, kimlik doğrulama aşamasında kalan belirsizliğin, yetkilendirme politikası belirtimine taşınması önerilmiştir. AeABAC modeli, performans metrikleri ile zenginleştirilerek kimlik doğrulama eşleşme puanının önceden belirlenmiş eşikten ne kadar uzak olduğunu nicelendirmektedir. Bu nicelendirmedeki yenilik, yanlış eşleşme oranına danışarak geniş bir biyometrik kimlik doğrulama cihazları ve algoritmaları yelpazesine kolayca normalleştirilebilmesidir. Bu nicelendirme, diğer özneliteler gibi yetkilendirme politikalarını tanımlamak için kullanılır. Yanlış Eşleşme Oranı (FMR) hesaplanarak ve Erişim Karar Belirsizlik Puanı (ADUS) tanımlanarak, farklı biyometrik cihazlar arasında normalizasyon sağlanmaktadır. Sonuç olarak ortaya çıkan erişim kontrol politikalarının özlü ve kolayca anlaşılabilir olması hedeflenmektedir. Ek olarak, genişletilen modelin farklı erişim politikalarının her akıllı cihaz işlevi için ayrıca belirtilebileceği şekilde ince taneli olması amaçlanmaktadır. Ayrıca AeABAC modelinin XACML dilinde uygulanabilir olduğu vaka çalışmalarıyla gösterilmektedir.

Akıllı ev ekosisteminde güvenlik genellikle kullanıcıların kimlik doğrulama ve yetkilendirme süreçleri ile sağlanır. "Sistemden kullanıcıya güven" sadece yetkili kullanıcıların hizmetlere erişimini sağlarken, "kullanıcıdan sisteme güven" oluşturmak da en az bu kadar önemlidir. Bu durum, özellikle çevrimiçi alışverişlerde kredi kartı bilgileri gibi hassas verilerin bazı hizmetlerin düzgün çalışabilmesi için gerekli olduğu durumlarda daha da önem kazanır. Dolayısıyla, kimlik doğrulama ve yetkilendirme süreçlerinin ötesinde, bu ekosistemin her bir hizmet için kullanıcıların veri mahremiyetinin korunduğuna dair güven duymalarını sağlaması gerekmektedir. Bu güvenin ayrıca kullanıcının mahremiyet tercihlerine uygun şekilde kişiselleştirilmesi de önemlidir.

Tezin son aşamasında iki yönlü bu güvenin sağlanabilmesi adına, AeABAC modeli kullanıcı mahremiyetini koruyacak şekilde Risk Tabanlı Mahremiyet Yaklaşımı entegre

edilerek RBP-AeABAC olarak genişletilmektedir. Kullanıcılar, paylaşılabilecek verilerin ifşa olasılığı ve ifşa etkisi üzerinden risk bazlı güven değerlendirmeleri yapabilmek için kendi mahremiyet profillerini tanımlayabilmektedir. Ayrıca, aynı işlevi sağlayan ancak farklı hassas veri setleri gerektiren hizmetler mevcut olabilir (örneğin, çek ile ödeme yapmak ya da kredi kartı kullanmak). Bu durum göz önüne alınarak kullanıcıların mahremiyet risk seviyelerini anlayarak bu değerlendirmeleri karşılaştırıp bilinçli kararlar almaları hedeflenmiştir. Ayrıca RBP-AeABAC modelinin XACML dilinde uygulanabilir olduğu kullanıcı senaryo çalışmalarıyla gösterilmektedir.

Bu tez kapsamında üç aşamada geliştirilen RBP-AeABAC modeli, sadece IoT cihazlarının güvenliğini iyileştirmekle kalmamakta, aynı zamanda biyometrik doğrulama, performans odaklı erişim kontrolü ve mahremiyet risk analizlerini bir araya getirerek IoT ortamlarında kullanıcılar ve sistemler arasında çift yönlü güvenin tesis edilmesini sağlayan özgün bir çözüm sunmaktadır.

1.1 Tezin Amacı

Nesnelerin İnterneti, birbirleriyle iletişim kuran birçok bileşenden oluştuğu için, mahremiyet ve güvenlik riskleri bulunmaktadır. Bu ekosistemin ağ, sistem ve güvenlik ihtiyaçlarını karşılamak üzere iyi tasarlanmış olması gerekmektedir. IoT tüketicileri, bu ekosisteme güvenmeli ve onları günlük yaşamlarında benimsemelidir.

IoT uygulamaları, sensörlerden, kullanıcılardan, cihazlardan ve diğer sistemlerden hassas bilgileri toplayabilir. Dahası, çeşitli cihazlar arasında kamu ve özel verileri birleştirebilirler. IoT cihazları giderek günlük alışkanlıklarımızın bir parçası haline geldiğinden, güçlü kimlik doğrulama ve erişim kontrol mekanizmalarının eksikliği güvenlik ve mahremiyet endişelerini artırmaktadır. Zayıf kimlik bilgileri, güçlü kimlik doğrulama mekanizmalarının eksikliği, kullanıcı mahremiyetinin korunmasındaki eksikler IoT sistemlerinin başlıca zayıf noktalarından biridir. Bu nedenle, bu tür ortamlardaki güvenlik

ve mahremiyet risklerini uygun şekilde ele almak ve azaltmak, sürdürülebilir büyüme için esastır.

Mahremiyet, bütünlük, erişilebilirlik, kimlik doğrulama, erişim kontrolü ve inkar edilemezlik gibi güvenlik karakteristikleri arasından, bu tez kapsamında IoT güvenliğinin kullanıcı kimlik doğrulama, erişim kontrolü ve mahremiyet yönlerine odaklanılmaktadır. Akıllı ev IoT cihazlarını yetkisiz veya potansiyel olarak kötü niyetli kullanıcılar tarafından kullanılmasından korumak için bir erişim kontrol modeli önerilmiştir. Ev IoT, kişisel veri mahremiyetini sağlamak ve yetkisiz erişimleri önlemek için ince taneli, detaylı, bağlamsal ve dinamik bir erişim kontrolüne ihtiyaç duyar. Bu nedenle, öznetelik tabanlı erişim kontrolü (ABAC) modeli ev IoT ortamları için uygun bir modeldir.

Genel olarak, akıllı ev kullanıcıları, akıllı ev cihazlarını kullanırken biyometrik kimlik doğrulama sistemlerini tercih etme eğilimindedirler. Tipik biyometrik kimlik doğrulama sistemlerinde, kullanıcıya bütün olarak izin verilir veya reddedilir. Ancak, tez kapsamında ABAC modelinin genişletilerek, iddia ettiği bir rolü olan bir kullanıcıya, kimlik doğrulama güvence seviyesine bağlı olarak belirli işlevler için ayrı ayrı izin verilmesi veya reddedilmesi amaçlanmaktadır. Sonuç olarak, erişim kararı politikası belirtiminin, (i) işlevsellik kritiklik seviyesi, (ii) kimlik doğrulama güvence seviyesi ve (iii) kullanıcı rolünden oluştuğu detaylı aynı zamanda özlü bir erişim kontrol modeli amaçlanmaktadır.

Tez içerisinde öncelikle ABAC modeli genişletilip, erişim izinlerini belirleme politikaları birkaç eşik değerine dayandırılıp kullanıcının kimlik doğrulama puanına göre erişim kararlarının verilmesi önerilmiştir. Ancak farklı eşik değerleri belirlemenin zorluklarından ve getireceği iş yükünden dolayı performans ölçütlerini kullanmanın daha uygun ve pratik olacağı ön görülmüştür.

Daha sonra ABAC modeli tekrar genişletilerek Kimlik Doğrulama Özellikli ABAC (Ae-ABAC) modeli önerilmiştir. Önceki modelden farklı olarak erişim izin kararlarını birkaç

eşik deęerine dayandırmak yerine performans metriklerinin kullanılması hedeflenmiştir. Kimlik doęrulandıktan sonra kullanıcılar kimlik doęrulama eşleşme puanı (AMS) alırlar. Ardından, kullanıcıların kimlik doęrulama eşleşme puanlarının Yanlış Eşleşme Oranı (FMR) hesaplanır. Erişim Kararı Belirsizlik Puanı (ADUS) olarak adlandırılmıştır. Cihaz işlevsellięi kritiklik seviyesi açısından temel, önemli ve kritik olarak sınıflandırılmıştır. Sonuç olarak, erişim kontrol politikaları ADUS , kullanıcı rolü ve talep edilen işlevin kategorisine göre tanımlanmaktadır. Bu yaklaşım, özellikle kullanıcı kimlik doęrulamasının biyometrik yöntemlerle gerçekleştirildięi IoT uygulamaları için daha özet ve uygun bir model sunmaktadır.

Bunun yanı sıra, akıllı ev ekosistemlerinin karmaşıklığı arttıkça, artan mahremiyet endişelerinin ele alınması amacıyla AeABAC modeli Risk Tabanlı Mahremiyet Yaklaşımı entegre edilerek RBP-AeABAC modeli olarak genişletilmiştir. Geleneksel yaklaşımlar genellikle sistemin kullanıcıya güvenine odaklanarak, sistemin kullanıcının kimliğini doęrulamasını sağlamaya çalışmıştır. Ancak akıllı ev ekosistemlerinde, kullanıcıların verilerinin nasıl toplandıęı, kullanıldıęı ve korunduęu konusunda güven duymalarını sağlamak amacıyla kullanıcıdan sisteme güvenin de geliştirilmesi gerekmektedir. Kullanıcı sisteme bağlanıp yetkilendirildikten sonra sistemin kullanıcının hangi verileri kullanacağı kullanıcının o sistemi kullanma kararını etkileyecektir. Dolayısıyla kullanıcılar ve sistemler arasında çift yönlü güvenin teşvik edilmesi önemlidir. RBP-AeABAC modeli mahremiyet açısından daha geniş bir bakış açısı sunarak akıllı ev ortamında kullanılan verilerin tespiti, bu verilerin ifşa olasılıklarının deęerlendirilmesi ve olası ifşalarda kullanıcının maruz kalabileceęi zararların incelenmesi hususlarını mahremiyet riski deęerlendirme yöntemi kapsamında ele almıştır. Böylece kullanıcılara açık ve net bir mahremiyet politikası sunarak, veri paylaşımı konusunda farkındalık kazandırarak karar almalarını sağlayacak imkanlar verilmiştir.

Ayrıca, RBP-AeABAC modeli, kullanıcıların mahremiyetlerini profillere göre özelleştirerek, özellikle çocuklar gibi savunmasız gruplara daha katı mahremiyet önlemleri

uygularken, yetişkinlere daha esnek seçenekler sunmaktadır. Kullanıcı profilleri, bireyin mahremiyet risklerini anlama ve yönetme kapasitesine göre belirlenmekte; çocuklar için daha fazla koruma sağlanırken, eşler ve gençler için daha esnek, güven temelli izin mekanizmaları kullanılmaktadır.

Son olarak, bir kullanıcı cihazın işlevini kullanmak istediğinde, mahremiyet politikası alternatif cihazlar üzerinden işlemin gerçekleştirilip gerçekleştirilemeyeceğini değerlendirir. RBP-AeABAC modeli (i) cihazın gerektirdiği hassas veriler, (ii) verilerin ifşa olasılığı, (iii) ifşa durumunda oluşacak etki ve (iv) kullanıcının mahremiyet profili gibi parametreleri dikkate alarak, kullanıcıya tercih yapmasında rehberlik eder.

Sonuç olarak, bu tez, IoT cihazlarının erişim kontrol mekanizmalarının güvenliğini geliştirmeye yönelik önemli katkılar sağlamakta; aynı zamanda biyometrik doğrulama, performans metrikleri odaklı erişim kontrolü ve mahremiyet risk analizlerini bir araya getirerek IoT ortamlarında hem sistemden kullanıcıya hem de kullanıcıdan sisteme güveni artıran yenilikçi bir çözüm sunmaktadır.

1.2 Tezin Literatüre Kattıkları

Bu tez kapsamında akıllı evlerin güvenliğinin sıkılaştırılması için kullanıcı kimlik doğrulama, erişim kontrolü ve mahremiyet güvenlik prensiplerine odaklanılmaktadır. Amaç, nesnelerin interneti özellikle de akıllı evler için bir erişim kontrol modeli oluşturarak akıllı ev cihazlarının yetkisiz veya potansiyel olarak zararlı kullanıcılardan korunmasını sağlamaktır. Ayrıca kullanıcıların kimlik doğrulama ve yetkilendirme işleminden sonra cihazlardaki ilgili işlevleri kullanırken mahremiyetlerinin gözetilmesi gerekmektedir. Dolayısıyla bu ekosistemde hem sistemden kullanıcıya güven hem de kullanıcıdan sisteme güven esas alınarak çift yönlü bir güven mekanizması inşa edilmelidir. Ev IoT, kişisel veri mahremiyetini sağlamak ve yetkisiz erişimleri önlemek için detaylı, bağlamsal ve dinamik erişim kontrolüne ihtiyaç duyar. Bu nedenle, Öznitelik Temelli Erişim

Kontrol modeli (ABAC), ev IoT ortamı için en uygun model olarak düşünülmektedir. Tez içerisinde birkaç aşamada genişletilen ABAC erişim kontrol modeli ile literatüre sağlanan katkılar aşağıdaki gibidir:

- Akıllı ev kullanıcılarının genellikle akıllı ev cihazlarını kullanırken biyometrik kimlik doğrulama sistemlerini tercih ettikleri görülmektedir. Tipik biyometrik kimlik doğrulama sistemlerinde, kullanıcıya genel olarak ya izin verilir ya da reddedilir. Ancak, tez kapsamında sunulan ABAC modelinde literatürden farklı olarak, kullanıcıların biyometrik sistemde kimlik doğrulaması yaptıklarında elde ettikleri kimlik doğrulama eşleşme puanına (AMS) göre kullanıcının kimlik doğrulama güvence düzeyi belirlenir. Kullanıcıya, rolüne ve kimlik doğrulama güvence düzeyine dayanarak cihazların fonksiyonları için ayrı ayrı izin verilir veya reddedilir. Literatüre kullanıcıların kimlik doğrulama güvence düzeyine göre cihazların belirli işlevlerine ayrı ayrı izin veren bir erişim kontrol modeli önerilerek katkı sağlanmaktadır.
- Kimlik Doğrulama Özellikli ABAC (AeABAC) modeli ile erişim izin kararlarında performans metriklerinin kullanılması hedeflenmiştir. Kimlik doğrulandıktan sonra kullanıcılar kimlik doğrulama eşleşme puanı (AMS) alırlar. Ardından, kullanıcıların kimlik doğrulama eşleşme puanlarının Yanlış Eşleşme Oranı (FMR) hesaplanır. Erişim Kararı Belirsizlik Puanı (ADUS) olarak adlandırılmıştır. Cihaz işlevselliği kritiklik seviyesi açısından temel, önemli ve kritik olarak sınıflandırılmıştır. Sonuç olarak, erişim kontrol politikaları ADUS, kullanıcı rolü ve talep edilen işlevin kategorisine göre tanımlanmaktadır. Bu yaklaşım, özellikle kullanıcı kimlik doğrulamasının biyometrik yöntemlerle gerçekleştirildiği IoT uygulamaları için daha özet ve uygun bir model sunarak literatüre katkı sağlamaktadır.
- Sistemlerde kullanıcıların kimlik doğrulama ve yetkilendirme işlemlerinin ardından, kullanıcıların kullandıkları sistemlere güvenebilmesi için mahremiyet endişelerinin giderilmesi, farkındalıklarının artırılması ve mahremiyetlerinin etkin bir

şekilde korunması gerekliliği ortaya çıkmıştır. Bu doğrultuda, Risk Tabanlı Mahremiyet Yaklaşımı, AeABAC modeline entegre edilerek RBP-AeABAC modeli geliştirilmiştir. Bu model, iki yönlü güvenin tesis edilmesini amaçlayarak kullanıcı mahremiyetini korumayı hedeflemektedir. Önerilen Risk Tabanlı Mahremiyet Yaklaşımı, akıllı ev ortamında kullanılan mahremiyet profil bilgilerini belirleyerek mahremiyet risk değerlendirmesi yapar, ifşa olasılığını değerlendirir ve ifşa durumunda kullanıcıların karşılaşabileceği potansiyel zararları inceleyerek kullanıcıların sistemlere güvenini artırmayı amaçlar. Sonuç olarak, veri toplama ve ifşasıyla ilgili şeffaf ve bilgilendirici mahremiyet politikaları ile kullanıcı farkındalığı artırılıp mahremiyeti korunmaktadır.

- RBP-AeABAC modeli bir kullanıcı cihazın işlevini kullanmak istediğinde, mahremiyet politikası işlemin başka cihazlarla gerçekleştirilebilirliğini değerlendirir. RBP-AeABAC modeli, kullanıcının tercih yapabilmesi için (i) cihazın topladığı hassas veriler, (ii) veri ifşa olasılığı, (iii) ifşa durumunda ortaya çıkabilecek etkiler ve (iv) kullanıcının mahremiyet profili gibi parametreleri göz önünde bulundurarak rehberlik sağlayarak literatüre farklı bir yöntem katmaktadır.
- Son olarak bu tez kapsamında, 'sistemden kullanıcıya güven', kimlik doğrulama ve yetkilendirme yoluyla sağlanırken, 'kullanıcıdan sisteme güven' mahremiyet politikaları ve profilleri tarafından yönlendirilen mahremiyet risk değerlendirmeleriyle sağlanır. Bu tez, IoT ortamlarında kullanıcı ve sistem arasında çift yönlü güvenin tesis edilmesini sağlayan özgün bir çözüm sunarak literatüre katkı sağlamaktadır.

1.3 Tezin Düzeni

Tezin geri kalan kısmı dört bölümden oluşmaktadır. İkinci bölümde ABAC Modelinin kimlik bilgisi ile desteklenerek IoT için genişletilmesi açıklanmaktadır. Erişim kontrol modellerinden, ABAC modelinden, nesnelerin internetindeki erişim kontrol gereksi-

nimlerinden ve ABAC'ın neden uygun bir model olduğundan bahsedilmiştir. Bu konuda yapılan literatür taraması sunularak, ABAC modelinin kimlik bilgisi ile nasıl genişletildiği ve nasıl yetkilendirme yapıldığı açıklanmıştır.

Üçüncü bölümde bir adım ileriye gidilerek akıllı evlerde kimlik doğrulama özellikli ABAC (AeABAC) modeli sunulmuştur. Kullanıcı kimlik doğrulamasının güvence düzeyinin nasıl elde edildiği birkaç senaryo ile açıklanmıştır. AeABAC modelinin mimarisi, formel dilde ifade edilişi, işlevsel temelli erişim kararlarının nasıl alındığı ve modelin uygulanabilirliği gösterilmiştir. Ayrıca akıllı ev senaryoları ve XACML uygulamaları sunulmuştur. AeABAC modelinin literatürdeki yeri literatür karşılaştırması yapılarak açıklanmıştır. Son olarak birkaç IoT çerçevesine AeABAC modelini uyarlama çalışmaları sunulmuştur.

Dördüncü bölümde, Risk Tabanlı Mahremiyet Yaklaşımlı AeABAC (RBP-AeABAC) modeli detaylandırılmaktadır. Literatür taraması aracılığıyla, kullanıcılar ve üreticiler açısından mahremiyet beklentileri ve algıları incelenmiştir. Mahremiyet normları ve politikaları üzerinde durulmuş; literatürdeki akıllı evlerde mahremiyet sağlama önerileri sunulmuştur. Ardından, RBP-AeABAC modelinde akıllı evlerde kullanıcı mahremiyeti risk değerlendirmesi, iki ana boyut olan ifşa etkisi ve ifşa olasılığı üzerinden ele alınmıştır. Bu metriklerin nasıl elde edileceği ve mahremiyet profilleri ile politikalarının gerekliliği açıklandıktan sonra, iki anket veri seti kullanarak kullanıcı mahremiyeti risk değerlendirmesi yapma yöntemimiz sunulmaktadır. Son olarak, örnek bir akıllı ev ekosisteminde kullanıcı mahremiyeti risk değerlendirmesini somutlaştıran iki senaryo örneği verilmektedir.

Beşinci ve son bölümde tez kapsamında yapılan çalışmalara ait genel bir değerlendirme yapılmış, ayrıca gelecekte yapılabilecek çalışmalar için çeşitli öneriler sunulmuştur.



2. ABAC MODELİNİN KİMLİK BİLGİSİ İLE DESTEKLENEREK IOT İÇİN GENİŞLETİLMESİ

Bu bölümde erişim kontrol modellerinden bahsedilecek, IoT kapsamındaki erişim kontrol ihtiyaçları anlatılacaktır. ABAC modelinin diğer modellere göre avantajları öne çıkarılıp neden IoT için uygun olduğu açıklanacaktır. IoT’de erişim kontrol uygulamaları ile literatür taraması gösterilecektir. Nihayet ABAC’ın kimlik bilgisi ile desteklenerek IoT için genişletilmesi ve erişim karar mekanizması detaylı olarak ele alınacaktır.

Tezin bu bölüm kapsamında yapılan araştırmanın çıktısı 2020 International Conference on Information Security and Cryptology (ISCTURKEY)’de "Extending Attribute-Based Access Control Model with Authentication Information for Internet of Things" başlıklı bildiri olarak yayınlanıp sunulmuştur[15].

2.1 Erişim Kontrol Modelleri

Kimlik doğrulama (Authentication), erişim kontrolü (access control) ve yetkilendirme (authorization) bilgisayar güvenliğindeki temel üç kavramdır.

Kimlik doğrulama kullanıcının kim olduğunu doğrulama işlemidir. Geleneksel kimlik doğrulama yöntemlerinde kullanıcılar giriş yapmak istediği sisteme kullanıcı adı ve parola girer, ilgili sistemde depolanan kullanıcı bilgilerine göre kullanıcıların kimlik doğrulaması yapılır. Günümüzde ise teknolojinin hayatımızdaki yerinin giderek artmasıyla birlikte kullanıcı adı ve parola yerini akıllı kartlar, parmak izleri ve yüz tanıma gibi biyometrik kimlik doğrulama sistemleri almaya başlamıştır.

Erişim kontrol kuralları ve politikaları, hangi kullanıcının hangi kaynağa hangi izinlerle (R, W, RW) erişebileceğini tanımlar. Erişim kontrolleri, kimlik doğrulama adımından sonra gelir ve kullanıcının hangi kaynaklara erişim iznine sahip olduğunu belirler [71]. Son olarak, yetkilendirme, kimlik doğrulaması yapılmış kullanıcıların ilgili kaynağa

eriştikten sonra neler yapabileceğine izin verme sürecidir. Erişim kontrol mekanizmaları, kaynaklardaki yetkilendirmeyi sağlar. Kullanıcıların kaynaklar üzerinde farklı yetkileri/izinleri olabilir. Bazı kullanıcıların ilgili kaynakta sadece okuma hakkı varken bazı kullanıcıların yazma hakkı da bulunabilir. Tüm bu izinler, kaynaklar ve kullanıcılar ile ilgili belirli kurallar tanımlanarak sağlanır. Erişim kontrol kuralları ile korunan kaynaklara yetkisiz erişimin engellenmesi hedeflendirir. Çeşitli erişim kontrol yöntemleri bulunmaktadır. Aşağıda bu yöntemlerinden bazıları sıralanmıştır:

İhtiyari Erişim Kontrol Modeli (DAC): Kullanıcıların kendi kaynaklarının erişim yetkilerini yönettiği erişim kontrol türüdür. Kaynak sahibi kimlerin kaynağa ne haklarla erişeceğini tanımlar. Örneğin DAC modeli işletim sistemlerinde dosya sahiplerinin dosyalarına kimlerin hangi yetkiyle erişeceğini tanımlamakta kullanılır.

Zorunlu Erişim Kontrol Modeli (MAC): Kullanıcılara kaynaklarla ilgili erişim yönetim yetkisi verilmez, bunun yerine merkezi bir kural yönetimi vardır. Her bir kaynağın mahremiyet derecesi vardır ve kullanıcılar izin verilen mahremiyet derecesi seviyesindeki kaynaklara erişebilir. Bell-LaPadula ve Biba bilinen MAC modelleridir.

Rol Temelli Erişim Kontrolü (RBAC): 1992’de NIST tarafından önerilen RBAC modeli, kullanıcılar, roller, oturumlar ve yetkilendirmelerden oluşur. Bu modelde, erişim kuralları roller temel alınarak tanımlanır. Erişim izinleri kullanıcılar yerine rollere tanımlanır. Kullanıcılara roller atanır ve bu rollere göre kaynaklara erişim yetkileri tanımlanır. Bir kullanıcıya birden fazla rol atanabilir ve bir kaynağa birden fazla rol erişebilir. Merkezi olarak yönetilir [37]. Küçük ortamlarda kullanışlı olsa da, yüksek rol sayısı nedeniyle büyük ortamlarda yönetilmesi zor olabilir.

Öznitelik Temelli Erişim Kontrolü (ABAC) modelinde erişim talep eden kullanıcılara sahip oldukları özniteliklere (attribute) göre erişim kuralları değerlendirilerek ilgili kaynağa erişim izni verilir veya reddedilir. ABAC modelinde öznitelikler kullanıcılara (subject), kaynaklara (object) ve ortama (environment) ilişkin olabilir. Öznitelikler, ta-

leple ilgili bazı bilgileri içeren bir ad ve değerden oluşur. Öznitelikler, MAC'deki gibi güvenlik seviyeleri, DAC'deki gibi erişim kontrol listeleri, RBAC'deki gibi roller olabilir.

2.2 Öznitelik Temelli Erişim Kontrolü (ABAC)

Geleneksel erişim kontrol modellerinin aksine, ABAC, erişim kararlarını sadece kullanıcı ve kaynağa göre vermez. Bu modelde kullanıcıların kaynaklara erişim istekleri, kullanıcıların, kaynakların ve çevrenin özniteliklerine bağlı olarak kabul edilir veya reddedilir [56]. Öznitelikler bir ad ve bir değerden oluşur. Kullanıcı (Subject) öznitelikleri, bir kaynağa istekte bulunan özneyi tanımlar. Yaş, rol, departman, yönetim seviyesi kullanıcı özniteliklerine örnek olarak verilebilir. Öznitelikler kullanıcı rolü gibi statik veya yaş ve zaman gibi dinamik olabilirler. Kaynaklar, ABAC kuralları ve politikaları tarafından yönetilir ve öznitelikleri kaynak türü, kaynak özelliği, sınıflandırma vb. gibidir. Son olarak, çevre (environment) öznitelikleri konum ve zaman gibi dinamik öznitelikler ile ilgili olabilir [37].

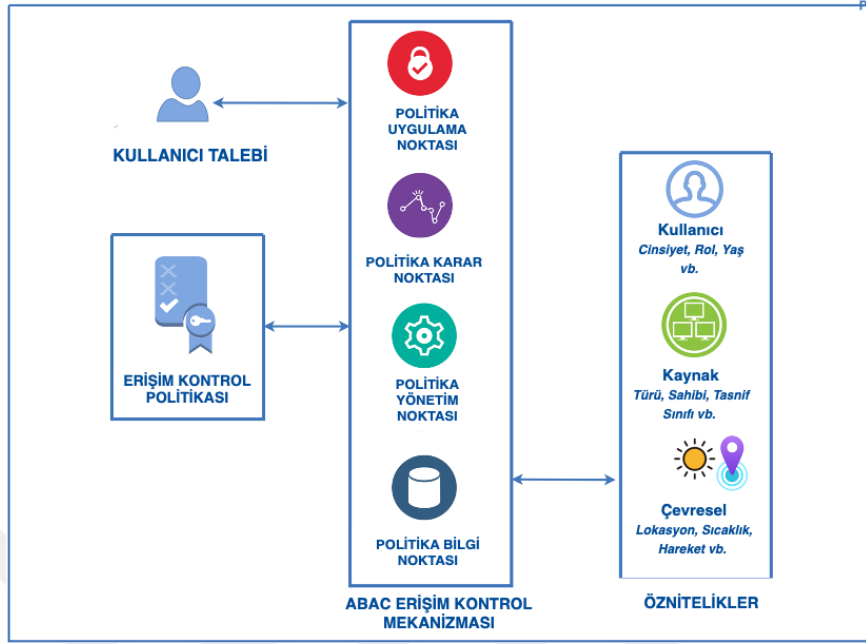
ABAC'ın geçmişte oldukça yaygın olarak kullanılan ancak büyük yapılarda rol patlaması nedeniyle karmaşık ve zor yönetilebilen bir hal alan RBAC'e göre avantajı ABAC'da sadece kullanıcıların rollerine göre değil kullanıcıların, kaynakların ve ortamın birçok farklı özneliğine göre erişim kontrolleri tanımlanabiliyor olmasıdır [75]. ABAC yapısında daha fazla rol eklemek yerine politika kuralına başka bir mantıksal koşul eklenerek rol yerine kurallara odaklanılır. Gerçek hayat senaryolarında erişimler sadece rollere bağlı olmaz, başka parametrelerin de değerlendirilme ihtiyacı bulunur. Ayrıca ABAC yapısında bulunan ortam öznitelikleri sayesinde kullanıcının IP adresi, konumu, zaman/gün, günün saati, tehdit seviyesi gibi özellikler kullanarak erişim kararlarını statik değil de dinamik olarak verebilir[69]. ABAC modelini destekleyen açık standartlar ve yaklaşımlar vardır, bu konuda en çok bilinen ve kabul edilen açık standart Extensible Access Control Markup Language (XACML) dir. XACML modelinde kurallar, politika-

lar, kural ve politikayı beraber içeren algoritmalar, kullanıcı, kaynak, aksiyon ve ortam durumlarını ele alan öznitelikler bulunmaktadır.

2.2.1 Genişletilebilir erişim kontrol işaretleme dili (XACML)

Standart Genişletilebilir Erişim Kontrol İşaretleme Dili (XACML), ABAC modeline dayanan OASIS standardıdır. Erişim kontrol politikalarını ve istek/yanıt dilini ifade etmenin genel bir yolunu tanımlar. XACML standardı, politikalara göre yetkilendirme taleplerini değerlendirip bir cevap dönecek mimariyi ve süreci belirler. Ayrıca, erişim kararlarını hesaplama ve uygulama yöntemleri için de bir mimari sağlar. NIST NGAC, ABAC'yı destekleyen başka bir açık standarttır, ancak örnek kurallar ve politikaları uygulamak açısından öznitelik ve politika yönetimindeki gücü nedeniyle XACML daha çok tercih edilir [29]. XACML'in yapısı, kurallar, politikalar, kurallar ve politikalar için algoritmalar ve özniteliklerden oluşur. XACML'nin esnekliği, daha detaylı ve esnek erişim politikaların oluşturulmasını sağlar. XACML'in mimarisinde aşağıdaki bileşenler bulunur[54]:

- Politika Uygulama Noktası (Policy Enforcement Point (PEP)): Kullanıcıların kaynaklara erişim isteklerini karşılar; PDP'de alınan yetkilendirme kararlarını uygulayarak erişim isteklerini engeller veya izin verir.
- Politika Karar Noktası (Policy Decision Point (PDP)): Yetkilendirme kararlarını vermek için erişim taleplerini mevcut politikalara karşı değerlendirir ve sonuca bağlar. Ayrıca, gerekiyorsa istekteki eksik öznitelikler için Politika Bilgi Noktası'ndan (PIP) daha fazla öznitelik talep eder.
- Politika Bilgi Noktası (Policy Information Point (PIP)): İstekte bulunmayan ek öznitelikleri PDP'ye sağlayarak öznitelik değerleri kaynağı görevi görür.
- Politika Yönetim Noktası (Policy Administration Point (PAP)): Yetkilendirme po-

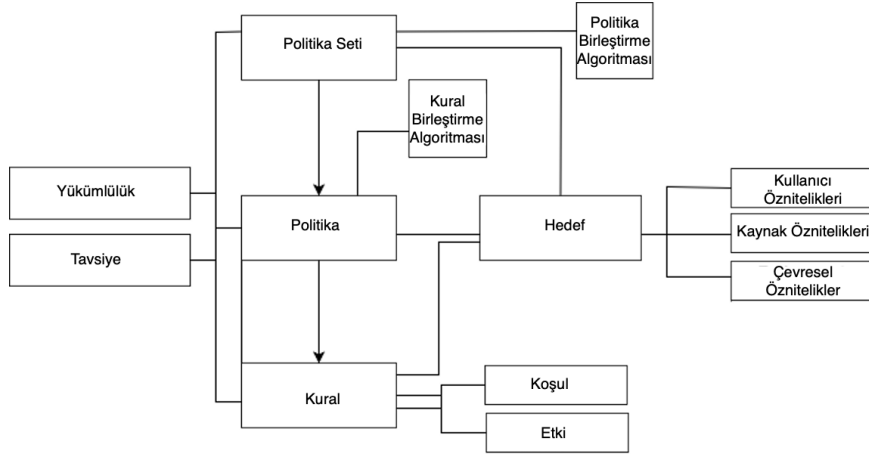


Şekil 2.1: ABAC modeli

litikalarını yönetmek, oluşturmak, güncellemek, silmek için kullanılır. Politikaları PDP için kullanılabilir hale getirir.

NIST ABAC rehberinde tasvir edilen üst seviyeli ABAC tanımı, Şekil 2.1’de yeniden çizilmiştir. Bir kullanıcı korunan bir kaynak üzerinde belirli bir işlem yapmak istediğinde, ilk olarak PEP bu isteği karşılar ve PDP’ye yetkilendirme kararı için istek gönderir. İstek, talep edilen erişim için kullanıcıyı, eylemi, kaynağı ve ortamı tanımlayan özniteliklerden oluşur. İstekteki öznitelikler politikalardaki öznitelik değerleriyle karşılaştırılarak yetkilendirme kararı İzin Ver, Reddet, Uygulanamaz veya Belirlenmedi olarak verilir ve bu karar PDP’den PEP’e bir cevap olarak geri gönderilir.

Politikalar, mantıksal koşullar olarak kabul edilir [29]. Çok detaylı olabilirler ve belirli bir kullanıcı için belirli bir nesne üzerinde belirli bir zaman aralığında erişimi kontrol edebilirler. Ancak birden fazla zaman aralığından sorumlu olan ve birçok farklı kullanıcı, uygulama ve aktör için erişimi kontrol eden çok daha genel politikalar yazmak da mümkündür. Esneklik, yetkilendirmenin tasarımı için ana unsurdur [21]. Yetki, herhangi



Şekil 2.2: OASIS XACML Akış Diyagramı

bir özneteliğin kullanılabileceği şekilde tasarlanmıştır. Politikalar çok çeşitli özneteliklere göre oluşturulabilir. Bir PEP'ten bir PDP'ye bir istek gönderildiğinde, bu istek neredeyse sadece özneteliklerden oluşur ve erişim kararlarını vermek için bir politikadaki öznetelik değerleri ile karşılaştırılır. Örneğin bir politikada bir öznetelik belirtilmişse ve bu öznetelik yetkilendirme isteği içerisinde bulunamazsa, erişim reddedilir. Birden fazla kullanıcı ve nesne için birden fazla zaman aralığında geçerli olan genel politikalar da vardır. Bir politikanın gelen isteğe uygulanacağı belirlendikten sonra, politikanın kuralları değerlendirilir. Bir politikada XACML politikası temel mantığını içeren çok sayıda Kural (Rule) bulunabilir. Kurallarınsa temel çekirdeğini mantıksal işlevler olan Koşullar (Conditions) oluşturur. Eğer Kuraldaki Koşul doğru olarak değerlendirilirse, Kuralın Etkisi (Effect) İzin veya Reddetme değeri döndürülür. Koşulun değerlendirme sonucu bir hata (Belirsiz) veya Uygulanamaz da olabilir. Bir koşul senaryolara göre çok kompleks yapılarda oluşturulabilir[54]. Yukarıda bahsedilen mimari için OASIS XACML akış diyagramı Şekil 2.2'de verilmiştir.

2.3 Nesnelerin Internetinde Eriřim Kontrol İhtiyaçları ve ABAC

Nesnelerin interneti, gelişmiş ve kolayca yönetilebilir sistemler sağlayarak yaşamlarımızı daha konforlu hale getirmektedir, ancak IoT cihazlarındaki güvenlik açıkları kullanıcı memnuniyetsizliğine, mahremiyet ihlallerine, finansal kayıplara ve hatta yaşam kayıplarına (örneğin saldırganlar akıllı araçlar gibi kritik varlıkları ele geçirdiğinde) neden olabilir. Bu nedenle, teknoloji dönüşümünü doğru şekilde gerçekleştirerek güvence altına almak son derece önemlidir[28]. Nesnelerin internetinde en büyük güvenlik endişelerinden biri yetkisiz erişim ve kontroldür. Yetkisiz kullanıcıların cihaz kontrolünü ele geçirmesi ve cihazı kendi isteği doğrultusunda kullanması veya zararlı ağlara dahil etmesi hiçbir şekilde istenmeyen bir durumdur[52]. Dolayısıyla kimlik doğrulama ve erişim kontrolü teknolojileri, Nesnelerin İnterneti'ndeki güvenlik ve mahremiyet sorunlarına karşı ana unsur olarak ele alınır[55].

Eriřim kontrol modelleri güvenlik, mahremiyet ve işlevselliği göz önünde bulundurmaktadır. Öncelikle, sadece kullanıcının cihaza erişiminin olup olmaması yeterli bir erişim kontrolü oluşturmaz. Eriřim izinlerinin cihaza değil, cihazın işlevlerine dayandırılması gerekir. Örneğin Google Home dijital ses asistanı cihazının internetten alışveriş yapma, müzik çalma, evdeki diğer aletleri açıp kapama gibi birden fazla fonksiyonu bulunmaktadır. Bu cihaz üzerinden evde bulunan kişilerden hangilerinin müzik çalma yetkisine sahip olacağı ile çevrimiçi alışveriş yapma yetkisine sahip olacağı ayrı ayrı tanımlanmalıdır ki eve gelen bir misafir veya evdeki küçük bir çocuk bu cihaz ile online alışveriş yapmasın. Dolayısı ile nesnelerin internetinde cihaz bazlı değil de cihazlarda bulunan özellik bazlı bir erişim kontrolü sistemine ihtiyaç bulunmaktadır. Cihazın her bir işlevi için erişim izinleri oluşturulmalıdır, böylece bir kullanıcı, bilgi güvenliğinin "en az ayrıcalık" ilkesine göre cihazların sadece gereken işlevlerine erişir. ABAC modelinde, geleneksel erişim kontrol modellerine göre ince taneli detaylı erişim kontrol kuralları ve politikaları tanımlamak mümkündür[15]. Ayrıca, IoT dinamik bir ortamdır, bu nedenle dinamik erişim kontrol kurallarına ihtiyaç duyar. ABAC yöntemi, sadece

kullanıcıların rollerine değil, aynı zamanda kaynakların ve ortamın özniteliklerine bağlı olarak erişim kararını verir. Çevresel koşulların (konum, tarih ve saat, tehdit seviyeleri ve IP adresi gibi) yardımıyla, ABAC modeli dinamik erişim kontrol kuralları sağlayabilir [69]. ABAC'ın nesnelerin internetinde kullanılmasının başka bir avantajı ABAC modelinde, ilgili politika ve kurallardaki tüm kriterler karşılanırsa erişim izni verilmesi, aksi takdirde reddedilmesidir [55]. Erişim politikaları ve kuralları, farklı kullanıcı, nesne ve çevre öznitelik değerlerinin farklı varyasyonlarını içerir. Sonuç olarak, farklı erişim koşulları kombinasyonlarının sayısı, geleneksel erişim kontrollerinin sunduğundan çok daha fazladır [69]. Bu yönüyle ABAC nesnelerin interneti ortamı için ince taneli bir erişim kontrol modeli sunar. Ek olarak, NIST ABAC kılavuzuna göre[37], çevresel öznitelikler öznelerden veya nesnelerden bağımsızdır ve mevcut zaman, konum ve tehdit seviyesi gibi faktörleri içerebilir. Yapılan çalışmalar, ABAC modelinin farklı tehdit seviyelerini çevresel veya kullanıcı öznitelikleri olarak nasıl yorumlayabileceğini göstermektedir. Belirlenen bir risk seviyesi belirli bir eşik değerini aştığında, tanımlanan politika ve kurallara göre otomatik olarak reddedilebilir[69]. Örneğin, mevcut bir erişim politikasında kullanıcı erişim risk puanının eşik değeri olarak 5 belirlenmiştir. Bir kullanıcı kurumsal ağda ise ve tek faktörlü kimlik doğrulama yöntemiyle doğrulanıyorsa, risk puanı 3 olarak değerlendirilir ve bu kullanıcı erişim izni alır. Ancak, aynı kullanıcı uzaktaysa ve tek faktörlü kimlik doğrulama yöntemiyle doğrulanıyorsa, risk puanı 7 olarak hesaplanır ve bu durumda kullanıcı reddedilir. Eğer aynı uzaktaki kullanıcı çok faktörlü kimlik doğrulama yöntemiyle doğrulanırsa, risk puanı 4'e düşer ve bu kullanıcı erişim izni alır. ABAC modeli sayesinde çevresel öznitelikler kullanılarak bu tür senaryoların uygulanması mümkündür[69]. Nesnelerin internetine ABAC'ı daha uygun kılan bir diğer neden, uyumluluğu desteklemesidir. Bilinmeyen kullanıcıların özellikleri, var olan bazı politika ve kuralların kriterlerini karşıladığı sürece, kullanıcı ilgili kaynağa erişim kazanır. Özetlemek gerekirse, IoT'nin dinamik ve değişken doğası nedeniyle, dinamik, bağlamsal ve ince taneli politikaları destekleyen bir erişim kontrol mekanizmasına ihtiyacı vardır. Bu nedenle, ABAC modeli, esnek ve dinamik

eriřim kontrol kuralları oluřturarak IoT'ye iyi uyum saęlar. Eriřim izinleri, kimlikler iin deęil, znitelikler iin tanımlanır. Kullanıcı odaklı deęildir; bunun yerine, bir dizi znitelik iin izin verilen iřlemleri belirler. evresel zellikler, mevcut zaman, konum, sensrler, tehdit seviyesi, IP adresi ve dięer bileřenler hakkında bilgi olarak baęlam- sal bir farkındalık oluřturur. Tm bu avantajlarla, ABAC, nesnelerin internetine uygun senaryoları uygulayarak gereksinimlerini karřılamayı kolaylařtırır.

2.4 Literatr Taraması

IoT'de, eriřim kontrol politikalarının btn cihaza deęil de cihazın ayrı ayrı zellik- lerine gre tanımlanması gereklidir. W. He ve ekibi tarafından yapılan bir arařtırmada [34], ayrı ayrı cihaz zellikleri iin 450 katılımcıya, hangi kořullar altında (zaman, ko- num, vb.) ilgili zellięin kim tarafından kullanılmasını tercih ettikleri sorulmuřtur. Ka- tılımcıların cevapları, kullanıcı rollerine, cihazın yeteneklerine, gnn zamanına, kulla- nıcı yařına ve dięer evresel kořullara baęlı olarak deęiřiklik gstermiřtir. Farklı roller ve iliřkiler iin eriřim kararlarının, detaylı bir řekilde nasıl deęiřtięini aık bir řekilde gstermiřlerdir. Eriřim kontrol politikalarının hangi baęlamsal faktrlere dayandıęını sorgulamıřlardır. Ayrıca, yanlış eriřim kararlarının sonularını da incelemiřlerdir. rne- ğin, Google Home gibi bir dijital ses asistanının eřitli yetenekleri vardır, mzik alma ve evrimii alıřveriř yapma gibi. Bu cihazda, hangi kullanıcının hangi zellięi kullana- bileceęinin net bir řekilde tanımlanması gerekmektedir, bylece evdeki bir misafir veya ocuk bu cihaz aracılıęıyla evrimii alıřveriř yapamaz. W. He ve ekibi [34], IoT'de ince taneli eriřim kontrol ihtiyaını iyi tanımlar ve eřitli ev IoT senaryoları sunarlar. Cihaz bařına deęil, iřlevsellięe dayalı olarak daha ayrıntılı bir eriřim kontrol gerekli- lięine vurgu yaparlar. Ev IoT'nin eriřim kontrol ve kimlik doęrulama gereksinimlerini derinlemesine ele almalarına ve iřlevsellięe dayalı eriřim kontrollerinin tm cihazlara gre ne kadar nemli olduęuna odaklanmalarına raęmen, nerdikleri eriřim kontrol zelliklerini herhangi bir eriřim kontrol modeline baęlamamaktadırlar.

İşlevselliğe dayalı erişim kontrolü, tüm cihaza göre değil de cihazın işlevselliğine odaklanarak yapılması gerekliliğini vurgulayan başka bir çalışma, S. Lee ve ekibi tarafından sunulmuştur [43]. Her cihazın işlevselliğini ayırırlar ve her biri için erişim kontrol politikalarını tanımlayan bir işlevselliğe odaklanan erişim kontrol (FACT) çerçevesini önerirler. Bu şekilde, bir işlevselliğin herhangi bir kesintisinin diğer işlevselliği etkilememesi nedeniyle sistemin kullanılabilirliğini artırır. Ayrıca, sadece gereksinim duyulan işlevselliğe erişim sağlayarak kullanıcılara en az ayrıcalığı vererek ince taneli erişim kontrolünü sağlamayı hedefler. Bu çalışma, IoT’de işlevsellik tabanlı erişim kontrolünün önemini göstermektedir.

Yalçinkaya ve ekibi [69], Bilgi Kontrol Sistemleri (ICT) için erişim kontrol sistemlerinin önemine değinir ve geleneksel erişim kontrol modellerini inceler. En uygun model olarak ABAC’ı önerirler. ABAC’ın yapısını ve bileşenlerini açıklarlar. Merkezi olarak yönetilen erişim kontrol politika mekanizmasına sahip olması ve ince taneli erişim kontrolü sağlama kabiliyeti nedeniyle ICT için ABAC’ı tavsiye ederler. ICT ve IoT’nin gereksinimleri ve yapısı benzerlik gösterdiği için bu çalışma ABAC’ın IoT’ye nasıl adapte edilebileceğine dair ipuçları sunar.

Bezawada ve diğerleri [12], IoT erişim kontrolü için ABAC modelinin kullanımını önerir. Ev IoT’deki güvenlik zorluklarını belirtir ve ABAC modelinin uygulanması için NIST Next Generation Access Control (NGAC) tercih ederler. Ev IoT için ABAC’ı NIST NGAC ile ağ seviyesinde politikaları uygulayarak entegre ederler. Ağ seviyesinde ABAC entegrasyonu ile ilgili faydalı bir tartışma sunarlar. Ancak ağ düzeyinde erişim kontrolünü ve kullanıcı kimlik doğrulamasını vurgulayıp cihazların işlevleri için erişim kontrol politikalarına ihtiyaç duyulmasını gözardı ederler.

Sun ve Yin ve diğerleri [65], ABAC ve RBAC’ı birleştirerek Öznitelik Rol Temelli Hibrit Modeli (ARBHAC) önerirler. Büyük ölçekli dinamik ortamlarda RBAC’nin yetersizliğini ABAC ile birleştirerek çözmeyi hedefler. Ayrıca, ABAC’ın politika yönetimi ve izin atama açısından karmaşık olduğunu belirler ve bunu RBAC’nin rol yönetimi ile

birleřtirerek kolaylařtırmaya alıřırlar. Ancak, bu model politika tekrarı ve akıřmasına neden olabilir ve ynetim aısından zorluklar oluřturabilir.

A.T. Rath ve J.N. Colin[57], kimlik doęrulama sistemi ile eriřim kontrol modelini birleřtirerek ABAC modelini geniřletirler. Kullanıcı temelini oluřturmak ve kullanıcıların eriřim gnlklerini analiz etmek iin UBA'nın iliřki kural ęrenimini kullanırlar. Daha sonra, bu temeli kullanarak kullanım anormalliklerini tespit ederler. Kullanıcı temelini, kullanıcının davranıř analizi deęiřkeni olarak kullanarak, eriřim politikalarında kullanıcının kesinlik olasılıęını ierirler. Bu bilgi, doęrulanmıř kullanıcının UBA analizinden elde edilir. Rath ve Colin, farklı eřikler iin eřitli politikalar tanımlarlar, ancak farklı iřlevler iin farklı eřikler sunmazlar. Odaklarını sadece kullanıcının davranıř znitelięine dayalı olarak kullanıcının kt niyetli veya meřru olup olmadıęına evirirler.

Rath ve Colin tarafından gerekleřtirilen bařka bir alıřmada [58], dinamik risk-bilinli eriřim kontroln nererek ABAC gibi dięer eriřim kontrol sistemleriyle birleřtirirler. Risk-bilinli eriřim kontrol modelinde, kullanıcının doęrulanmıř olsa bile, talebin risk deęeri bazı teknikler kullanılarak deęerlendirilir ve tahmin edilen risk deęeri ile kullanıcıya atanmıř eriřim talebi tekrar deęerlendirilir. Risk-bilinli bilgi, talebin iliřkili riskle iliřkilendirilmıř olduęu risk gemiři veya dięer veri setlerinden gelir. Modellerinde, risk-bilinli bilgiyi ve risk tahmin motorunu ayrı varlıklar olarak ele alırlar. Risk deęerini, risk tahmin bilgisine ve fonksiyona dayalı olarak risk tahmin motoru aracılıęıyla hesaplarlar. Risk tahmin motorunu, karar verme noktasının (PDP) bir bileřeni olarak dřnrlar. Son olarak, riski en aza indirmek veya nlemek iin bazı iřlemleri zorlamak iin risk-kaınma uygulama modln kullanırlar. İřlemleri zorlamak iin, kullanıcıların kimliklerini kanıtlamalarını gerektiren eylemleri zorunlu kılarlar. Risk deęerini hesaplamak iin, kullanıcı eriřim gnlklerine İliřki Kural ęrenme (Association Rule Learning) teknięini uygularlar, kullanıcı eriřim desenini alır ve eriřim talebi iin risk deęerini tahmin ederler. Bu deęeri ABAC kurallarında ve politikalarında kullanırlar. Srekli yetkilendirme ve srekli karar verme zerine alıřsalar da, IoT eriřim kontrol-

Çizelge 2.1: Nesnelerin Internetinde Erişim Kontrol Gereksinimleri Anketi

Ref No	Erişim Kontrol Metodu	Kullanıcı Kimlik Doğrulama Güvencesi	Ayrıntılılık
[57]	ABAC	Evet	Hayır
[69]	ABAC	Hayır	Evet
[65]	Öznitelik ve Rol Temelli Hibrit	Hayır	Evet
[12]	ABAC	Hayır	Hayır
[34]	Belirtilmemiş	Hayır	Evet
[23]	Bağlamlar-Durumlar-Farkındalık ile ABAC	Hayır	Hayır
[58]	Adaptif Risk Farkındalıklı ABAC	Evet	Hayır
[7]	Belirtilmemiş	Hayır	Hayır
[43]	İşlevsellik Merkezli Erişim Kontrol Sistemi	Hayır	Evet
MODELİMİZ	Genişletilmiş ABAC	Evet	Evet

nün detaylı ve ince taneli politika ihtiyaçlarını dikkate almazlar.

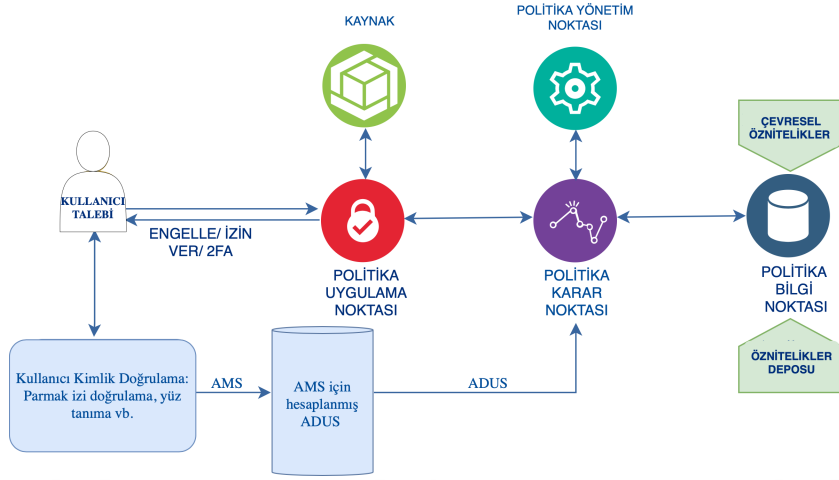
Yukarıda belirtilen IoT erişim kontrolü gereksinimleri açısından ilgili çalışmaları Çizelge 2.1 özetlemektedir.

2.5 Kimlik Bilgisi ile Desteklenmiş Öznitelik Tabanlı Erişim Kontrol Modelinin Genişletilmesi

İlgili çalışmalarda, IoT’de erişim kontrolüne ilişkin bir takım öneriler sunulmuştur. Bu önerilerin bazıları, IoT için detaylı bir erişim kontrolü modelinin gerekli olduğunu vurgulamaktadır. Ancak, şu ana kadar yapılan çalışmaların hiçbiri, kullanıcı kimlik doğrulamasının güvenlik düzeyinden bahsetmemiştir. [57] kullanıcı kesinliğini göz önünde

bulundurmasına rağmen, bunu kullanıcının kimlik doğrulama eşleşme puanıyla ilişkilendirmemekte; bunun yerine, kullanıcının kesinliğini belirlemek için davranış anormalliklerini kullanmaktadır. Literatürdeki bazı çalışmalar sadece kimlik doğrulamaya odaklanırken, diğerleri ise sadece erişim kontrolü yönlerine odaklanmıştır. Ancak, IoT için erişim kontrolü modeline hem kimlik doğrulaması hem de erişim kontrolünün dahil edilmelidir. Sonuç olarak, IoT’de kullanılacak en güvenli erişim kontrolü modeli, kullanıcı kimlik doğrulamasının güvenlik düzeyini erişim kontrolü kararlarında kapsamalı ve cihaz işlevlerine yönelik detaylı izinleri sağlamalıdır. IoT’nin karmaşık yapısı ve doğası göz önüne alındığında, fiziksel ve davranışsal biyometrik kimlik doğrulama yöntemlerinin geleneksel kimlik doğrulama yöntemlerinin yerini alması beklenmektedir. Fiziksel biyometrikler, insan vücudunun ölçümleriyle ilgilidir ve yüz şekli, el geometrisi, parmak izi gibi verilere dayanabilir. Davranışsal biyometrikler ise kullanıcıların benzersiz hareketleri veya alışkanlıklarıyla ilişkilendirilir ve klavye vuruş dinamikleri, konuşma desenleri ve imzalar gibi verileri kullanır. Genellikle, ilk adım kullanıcı kimlik doğrulamasıdır. Kimlik doğrulaması kullanıcının biyometrik verisiyle kimliğinin doğrulandığı veya doğrulanmadığı varsayımına dayanır. Öte yandan, biyometrik kimlik doğrulama sistemleri, kullanıcının kimlik doğrulama eşleşme puanını belirlemek için ön işleme, puanlama ve eşikleme adımlarını kullanır ve bu puan, belirlenen eşik değerinin üzerindeyse erişim sağlanır, aksi takdirde reddedilir[64]. Kullanıcı kimlik doğrulama eşleşme puanı, genellikle 0 ile 100 arasında bir değere sahiptir. Dolayısıyla bu değer farklı olduğunda, cihazların işlevleri için farklı izinlerin verilmelidir. Kullanıcının kimlik doğrulama eşleşme puanının örneğin 50 olması ile 90 olması erişim izni açısından farklı kararlar aldırmalıdır. Tezin amacı, kullanıcının aldığı farklı kimlik doğrulama eşleşme puanlarına dayalı olarak daha esnek ve detaylı erişim kontrol politikalarını tanımlamayı mümkün kılmaktır.

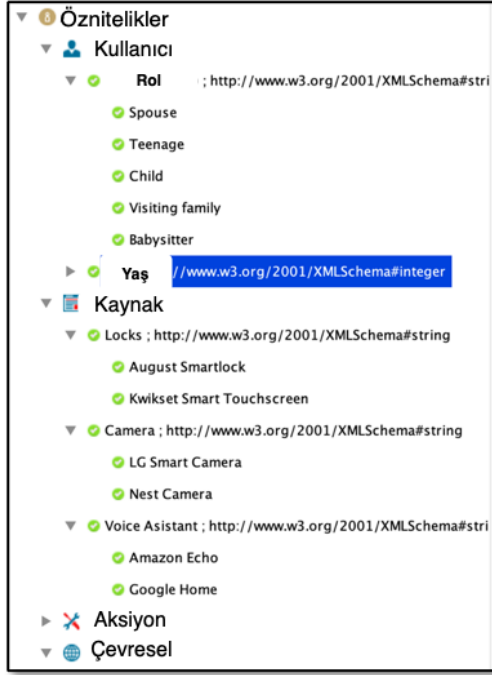
Tez kapsamında genişletilmiş ABAC modeline bir kullanıcının kimlik doğrulama puanı ortam özniteliği olarak eklenmiştir. İlgili kaynaklara tam veya kısmi erişim izinleri vermek için erişim kontrol politikalarında bu puan da bir öznitelik olarak kullanılır. Ör-



Şekil 2.3: Genişletilmiş ABAC Modeli

neğin, bir kullanıcının yetişkin rolü için belirlenen kimlik doğrulama eşleşme puanı 60 ise, bu kullanıcı çevrimiçi alışveriş yapamaz ancak Google Home cihazı aracılığıyla müzik çalabilir. Öte yandan 90 ise bu yetişkin kullanıcı çevirim içi alışveriş yapabilir. Biyometrik kimlik doğrulaması gerçekleştirildikten sonra, kullanıcının kimlik doğrulama eşleşme puanı saklanır. Ardından, bu puan, erişim kararları sırasında Politika Karar Noktası (PDP) tarafından dikkate alınır. Kullanıcı, bir kimlik doğrulama eşleşme puanı alır ve bu puan isteğe başka bir ortam özniteliği olarak eklenir. Daha sonra, Politika Uygulama Noktası (PEP), erişim isteğini karşılar ve bu kararı yetkilendirme kararı vermek için Politika Karar Noktasına iletilir. Kimlik doğrulama eşleşme puanı ayrıca Politika Karar Noktasına iletebilir. PDP, erişim kararı sırasında bu puanı da dikkate alır ve istekteki diğer özniteliklerle birlikte erişim kararını verir. Klasik ABAC'te kısmi izinler bulunmamaktadır, ancak genişletilmiş ABAC'de PDP, kullanıcının kimlik doğrulama eşleşme puanına dayalı olarak kısmi izinler verebilir. Ardından, PDP aldığı yetkilendirme kararını PEP'e iletir. PEP, belirlenen yükümlülükler ve PDP'nin verdiği karara dayanarak konunun erişimini tamamen veya kısmen sağlar veya reddeder. Genişletilmiş ABAC mimarisi Şekil 2.3'de sunulmuştur.

W. He ve ekibi tarafından gerçekleştirilen [34] çalışmadan esinlenerek, kamera, akıllı



Şekil 2.4: Akıllı Evdeki Özniteliklerin Detayları

ışıklar, akıllı kilitler ve sesli asistanlardan oluşan küçük bir ev IoT ortamıyla ilgili senaryo belirlenmiştir. Senaryodaki akıllı evde yazılım güncellemesi yapma, müzik çalma, çevrim içi alışveriş yapma, kamerayı açma/kapatma, ışıkları açma/kapatma, kamera açısını değiştirme ve kapıyı açma/kapatma gibi işlemler gerçekleştirilebilir. Kullanıcı rolleri arasında Eş, Yetişkin, Çocuk, Bebek Bakıcısı veya Ziyaretçi aile üyesi gibi farklı profiller bulunabilir. Ayrıca, kullanıcının zamanı, konumu, yaşı ve cihazın durumu gibi faktörler de dikkate alınır.

Genişletilmiş ABAC modelinin işleyişini açıklamak için, bu küçük ev IoT senaryosunu Security Policy Tool adlı XACML editöründe simüle edilmiştir. Kullanıcı, kaynak ve ortam öznitelikleri detaylı bir şekilde Şekil reffig:example’de gösterilmiştir.

Kimlik doğrulama eşleşme puanı bir ortam özneliği olarak modele dahil edildiği için diğer özniteliklerle aynı şekilde değerlendirilmektedir. Örnek bir senaryo olarak, Google Home Ses Asistanı cihazının çevrim içi alışveriş özelliği için bir erişim kontrol politikası oluşturulabilir. Kullanıcının kimlik doğrulama puanı 90 ve üstü ise, erişim

kuralı ve politikası gereksinimlerini karşılar ve erişim sağlanır. Dolayısıyla, kullanıcının rolü ya Eş ya da Yetişkin ise ve kimlik doğrulama puanı 90 ve üstü ise ve konum evdeyse, erişim izni verilir; aksi takdirde, erişim reddedilir. Kimlik doğrulama eşleşme puanı bir ortam özelliği olarak ele alındığı için, her senaryo için politikalar belirlenmelidir. Aşağıda verilen kod örneği, XACML Politikasına kimlik doğrulama puanının nasıl dahil edileceğine dair bir örnek sunmaktadır.

```
<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.w3.org/2001/XMLSchema#boolean-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">
    True</AttributeValue>
  <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0::attributecategory:environment"
    AttributeId="urn:oasis:names:tc:xacml:1.0:environment:90PercentAuthenticated"
    DataType="http://www.w3.org/2001/XMLSchema#boolean" MustBePresent="true">
</AttributeDesignator>
</Match>
```

Bir başka erişim kontrol politikası da Google Home Ses Asistan cihazının çevrimiçi alışveriş özelliği için, kullanıcının kimlik doğrulama puanı 90'dan az ise, diğer istek özelliklerine bakılmaksızın erişimin reddedilmesidir. Google Home Ses Asistan cihazının çevrimiçi alışveriş özelliği için başka bir erişim kontrol politikası, kullanıcının kimlik doğrulama puanı 90'dan düşükse, diğer istek özelliklerine bakılmaksızın erişimin reddedilmesidir. Ayrıca, Google Home Ses Asistan cihazının müzik çalma özelliği bulunmaktadır. Müzik çalma, online alışveriş kadar kritik bir özellik olmadığı için, erişim kontrol politikası daha esnek olabilir. Örneğin, kimlik doğrulama puanı 60 ve üzeriyse, konum ev ve kullanıcının rolü Eş, Yetişkin, Çocuk, Bebek Bakıcısı veya Ziyaretçi ise, erişim sağlanır, aksi takdirde reddedilir.

Başka bir senaryoda, kameranın açısını değiştirmek veya kamerayı açıp kapatmak dikkatle yönetilmesi gereken ciddi eylemler olabilir. Eğer kullanıcı Bebek Bakıcısı ise, kameraya herhangi bir erişim yasaklanmalıdır. Bu nedenle, bu durum için erişim kont-

rol politikası, kullanıcı rolünün Bebek Bakıcısı olduğu ve bir kamera kaynağı için bir talep yapıldığında, diğer talep özellikleri göz önüne alınmaksızın erişimin reddedilmesi olabilir. Öte yandan, eğer zaman 18:00'den sonra ise ve konum ev ise, kullanıcı rolü Eş ise ve kimlik doğrulama puanı 90 ve üzeriyse, o zaman kameranın kapatılması için izin verilir[15].

Son senaryo olarak, kilitlerin ve ışıkların kaynaklar olarak düşünüldüğü bir senaryoyu ele alalım. Çocuğun ışıkları açıp kapaması büyük bir sorun olmamalıdır, ancak çocuğun kendiliğinden kapıyı açması sorun olabilir. Işıklar için bir erişim kontrol politikası, kimlik doğrulama puanının herhangi bir rol için 60 ve üzeri ve konumun ev olduğu ve zamanın 17:00'den sonra olduğu durumlarda ışıkların açılması için erişim sağlanabilir. Son olarak, kilitler için erişim kontrol politikası, rolün Çocuk olduğu, kimlik doğrulama puanının 70 ve üzeri olduğu ve konumun ev olduğu durumlarda erişimin reddedilmesi olabilir.

2.6 Kullanıcı Kimlik Doğrulaması ve Yetkilendirme

Biyometrik sistemler, erişim isteklerini izin verme veya reddetme konusunda karar vermek için algoritmalar kullanır. Kimlik doğrulama eşleştirme puanını (AMS) hesaplamak için ön işleme, puanlama ve eşikleme aşamalarını yürütürler ve bu sayede kimlik doğrulama kararı alırlar [64]. AMS, toplanan örnekler ile sunulan örnek arasındaki benzerliği ölçerek elde edilir. Eğer skor önceden belirlenmiş bir eşiğin üzerindeyse, bir eşleşme kararı alınır; aksi takdirde, bir eşleşme olmadığına karar verilir [25]. İki tür hata oranı vardır: Yanlış Eşleşme Oranı (Yanlış Kabul Oranı) ve Yanlış Eşleşmeme Oranı (Yanlış Reddetme Oranı). Eğer sahtekarın örneği meşru bir kullanıcının şablonuyla yanlışlıkla eşleştirilirse, bu bir Yanlış Eşleşme olarak adlandırılır. Diğer yandan, eğer meşru bir kullanıcının örneği eşleştirilmediyse, bu bir Yanlış Reddetme olarak adlandırılır. Hata oranları, eşik değerine bağlıdır, yani eşik değeri değiştikçe hata oranları da değişir [22]. Dolayısıyla, eşik değerinin belirlenmesi, meşru kullanıcılara erişim izni verme açısın-

dan hayati öneme sahiptir. [64]'da belirtildiği gibi, eşik değeri seçimi, iki hata türü arasında bir denge oluşturur. Puanlama işleminden sonra, puan eşik değerinden büyükse, erişim sağlanır. Ancak, puan eşik değerinden küçükse, erişim reddedilir. Sugrim ve diğerleri [64], kimlik doğrulama sistemlerindeki ön işleme, puanlama ve eşikleme işlemlerini açıklarken eşik değerinin önemini vurgular. Eşik değerlerinin seçimi, erişim kontrol kararlarının etkinliğini belirler, bu nedenle kurallar ve politikalar için uygun eşik değerlerinin seçilmesi önemlidir.

Ev IoT kullanıcıları genellikle erişim kontrol kararlarını hem kullanıcının rolüne hem de cihazın yeteneklerine dayandırma eğilimindedir. Örneğin, bir aile üyesinin kamera kayıtlarına erişmesi sorun yaratmayabilirken, bir bebek bakıcısının aynı kayıtlara erişmesi ciddi sonuçlara yol açabilir[34]. Dolayısıyla, yanlış yetkilendirme kararlarının etkisi, kullanıcının rolüne ve cihazın sağladığı işlevselliğe bağlıdır. Bir kişinin gerçekten izin verilmek istenen kişi olduğunu güvence altına almak, cihazın kötü niyetle kullanılmasını önlemek açısından kritik öneme sahiptir. Diğer önemli bir konu da işlevin alışılmadık şekillerde kullanılmasıdır [34]. Genişletilmiş ABAC modelinde, kimlik doğrulama puanı için bir eşik değeri belirlemek, kullanıcının kimliğini doğrulamak için önemlidir. Farklı erişim politikaları oluşturmak için çeşitli eşik değerlerine ihtiyaç vardır. Örneğin:

- 90 ve üzeri: Tam erişim için bir eşik değeri olabilir.
- 80 ile 90 arası: Kritik erişim için bir eşik değeri olabilir.
- 60 ile 80 arası: Önemli erişim için bir eşik değeri olabilir.
- 50 ile 60 arası: Temel erişim için bir eşik değeri olabilir.
- 50'nin altında: Tüm erişimin reddedilmesi için bir eşik değeri olabilir.

Bu nedenle, doğru bir eşik değeri seçimi, kimlik doğrulamanın etkinliği açısından kritik öneme sahiptir[15]. Temel soru, en uygun eşik değerinin nasıl seçileceğidir. Kullanıcılar her erişim politikası için eşik değerlerini manuel olarak belirleyebilir veya UBA gibi

makine öğrenimi teknikleri uygulanabilir. İlk seçenek pek pratik değildir çünkü çeşitli senaryolar için birçok eşik değeri belirlenmesi gerekecektir. Bu da kullanıcılara ağır bir yük getirecektir. Bir diğer alternatif bir yaklaşım olarak performans metrikleri kullanılabilir. [64]'de belirtildiği gibi, bir eşik seçimi, hata türleri arasında bir dengeyi gösterir. Hatanın tamamen ortadan kaldırılması mümkün olmasa da, bir hata türünü diğerine dönüştürmek mümkündür. Sonuç olarak, iyi bir ayrım sağlayan bir puanlama işlevi varsa, birçok farklı eşik seçimi mevcut olacaktır. Eşit Hata Oranı (EER) ve Maksimum Doğruluk (ACC) gibi performans metrikleri, belirli bir eşik belirler ve bunun için bir performans metrik değeri alır. Genellikle, bu metriği optimize etmek için bir eşik seçilir. Örneğin, Alıcı Operatör Karakteristik Eğrisi (ROC), kimlik doğrulama eşik değerlerinin puanın mümkün olan maksimum değerlerinden minimum olası değerlerine kadar değiştirilmesiyle hesaplanır ve her eşik değeri için Gerçek Pozitif Oranı (TPR) ve Yanlış Pozitif Oranı (FPR) hesaplanır. Daha sonra hesaplanan ROC Eğrisini özetlemek için EER, ROC Eğrisi Altındaki Alan (AUROC) ve Gini Katsayısı (GC) performans ölçümleri kullanılır. Akıllı ev özelinde düşünülürse, EER'in 0.4'ün altında olduğu bir performans metriği ROC eğrisi ise, erişim sağlanır. Örneğin, talep edilen işlev kritikse, örneğin kamerayı kapatma gibi, erişim kontrol politikası şöyle olabilir: eğer zaman 18:00'den sonra ise ve konum ev ise ve konunun kimlik doğrulama puanına karşılık gelen EER 0.2'nin altında ise, o zaman kamerayı kapatma erişimi sağlanır. Bu yöntem, her senaryo için tüm eşik değerlerini tanımlama zorunluluğunu ortadan kaldırır. Ancak, bu performans metriklerinin her zaman mevcut olmayabileceğini unutmamak gerekir[15].



3. AKILLI EVLERDE KİMLİK DOĞRULAMA ÖZELLİKLİ ABAC (AeABAC)

Tezin bu bölümü kapsamında yapılan çalışmanın çıktısı International Journal of Information Security Dergisinde "Authentication-enabled attribute-based access control for smart homes" başlıklı makale olarak yayınlanmıştır [14].

İkinci bölümde genişletilen ABAC modelinde [15] erişim kararları belirlenen eşik değerlerine göre verilmekteydi. Ancak birkaç eşik değeri belirlemenin zorluğu belirtilerek performans metriklerinin kullanılması önerilmişti. Bu bölümde, birkaç eşik değeri belirlemek yerine performans metriklerinin kullanılmasına odaklanılacaktır. Performans metrikleri derinlemesine tartışılarak kimlik doğrulama eşleme skorunun FMR'nin hesaplanıp kullanılması önerilecektir. Kullanıcı kimlik doğrulamasının genellikle biyometrik yöntemlerle yapıldığı IoT uygulamaları için daha özlü ve uygun bir model sunulacaktır.

Bu bölümde AeABAC (Kimlik Doğrulama Yeteneğine Sahip ABAC) modeli mimarisi ve nasıl çalıştığı açıklanacaktır. Kullanıcı kimlik doğrulamasının güvence düzeyinin nasıl belirlendiği senaryolarla anlatılacaktır. Akıllı evler için önerilen AeABAC modelinin bileşenleri, öznitelikleri formel dilde ifade edilecektir. İşlevsellik temelli erişim karar mekanizması açıklanarak AeABAC modelinin uygulanabilirliği gösterilecektir. Örnek akıllı ev senaryolarının XACML uygulaması gösterilecektir. AeABAC modelinin literatür karşılaştırması yapılacaktır. Son olarak AeABAC modelinin mevcut IoT platformlarına uyarlama çalışmaları gösterilecektir.

3.1 AeABAC Modeli

Genişletilmiş ABAC modelinde, kullanıcılar (iddia edilen rolle) erişim isteği gönderdikten ve biyometrik araçlar aracılığıyla kimlik doğrulandıktan sonra bir kimlik doğrulama eşleşme puanı (AMS) elde ederler. Daha sonra, kullanıcıların kimlik doğrulama eşleşme

puanlarının Yanlış Eşleşme Oranı (FMR) hesaplanır. Bu puan, Erişim Kararı Belirsizlik Puanı (ADUS) olarak adlandırılır. ADUS, kullanıcı isteğine normal bir öznitelik olarak eklenir. Ardından, erişim istenen akıllı ev cihazı işlevi için erişim kararı, ADUS, kullanıcının rolü ve diğer çevresel özelliklere göre verilir. Örneğin, akıllı ev kullanıcıları genellikle Google Home gibi ses asistanlarını kullanarak akıllı ev cihazlarını yönetirler. Bu şekilde, sadece "Hey Google, şunu yap" diyerek evi süpürebilir, çevrimiçi alışveriş yapabilir veya müzik çalabilir.

Genellikle kimliği doğrulanmış ev kullanıcıları, belirli işlevleri kullanmaları gerektiğinde bile tüm akıllı cihazlara bütün işlevleriyle birlikte erişime izin verilir. Ancak, genişletilmiş ince taneli modelde, örneğin, yetişkin rolündeki kimliği doğrulanmış kullanıcının ADUS'u FMR1000'den daha güçlü değilse, çevrimiçi alışveriş yapamaz, ancak Google Home Asistanı aracılığıyla müzik çalabilir. Ancak ADUS'u daha güçlüyse (örneğin, FMR10000'de) çevrimiçi alışveriş yapabilir veya diğer kritik işlevleri çalıştırabilir. FMR100, FMR1000 ve FMR10000 göstergeleri sırasıyla 1/100, 1/1000 ve 1/10000 özgüllük seviyelerindeki FMR seviyeleridir. ADUS bir FMR metriği olduğundan, ADUS ne kadar küçük olursa, kullanıcı kimlik doğrulamasının güvenilirliği o kadar kesin olur. Bölüm 2'de sunulan modelde erişim kararları verirken kullanılan AMS yerine (Kimlik Doğrulama Eşleşme Puanı) bu bölümde sunulan modelde ADUS'un kullanılmasının motivasyonu, geniş bir biyometrik cihaz ve algoritma yelpazesinde normalleştirmeyi kolaylaştırmak ve kısa ve öz politika spesifikasyonu yapmaktır[14].

IoT'de işlev odaklı erişim kontrolüne olan ihtiyaç fark edilse dahi literatürde bu konuya henüz yeterince dikkat edilmemiştir. Sınırlı sayıda çalışma, IoT erişim kontrolünde işlev odaklı bir yaklaşımın önemini belirtmektedir. Bölüm 2.4'de bu konudaki literatür taraması sunulmuştur. Literatüre katkı sağlayarak cihaz işlevlerinin temel, önemli ve kritik düzeyine dayalı erişim kararlarının tanımlanması önerilmektedir. ABAC mimarisi esnekliği sayesinde cihaz kritiklik seviyesi, diğer çevresel öznitelikler gibi normal bir öznitelik olarak ele alınabilir. Bu şekilde, erişim politika kurallarının, işlevsellik ba-

şına belirlenmesi yerine işlevsel kritiklik seviyesine göre belirlenmesi nedeniyle erişim politikalarının sayısı önemli ölçüde azaltılabilir.

Bu tez kapsamında bu bölümde genişletilen Kimlik Doğrulama Özellikli ABAC(AeABAC) modeli Bölüm 2’de sunulan modelin üstüne kimlik doğrulama eşleşme puanını ve cihaz işlevlerinin kritiklik seviyesini de ekler. AeABAC modelinde erişim kararları kimlik doğrulama eşleşme puanının ADUS’una, kullanıcının rolüne, ve işlevlerin kritiklik seviyesine göre verilir. Erişim kararları izin vermek, reddetmek veya yükseltmek olabilir.

3.2 Kullanıcı Kimlik Doğrulamasının Güvence Düzeyi

Normalde erişim talebi sadece kullanıcı için hesaplanan AMS belirli bir eşik üzerindeyse kabul edilir. AeABAC modelinde ise erişim kararı vermek için AMS’yi doğrudan kullanmak yerine, bu puanı FMR ile karşılaştırılabilir hale getirmek önerilmektedir. Sonraki adım ise cihazlar ve algoritmalar için FMR seviyelerinin nasıl elde edileceğidir. Bu bilgiyi elde etmek için (i) işletim sırasında büyük ölçekli giriş örneklerini toplamak, (ii) üreticinin teknik dokümanlarında verilen özelliklere başvurmak veya (iii) karşılaştırmalı hizmetlerden faydalanmak mümkündür.

Bu tezde FVC-onGoing projesinin FV-HARD-1.0 benchmark sonuçları kullanılmıştır[36],[24]. Bu proje, parmak izi doğrulama gibi çeşitli biyometrik algoritmalar için belirli veri kümeleri ve test protokolleri sunar [46]. Aynı benchmark üzerinde birçok algoritmanın performansını karşılaştırır ve istatistiksel sonuçlarını yayımlar.

Parmak izi doğrulama örneğinde, Yanlış Eşleşme Oranı (FMR) ve Yanlış Eşleşmeme Oranı (FNMR), farklı eşik değerlerinde hesaplanır. FNMR ve FMR’yi hesaplamak için, gerçek (aynı parmak izinden gelen iki parmak izini eşleştirme) ve sahte (farklı parmaklardan gelen iki parmak izini eşleştirme) denemeleri yapılır.

Gerçek (genuine matching score)ve sahte eşleşme puanı (impostor matching score) da-

ğılımları, FVC-onGoing projesinin web sitesinde bir histogram olarak çizilir. Parmak izi doğrulamada, yüksek eşleşme puanları, daha yakın eşleşen görüntülerle ilişkilendirilir. Sahte ve gerçek eşleşme puanı dağılımları, 0.0 ile 1.0 arasındaki eşik değerleri için elde edilir. Diğer puan dağılımları arasında, FMR ve FNMR puanları 0,0 ile 1,0 arasında değişen t eşiği için hesaplanır ve ardından Karar Hata Takası (DET) grafiği çizilir; burada $(FMR(t), FNMR(t))$ çiftleri iki eksen [46] boyunca çizilir.

Cihazdan cihaza ve algoritmadan algoritmaya değişmeyen kapsamlı ve özlü bir politika belirleme için bir normalleştirme gereklidir. Bu noktada, AMS'nin eşik değerinden ne kadar uzakta olduğunu veren FMR iyi bir seçimdir. Aslında, görünüşte benzer AMS'ler için önemli FMR farklılıkları olabilir. Benzer şekilde, farklı biyometrik sistemlerde görünüşte benzer olmayan AMS'ler, yine de karşılık gelen eşik değerlerinden benzer uzaklıklarda olabilir, ancak yine de önemli ölçüde farklı FMR'ler sergileyebilir. Daha somut olmak için aşağıda üç senaryo verilmiştir.

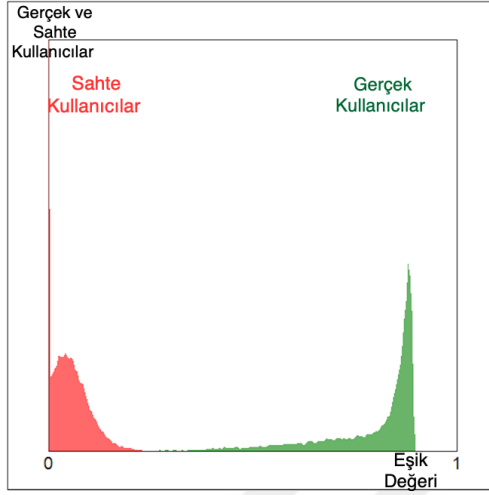
3.2.1 1. Senaryo

İlk senaryoda, Bob ve Mary adında iki kullanıcının aynı akıllı cihazı kullanacağı varsayılmaktadır. FVC-onGoing projesinde sunulan FV-HARD-1.0 benchmarkındaki parmak izi eşleme algoritması olan HXKJ V4.3'ü kullanan bir parmak izi sensörü aracılığıyla kullanıcıların kimliğini doğrulayan aynı akıllı kapı açma sistemini kullanırlar. Bob akıllı kapıyı parmağıyla açmaya çalışır ve AMS değeri olarak 0.8 alır. Daha sonra Mary, parmak iziyle akıllı kapıyı açmaya çalışır ve AMS değeri olarak 0.7 alır. Eşik değeri T , $FMR(T) = FMR_{110}$ 'u karşılayacak şekilde seçildiği varsayılmıştır. Bir kullanıcının AMS değerinin 0.7 veya 0.8 olması durumunda nasıl bir fark olacağı analiz edilmek istenmektedir. Bu noktayı açıklığa kavuşturmak için, parmak izi eşleme algoritmasının HXKJ V4.3'ün performans sonuçları kullanılmıştır. Eşleşme puanlarının FMR'ine dayalı olarak erişim kararları alınması önerilmektedir. AMS değeri 0.7 ve AMS değeri 0.8 için FMR ve FNMR hesaplanmalıdır. Bu algoritmanın DET grafiği,

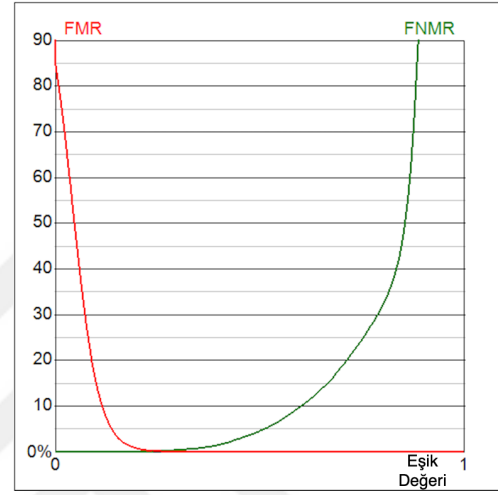
gerekli bilgiyi sağlamaktadır. DET grafiği, FMR'nin 0.01, 0.001 ve 0.0001 olduğu durumlarda karşılık gelen FNMR değerlerini gösterir. HXKJ V4.3 algoritmasının puan histogramı, eşleşme oranı grafiği ve DET grafiği Şekil 3.1'de verilmiştir. $AMS \approx 0.7$ olduğunda, FMR'nin $FMR(T+0.1)$ 'e yakın olduğu varsayılır. $AMS \approx 0.8$ olduğunda, FMR'nin $FMR(T+0.2)$ 'ye yakın olduğunu varsayılır. İki AMS arasında az bir fark olmasına rağmen, bu iki skor için karşılık gelen FMR değerleri önemli ölçüde farklılık gösterir (bir büyüklük sırası)[14]. Bu senaryo için FMR değerleri Şekil 3.2'de gösterilmiştir.

3.2.2 2. Senaryo

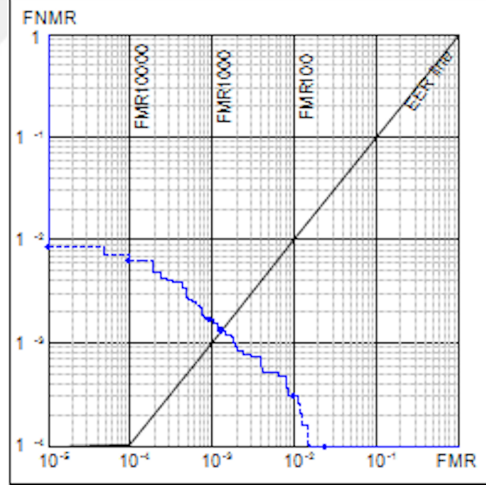
Bu senaryoda, tek kullanıcı olarak Bob'un farklı biyometrik kimlik doğrulama algoritmaları kullanan iki akıllı cihazı kullandığı varsayılmaktadır. Bunlardan ilki, FV-HARD-1.0 üzerinde HXKJ V4.3 [24] parmak izi algoritmasını kullanan ilk senaryo ile aynı akıllı kapı kilidi, diğeri ise FV-HARD-1.0 üzerinde parmak izi eşleştirme algoritması MMFV 12.0 kullanan bir akıllı kameradır. MMFV 12.0 algoritmasının puan histogramı, eşleşme oranı grafiği ve DET grafiği Şekil 3.3'de verilmiştir[36], [24]. İki sistem, aynı kullanıcı için farklı güven seviyelerine sahip olabilir. Örneğin, $FMR(T)$ 'nin $FMR110$ olduğu durumda Bob, akıllı kilitte AMS değeri olarak 0.7 alır, bu skora karşılık gelen FMR, $FMR(T+0.2)$ 'dir. Buna karşılık, akıllı kamerada AMS değeri olarak 0.4 alır. Burada eşik $FMR(T)$ $FMR120$ 'ye eşittir. Karşılık gelen FMR, MMFV 12.0 eşleme algoritması için iyi olan $FMR(T+0.2)$ civarına düşer. İki AMS karşılaştırıldığında, Bob'un kimliğiyle ilgili kalan belirsizlik farklılık gösterir. Hatta eşleme puanları ilgili eşik T 'nin 0.2 puan önündedir. Bu durum Şekil 3.4'de gösterilmiştir. Bu nedenle, FMR'ye dayalı erişim kararları, kimlik doğrulama güven düzeyinde daha kesin bir bilgi sağlar[14].



(a) HXKJ V4.3 Histogramı

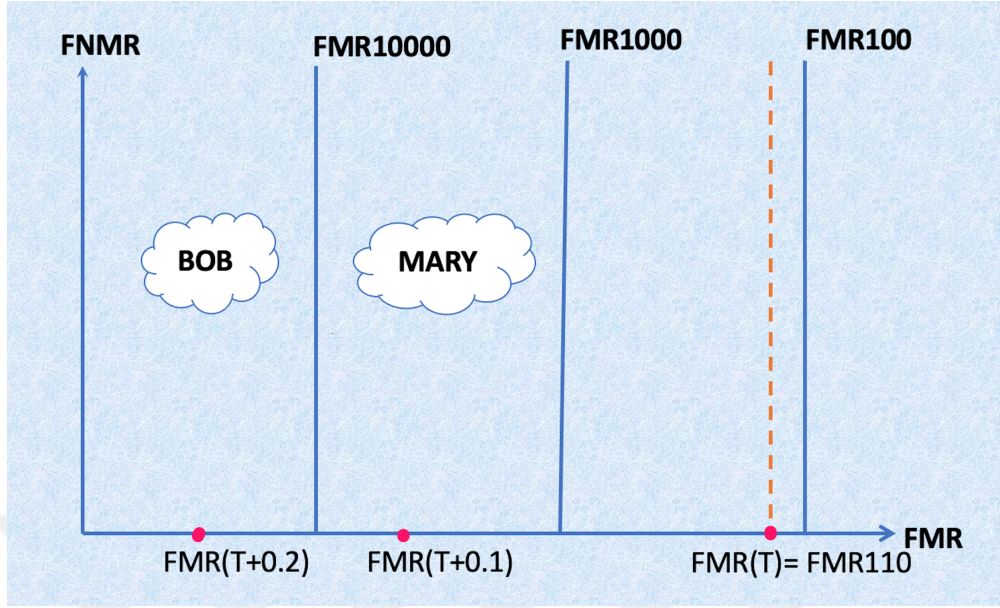


(b) HXKJ V4.3 için Eşleşme Oranı Grafiği



(c) HXKJ V4.3 için DET Grafiği

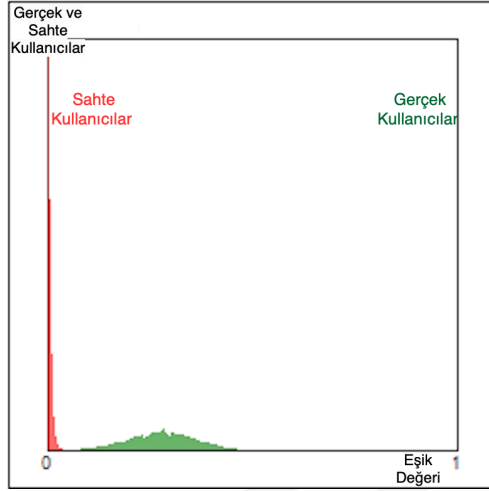
Şekil 3.1: HXKJ V4.3 Metrikleri [36].



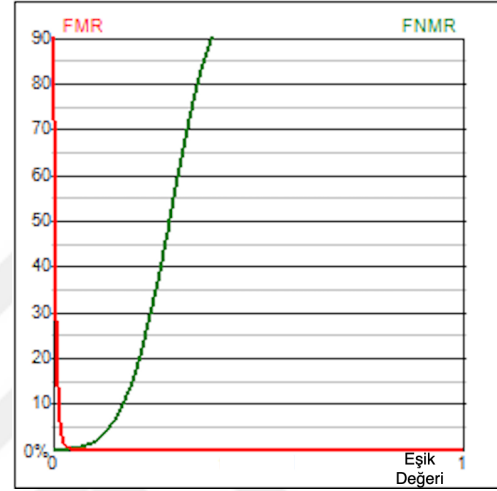
Şekil 3.2: Senaryo I için FMR Değerleri

3.2.3 3. Senaryo

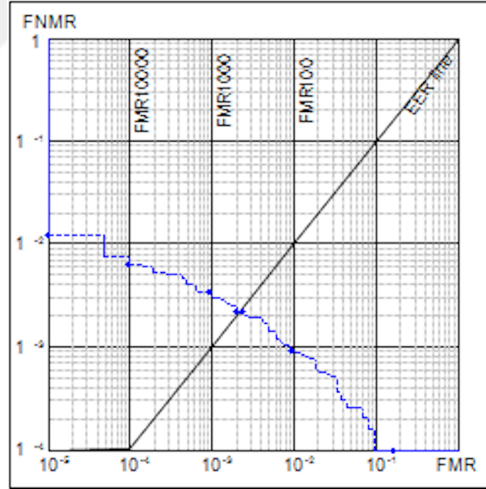
Bu senaryo, Senaryo I'ye benzerlik göstermektedir. Yine iki kullanıcı, Eric ve Jane olduğunu varsayılmaktadır, ancak bu sefer kimlik doğrulaması için palmiye izi doğrulamasını kullanmaktadırlar. Kullanıcılar, kimlik doğrulamasını sağlayan aynı akıllı güvenlik kamerasını kullanmaktadırlar. Bu kamera, FV-HARD-1.0'deki sunulan PV-FULL-1.0 benchmarkındaki HXKJ 3.02 algoritmasını kullanmaktadır. Eric ve Jane'in akıllı kamera erişim denemelerinde AMS değerlerinin sırasıyla 0.5 ve 0.6 olduğu varsayılmaktadır. Eşik değeri T'nin $FMR(T) = FMR120$ 'yi karşılayacak şekilde seçildiği farzedilir. AMS değerlerinin 0.5 veya 0.6 olması durumunda kimlik doğrulama güven düzeylerinin ne kadar farklı olduğu analiz edilmektedir. Bu noktayı açıklığa kavuşturmak için, HXKJ 3.02 algoritmasının PV-FULL-1.0 için performans sonuçlarını kullanılmaktadır. HXKJ 3.02 algoritmasının puan histogramı, eşleşme oranı grafiği ve DET grafiği Şekil 3.5'de verilmiştir[36], [24]. Bu çizimler, analizin yapılabilmesi için bilgilendiricidir. İki AMS'yi hizalamak için, AMS değeri 0.5 olduğunda FMR'nin $FMR(T+0.1)$ 'e yakın olduğu ve AMS değeri 0.6 olduğunda FMR'nin $FMR(T+0.3)$ 'e yakın olduğu



(a) MMFV 12.0 Histogramı

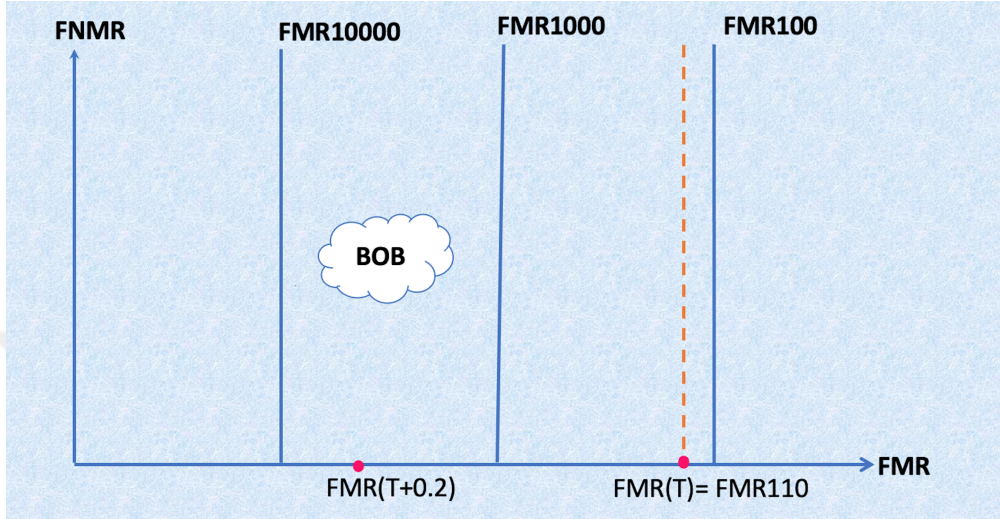


(b) MMFV 12.0 için Eşleşme Oranı Grafiği

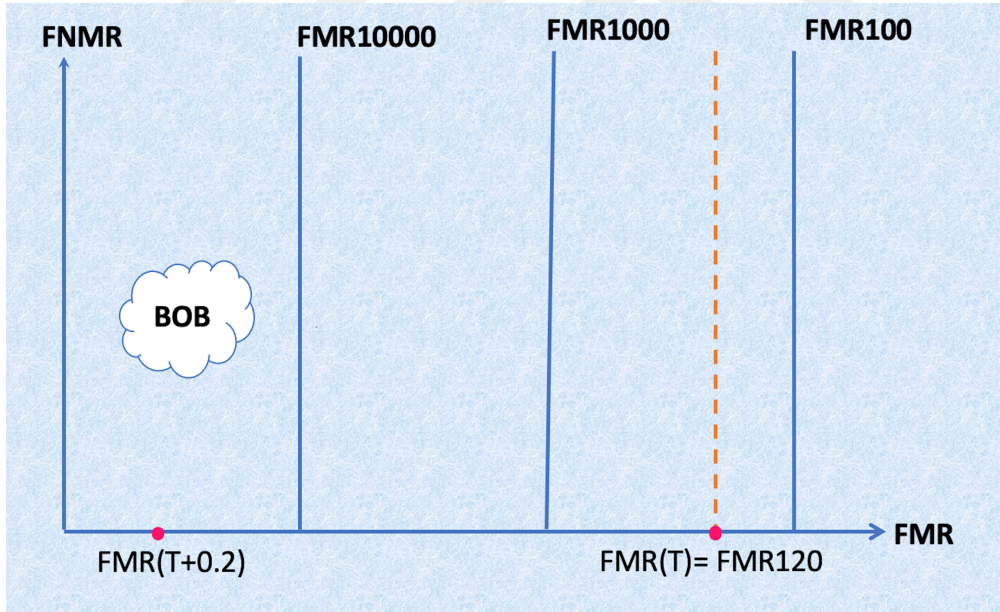


(c) MMFV 12.0 için DET Grafiği

Şekil 3.3: MMFV 12.0 Metrikleri[36].



(a) Sistem 1



(b) Sistem 2

Şekil 3.4: Senaryo II için FMR değerleri

varsayılmaktadır[14]. Her iki AMS'nin hafifçe farklı olmasına rağmen, Şekil 3.6'da görüleceği gibi FMR açısından bir büyüklük sırası farkı olduğu görülmektedir.

3.3 Akıllı Evler için AeABAC Modeli

Nesnelerin interneti uygulamaları üç ana kategoride ele alınabilir: akıllı ev, akıllı sağlık ve akıllı şehir. Bu bölümde akıllı evlere yoğunlaşıp AeABAC modelinin gerçek senaryolarla kullanımı ve uygulanabilirliği ele alınacaktır. AeABAC modeli akıllı evlerde kullanıcı-cihaz etkileşimi için geliştirilmiştir. AeABAC modelinin formel bir spesifikasyonunu, Ameer vd. [6] çalışmasında sunulan temel çerçeveye dayanarak önerilmektedir. Ameer vd.[6] tarafından yapılan çalışmanın bir uzantısı olan AeABAC, ADUS'u önemli bir öznelik olarak tanıtır. AeABAC modelinin ana bileşenleri şunlardır: Kullanıcılar (U), Oturumlar (S), Cihazlar (D), Çevresel Durumlar (ES) ve Politikalar (P).

3.3.1 Tanımlar

Kullanıcılar(U): Cihazlarda işlemleri gerçekleştiren varlıkların kümesi.

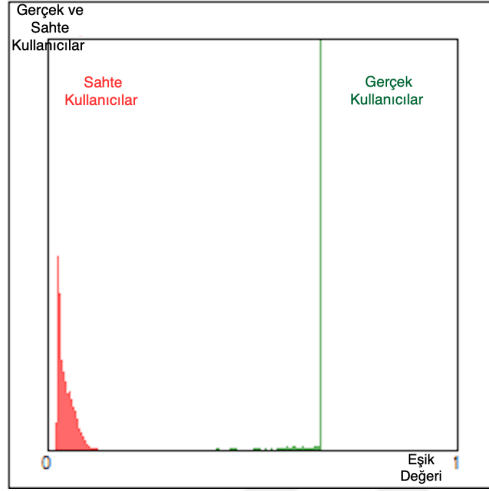
Oturumlar(S): Kullanıcıların cihazlarda eylem gerçekleştirirken oluşturduğu ve sonlandırdığı tüm kullanıcı oturumlarının kümesi. Her oturum, oturumu yöneten bir kullanıcıyla ilişkilendirilir.

Cihazlar(D): Akıllı ev cihazlarının kümesi, örneğin akıllı kapı kilitleri, kameralar ve ses asistanları.

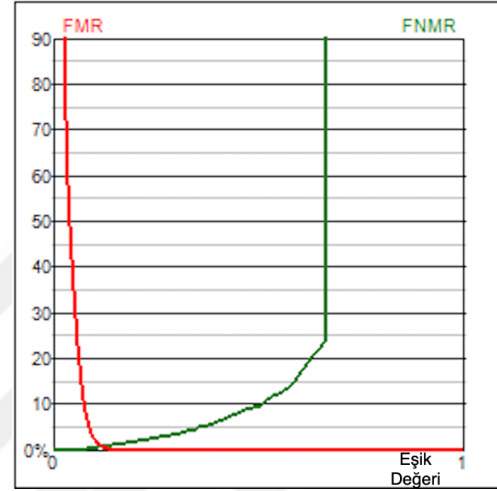
Cihaz İşlevleri(DF): Kullanıcıların cihazlarda gerçekleştirebileceği işlevlerin cihaz üreticisi tarafından tanımlanan kümesi.

İşlev Kritiklik Seviyesi : Cihaz işlevlerinin temel, önemli, kritik gibi kritiklik seviyesini tanımlayan atomik bir öznelik.

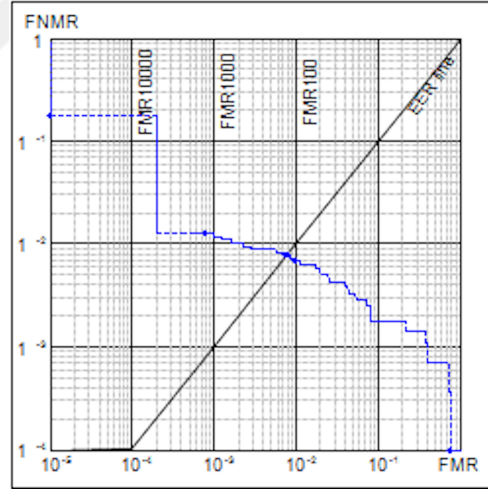
Kimlik Doğrulama Eşleştirme Puanı (AMS(u)): Kullanıcıyı doğrulayan biyometrik sistemin hesapladığı, 0.0 ile 1.0 arasında bir değere sahip bir kullanıcı özneliği



(a) HXKJ 3.02 için Histogram

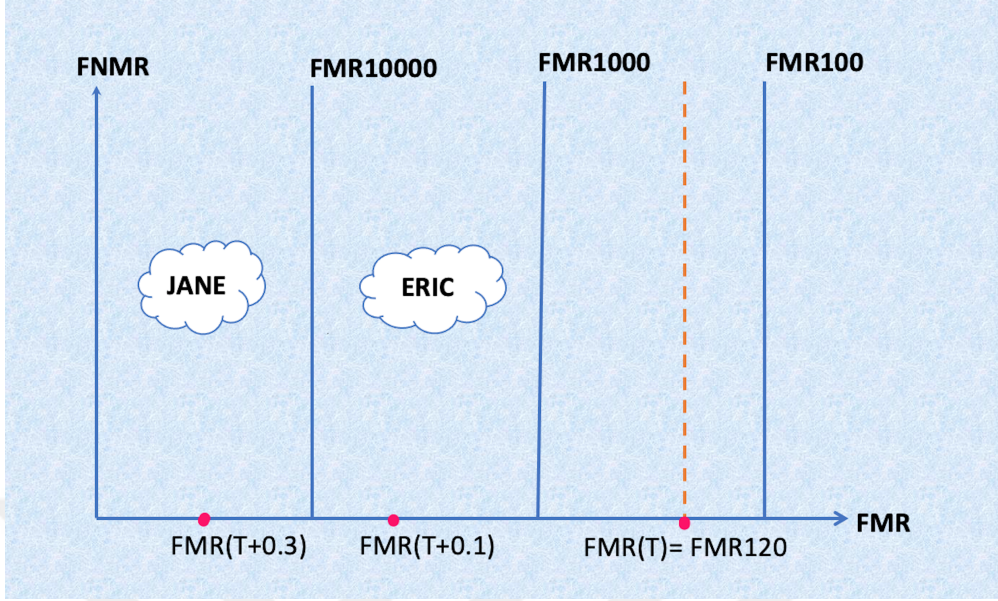


(b) HXKJ 3.02 için Eşleşme Oranı Grafiği



(c) HXKJ 3.02 için DET Grafiği

Şekil 3.5: HXKJ 3.02 Metrikleri [36].



Şekil 3.6: FMRs for the Scenario III

Erişim Kararı Belirsizlik Puanı(ADUS(u)): Kullanıcının kimlik doğrulama eşleştirme puanını girdi olarak alan ve kullanıcı için AMS'ye göre FMR'ı veren fonksiyon. $FMR(AMS(u))$ 'un sonucunu döndürür.

Çevresel Durumlar (ES): Belirli bir zamandaki mevcut durumu temsil eden çevresel durumların kümesi, örneğin IP adresi, sıcaklık, zaman veya hava durumu.

3.3.2 Öznitelikler

Kullanıcılar, oturumlar, cihazlar, çevresel durumlar, cihaz işlevleri ve işlemler özniteliklere sahiptir. Tüm öznitelikler kümesi, Kullanıcı Öznitelikleri (UA), Oturum Öznitelikleri (SA), Cihaz Öznitelikleri (DA), Cihaz İşlevleri Öznitelikleri (DFA), İşlem Öznitelikleri (OA) ve Çevresel Durum Öznitelikleri (EA) olarak oluşur. Öznitelikler, bir varlığı girdi olarak alıp bir değer döndüren fonksiyonlar olarak düşünülebilir. Atomik veya küme değerine sahip olabilirler. Sonlu bir atomik değerler koleksiyonu, bir özniteliğin aralığını tanımlar. Küme değerli bir öznitelik, aralığın bir alt kümesini döndürür, ancak atomik değerli bir öznitelik kendi aralığından bir değer döndürür.

Her öznitelik $att \in UA \cup SA \cup DA \cup DFA \cup ESA$ $Range(att)$ ile gösterilen sonlu bir atomik değerler kümesine sahiptir. $attType(att) \in \{kme, atomik\}$ özneliğin küme veya atomik değere sahip olacağını belirler.

Kullanıcı Öznitelikleri (UA): Rol, yaş ve cinsiyet gibi kullanıcı öznitelikleridir. UA'daki att_u , U'daki kullanıcıları öznitelik değerlerine eşler.

$att_u : U \rightarrow 2^{Range(att_u)}$ if $attType(att_u) = \text{küme}$

$att_u : U \rightarrow Range(att_u)$ if $attType(att_u) = \text{atomik}$

Oturum Öznitelikleri (SA): Kullanıcı öznitelikleri kümesi olup oturumu başlatan kullanıcının özniteliklerini alır. Formel olarak $SA(s) \subseteq UA(sessionUser(s))$ her bir $s \in S$. SA'daki her öznitelik işlevi $att_s \in SA$, S'deki oturumları öznitelik değerlerine eşler.

$att_s : S \rightarrow 2^{Range(att_s)}$ if $attType(att_s) = \text{küme}$

$att_s : S \rightarrow Range(att_s)$ if $attType(att_s) = \text{atomik}$

Cihaz Öznitelikleri (DA): Akıllı cihazları tanımlayan özniteliklerin kümesidir. Kısmi fonksiyonlardır, bu nedenle bazı cihazlar atanmış özniteliklere sahip olmayabilir. DA'daki her öznitelik işlevi $att_d \in DA$, D'deki her cihazı öznitelik değerlerine eşler.

$att_d : D \rightarrow 2^{Range(att_d)}$ if $attType(att_d) = \text{küme}$

$att_d : D \rightarrow Range(att_d)$ if $attType(att_d) = \text{atomik}$

Cihaz İşlevleri Öznitelikleri(DFA): Akıllı cihaz fonksiyonlarını tanımlayan özniteliklerin kümesi, açma/kapatma, çevrimiçi alışveriş, müzik çalma ve ışıkları açma/kapama gibi. DFA'daki her öznitelik işlevi $att_{df} \in DFA$, DF'deki her cihaz fonksiyonunu öznitelik değerlerine eşler. Her cihaz işlevinin temel, önemli ve kritik olmak üzere bir türü vardır.

$att_{df} : DF \rightarrow 2^{Range(att_{df})}$ if $attType(att_{df}) = \text{küme}$

$att_{df} : DF \rightarrow Range(att_{df})$ if $attType(att_{df}) = \text{atomik}$

Çevresel Durum Öznitelikleri (ESA): Sıcaklık, zaman veya hava gibi geçerli çevresel durumu temsil eden özniteliklerin kümesidir. ESA'daki her öznitelik işlevi $att_{es} \in ESA$,

ES'deki çevresel durumları öznitelik değerlerine eşler.

$att_{es} : ES \rightarrow 2^{Range(att_{es})}$ if $attType(att_{es}) = \text{küme}$

$att_{es} : ES \rightarrow Range(att_{es})$ if $attType(att_{es}) = \text{atomik}$

Politikalar(P): Temel bileşenler üzerindeki yetkilendirmeler politikalar veya yetki kuralları aracılığıyla belirlenebilir. Politikalar, oturum, cihaz ve çevresel öznitelikler için örneğe özgü boolean işlevlerdir ve istenen işlemlerin izin verilip verilmeyeceğini değerlendirir.

Erişim Kararı: Her erişim kararı, oturum sırasında ADUS (Yetkilendirme Karar Puanı) değerine sahip olan kullanıcı $u \in U$ ile ilgili altı girdiyi değerlendirir. Oturum $s \in S$ sırasında, kullanıcının cihaz $d \in D$ üzerindeki cihaz işlevi $df \in DF$ için bir işlem gerçekleştirmeye yetkilendirilip yetkilendirilmediği, ayrıca bu işlemin gerçekleşeceği çevresel durumlar $es \in ES$ ile uyumlu olup olmadığını belirler. Dolayısıyla, her erişim kararı, kullanıcının belirli bir cihazda belirli bir işlemi gerçekleştirmesi gerekip gerekmediğini belirleyen bir öznitelik tabanlı yetkilendirme politikası ile ilişkilidir. Bu yetkilendirme politikası, erişim kararını almak için kullanıcının oturum, çevresel durumlar, cihaz, cihaz öznitelikleri ve ADUS'u karşılaştırır.

3.3.3 Örnekler

Aşağıda, AeABAC modelinin bileşenlerini ve yapılandırmalarını göstermek için bazı örnek kurallar tanımlanmıştır. İlk kuralda, FMR1000'den daha güçlü ADUS'a sahip olan eş ve genç rolleri ev içindeki herhangi bir cihazın önemli işlevlerine erişebilir. İkinci kuralda, ev içindeki en az FMR100 sahip olan tüm kullanıcılar basit cihaz fonksiyonlarını gerçekleştirebilir. AeABAC modeli yapılandırılabilir ve aşağıdaki gibi formel erişim kuralları yazılabilir[14]:

$U = \{ \text{Tracy, Bob, Meggy} \}$

$UA = \{ \text{Role, Location} \}$

$\text{Role}(u) : U \rightarrow \{ \text{eş, çocuk, genç, bakıcı, misafir} \}$

$\text{Location}(u) : U \rightarrow \{ \text{içeri, dışarı} \}$

$\text{Role}(\text{Tracy}) = \text{eş}$

$\text{Role}(\text{Bob}) = \text{genç}$

$\text{Role}(\text{Meggy}) = \text{bakıcı}$

$SA = \{ \text{Role, Location} \}$

$D = \{ \text{GoogleHomeAssistant, PhilipsHueLamp, AndroidBox, DoorLock, Camera} \}$

$DF_{\text{GoogleHomeAssistant}} = \{ \text{OnlineShopping, PlayingMusic, TurningOn, TurningOff} \}$

$DF_{\text{AndroidBox}} = \{ \text{NetFlix, Youtube, Spotify, PlayGame} \}$

$DF_{\text{PhilipsHueLamp}} = \{ \text{ON, OFF} \}$

$DF_{\text{DoorLock}} = \{ \text{Open, Close} \}$

$DF_{\text{Camera}} = \{ \text{Open, Close, ChangeAngle, ViewRecords} \}$

$DFA = \{ \text{Type} \}$

$\text{Type}(df) : DF \rightarrow \{ \text{Temel, Önemli, Kritik} \}$

$\text{Type}(\text{OnlineShopping}) = \text{Type}(\text{ChangeAngle}) =$

$\text{Type}(\text{ViewRecords}) = \text{Kritik}$

$\text{Type}(\text{ON}) = \text{Type}(\text{OFF}) = \text{Type}(\text{PlayGame}) =$

$\text{Type}(\text{Open}) = \text{Type}(\text{Close}) = \text{Önemli}$

$\text{Type}(\text{PlayingMusic}) = \text{Type}(\text{NetFlix}) = \text{Type}(\text{Youtube}) = \text{Type}(\text{Spotify}) = \text{Temel}$

$ES = \{ \text{Now} \}$

$ESA = \{ \text{day} \}$

$\text{day}(es) : ES \rightarrow \{ \text{S, M, T, W, Th, F, Sa} \}$

Yukarıki senaryo formel olarak şöyle yazılabilir:

Birinci Kural: $\text{isAllowable}(s:S, ADUS(u), es:ES, d:D, df:DF) = (\text{Role}(s) = \text{genç} \vee \text{Role}(s) = \text{eş} \wedge ADUS(u) < FMR1000 \wedge (\text{Type}(df) = \text{Önemli})) \wedge \text{Location}(s) = \text{inside}$

İkinci Kural: $\text{isAllowable}(s:S, ADUS(u), es:ES, d:D, df:DF) = (ADUS(u) < FMR100$

$\wedge \text{Type(df)} = \text{Temel} \wedge \text{Location(s)=içeri}$)

3.3.4 İşlevsellik Temelli Erişim Kararları

İşlevsellik temelli erişim kontrol politikalarını belirlemek, en güvenli erişim denetimini sağlamak için oldukça önemlidir. Ayrıca, erişime izin verilen kişinin cihazın kötüye kullanımını önleyen kişi olduğundan emin olmak da kritik bir husustur. AeABAC modelinde bir kullanıcının kimliğini sağlamak için ADUS'u ölçmek ve bir kimlik doğrulama puanı belirlemek büyük önem taşımaktadır. Erişim kararları temel, önemli ve kritik olmak üzere üç farklı fonksiyonellik seviyesine ayrılmıştır.

Temel işlevler, yetkisiz erişim durumunda genellikle riskli olarak kabul edilmez. Bunlar arasında elektrik süpürgesi çalıştırma, ışıkları açma, televizyonu açma veya müzik çalma gibi işlemler bulunabilir. Önemli işlevler ise, kötü niyetli veya yetkisiz erişimlerin gerçekleşmesi durumunda riskli olarak kabul edilir. Kapıyı kilitleme, fırını açma veya çim biçme makinelerini çalıştırma gibi işlemler buna örnektir. Son olarak, kritik işlevler, yetkisiz erişimlerin gerçekleşmesi durumunda en riskli olanlardır. Kamera açma/kapatma, çevrimiçi alışveriş yapma ve erişim kayıtlarını silme gibi işlemler bu kategoride yer alır.

Önemli ve kritik işlevlerin bile farklı şekilde ele alınması gerektiğini unutmamak önemlidir. İzin ve reddetme kararlarının yanı sıra, manuel ayrıcalık artırımı da yapılabilir *Kullanıcıya Sor*. AeABAC modelinin kullanışlı bir özelliği ise, basit kuralların bir tablo kullanılarak kolayca düzenlenebilmesidir. Her kritiklik seviyesi için ayrı tablolar bulunur ve her tablodaki satırlar rolleri temsil ederken, sütunlar çeşitli belirsizlik seviyelerine karşılık gelir. Benzer şekilde, işlevler de kritiklik seviyelerine göre atanabilir. Tablo kural düzenleme, politika belirtme için önemli bir kolaylık sağlar. Erişim karar kurallarının tablosal gösterimi Şekil 3.7'de, işlevlerin kritiklik seviyelerinin tablosal gösterimi Şekil 3.8'de verilmiştir.

KRİTİK FONKSİYONLAR	ADUS≤FMR10000	FMR10000<ADUS≤FMR1000	ADUS>FMR1000
Eş	İzin Ver	Kullanıcıya Sor	Reddet
Genç	İzin Ver	Kullanıcıya Sor	Reddet
Çocuk	Reddet	Reddet	Reddet
Bakıcı	Reddet	Reddet	Reddet
Misafir	Reddet	Reddet	Reddet

ÖNEMLİ FONKSİYONLAR	ADUS≤FMR10000	FMR10000<ADUS≤FMR1000	ADUS>FMR1000
Eş	İzin Ver	Kullanıcıya Sor	Reddet
Genç	İzin Ver	Kullanıcıya Sor	Reddet
Çocuk	Reddet	Reddet	Reddet
Bakıcı	İzin Ver	Kullanıcıya Sor	Reddet
Misafir	İzin Ver	Kullanıcıya Sor	Reddet

TEMEL FONKSİYONLAR	ADUS≤ FMR100
Eş	İzin Ver
Genç	İzin Ver
Çocuk	Reddet
Bakıcı	İzin Ver
Misafir	İzin Ver

Şekil 3.7: Erişim karar kurallarının tablosal gösterimi

FONKSİYON KRİTİKLİK DÜZEYİ	FONKSİYON ADI
Kritik	- Online Alışveriş - Kamera Açma Kapama
Önemli	- Açma Kapama - Yönetici Özellikleri
Temel	- Müzik Çalma - Işık Açma Kapama

Şekil 3.8: Cihaz İşlevlerinin kritiklik seviyelerinin tablosal gösterimi

3.3.5 Uygulanabilirlik

Tez kapsamında önerilen AeABAC modelinin amacı akıllı cihazların yetkilendirme sürecini doğru ve verimli hale getirmektir. AeABAC modelinin uygulanabilirliğinin değerlendirilmesi için, akıllı ev ortamında n farklı biyometrik cihazın olduğu varsayılmaktadır. Yetkilendirme kararları, kritiklik seviyeleri ve ADUS'a dayandığından, AeABAC modeli içinde Şekil 3.7'te gösterildiği gibi her kritiklik seviyesi için yalnızca bir kuralın tanımlanması yeterlidir. ADUS metriği, tüm cihazlar arasındaki belirsizlik seviyelerini normalize ettiği için her bir biyometrik kimlik doğrulama cihazı için ayrı bir kural tanımına ihtiyaç yoktur. Ancak, aynı ADUS skoru farklı AMS değerleri için her cihazda muhtemelen elde edileceğinden, AMS'ler açısından aynı etkinin istenmesi durumunda, Şekil 3.7'teki tabloların her cihaz için tekrar edilmesi gerekecektir.

Belirli bir yapılandırmada $n = 5$ farklı biyometrik cihaz olduğunu varsayılmaktadır. Şekil 3.7'te verilen kritik fonksiyonlar için aynı erişim kararlarının (ADUS terimlerinde kuralları tanımlayan) beş farklı cihaz için tekrarlanması, Şekil 3.9'te (AMS terimlerinde kuralları tanımlayan) ifade edilen senaryo için gereklidir. Her cihaz için tekrarın nedeni, beş cihaz için farklı AMS'lerde aynı ADUS'un elde edilmesidir. Örneğin, şekilden, $ADUS = FMR10000$ 'in Cihaz 1 için $AMS = 0.85$ 'te ve Cihaz 2 için $AMS = 0.6$ 'da elde edildiği görülebilir. Sonuç olarak, AeABAC kapsamlı, özlü ve etkili erişim politikaları sağlar[14].

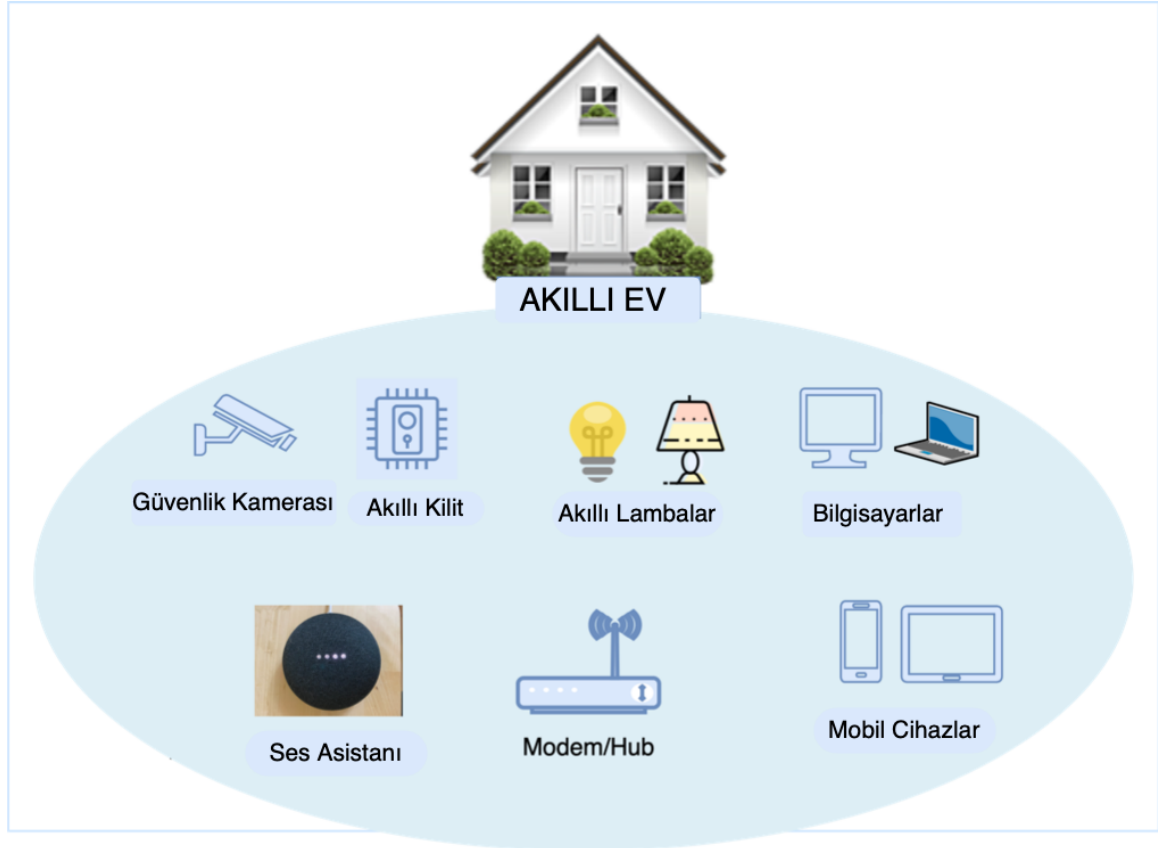
Çizelge 3.1, AeABAC modelinin temel ABAC modellerine kıyasla ne kadar özlü olduğunu göstermektedir. Özellikle, 35 kural içeren belirli bir örneğe(Şekil 3.7) ve 5 cihaz ve 175 kural içeren senaryoya (Şekil 3.9) ilişkin olarak ve genel durumda m kural ve n cihaz için durum değerlendirmesi yapılmıştır. Açıkça görülmektedir ki, AeABAC ile kural sayısı n kat daha azdır.

KRİTİK FONKSİYONLAR CİHAZ 1	AMS $\geq$ 0.85	0.85>AMS $\geq$ 0.7	AMS<0.7
Eş	İzin Ver	Kullanıcıya Sor	Reddet
Genç	İzin Ver	Kullanıcıya Sor	Reddet
Çocuk	Reddet	Reddet	Reddet
Bakıcı	Reddet	Reddet	Reddet
Misafir	Reddet	Reddet	Reddet
KRİTİK FONKSİYONLAR CİHAZ 2	AMS $\geq$ 0.6	0.6>AMS $\geq$ 0.5	AMS<0.5
Eş	İzin Ver	Kullanıcıya Sor	Reddet
Genç	İzin Ver	Kullanıcıya Sor	Reddet
Çocuk	Reddet	Reddet	Reddet
Bakıcı	Reddet	Reddet	Reddet
Misafir	Reddet	Reddet	Reddet
KRİTİK FONKSİYONLAR CİHAZ 3	AMS $\geq$ 0.4	0.4>AMS $\geq$ 0.2	AMS<0.2
Eş	İzin Ver	Kullanıcıya Sor	Reddet
Genç	İzin Ver	Kullanıcıya Sor	Reddet
Çocuk	Reddet	Reddet	Reddet
Bakıcı	Reddet	Reddet	Reddet
Misafir	Reddet	Reddet	Reddet
KRİTİK FONKSİYONLAR CİHAZ 4	AMS $\geq$ 0.7	0.7>AMS $\geq$ 0.55	AMS<0.55
Eş	İzin Ver	Kullanıcıya Sor	Reddet
Genç	İzin Ver	Kullanıcıya Sor	Reddet
Çocuk	Reddet	Reddet	Reddet
Bakıcı	Reddet	Reddet	Reddet
Misafir	Reddet	Reddet	Reddet
KRİTİK FONKSİYONLAR CİHAZ 5	AMS $\geq$ 0.5	0.5>AMS $\geq$ 0.4	AMS<0.4
Eş	İzin Ver	Kullanıcıya Sor	Reddet
Genç	İzin Ver	Kullanıcıya Sor	Reddet
Çocuk	Reddet	Reddet	Reddet
Bakıcı	Reddet	Reddet	Reddet
Misafir	Reddet	Reddet	Reddet

Şekil 3.9: AMS kullanıldığı durumda 5 farklı biyometrik cihaz için erişim kararlarının tablosal gösterimi

Çizelge 3.1: Erişim Kontrol Politikalarındaki Kural Sayısı

Cihaz Sayısı	ABAC (AMS Kullanıldığında)	AeABAC (ADUS Kullanıldığında)
5	$n \times 35 = 175$	35
n	$n \times m$	m



Şekil 3.10: Örnek Akıllı Ev Ortamı

3.4 Örnek Akıllı Ev Senaryoları ve XACML Uygulaması

Bu senaryoda küçük ev ortamında Google Home Assistant, Philips Hue Akıllı Kilit ve Xiaomi Mi Ev Güvenlik Kamerası bulunmaktadır, Şekil 3.10'de görselleştirilmiştir. Politika bileşenlerinden kullanıcı rolleri, eş, çocuk, genç, bakıcı ve misafir olarak tanımlanmıştır. Senaryolar Security Policy Tool aracı kullanılarak XACML'de uygulanmıştır. Kullanıcı, Kaynak, Ortam ve Eylemler gibi bileşenler, Şekil 3.11 ve 3.12'de

gösterildiği gibi tanımlanmıştır. ADUS seviyeleri *güçlü* ($ADUS \leq FMR10000$), *iyi* ($FMR10000 < ADUS \leq FMR1000$), *zayıf* ($FMR1000 < ADUS \leq FMR100$) ve *düşük* ($FMR100 < ADUS$) olarak belirlenmiştir. Her kritiklik seviyesi için izin ve reddetme kuralları politikaları, modülerlik açısından farklı bölümlerde ifade edilebilir (Şekil 3.13). Bu politika bileşenleri kullanılarak, kritik işlevlere yansıtılmış dört izin kuralı örneği içeren bir XACML politika belirtimi, EK-1’de verilmiştir.

3.5 AeABAC Modelinin Literatür Karşılaştırması

IoT için erişim kontrolünü geliştirmek için birkaç model önerilmiştir. Bazıları ABAC’a uzantılar sunar [57], [58], bazıları ise IoT için ABAC kullanımını önerir [23],[12], [65]. Diğer çalışmalar ise blockchain teknolojisi ile ABAC modelini birleştirerek IoT’deki hassas verilere güvenli erişimi sağlamayı önerir[4], [62]. Song vd. [62], güvenilir bir erişim kontrol modeli oluşturmak için akıllı sözleşmelerin kullanılmasını önerirken, Ag-hili vd. [4] veri bütünlüğünü korumak için yetkili şifreleme stratejisi kullanan, güvenlik seviyesi doğrulaması ve dinamik özellikleri dikkate alan MLS-ABAC (Çok Seviyeli Güvenlik ABAC) şemasını önerir. [4], güvenlik ve mahremiyeti kısmi şifre çözme öncesinde bir güvenlik seviyesi doğrulaması ekleyerek IoT sistemlerinin iyileştirilmesini amaçlar, ancak AeABAC modeli kimlik doğrulamanın güvenlik seviyesini artırır.

[16], IoT’de kenar-merkezli erişim kontrol yapısını kullanarak, verileri birçok dijital ikize bölen Tag-Based Access Control tasarımını önererek kullanır. Gölgeler içinde belirli veri alt kümelerine erişim sağlamak, verilerin belirli bir gölgedeki etiketlere bağlı olduğu için türüne göre etiket tabanlı bir erişim kontrolüdür. [31], ev içi IoT uygulamaları için ABAC’ı kullanmak için bir prototip sunar. Kullanıcıları, cihazları ve işlem özniteliklerini değerlendirerek cihaz düzeyinde politikalar tanımlarlar. AeABAC, politikaları cihazın işlevselliği düzeyinde tanımlaması açısından farklıdır.

Ayrıca, [32], akıllı ekosistemler için Activity-Centric Access Control (ACAC) mode-



Şekil 3.11: Kullanıcı, Kaynak ve Aksiyon Öz nitelikleri

lini sunar. Bir aktivite, farklı cihazların belirli bir zamanda gerçekleştirebileceği işlevler olarak tanımlanır. Bir cihaz bir veya birden fazla aktivite gerçekleştirebilir. Aktiviteler birbiriyle ilişkili olabilir veya belirli bir sırayla gerçekleştirilmeleri gerekebilir. Erişim kararlarında çevresel koşulları, yükümlülükleri ve aktivitelerin değişkenliğini değerlendirirler. Önerilen model, ince taneli işlevsellik tabanlı bir erişim kontrol modeli olarak

- ▼  **ÇEVRESEL**
 - ▼  **LOKASYON** <http://www.w3.org/2001/XMLSchema#string>
 -  At Home
 -  Outside Home
 -  Work
 - ▼  **ZAMAN** <http://www.w3.org/2001/XMLSchema#string>
 -  Morning
 -  Noon
 -  Evening
 -  Night
 - ▼  **FMR ARALIĞI** ; <http://www.w3.org/2001/XMLSchema#string>
 -  Strong FMR
 -  Good FMR
 -  Weak FMR
 -  Low FMR

Şekil 3.12: Çevresel Öznitelikler

- ▼  **Model**
 - ▼  **ABAC**
 -  ImportantPermitsPolicy: Deny-overrides & Deny Biased
 -  ImportantDeniesPolicy: Deny-overrides & Deny Biased
 -  CriticalDeniesPolicy: Deny-overrides & Deny Biased
 -  CriticalPermitsPolicy: Deny-overrides & Deny Biased
 -  BasicPermitsPolicy: Deny-overrides & Deny Biased
 -  BasicDeniesPolicy: Deny-overrides & Deny Biased

Şekil 3.13: Akıllı Ev ABAC Politikaları

düşünülebilir. Daha sonra [49]'da, Sandhu ve arkadaşları, [32]'de sunulan ACAC'nin bileşenlerini tanımlar ve diğer modellerle karşılaştırır. IoT için ince taneli bir erişim kontrol modeline ihtiyaç duyulduğunu dikkate alsa da, AeABAC modeli kullanıcı kim-

lik doğrulamasının güvence düzeyini istatistiklerden (sınırlı FMR aracılığıyla) dikkate alarak cihaz işlevselliği için ince taneli izinler veren ilk çalışma olarak gözlemlendi. [57] çalışmasında, kullanıcının güvenilirliği göz önünde bulundurulur, ancak bu, davranış anormallik teknikleri aracılığıyla hesaplanır. Benzer şekilde, [58] çalışmasında, kullanıcıyla ilişkilendirilen riskin olasılığını elde etmek için bazı makine öğrenimi teknikleri kullanılır. Makine öğrenimi yaklaşımı büyük girişim günlüklerine dayandığı için soğuk başlangıçlı değildir. AeABAC modeli, kullanıcı kimlik doğrulamasının güvence düzeyini istatistiksel bir bakış açısıyla (sınırlı FMR aracılığıyla) dikkate alan ve buna göre cihaz işlevselliği için ince taneli izinler veren ilk çalışmadır [14]. IoT’de işlevsellik odaklı erişim kontrolüne olan ihtiyaç belirgin olsa da, bugüne kadar yeterince dikkat edilmemiştir. Bazı çalışmalar, IoT erişim kontrolünde işlevsellik odaklı bir yaklaşımın önemini belirtir [43], [34]. [34], bir akıllı evde kimlik doğrulamanın cihaz başına tek bir kullanıcıya dayandığı bir boşluğa dikkat çeker. Kullanıcı çalışması gerçekleştirerek, akıllı ev kullanıcılarının tek bir cihazın farklı işlevleri için farklı erişim kontrol politikalarını tercih ettiğini bulmuşlardır. Ayrıca, kullanıcının konumu, hava durumu ve zaman gibi koşullar altında hangi işlevi kullandığını da dikkate alırlar. Ne yazık ki, [34], bu yaklaşımı herhangi bir erişim kontrol modeliyle ilişkilendirmez. [74], [34] ve diğer çalışmalarda belirtilen çoklu kullanıcı akıllı evlerin güvenlik ve mahremiyet ihtiyaçlarını ele alarak akıllı ev uygulaması tasarlar. Yaklaşımları rol tabanlı, konum tabanlı, denetleyici ve reaktif erişim kontrollerini içerse de, kullanıcının gerçek kimliğinin belirsizliğini kimlik doğrulaması sırasında dikkate almazlar.

Özetle, Çizelge 3.2, tez kapsamında önerilen AeABAC’ı literatür içinde konumlandırır ve diğer çalışmalarla beş boyutta karşılaştırır: Kullanıcı Kimlik Doğrulama Güvence Düzeyi, Soğuk Başlangıç (yani, kullanıcının kimliğinin belirsizliğinin değerlendirilmesinin büyük girişim günlükleri gerektirip gerektirmediği), İşlevsellik Odaklı, İşlevsellik Kategorizasyonu ve Sınırlı FMR [14].

Çizelge 3.2: AeABAC Modelinin Literatür İçinde Konumlandırılması

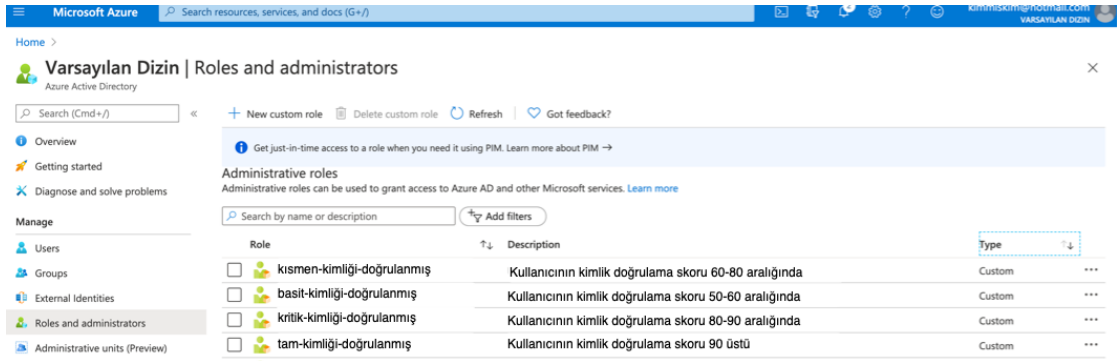
Kaynak	Erişim Kontrol Modeli	Güvence Düzeyi	Soğuk Başlangıç	İşlevsellik Odaklı	İşlevsellik Kategorizasyonu	Sınırlı FMR
[57]	ABAC	Evet	Hayır	Hayır	Hayır	Hayır
[58]	Adaptif Risk Odaklı ABAC	Evet	Hayır	Hayır	Hayır	Hayır
[32]	Aktivite Odaklı Erişim Kontrolü	Hayır	GD	Evet	Kısmi	Hayır
[43]	İşlevsellik Odaklı Erişim Kontrolü	Hayır	GD	Evet	Hayır	Hayır
[34]	GD	Hayır	GD	Evet	Kısmi	Hayır
[49]	Aktivite Odaklı Erişim Kontrolü	Hayır	GD	Evet	Kısmi	Hayır
[74]	ABAC	Hayır	GD	Hayır	Hayır	Hayır
[16]	Etiket Tabanlı Erişim Kontrolü	Hayır	GD	Hayır	Hayır	Hayır
[31]	ABAC	Hayır	GD	Hayır	Hayır	Hayır
[62]	ABAC	Hayır	GD	Hayır	Hayır	Hayır
[4]	Çok Düzeyli Güvenlik ABAC (MLS-ABAC)	Hayır	GD	Hayır	Hayır	Hayır
AeABAC	AeABAC	Evet	Evet	Evet	Evet	Evet

3.6 Mevcut IoT Çerçevelerine Modelimizi Uyarlama Çalışmaları

Bu bölümde 2. bölümde genişletilen ABAC modelinin Azure IoT çerçevesine uyarlanabilirliği ile AeABAC modelinin ThingsBoard Platformuna uyarlanabilirliği incelenecektir.

3.6.1 Azure IoT

Azure IoT platformu, erişim kontrolü yönetimi için Azure Active Directory’i kullanmaktadır. RBAC’den faydalanması yönetim kolaylığı sağlamaktadır. Rollerin erişim izinleri IoT cihazlarına atanır. Birçok yerleşik rol bulunur ve ayrıca özel roller oluşturulabilir. Senaryoları uygulamak için, 2.6 bölümünde tanımlanan her eşik değerine karşılık gelen özel roller oluşturulmuştur. Bu rollerin hangi işlemleri gerçekleştirebileceği, bu roller için izinleri detaylı olarak atayarak belirlenmiştir. Örneğin, kimlik doğrulama puanı 90 ve üzerinde olan bir kullanıcı tam yetkilendirilmiş bir role sahip olacaktır. Kullanıcı, istenen kaynak üzerinde tüm eylemleri gerçekleştirebilir. Kimlik doğrulama puanı 95 olan bir kullanıcı tam yetkilendirilmiş bir role atanacak ve istenen kaynak için oluşturma, güncelleme, okuma ve silme izinlerine sahip olacaktır. Kimlik doğrulama puanı 55 olan bir kullanıcıya basit yetkilendirilmiş bir rol atanacak ve istenen kaynak



Şekil 3.14: Azure Platform’unda Özel Tanımlanmış Roller

için sınırlı okuma izinlerine sahip olacaktır. Azure IoT üzerinde oluşturulan roller ve yetkileri Şekil 3.14 ve 3.15’de gösterilmiştir.

Azure IoT’da izinlerin cihaz başına değil, cihaz işlevlerine göre atanabileceği mümkün görünmektedir. Daha ayrıntılı bir erişim kontrolü oluşturabilmek için, işlev seviyesinde izin atamasına ihtiyaç vardır. Azure IoT çerçevesi bu açıdan genişletilebilir. Ayrıca, RBAC temelli olması nedeniyle öznetelikleri desteklemez. Bu sebeple dinamik erişim kararlarını desteklemesi kolay olmayacaktır. Bu nedenle, cihaz işlevleri ve özellikleri göz önünde bulundurarak detaylı bir erişim kontrol modülü ekleyerek Azure IoT çerçevesi genişletilebilir.

3.6.2 ThingsBoard

AeABAC modelindeki senaryoları uygulamak için açık kaynaklı IoT çerçevesi olan ThingsBoard Cloud Platformu kullanılmıştır. Bu platformu akıllı ev platformu olarak kullanmak için kullanıcılar, kullanıcı rolleri, cihazlar, cihaz işlev kritiklik seviyeleri ve kullanıcı yetkileri tanımlanmıştır. Bu ortamda tanımlanabilecek bileşenler ile eş, yetişkin, çocuk, bebek bakıcısı rolleri ve yetkilendirmeleri için birkaç örnek EK 2’de verilmiştir. Akıllı lamba, akıllı kapı, Google ses asistanı cihazlarının işlevleri ve bu işlevlerin kritiklik seviyeleri (Temel, Önemli, Kritik ve Yönetimsel) olarak tanımlanmıştır. ThingsBoard Platformunda detaylı yetkilendirme kullanıcı rolü için tanımlanan

gösterge panelinde yapılmaktadır. Bu senaryoda Eş rolündeki kullanıcının bütün cihaz işlevlerine, bebek bakıcısının önemli ve temel işlevlere, çocukların temel işlevlere eriştiğini gösteren ilgili gösterge panelleri Ek 2'deki şekillerde gösterilmiştir. Her ne kadar incelenen çerçeveler arasında AeABAC modeline en uyumlu olanı ThingsBoards Platformu olsa da ADUS skorunun birebir kullanımı mümkün olmadığı için modelin tüm ihtiyaçlarını karşılayamamıştır.



4. RİSK TABANLI MAHREMİYET YAKLAŞIMI İLE AeABAC (RBP-AeABAC) MODELİ

Bu bölümde önceki bölümde önerilen AeABAC modelinde mahremiyet konularının erişim kararlarıyla nasıl ilişkilendirilebileceği araştırılmıştır. Tez kapsamında geliştirilen AeABAC modeli için Risk Temelli Mahremiyet Yaklaşımı (RBP-AeABAC) model önerimiz sunulmaktadır.

Sensörler, cihazlar ve kullanıcılar gibi bileşenlerden oluşan akıllı ev ekosistemi, işlevlerini yerine getirebilmek için genellikle veri toplamak, işlemek ve depolamak zorundadır. Bu veriler, kişisel kimlik bilgileri, hassas kişisel veriler, davranış kalıpları, ses kayıtları, kamera görüntüleri, kapı kontrol komutları ve daha fazlasını içerebilir. Akıllı ev mahremiyeti ve güvenliğinin önemli bir yönü, bu hassas verilerin nasıl işlendiği ve depolandığıdır [77]. Geçmişte siber saldırılar, genellikle sistem hasarları ve hizmet kesintilerine odaklanmıştır. Ancak, yeni saldırı türleri, hem teknolojik hem de insani zafiyetlerden yararlanarak yasa dışı veya dolaylı yollardan veri toplama ve kullanma amacını taşımaktadır. Nesnelerin İnterneti (IoT) teknolojisi ilerledikçe, kişisel veri mahremiyetine yönelik tehditler hızla artmaktadır. Bu nedenle, akıllı cihazlardaki kişisel verilerin güvenliğini ve mahremiyetini sağlamak hem bir zorluk hem de bir sorumluluk haline gelmiştir.

ABD Federal Ticaret Komisyonu (FTC) ve Adalet Bakanlığı (DOJ), kısa bir süre önce Amazon'u Çocukların Çevrimiçi Mahremiyetini Koruma Yasası (COPPA) Kuralı'nı ihlal etmekle ve Alexa sesli asistan hizmeti kullanıcılarını veri silme yöntemleri konusunda yanıltmakla suçladı. Amazon'un çocukların verilerini ve coğrafi konum bilgilerini iç amaçlar için tutarak mahremiyet yasalarını ihlal ettiği iddia edilmektedir [20]. Haney ve arkadaşlarının çalışması [33], akıllı ev kullanıcıları tarafından dile getirilen birçok mahremiyet sorununu özetlemektedir. Bu endişeler, kullanıcı profilleri oluşturma, verilerin ticarileştirilmesi ve bildirilmeden veri toplanması gibi konuları içermektedir. Kullanıcılar özellikle evlerinden ayrıldıklarında günlük aktivitelerinin üçüncü şahıslara

ifşa edilmesi ve kişisel bilgilerinin pazarlama amacıyla satılması konusunda endişe duymaktadır [76]. Ayrıca, kendilerine sunulan bilgilerin doğruluğu konusundaki tutarsızlıklar nedeniyle veri toplama süreci de insanlar için bir endişe kaynağıdır.

Akıllı ev ekosisteminde güvenlik genellikle kullanıcıların ve/veya rollerin kimlik doğrulama ve yetkilendirilmesi yoluyla sağlanır. "Sistemden kullanıcıya güven", sistemin yalnızca yetkilendirilmiş kullanıcılara hizmetlerini sunmasını sağlamak için gereklidir. Ancak bu tez kapsamında, sistemin aynı zamanda "kullanıcıdan sisteme güven" sağlamak zorunda olduğunu, böylece kullanıcıların mahremiyet endişelerini hafifletmek gerektiği savunulur. Bu husus birçok yetkilendirilmiş hizmet, ilgili işlevi yerine getirmek için hassas verilere ihtiyaç duyduğu için önemlidir (örneğin, alışveriş yaparken kredi kartı bilgileri). Sonuç olarak, kimlik doğrulama ve yetkilendirmeye ek olarak, ekosistem her sunulan hizmet için veri mahremiyetini korumasına yönelik kullanıcı güveni sunmalıdır. Ayrıca, güven değerlendirmesi, kullanıcının mahremiyet profiline göre kişiselleştirilmelidir. Çift yönlü güven sağlamak amacıyla bu çalışma, kullanıcı mahremiyetini koruması için AeABAC modelini mahremiyet yaklaşımını da ekleyerek genişletmiştir. Kullanıcıların, mahremiyet profillerini belirtmelerine olanak tanımaktadır ve bu profiller, veri ifşası olasılığı ve ifşa etkisi üzerinden risk temelli güven değerlendirmeleri için kullanılacaktır. Ayrıca, bazen istenen işlevin farklı hizmetler (örneğin, çekle ödeme veya kredi kartı ile ödeme) aracılığıyla da gerçekleştirilebileceği ve bu hizmetlerin farklı setlerde hassas veriler gerektirdiği belirtilmektedir. Sonuç olarak, eşdeğer hizmetlerin mahremiyet koruması açısından güvenliğini bilen kullanıcı, ilgili değerlendirmeleri karşılaştırarak bilinçli bir seçim yapabilir.

Bu bölümde, akıllı evlerdeki mahremiyet endişelerine odaklanarak, literatürdeki ilgili çalışmalar sunulmaktadır. Daha sonra, akıllı evlerde kullanıcıların ve üreticilerin bakış açısından mahremiyet ele alınmakta ve politika standartları tartışılmaktadır. Akıllı ev ortamlarındaki mevcut mahremiyet politikalarının durumu incelenmektedir. Tez kapsamında geliştirilen AeABAC modeli için Risk Temelli Mahremiyet Yaklaşımı (RBP-

AeABAC) model önerimiz sunulmaktadır. İlk olarak, AeABAC modelinin "kullanıcıdan sisteme güven" ilkesini de ele alacak şekilde nasıl zenginleştirilebileceği açıklanmaktadır. Ardından, mahremiyet profilleri ve politikalarına olan ihtiyacı vurgulayan bu yaklaşım, ifşa olasılığı ve ifşa etkisinin nasıl değerlendirileceğini açıklamaktadır. Kullanıcı mahremiyet risk değerlendirmesi yöntemimiz, iki anket veri seti üzerinde sunulmaktadır. Daha sonra örnek bir akıllı ev ekosisteminde kullanıcı mahremiyet risk değerlendirmesini göstermek için iki senaryo sunulmaktadır.

4.1 Literatür Taraması

Güvenlik ve mahremiyet, özellikle görüntü işleyen cihazlar, örneğin akıllı güvenlik kameraları ve ses tanıma yazılımları, örneğin sesli asistanlar söz konusu olduğunda, büyük endişe kaynağıdır. Emami ve arkadaşlarının çalışması [27], kullanıcıların güvenlik ve mahremiyetle ilgili endişelerinin genellikle kullandıkları cihaz türüyle bağlantılı olduğunu göstermiştir. Çalışma ayrıca, teknik bilgiye sahip kullanıcıların güvenlikle ilgili sorunları daha iyi çözebildiğini ve cihaz kutularına besin ve enerji verimliliği etiketlerine benzer şekilde güvenlik ve mahremiyet etiketleri yerleştirilmesini önererek, kullanıcıların cihaz satın almadan önce mahremiyet risklerini değerlendirmelerine yardımcı olmayı amaçlamıştır.

Birçok çalışma, akıllı evlerde mahremiyeti sağlamaya yönelik stratejiler önermiştir. Kullanıcılar, genellikle karmaşık güvenlik sistemlerinde mahremiyetlerini korumakta zorlanmaktadır [17]. Kullanıcılar, mahremiyetlerinin yetersiz politika kararları veya beklenmeyen hatalar nedeniyle risk altında olduğunu düşünürken, üreticiler de bu sorumluluğun büyük bir kısmını taşımaktadır [17]. Teknik bilgiye sahip kullanıcılar, verilerini daha iyi koruyarak daha güvenli bir akıllı ev ortamı oluşturabilirler. Teknik bilgiye sahip olmayan kullanıcıların da mahremiyetlerini koruyabilmesi ve verilerinin kullanımı ve paylaşımı konusunda bilinçli onay verebilmeleri için kullanıcı mahremiyet farkındalığı, akıllı ev tasarımına entegre edilmelidir [27]. Bazı durumlarda, mahremiyet endişeleri

hane içinde de çatışmalara yol açabilir. Birçok yaşlı birey, yaşam kalitelerini artıracasına inandıkları ve acil bir durumda aile üyelerine haber verebilecekleri için akıllı ev teknolojilerini kullanmaya isteklidir. Aynı zamanda aile üyeleri, onları izlemek ve gerektiğinde yardım etmek isterler. Ancak yaşlı kullanıcılar, acil durumlar dışında aile üyeleri tarafından izlenmekten rahatsız olabilirler [44]. Li ve arkadaşları [44], canlı video akışları yerine görselleştirmeler aracılığıyla hassas verilerin aile üyeleriyle paylaşılmasını sağlayarak mahremiyet sorunlarını azaltmaya yardımcı olan iFloor sanallaştırma teknolojisini tanıtmıştır.

Vetrivel ve arkadaşları [68], akıllı ev cihazlarına yönelik güvenlik ve mahremiyet konusunda müşteri farkındalığını analiz etmiştir. Çalışma, cihazlarla ilgili geri bildirimin ticari olmayan, güvenilir kaynaklardan, örneğin müşteri yorumlarından alınmasının öneme dikkat çekmiştir. Müşteri yorumlarına dayalı bir mahremiyet derecelendirme sistemi oluşturmayı önererek, üreticilerin öznel değerlendirmelerine kıyasla daha gerçekçi bir değerlendirme sunmayı amaçlamışlardır. Bu şekilde, mahremiyet etiketleri gibi öznel çözümler yerine daha nesnel çözümler sunmayı hedeflemişlerdir [27]. Çalışma, güvenlik ve mahremiyet sorunlarının teknik ve teknik olmayan terimlerle düzenli olarak ele alındığını belirlemiş ve Amazon'un altı İngilizce konuşan ülkesindeki sitelerinde 83.686 yorumu analiz etmiştir. Yaklaşık %10'luk bir kesim güvenlik ve mahremiyet endişelerini dile getirmiştir. Bir mahremiyet derecelendirme sistemi, kullanıcıların cihaz satın alma kararlarını bilinçli bir şekilde vermelerini sağlayarak kullanıcıdan sisteme güvenin oluşturulmasına yardımcı olabilir.

Kelley ve arkadaşları [39], akıllı telefon uygulamalarındaki mahremiyetle ilgili hususları incelemiş ve kullanıcıların, bu uygulamaların önemli miktarda kişisel bilgiye erişmesine rağmen, uygulama indirirken genellikle mahremiyet konusunu dikkate almadıklarını gözlemlemiştir. Çalışma, kullanıcıların mahremiyet farkındalığını artırmak amacıyla uygulama indirme sırasında "Mahremiyet Bilgilerinin basit bir ekranda" gösterilmesini önermiştir. Araştırma, uygulama indirirken net bir mahremiyet bildirimi sunma-

nın, kullanıcıların mahremiyetlerini daha iyi anlamalarına, yönetmelerine ve önceliklendirmelerine yardımcı olduğunu sonucuna varmıştır. Mahremiyet yönetiminin bir diğer yönü de, kullanıcılardan izin isteme sıklığının doğru şekilde belirlenmesidir. Malkin ve arkadaşları [47], izinlerin ne sıklıkla istenmesi gerektiğini incelemiştir. Kullanıcılardan sürekli izin istenmesi durumunda, kullanıcılar rahatsız olabilir. Ancak, nadiren yapılan istekler mahremiyet riskleri doğurabilir. Bu çalışma, kullanıcı davranışına dayalı olarak izin isteklerini dinamik bir şekilde ayarlayan öğrenme tabanlı bir izin sıklığı tekniği önermiştir. Çalışma, kullanıcı kontrolü ve rahatlığı arasında denge sağlayarak kullanıcı dostu bir deneyim sunmayı, kullanıcıdan sisteme güveni korumayı ve kullanıcıların rahatsız olmasını en aza indirmeyi hedeflemektedir [47].

He ve arkadaşları [35], IoT cihazlarıyla kullanıcı etkileşimlerini inceleyerek mahremiyet riskleri ve tercihleri hakkında geri bildirim topladı ve etkin mahremiyet kararları alınmasını teşvik etti. Kullanıcıların kapsamlı mahremiyet ayarlarına ulaşmakta zorlandıklarını ve bu ayarların cihaz arayüzlerinde gizlendiğini buldular. Buna çözüm olarak, GDPR'da yer alan beş bağlamsal parametreye dayanan [1], 'mahremiyet profilleri' önerdiler. Bu parametreler, verilerin nerede depolandığı, hangi kişisel verilerin aktarılacağı, kimlerin bu verilere erişeceği ve neden, verilerin ne kadar süreyle saklanacağı gibi unsurları içerir [42]. Kullanıcılar, bu profilleri seçerek belirli mahremiyet tercihlerini ifade edebilirler [35]. Bu çalışma, kullanıcıdan sisteme güvene katkıda bulunsa da, cihaz ve veri türlerine göre özelleştirilemeyen yüksek seviyede mahremiyet profilleri sunmaktadır.

Alrawi ve arkadaşları [5], IoT cihazlarının güvenlik ve mahremiyetini değerlendirmek için "YourThings" adlı halka açık bir veri seti sunmuştur. Bu veri seti, çeşitli ev tabanlı IoT cihazları kullanılarak binlerce araştırma saati sonucunda oluşturulmuştur. Her IoT cihazı, cihaz, mobil, bulut ve ağ güvenliği açısından puanlanmıştır. Bu nedenle veri seti, kullanıcıların cihaz güvenliği ve mahremiyet risklerini sistematik olarak değerlendirmelerine olanak tanımaktadır. Bu da, cihazların güvenliğini değerlendirerek kullanıcıdan

sisteme güvenin inşa edilmesine katkıda bulunur. Bir başka çalışma [66], IoT mimarisinin uygulama, süreç, taşıma ve algılama katmanlarında mahremiyet ve güvenlik koruma çerçevesi sunmaktadır. IoT mahremiyet güvenli hizmet tanımlarında, blockchain, yapay zeka, mahremiyet koruma mevzuatı, erişim kontrolü, iletişim güvenlik protokolü ve donanım yazılımı güvenliği teknolojilerini ele almaktadır.

Yassine ve arkadaşları [70], IoT güvenlik risk değerlendirme metodolojilerini tehdit olasılığı, zafiyet ve etki değerlendirmesi olmak üzere üç ana bileşen etrafında yapılandırarak bir sınıflandırma sunmuştur. Bu bileşenler, ISO, NIST [30], OCTAVE ve OWASP gibi risk temelli çerçevelerle uyumludur, ancak özellikle mahremiyeti ele almamaktadırlar. Bu güvenlik risk değerlendirme çerçevelerinin akıllı evlerde uygulanması, akıllı cihazlardaki mahremiyet risklerini değerlendirerek kullanıcıdan sisteme güvenin daha da geliştirilmesine yardımcı olacaktır.

4.2 Akıllı Ev Ekosisteminde Mahremiyet

Bu bölümde, akıllı evlerde mahremiyet farklı açılardan ele alınmaktadır: kullanıcıların bakış açısı, cihaz üreticilerinin bakış açısı, mahremiyet normları ve mahremiyet standartları/politikaları bakış açısı. Bu perspektifler, RBP-AeABAC modeline yönelik geliştirdiğimiz ortak güvenlik ve mahremiyet önerimizin temelini oluşturmuştur.

4.2.1 Kullanıcıların perspektifinden mahremiyet

Akıllı cihazlarla ilgili mahremiyet endişeleri, kullanıcıların bu cihazları günlük hayatlarına dahil etmesine engel teşkil edebilir. Akıllı evlerin sunduğu birçok faydalı uygulama ve cazip özelliklere rağmen, kullanıcı taleplerini tam anlamıyla karşılayamamaktadırlar. Yüksek maliyetler ve uzun cihaz yenileme döngüleri, geniş çaplı benimsenme önündeki olası engeller arasında yer almaktadır [61]. Akıllı ev cihazları tarafından toplanan verilerle ilgili mahremiyet ve güvenlik sorunları, kullanıcıların en büyük endişelerin-

den biridir [73]. Kullanıcılar, hangi verilerin işleneceği, verilerin nasıl ve neden işleneceği, kimlerin bu verilere erişeceği, verilerin ne kadar süreyle saklanacağı ve verilerin işlenme nedenleri hakkında net ve açık bilgilere sahip olmayı beklerler. Kullanıcılara bu şeffaflığın sağlanması, veri toplamanın yararlarını daha iyi anlamalarını sağlayarak mahremiyet endişelerini hafifletmek ve böylece akıllı ev teknolojilerine güven ve uyum geliştirmek açısından kritik öneme sahiptir [61].

Kullanıcıların, farklı akıllı ev teknolojilerine karşı asimetrik kabul düzeyleri bulunmaktadır. Zimmermann ve arkadaşları [77], kullanıcıların akıllı ev teknolojileri ve bu teknolojilerle ilgili mahremiyet ve güvenlik unsurlarına yönelik görüşlerini toplamak amacıyla bir anket çalışması gerçekleştirmiştir. Araştırmacılar, kullanıcı yanıtlarına dayanarak, elektrik sayaçları, fitness takip cihazları, termostatlar, buzdolapları, güvenlik kameraları ve kapı kilitleri gibi çeşitli akıllı cihazları değerlendirmiş ve mahremiyet kabul edilebilirlik puanlarını hesaplamışlardır. Sonuçlar, fitness takip cihazları ve akıllı termostatlar (örneğin Nest) gibi cihazların daha düşük olumsuz kabul edilebilirlik puanlarına sahip olduğunu ve kullanıcıların bu cihazlardan veri paylaşımına daha fazla rahatlıkla yaklaştığını göstermiştir. Buna karşın, güvenlik kameraları ve kapı kilitleri gibi cihazlar, mahremiyetle ilgili daha yüksek olumsuz kabul puanları sergilemiş ve kullanıcıların bu teknolojilerin mahremiyet üzerindeki etkileri konusunda daha fazla endişe duyduklarını ortaya koymuştur.

Şeffaflık, kullanıcıların IoT ve akıllı ev teknolojilerini benimsemelerinde en önemli endişelerden biridir. IoT teknolojisinin hızlı büyümesiyle ilgili mahremiyet endişelerini ele almak adına şeffaflık ve kullanıcı kontrolünün önemine vurgu yapan Naeini ve arkadaşlarının [51] çalışması, giyilebilir cihazlar, akıllı kameralar ve kişisel veriler toplayıp işleyen bağlantılı araçlar gibi çok sayıda IoT bağlantılı cihazın bulunduğu ortamlarda tüketici mahremiyeti algılarını anlamaya odaklanmıştır. Çeşitli IoT senaryolarında, 1.000'in üzerinde katılımcıdan veri toplayarak, veri toplama, bilgi paylaşımı ve korunması konularında nasıl hissettiklerini incelemişlerdir. Bu çalışma, IoT mahre-

mahremiyetinin zorluklarına dikkat çekmiş ve birden fazla veri toplama noktası ve birbirine bağlı cihazlar arasında potansiyel bilgi paylaşımını vurgulamıştır. Sonuçlar, mahremiyet tercihlerinin bağlama göre büyük ölçüde farklılık gösterdiğini ortaya koymuştur. Katılımcılar genel olarak, kamu kurumları tarafından veri toplanmasına, özel kurumlara göre daha fazla rahatlıkla yaklaşmış ve doğrudan fayda sağladığında veri toplama işlemine daha olumlu bakmışlardır. Örneğin, parmak izi gibi biyometrik veri toplama işlemi, oda sıcaklığı veya fiziksel varlık gibi çevresel verilere kıyasla daha fazla mahremiyet endişesi yaratmıştır [51].

Mahremiyet endişeleri, kullanıcının rolü ve profiline göre de değişiklik gösterebilir. Örneğin, bakıcılar, akıllı gözetim sistemlerinin bulunduğu bir evde mahremiyetleri konusunda endişelenebilirler. Bazı bakıcılar sürekli izlenmekten ve kaydedilmekten rahatsız olabilirken, diğerleri güvenliği sağlamak ve sorumluluğu yerine getirmek açısından bu durumu değerli bulabilir ve evde sadece belirlenmiş özel alanlar talep edebilirler [11]. Benzer şekilde, gençler daha yüksek mahremiyet beklentilerine sahip olabilir ve mahremiyet standartları ev halkı üyeleri ile dışarıdan gelenler arasında farklılık göstermelidir [18]. Kirchbuchner ve arkadaşları [40], yaşlı bireylerin akıllı evlere nasıl baktığını araştırmıştır. Araştırma, veri paylaşımı konusundaki mahremiyet endişelerinin, verilerin alıcılarıyla ve cihazların kamera tabanlı olup olmamasıyla bağlantılı olduğunu ortaya koymuştur. Yaşlılar, sağlıkla ilgili durumlarda akıllı ev teknolojilerinin sağladığı güvenlik ve kolaylık avantajlarını kabul etmekle birlikte, ticari hizmet sağlayıcılarla veri paylaşmaktan ve kamera donanımlı cihazlarla izlenmekten rahatsız olduklarını belirtmişlerdir. Bu çalışma, kamera tabanlı çözümlerle ilgili mahremiyet endişelerinin, giyilebilir acil durum cihazlarına göre önemli ölçüde daha fazla olduğunu göstermiştir ve bu durum, akıllı sistemlerin "kullanıcıdan sisteme güven" oluşturma gerekliliğini daha da vurgulamaktadır.

Özetle, bu çalışmalar, kullanıcıların mahremiyetle ilgili endişelerini ortaya koymakta ve kullanıcıların IoT teknolojisinin sunduğu rahatlık ve avantajlar karşılığında bir mik-

tar mahremiyetten feragat etmeye istekli olabileceklerini göstermektedir. Ancak yine de verilerinin nasıl işlendiğini, kimlerin bu verilere erişeceğini ve verilerin nasıl korunup saklanacağını bilmek istemektedirler. Bu nedenle, RBP-AeABAC modeli, kullanıcıların mahremiyet endişelerini ele alarak "kullanıcıdan sisteme güven" oluşturmakta ve bunu, kullanıcı beklentilerini karşılayan şeffaf ve kolay erişilebilir mahremiyet politikaları sunarak başarmaktadır.

4.2.2 Üreticilerin perspektifinden mahremiyet

Üreticiler için, akıllı cihazlarda sadece kullanıcı kimlik doğrulama ve yetkilendirme uygulamak değil, aynı zamanda kullanıcı mahremiyeti endişelerini de ele almak, kullanıcılar ve cihazlar arasında çift yönlü güven inşa etmek için esastır. Kullanıcılar, bilgilerin rızaları olmadan işlendiği konusunda endişelenmemeli veya güvensiz hissetmemelidir. Akıllı ev teknolojisi geliştiricileri, mahremiyet endişelerini ele almak için güvenlik standartlarını ve en iyi uygulamaları takip etmelidir. Kullanıcılar, akıllı ev teknolojilerini hayatlarına dahil etmek isterken, aynı zamanda güvenlik ve mahremiyetlerinin de sağlandığından emin olmak isterler. Ayrıca, kullanılabilirlikten ödün vermek istemezler [38].

[51] tarafından gerçekleştirilen bir ankette, katılımcıların yaklaşık yarısı mahremiyetlerini korurken akıllı cihazlarını uzaktan kontrol etme arzusunu dile getirmiştir. Sonuç olarak, akıllı ev cihazı geliştiricilerinin, kullanıcıların teknolojik ve mahremiyet beklentilerini karşılaması gerekmektedir. Geliştiricilerin, veri paylaşımını kısıtlaması ve harici etkileşimleri en aza indirmesi önemlidir. Kullanıcıların bilgilerini üçüncü taraflarla nasıl paylaşacaklarını ve işleyeceklerini kontrol etmelerine izin vermek, mahremiyet haklarını korumak açısından kritik öneme sahiptir [51]. Singh ve arkadaşları tarafından yapılan başka bir ankette [61], yaşlı bireyler, bağımsızlıklarını artırmak, güvenliklerini sağlamak ve yaşam kalitelerini yükseltmek amacıyla akıllı ev teknolojilerine ilgi duymaktadır. Ancak bazı katılımcılar, yetersiz mahremiyet koruması ile ilgili endişelerini dile

getirmiştir. Bu nedenle, kullanıcılara net ve açık mahremiyet politikaları, standartları, veri güvenliği ve mahremiyet yönergelerinin sunulması çok önemlidir. Emami-Naeini ve arkadaşları tarafından gerçekleştirilen başka bir anket [27], insanların IoT cihazlarını satın aldıktan sonra mahremiyeti düşünmeye başladıklarını göstermiştir. Cihazın net ve yeterli bir mahremiyet politikasına sahip olması durumunda kullanıcılar bir nebze rahatlamış hissedebilir; aksi takdirde, cihazı satın aldıktan sonra bile kullanmaktan rahatsız olabilirler.

Cihaz üreticilerinin, bilgi akışlarını mahremiyet gereksinimlerine ve kullanıcı beklentilerine göre değerlendirmeleri tavsiye edilmektedir. Sesli asistanlar, akıllı televizyonlar ve akıllı oyuncaklar gibi cihazlarla ilgili geçmişte yaşanan mahremiyet ihlalleri, proaktif mahremiyet önlemlerinin gerekliliğini kanıtlamıştır. Güvenli tasarım süreci, gereksinimler aşamasında başlamalı, müşteri ihtiyaçları ve mahremiyet hakları dikkate alınarak güvenli ve mahremiyet odaklı akıllı sistemler oluşturulmalıdır [26]. Manandhar ve arkadaşlarının çalışması [48], akıllı ev cihazları için mevcut mahremiyet politikalarının durumunu araştırmış ve bu politikaların hangi verilerin toplandığını, paylaşıldığını ve işlendiğini ne kadar net açıkladığını incelemiştir. Özellikle üçüncü taraf veri paylaşımıyla ilgili mahremiyet endişeleri, kullanıcıların özel aktivitelerini veya hassas bilgilerini içerebileceği için akıllı ev cihazlarının benimsenmesini yavaşlatmıştır. Bu nedenle, satıcılar veri akışlarının kullanıcı mahremiyetini tehdit edebileceği durumlarda şeffaf olmalı ve gerekli önlemleri almalıdır [48].

Kullanıcı segmentasyonu, akıllı ev cihazlarının geliştirilmesinde önemli bir rol oynar. Barbosa ve arkadaşları [10], akıllı ev tüketicilerini, akıllı ev ortamında önceliklerine göre üç gruba ayırmıştır. İlk grup, uygun fiyatlı cihazlara odaklanırken, ikinci grup mahremiyeti tercih etmiş, üçüncü grup ise güvenilir ve etkili ürünler aramıştır. Bu farklı grupların tercihlerine hitap ederek, satıcılar ürün ve hizmetlerini müşterilerinin çıkarlarına daha iyi uyacak şekilde özelleştirebilir [10].

Anketler, "kullanıcıdan sisteme güven" oluşturma sürecinde, üreticilerin tüketicilerin

mahremiyet endişelerini hafifletme ve akıllı ev teknolojisinin daha geniş kullanımını teşvik etme sorumluluğu taşıdığını öne sürmektedir. Uzun vadeli güven oluşturmak için kullanıcı mahremiyetine proaktif bir yaklaşım gereklidir; buna şeffaf politikalar ve veri akışları üzerinde kullanıcı kontrolü de dahildir. RBP-AeABAC modeli, "kullanıcıdan sisteme güven" oluşturma sürecinin bir parçası olarak anket verilerini kullanmaktadır.

4.2.3 Mahremiyet normları

Çok sayıda cihaz, üreticilerin işlettiği bulut sunucularına sensör kayıtları ve kullanıcı etkileşimlerini doğrudan iletir. Genellikle, üreticiler tüketicilere mahremiyet politikaları ve son kullanıcı lisans anlaşmaları sunarlar; ancak, bu politikalar geniş kabul gören mahremiyet normlarıyla uyumlu olmayabilir [8]. Tüketicilerin mahremiyet endişelerini azaltmak için cihaz üreticileri, bir cihazın yalnızca acil durum gibi gerekli veri aktarımı durumlarında belirli bilgileri ilettiğini mahremiyet politikalarında açıkça belirtebilirler [48].

Akıllı ev IoT cihazlarının kişisel veri toplama ve paylaşma şekilleri ve kullanıcıların bu cihazların ev ortamlarındaki mahremiyetle ilgili etkilerini nasıl algıladıkları değerlendirilmektedir [8]. Akıllı evlerin hızla yaygınlaştığı bir ortamda mahremiyet normlarının nasıl belirlendiği ve algılandığı önemlidir. Bağlamsal Bütünlük (Contextual Integrity, CI) teorisi, mahremiyet normlarının verilerin toplandığı ve kullanıldığı bağlama bağlı olarak değişebileceğini vurgular. Bu durumda, bağlam, akıllı evlerin özel ortamını ve kullanıcılar ile bu cihazlar arasındaki etkileşimlerini ifade eder.

Mahremiyet normları, akıllı evlerde belirlenir ve kullanıcıların bu ortamdaki veri mahremiyeti hakkındaki algılarını ve davranışlarını etkileyen faktörleri açıklar. Bu mahremiyet normlarını anlamak, cihaz üreticileri, tasarımcılar ve araştırmacıların mahremiyet bilincine sahip ve kullanıcı odaklı IoT cihazlarını ve hizmetlerini geliştirmeleri için önemlidir. Bu çalışma [8], akıllı evlerle ilgili Bağlamsal Bütünlük ile ilgili bilgi akışı

parametrelerini seçmek için kullanılan bir anket yöntemini açıklar. Parametreler, gönderenler, alıcılar, öznitelikler, konular ve iletim prensiplerini içerir.

Herhangi bir parametrede yapılan değişiklik, mahremiyet normu ihlaline yol açabilir. Yöntem esnekliği, cihaz üreticileri, düzenleyiciler, tüketici savunucuları veya akademik araştırmacılar gibi farklı paydaşların, çeşitli akıllı ev cihazlarında veya bilgi toplama uygulamalarında özel mahremiyet normlarını keşfetmek için anket yöntemi kullanılması önerilir [8]. Bu sayede kullanıcılar seçenekler arasından mahremiyet tercihlerini belirtebilir. Örneğin, bir kişi, sağlık verilerini sağlık uygulamaları ile veya aile bireyleri ile paylaşmanın kabul edilebilir olduğunu düşünebilirken, bu verilerin reklam amacıyla kullanılmasını kabul edilemez bulabilir. Her gönderen/öznitelik ve alıcı/iletim prensibi çifti için, farklı parametreler içeren bilgi akışları için ortalama kabul edilebilirlik puanları hesaplanmıştır. Çalışmanın [8] sonucuna göre, veri "sahibi izin vermişse" iletim ilkesi, alıcıya bakılmaksızın tutarlı bir şekilde pozitif kabul edilebilirlik puanları alırken, "bilgi reklam amacıyla kullanılıyorsa" veya "bilgi süresiz olarak saklanıyorsa" gibi iletim prensipleriyle ilişkilendirilen parametreler en düşük kabul edilebilirlik puanlarına sahiptir. En kabul edilebilir gönderenler arasında enerji ölçer ve egzersiz takip cihazı bulunurken, en az kabul edilebilir olanlar arasında güvenlik kamerası ve ses asistanı bulunmaktadır [8].

Son olarak üreticiler ürünlerine üçüncü taraf kütüphaneler ve hizmetler entegre ederken dikkat göstermelidir, çünkü bu hizmetler genellikle açıklanmamış alıcılara bağımsız bilgi akışlarına neden olur [8]. Ayrıca, bilgi akışları, özelliğin cihazın temel işlevine daha yakından bağlı olduğunda daha kabul edilebilir olarak görünmektedir. Cihazın sadece gerektiği durumlarda üçüncü taraf bilgi akışı sağlaması mahremiyet hususları açısından önemlidir. [[8]'daki anket sonucuna göre İnternet Servis Sağlayıcıları ve reklam firmaları veri paylaşması açısından en az kabul edilebilir alıcılar arasında yer almaktadır.

4.2.4 Mahremiyet politikaları

Mahremiyet endişeleri, akıllı ev teknolojisinin benimsenmesinde önemli bir engeldir [18]. Kullanıcılar, bilgilerinin nasıl kullanılacağını bilme hakkına sahiptir, özellikle cihaz verileri kullanıcı profilleri oluşturmak için kullanılabileceği durumlarda. Mahremiyet politikası, kuruluşların veri toplama ve paylaşım uygulamalarını kullanıcılara iletikleri birincil ve yasal olarak bağlayıcı mekanizmadır.

Akıllı cihazlar için mahremiyet politikaları, kullanıcı verilerinin nasıl işleneceğini açıkça belirtmelidir. GDPR (Genel Veri Koruma Yönetmeliği) ve ülkeye özgü uyarlamaları gibi düzenlemelere göre, kullanıcılar kişisel verilerinin ne zaman kullanıldığını, işlendiğini veya saklandığını bilgilendirilmelidir. GDPR kapsamında, bireyler hangi verilerin işlendiğini, kim tarafından, hangi amaçlarla ve hangi yasal gerekçelerle işlendiğini bilme hakkına sahiptir. Ayrıca, verilerin transfer edileceği alıcılar hakkında da bilgilendirilmelidirler. Veri sorumluları, bireylerin bu noktalar hakkında net ve kapsamlı bir şekilde bilgilendirildiğinden emin olmalıdır [41].

Veri işleme süreçlerinde şeffaflık sağlanması, mahremiyet endişelerini hafifletmek ve akıllı ev cihazlarının daha geniş kabulünü sağlamak açısından kritik bir rol oynar. [48], yaklaşık 600 akıllı ev satıcısının ve cihazlarının mahremiyet politikalarını incelemiştir. Mahremiyet politikalarının erişilebilirliği, bu politikaların satıcıların web siteleri veya akıllı ev uygulamaları aracılığıyla kolayca erişilebilir olup olmadığına göre değerlendirilmiştir. Politikaların içerikleri, veri toplama, kullanma, paylaşma ve depolama hakkında hangi bilgilerin açıklandığını belirlemek için incelenmiştir. Çalışmanın bulguları, akıllı ev sektöründeki mahremiyet politikası uygulamalarına dair önemli içgörüler sağlamıştır. Önemli bir oran (yüzde 10.57), mahremiyet politikası olmaksızın, bazı şirketlerin güvenlik kameraları ve bebek monitörleri gibi mahremiyete duyarlı cihazlar satmasına rağmen, bu politikaları şirket web sitelerinde bile bulundurmamıştır. Satıcıların çoğu (yüzde 43.52), mahremiyet politikalarını akıllı ev cihazlarına uyarlamamış,

bunun yerine veri toplama ve paylaşma hakkında yeterli bilgi içermeyen genel politikalar sunmuştur. Şirketlerin yalnızca yüzde 64.38'i cihaz mahremiyet politikalarını web sitelerinde kolayca erişilebilir hale getirmiştir. Yaklaşık yüzde 26.84'ü ise web sitesi mahremiyet politikalarını erişilebilir hale getirmemiştir.

Net ve anlaşılır mahremiyet politikaları, kullanıcıların sistemlere olan güvenini inşa etmede hayati önem taşır. BITAG'ın Nesnelerin İnterneti (IoT) Güvenlik ve Mahremiyet Tavsiyeleri Raporu, IoT cihazları için kullanıcı dostu mahremiyet politikalarının gerekliliğini vurgular [2]. Bu politikalar, kullanıcı mahremiyeti endişelerini doğrudan ele almalıdır. Örneğin, bir cihazın politikası, belirli verilerin yalnızca acil durumlarda paylaşıldığını belirtirse, bu durum kullanıcıların mahremiyetle ilgili endişelerini azaltmaya yardımcı olabilir. Apthorpe ve arkadaşları [8], kullanıcıların bilgi paylaşımını acil durumlarla sınırlı olduğunda daha kabul edilebilir bulduğunu ortaya koymuştur.

Ayrıca, IoT cihazları daha sıkı mahremiyet kontrolleriyle inşa edilmelidir. [60]'ye göre, kullanıcılara ve cihazlara tam erişim sağlamak, gereksiz uygulama kurulumlarına ve mahremiyet ihlallerine yol açabilir. Üçüncü taraf hizmetleri içeren durumlarda, beklenmedik veri akışları meydana gelebilir. Kullanıcıların yalnızca yetkili oldukları işlemlere erişebildiğinden emin olmaya çalıştığımız gibi [14], cihazların da yalnızca işlevlerini yerine getirmek için gerekli olan minimum veri miktarını kullanmaları kısıtlanmalıdır. Bu ilke, sistem işlevselliği ile kullanıcı mahremiyetini koruması arasındaki dengeyi sağlayarak çift yönlü güvenin temelini destekler. Sonuç olarak, akıllı cihazlar geliştirilirken kullanıcı ve cihaz iletişim gereksinimleri, mahremiyet standartları ve kullanıcı beklentileri dikkate alınmalıdır.

Akıllı evlerde farklı kullanıcılar arasında mahremiyet endişeleri ve beklentileri değişiklik gösterebilir; bu da mahremiyet politikalarının bu farklılıklara uyum sağlamasını ve potansiyel mahremiyet ihlallerini önlemesini gerektirir [18]. Ayrıca, mahremiyet politikalarının iyileştirilmesi, şeffaflığı artırabilir ve satıcıların yasal gerekliliklere uymalarını sağlayabilir. Mahremiyet politikalarının netliğinin ve erişilebilirliğinin artırılması,

şeffaflığı artırmanın ve "kullanıcıdan sisteme güven" oluşturma'nın önemli bir adımıdır [48]. Cihazlar arasında mahremiyet politikalarının standart hale getirilmesi, kullanıcıların akıllı ev teknolojilerini satın alırken daha bilinçli kararlar vermelerine olanak sağlayarak, RBP-AeABAC modelinin vaat ettiği gibi kullanıcılar ve sistemler arasında çift yönlü güveni teşvik edebilir.

4.2.5 RBP-AeABAC Modeli

Akıllı ev ekosistemleri karmaşıklık açısından büyüdükçe, mahremiyet endişelerinin ele alınması, özellikle kullanıcılar ve sistemler arasında çift yönlü güvenin teşvik edilmesi açısından kritik hale gelmiştir. Geleneksel yaklaşımlar, öncelikli olarak sistemden kullanıcıya güvene odaklanmış ve sistemin kullanıcının kimliğine güvenmesini sağlamaya çalışmıştır; ancak akıllı ev ekosistemi, kullanıcıların verilerinin nasıl toplandığı, kullanıldığı ve korunduğu konusunda güven duymalarını sağlayarak kullanıcıdan sisteme güveni de sağlamalıdır.

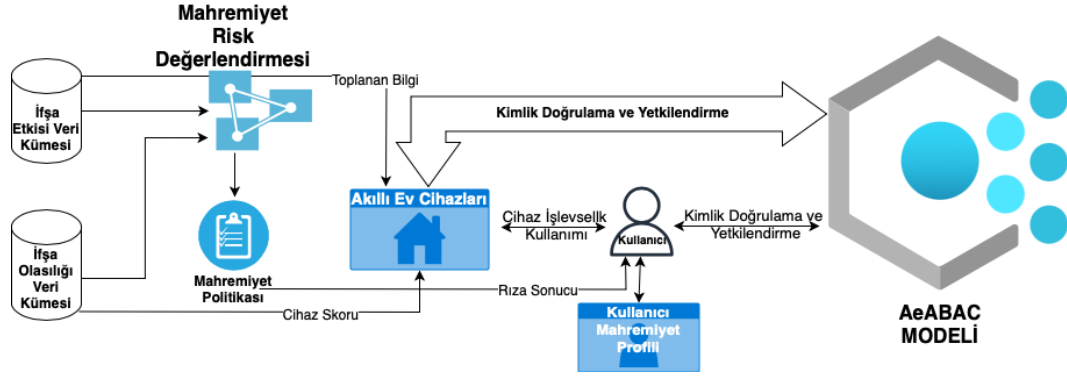
Yapılan literatür incelemeleri, akıllı evlerde mahremiyet sorunlarını ele alma konusunda önemli bir boşluk olduğunu ve kullanıcıları güvence altına almanın, farkındalıklarını artırmanın ve mahremiyetlerini korumanın gerekliliğini ortaya koymaktadır. Kullanıcılar, evlerinde kullandıkları sistemlere güvenmelidir. AeABAC modeline, literatürdeki bu boşluğu doldurmak için mahremiyetle ilgili gereksinimler eklenmiştir. Önerilen Risk Tabanlı Mahremiyet Yaklaşımı ile AeABAC (RBP-AeABAC) modeli, kullanıcıların verilerinin nasıl yönetildiği konusunda kendilerini güvende hissetmelerini sağlayarak mahremiyet tercihlerini ve onay mekanizmalarını entegre eder (Şekil 4.1). Model, akıllı ev ortamında paylaşılan verilerin türleri, paylaşılan verilerin ifşa edilme riski ve paylaşılan verilerin açığa çıkması durumunda kullanıcıların karşılaşılabileceği zararlar gibi faktörleri incelemektedir.

Tezin önceki bölümünde [15], [14], odak noktası, akıllı cihazlara erişim sağlamak için

kullanıcıların kimlik doğrulaması, kimlik doğrulamanın güvenilirlik seviyesinin belirlenmesi ve kimliği doğrulanmış kullanıcılar için yetkilendirme sürecinin detaylandırılmasıydı. Ana odak, akıllı sistemlerde kullanıcı kimlik doğrulaması ve yetkilendirmesiydi. Bir kullanıcı biyometrik yöntemlerle kimliği doğrulandıktan sonra, bu kimlik doğrulamanın güvence seviyesi, Erişim Kararı Belirsizlik Puanı (ADUS) olarak hesaplanır. Bu puan, cihaz işlevlerine erişim izni verme sürecini etkiler ve böylece "sistemden kullanıcıya güven" tesis edilir. Kullanıcılar, talep edilen işlevin kritikliği, rolleri ve ADUS'a göre cihaz işlevlerini kullanma yetkisine sahiptir. Detaylı erişim kontrol politikaları tanımlanmış ve kullanıcının cihaz üzerindeki hangi işlevleri kullanabileceği belirtilmiştir. Bu mekanizmalar, yalnızca yetkili kullanıcıların belirli cihaz işlevlerine erişebilmesini sağlarken, bilgi güvenliğinin "en az ayrıcalık" ilkesine uygun olmuştur.

Bu bölümde sunulan RBP-AeABAC modeli, "kullanıcıdan sisteme güven" sağlamaya odaklanmakta ve kullanıcıların akıllı ev cihazlarıyla etkileşimde bulunurken mahremiyetlerinin korunduğuna emin olmalarını hedeflemektedir. Bu noktaya kadar talep akışı kullanıcıdan cihaza doğru ilerlerken, bu noktada sistem, kişisel verilere erişmeden önce kullanıcı onayını gerektirmektedir. Artık eylemin gerçekleştirilmesine izin vermek kullanıcıya bağlıdır, çünkü verilerini paylaşmaya onay vermesi gerekmektedir. Kimlik doğrulama ve yetkilendirmeden sonra, vurgulanan nokta, cihazın çalışabilmesi için hangi bilgilere ihtiyaç duyulduğunu belirlemek ve yetkilendirilmiş cihazın güvenliğini değerlendirmektir. Bu yaklaşım, kullanıcıları veri paylaşımıyla ilgili karar alma sürecine aktif katılımcılar haline getirerek onları güçlendirmektedir. Paylaşılan verilerin ifşa edilme etkisi ve ifşa olasılığı değerlendirilerek bir mahremiyet riski değerlendirmesi yapılır.

RBP-AeABAC modeli, kullanıcının savunmasızlığı ve mahremiyet risklerini anlama seviyesine göre mahremiyet korumalarını kişiselleştirerek "kullanıcıdan sisteme güven" ilkesini önceliklendirmektedir. Yalnızca verilerin hassasiyetine odaklanmak yerine kullanıcının savunmasızlığının dikkate alınması, mahremiyet önlemlerinin en çok ihtiyaç duyulan alanlarda en etkili olmasını sağlar. Örneğin, paylaşılan verilerin ifşa edilmesi-



Şekil 4.1: AeABAC için Risk Tabanlı Mahremiyet Yaklaşımı (RBP-AeABAC)

nin sonuçlarını tam olarak anlamayabilecek çocuklar veya misafirler daha sıkı mahremiyet kontrollerine ihtiyaç duyarken, mahremiyet konularında daha bilinçli olan yetişkinler için daha esnek mahremiyet kontrolleri uygulanabilir. Bu, kullanıcıların rolüne ve mahremiyet risklerini kavrayıp yönetme yeteneklerine göre güvenlik derecesini ayarlayarak mahremiyete kullanıcı merkezli bir yaklaşım sunmaktadır.

4.3 Akıllı Evlerde Kullanıcı Mahremiyet Risk Değerlendirmesi

Akıllı evlerde mahremiyet odaklı bir yaklaşım benimsendiğinde, OCTAVE (Operasyonel Olarak Kritik Tehdit, Varlık ve Zayıflık Değerlendirmesi) yöntemi, varlıkları anlamak, tehditleri tanımlamak ve riskleri değerlendirmek için kullanarak bilinçli kararlar almak amacıyla yansıtılır[9]. Özellikle, mahremiyet risk analiz modelimizi OCTAVE çerçevesi ile aşağıdaki gibi ilişkilendirilmektedir:

- Varlık Tanımlama: Akıllı ev ortamında her akıllı cihazı, akıllı ev ortamındaki kritik bir varlık olarak kabul edilir.
- Tehdit Profili: Olası mahremiyet tehditleri, anket veri setinden uyarlanan cihaz risk puanlarına dayanarak değerlendirilir [5].
- Risk Değerlendirmesi: Cihaz risk puanları, kullanıcıdan sisteme güven dinamik-

lerini yansıtan güncel veri setinden elde edilen bilgi ifşa maliyeti ile birleştirilir [19]. Bilgi ifşa maliyeti, ifşa etkisini belirlerken, cihaz risk puanları ifşa olasılığını belirler. Bu, OCTAVE'nın tehditlerin olasılığını ve etkilerini değerlendirme yöntemine benzer.

- Karar Verme: Mahremiyet politikaları ve mahremiyet profilleri, kullanıcıların bilinçli kararlar almasına olanak tanır ve bu da 'kullanıcıdan sisteme güven' ilkesini pekiştirir.

Sonuç olarak, mahremiyet risk analizi, iki temel boyut olan *ifşa etkisi* ve *ifşa olasılığı* temelinde gerçekleştirilir. Bu iki boyut boyunca mahremiyet riskleri analiz edilerek, kullanıcıların mahremiyet risklerini her iki açıdan anlamalarına yardımcı olmak ve buna göre onay vermelerini sağlamak hedeflenir.

4.3.1 İfşa Etkisi

İfşa etkisi değerlendirmesi, akıllı cihazlarla paylaşılan verilerin ifşa edilmesinin sonuçlarını belirler. Çeşitli çalışmalar, IoT olaylarının etkisini üç temel unsur olan mahremiyet, bütünlük ve erişilebilirlik temelinde sınıflandırmaktadır [70]. Çalışmamız, özellikle hassas bilgilerin ifşasını, itibar kaybını ve bunun sonucunda ortaya çıkan mali sonuçları içeren mahremiyetin etkisine odaklanmaktadır.

Akıllı cihazların kullanabileceği farklı bilgi türleri vardır. Çalışma [13], akıllı cihazlar tarafından toplanan veri türlerini hane halkı, aile, biyometrik, bağlamsal ve diğer veriler olarak sunmaktadır. Bir başka çalışma [63], akıllı cihazların toplayabileceği kişisel bilgileri sıralamaktadır. Zang ve diğerleri [72], on altı tür kişisel bilgiyi tanımlamakta ve bunları isim, adres, doğum tarihi, davranış (örneğin, arama), tıbbi ve konum gibi kişisel tanımlayıcı bilgiler olarak sınıflandırmaktadır. Coleti ve diğerleri [19], bilgileri tanımlama, konum, cihaz ve mali olarak sınıflandırmaktadır. Ayrıca, GDPR [1] ve KVKK [41] düzenlemeleri, hassas kişisel bilgileri ve diğer kişisel bilgileri tanımlamaktadır.

Çizelge 4.1: Akıllı Ev Ortamı İçin Bilgi Kategorileri.

Veri Kategorisi	Akıllı Ev Ortamında Kullanılan Veri
Hassas Kişisel	Ses Biyometrisi Yüz Biyometrisi Video Kaydı İrk Etnik Genetik Bilgi Sağlık Bilgileri (örneğin, tıbbi geçmiş) Kimlik Kartı GPS Koordinatları
Kişisel	İsim Yaş Konum (Evde, dışarıda) Adres E-posta adresi Telefon numarası Sosyal güvenlik numarası (veya TCKN) Doğum tarihi Kullanıcı Giriş Bilgileri Kalp Atış Hızı, Uyku Davranışı Kilo, Boy IP adresi
Finansal	Finansal bilgiler (örneğin, banka hesap numaraları) Banka hesap geçmişi Kredi Kartı Bilgileri
Cihaz	Zaman Varsayılan Giriş Bilgileri

Bu çalışmalardan yola çıkarak, akıllı ev ekosistemine yansıtılan bilgi kategorilerini belirledik. Çizelge 4.1’da bu kategoriler sunulmaktadır: *hassas kişisel*, *kişisel*, *finansal* ve *cihaz bilgisi*.

Çalışma [19], 59 akıllı ev cihazının mahremiyet politikaları ve kullanım kılavuzlarının niteliksel bir incelemesini gerçekleştirmiştir. Analiz, hangi kişisel verilerin işlendiğini ve bu belgelerin ilgili kişisel verilerin işlenmesinde kullanılan prosedürler hakkında ne kadar ayrıntı sağladığını doğrulamayı hedeflemiştir. Bir anket veri seti üretilmiş ve akıllı cihazlar tarafından kullanılan bilgiler dört kategori altında sınıflandırılmıştır: tanımlama, konum, cihaz ve finansal. Bu veri setindeki akıllı cihazlar arasında, akıllı ev ekosistemiyle ilgili dokuz akıllı cihaza odaklanıldı. Bu dokuz cihazın topladığı bilgiler Şekil 4.2’te gösterilmektedir.

İfşa etkisini değerlendirirken, her bir bilginin ne kadar önemli veya riskli olduğunu ölç-

Device Vendor	Name	Address	Email	Behavioral	Sensitive	Identification	Biometric	Third Party	ID App	Credit Card	Purchase	Financial	Billing	Location
Amazon Echo	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	No	No	No	Yes
AirPlay Apple	Yes	Yes	Yes	No	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Google Home	Yes	No	No	Yes	Yes	No	Yes	Yes	No	Yes	No	No	No	Yes
Google Nest G	Yes	No	No	Yes	Yes	No	Yes	Yes	No	Yes	No	No	No	Yes
Logitech Security Camera	Yes	No	Yes	No	No	No	No	Yes	No	No	Yes	No	No	Yes
Philips Hue Hub	Yes	No	Yes	No	No	No	No	Yes	No	No	Yes	No	No	No
Smart Tv Samsung	Yes	Yes	Yes	No	No	No	No	Yes	No	Yes	No	No	Yes	Yes
Samsung Smartthing	Yes	Yes	Yes	No	No	No	No	Yes	No	Yes	No	No	Yes	Yes
Arc speaker Sonos	Yes	No	Yes	No	No	No	No	Yes	No	No	No	No	No	No

Şekil 4.2: Kategorilerine Göre Akıllı Ev Ortamında Kullanılan Bilgiler.

mek için bir metriğe ihtiyaç vardır. Örneğin, yüz biyometrik verilerinin ele geçirilmesi önemli bir mahremiyet ihlali oluştururken, yalnızca yaş bilgisinin ele geçirilmesi o kadar da önemli değildir. Ayrıca, bazı bilgiler ifşadan sonra kolayca geri kazanılabilir; örneğin, kredi kartı bilgileri çalındığında, kredi kartı bloke edilebilir.

Bilgileri aşağıdaki dört kriter temelinde değerlendiriyoruz:

- **Hassas Kişisel Bilgi (SPI):** Genellikle yasal olarak korunan, son derece kişisel ve gizli bilgileri kapsar. Bu tür veri ifşaları, ciddi mahremiyet ihlallerine ve bireysel zararlara yol açabilir. GDPR [1] ve KVKK [41] tarafından, bireylerin ırk veya etnik kökeni, siyasi görüşleri, dini veya felsefi inançları, sendika üyeliği, genetik bilgileri, benzersiz kimlik için biyometrik verileri, sağlıkla ilgili bilgileri veya cinsel yaşamlarıyla ilgili detaylar gibi bilgilerin işlenmesi yasaklanmıştır. Kullanılan veri setimizde biyometrik veriler, kimlik belgeleri ve sağlık bilgileri gibi örnekler bulunmaktadır. Bu bilgilerin hassasiyetine bağlı olarak 0 ile 4 puan arasında değişmektedir.
- **Kişisel Bilgi (PI):** Bir kişiyi tanımlayabilen ancak SPI kadar hassas olmayan verileri içerir. Bu bilginin korunması hala önemlidir, ancak ifşanın sonuçları genellikle daha az kritik olmuştur. Kullanılan veri setimizde isim, adres, e-posta ve telefon numarası gibi PI örnekleri vardır. Burada, bu bilgilere dayanarak birinin tanınmasının ne kadar kolay olduğuna bağlı olarak 0 ile 2 puan arasında bir puan aralığı bulunmaktadır.

- Geri Kazanılabilir Bilgi (RI): Kaybedildiğinde veya ifşa edildiğinde kolayca geri kazanılabilen veya değiştirilebilen bilgileri içerir. Bilgiler kolayca geri kazanılabiliyorsa, ifşanın risk seviyesi daha düşüktür. Kullanılan veri setinden Apple ID ve Kredi Kartı Numarası gibi örnekler bulunmaktadır. Kolayca geri kazanılabilir olduğunda negatif (-1), geçerli olmadığında 0 olarak değerlendirilir; bu da genel risk puanını azaltır.
- Finansal Etkili Bilgi (FCI): Ifşa edildiğinde mali kayba veya dolandırıcılığa yol açabilecek her türlü bilgiyi içerir. Potansiyel finansal etkisi yüksek olan bilgilerin kritikliği de artmaktadır. Kredi kartı bilgileri, mali hesap detayları ve fatura bilgileri gibi örnekler bu grupta yer almakta; ifşanın potansiyel mali etkisine bağlı olarak 0 ile 3 puan arasında değişmektedir.

Toplam Puan ve Kritiklik Haritalaması: Veri setindeki her bir bilgi [19] hassas kişisel bilgi, kişisel bilgi, geri kazanılabilir bilgi ve finansal etkili bilgi açısından değerlendirilir. Puanlar, her kriterin yukarıda verilen açıklamasındaki aralığa dayanarak belirlenmektedir. Her bir bilginin toplam puanı, dört kriterden alınan puanların toplamı ile hesaplanmaktadır. Toplam puan, kritiklik seviyesine aşağıdaki şekilde ilişkilendirilmektedir:

- Yüksek Kritik (7 ile 10 puan): Ifşa edildiğinde önemli zarar veya kayba yol açabilecek bilgiler.
- Orta Kritiklik (4 ile 6 puan): Hassas olan ancak yüksek kritik verilerden daha düşük bir etkiye sahip bilgiler.
- Düşük Kritiklik (1 ile 3 puan): Ifşa edilirse sınırlı etkiye sahip daha az hassas bilgiler.
- Kritiklik Yok (0 puan): Ifşa edildiğinde minimal veya hiç risk taşımayan bilgiler.

Çizelge 4.2, veri setindeki her bir bilginin [19] dört kriterine göre (i) puanını, (ii) tüm kriterler için toplam puanı ve (iii) bu toplam puana karşılık gelen bir ifşa etkisi seviyesine

ilişkilendirilmesini sunmaktadır. Bu ilişkilendirme, her bir bilginin mahremiyet ifşa maliyeti ile ilgili net bir bakış açısı sağlamaktadır. Bu kategorilendirme, bu tür bilgilerin ifşasının potansiyel risklerini yansıtmaktadır. Farklı bilgi türlerinin kritikliğini değerlendirmek için nesnel bir yöntem sunarak daha etkili risk yönetimi ve veri güvenliği yöntemlerine olanak tanımaktadır.

Çizelge 4.2: Veri Setindeki Bilgilerin İfşa Etkisi

Information/Device	Sensitive Personal Information (0-4)	Personal Information (0-2)	Is Recoverable (0,-1)	Financial Cost (0-3)	Total Points	Disclosure Impact
Name	0	2	0	0	2	Low Criticality
Address	0	2	0	1	3	Low Criticality
Email	0	2	0	1	3	Low Criticality
Country	0	1	0	0	1	Low Criticality
Nickname	0	1	0	0	1	Low Criticality
Phone	0	2	0	0	2	Low Criticality
Site	0	0	0	0	0	No Criticality
Company data	0	1	0	1	2	Low Criticality
Office	0	1	0	0	1	Low Criticality
Behavioral Data	2	2	0	2	6	Moderate Criticality
Other Sensitive Data	3	2	0	2	7	Highly Critical
Postal Code	0	1	0	0	1	Low Criticality
Residence Data	0	1	0	1	2	Low Criticality
Identification Documents	4	0	0	3	7	Highly Critical
Date of birth	1	2	0	1	4	Moderate Criticality
Gender	0	1	0	0	1	Low Criticality
Telephone Data	0	2	0	0	2	Low Criticality
Product Use	1	1	0	1	3	Low Criticality
Biometric Data	4	2	0	2	8	Highly Critical
Location Photo	3	2	0	2	7	Highly Critical
Image	1	1	0	2	4	Moderate Criticality
Image/Picture	1	1	0	2	4	Moderate Criticality
Audio	2	1	0	1	4	Moderate Criticality
Third Party Data	0	1	0	1	2	Low Criticality
Billing Information	1	1	0	3	5	Moderate Criticality
Language	0	0	0	0	0	No Criticality
Marital status	0	1	0	0	1	Low Criticality
Location	3	2	0	2	7	Highly Critical
Time Zone	0	0	0	0	0	No Criticality
IDApple	0	1	-1	1	1	Low Criticality
Credit Card Information	2	0	-1	3	4	Moderate Criticality
Purchase Data	1	1	-1	3	4	Moderate Criticality
Financial data	2	0	-1	3	4	Moderate Criticality
Billing Information	1	1	0	3	5	Moderate Criticality
Location	3	2	0	2	7	Highly Critical
Operational data	0	1	0	0	1	Low Criticality

4.3.2 İfşa Olasılığı

IoT mahremiyetine yönelik en sık tehditler veri sızıntısı, dinleme ve bilgi ifşasıdır. Bu tehditleri azaltmak ve kullanıcıdan sisteme güven inşa etmek için IoT donanım, yazılım ve ağ katmanlarının güvence altına alınması esastır. Donanım ve yazılımdaki anonim-

leřtirme ve kimlik gizleme, bilgi ifřasını önlemeye yardımcı olabilir. Üreticilerin hassas verilere erişim sağlamaktan kaçınması, veri kullanımında řifreleme uygulaması ve fiziksel cihaz erişimini sınırlama, verileri dinlenme halinde koruma ve sabit řifre kullanımından kaçınma gibi erişim kontrol önlemlerini uygulaması gerekmektedir [70].

Alrawi ve diğeri [5], 45 akıllı ev cihazından oluşan bir IoT test ortamı oluşturmuş ve güvenlik değeriendirmesi gerçekleřtirmiřtir. Güvenlik değeriendirme sonuçları, Your Things projesi olarak kamuya açık bir řekilde yayınlanmıřtır ve web sitesinde ¹ mevcuttur. Your Things projesindeki puan hesaplaması, her akıllı ev cihazını dört bileřen üzerinden değeriendirmeyi içermektedir: *cihazın kendisi, mobil uygulama, bulut uç noktaları ve ağı iletiřimi*. Her bileřenin belirli değeriendirme kriterleri bulunmaktadır ve farklı dağıtım senaryoları veya tehdit modelleri için ayarlanabilir ağırlıklar uygulanabilmektedir.

Cihaz güvenlik puanı, internet eşleřtirme, yapılandırma, güncellenebilirlik, açığa çıkan hizmetler ve güvenlik açıkları temelinde değeriendirilmektedir [5]. Güvenlik açığı değeriendirmesi bu kategoride ana ağırlığı belirlemektedir. Common Vulnerability Scoring System (CVSS) puanı, çeřitli cihazlarda keřfedilen güvenlik açıklarını listeleyen CVE veritabanından elde edilmektedir. CVSS, güvenlik açıklarının ciddiyetini analiz etmek için standart bir teknik sağılayarak, kullanıcı ile sistem arasında güven inşa etmeye yardımcı olur [50]. Raporlanan güvenlik açıklarını düzenli olarak değeriendirip sıralar [59]. ABD merkezli FIRST.Org, dünya genelindeki bilgisayar güvenliğı olaylarına yanıt veren ekiplerine (CSIRT) destek sağılayan kar amacı gütmeyen bir kuruluřtur ve CVSS spesifikasyonlarını yönetmektedir. CVSS, organizasyonların güvenlik açıklarını önceliklendirmelerine ve en önemli olanları belirlemelerine olanak tanır. Güvenlik açığı değeriendirmesi için Nessus Tarayıcı kullanılarak, belirlenen güvenlik açıklarına bir ila on arasında dereceler atanmaktadır ve bu dereceler düşük, orta, yüksek veya kritik olarak kategorize edilmektedir. Mobil uygulamalar, veri sızıntısı, programlama hataları

¹<https://yourthings.info/>

ve aşırı ayrıcalıklı talepler gibi güvenlik sorunları açısından statik analiz ile değerlendirilmektedir [5]. Bu analizler için MobSF [3], Qark [45] ve bazı Kryptowire hizmetleri kullanılmaktadır. Bulut uç noktaları, alan kategorileri, TLS/SSL yapılandırmaları ve savunmasız hizmetler (örneğin, açık metin kimlik doğrulama) açısından incelenmektedir. Ağ iletişimi, protokoller, ortadaki adam saldırısı riskleri ve bileşenler arasındaki trafiğin şifrelenmesi açısından analiz edilmektedir. İletişim kanallarını analiz etmek ve profillemek için Nessus Network Monitor, ntop-ng, Wireshark ve sslsplit araçları kullanılmaktadır. Her bileşen, verilerin nasıl işlendiği, kullanılan şifreleme seviyesi ve güvenlik açığı yönetim yaklaşımı gibi belirli güvenlik ve mahremiyet kriterlerine göre değerlendirilmektedir. Bu değerlendirmeler, cihazın genel güvenlik durumunu oluşturmak için bir araya gelmekte ve puanlar güvenlik riski ile ters orantılı olarak, daha yüksek puanlar daha kötü güvenlik durumunu göstermektedir. Nihai puan, her bileşene atanan puanların toplanmasıyla elde edilmekte ve bu toplam, değerlendirmeyi farklı tehdit modellerine uyacak şekilde kolaylaştıran bir notaya dönüştürülmektedir.

Araştırmamız için bu veri seti, [5] mahremiyet kriterleri temelinde yapılandırılmıştır. Cihazların mahremiyetteki güçlerini ölçmeye odaklandığımızdan, YourThings web sitesinde her kategori için yalnızca mahremiyet ile ilgili özellikler seçilmiştir. YourThings portalında açıklanan puanlama metodolojisine göre, her kategori için mahremiyet açısından puanlar yeniden hesaplanmıştır. Bu yeniden hesaplama, akıllı ev sisteminin kullanıcıdan sisteme güven endişelerini etkili bir şekilde ele almasını sağlamak amacıyla gerçekleştirilmiştir. Örneğin, cihaz puanı, Cihaz Sorunları (CVSS) puanı düşük, orta, yüksek ve kritik olarak ele alınan güvenlik açıklarına göre hesaplanmıştır. Ağ puanı, mahremiyet metrikleri ile özellikle yeniden değerlendirilmiş ve böylece analizimizin mahremiyet merkezli değerlendirmeleri yansıttığı güvence altına alınmıştır. Mobil puan, tüm özelliklerin mahremiyetle ilgili olması nedeniyle orijinal veri seti ile aynı kalmıştır. Bulut puanı da yalnızca mahremiyet ile ilgili metrikleri dikkate alarak yeniden hesaplanmıştır. Sonuç olarak, cihazın güvenlik durumu değerlendirilmiş ve bu durum ifşa olasılığını belirlemiştir. İlk olarak, bu dört kategori arasında puanların minimum toplamı

kullanılarak cihazın güvenlik çerçevesindeki en zayıf halkası belirlenmeye çalışılmıştır. Cihaz bulut entegrasyonu kullanmıyorsa ancak ağ ve mobil bileşenlere dayanıyorsa, uygulanabilir her kategori için minimum puan alınacaktır.

Sonuç olarak, bulut entegrasyonu olmayan bir cihaza, kalan kategorilerden minimum puanlar atanacaktır. Bu yaklaşım, mahremiyet risklerinin daha titiz bir değerlendirmesini sağlamak amacıyla tasarlanmıştır. Ancak, bu yaklaşım, çok sayıda cihazın kullanılmasını sınırlandırabilir, çünkü çoğu cihaz, minimum toplamının daha sıkı mahremiyet koruma sağlasa bile çok düşük puanlar alır. Bu durum göz önünde bulundurularak, akıllı ev senaryolarımızı daha uygulanabilir kılmak için dört kategori arasındaki puanların ortalaması alınmayı tercih edilmiştir. İki veri setindeki modellememiz [5] ve [19] cihaz adı temelinde birleştirildi. Elde edilen veri seti, örnek akıllı ev senaryolarımız için yeterli olan dokuz cihazı içermektedir. Her bir cihaz için yeniden hesaplanan puanlar Çizelge 4.3'te sunulmaktadır.

Çizelge 4.3: Mahremiyet Kriterlerine Dayalı Cihaz Güvenlik Puanları

Cihaz Marka Model	Normalize Edilmiş Cihaz Skoru	Normalize Edilmiş Mobil Skoru	Normalize Edilmiş Bulut Skoru	Normalize Edilmiş Ağ Skoru	Cihaz Puanı	Mobil Puanı	Bulut Puanı	Ağ Puanı	Genel Skor	Genel Puan
Amazon Echo	1	0,4615	0,5692	1	A	D	D	A	0,76	C
Apple HomePod	1	1	0,3846	0,9286	A	A	D	A	0,83	B
Google Home	0,9583	0,6923	0,9231	0,7857	A	D	A	C	0,84	B
Google Home Mini	0,875	0,6923	0,9231	0,7857	B	D	A	C	0,82	B
Logitech Logi Circle	0,9167	0,6923	0,6923	0,9286	A	D	D	A	0,81	B
Nest Camera	1	0,6923	0,6308	0,9286	A	D	D	A	0,81	B
Nest Guard	1	0,6923	0,5692	1	A	D	D	A	0,82	B
Philips HUE Hub	0,875	0,9231	0,9385	0,9286	B	A	A	A	0,92	A
Samsung SmartThings Hub	1	1	0,6	0,9286	A	A	D	A	0,88	B
Samsung SmartTV	0,875	0,6923	0,7077	0,7857	B	D	C	C	0,77	C
Sonos	0,875	0,6923	0,8923	0,5	B	D	B	D	0,74	C

Bir cihazın ifşa olasılığı, cihazın mahremiyet puanı tarafından belirlenmektedir. Bu puan, dört bileşen puanının ortalamasıdır: Cihaz Puanı, Mobil Puan, Bulut Puanı ve Ağ Puanı. YourThings projesinin metodolojisi, daha yüksek puanın daha kötü bir güvenlik durumu gösterdiği ters bir puanlama sistemi kullanmaktadır. Hesaplama şu adımları takip etmektedir: İlk olarak, her bileşen (cihaz, mobil, bulut, ağ) için puanlar toplanır. Ardından, bu kategori için toplam mümkün puana bölünür. Son puan, elde edilen sonuç

1'den çıkarılarak bulunur. Derece ataması aşağıdaki eşik değerlerine göre yapılmaktadır:

- A Derecesi: Puan ≥ 0.9
- B Derecesi: Puan ≥ 0.8
- C Derecesi: Puan ≥ 0.7
- D Derecesi: Puan < 0.7

Sonuç olarak, ifşa olasılığını belirleyen cihaz mahremiyet puanı, dört bileşen puanının ortalaması olarak hesaplanmaktadır. Toplam sonuç temelinde, ifşa olasılığını dört farklı kategoriye sınıflandırılmaktadır:

- **Yüksek:** D Derecesi
- **Orta:** C Derecesi
- **Düşük:** B Derecesi
- **Çok Düşük:** A Derecesi

Bu puanlama sistemi, her cihazın ifşa olasılığını nesnel bir şekilde değerlendirmemizi sağlamakta olup, mahremiyet analizimiz için kritik öneme sahiptir. Hesaplanan ifşa olasılığı ve ifşa etkisi ile mahremiyet profilleri tanımlayabilir, mahremiyet riski analizleri gerçekleştirebilir ve buna göre bilinçli mahremiyet kararları alabiliriz.

4.3.3 Mahremiyet Profilleri

[15] ve [14] çalışmalarında sunulan AeABAC modelinde, akıllı ev sistemlerindeki kullanıcılar, daha önce tanımlanan diğer niteliklerin yanı sıra, rollerine göre kimlik doğrulama ve yetkilendirme işlemlerine tabi tutulmaktadır. Bir kullanıcının rolü, sadece

eriřim kararlarında deęil, aynı zamanda mahremiyet kararlarında da önemli bir rol oynamaktadır. Tezin önceki bölümündeki akıllı ev ortamına benzer olarak, sunum amacıyla akıllı evimizde beř kullanıcı rolü olduęu varsayılmaktadır: eř, genç, çocuk, misafir ve bakıcı. Genel olarak kendi mahremiyetlerini daha iyi deęerlendirebilen yetişkinlerin mahremiyeti üzerine, çocuklar gibi kullanıcıların mahremiyetini önceliklendirmesi hedeflenir.

Bu strateji, mahremiyet açısından en savunmasız kullanıcı grupları, özellikle çocuklar, için en sıkı koruma önlemlerinin uygulanmasını sağlar. Böylece, yalnızca verilerin hassasiyetine odaklanmak yerine, kullanıcıların savunmasızlığı göz önünde bulundurulmuştur. Gerektiğinde, daha genç veya bilgi düzeyi düşük kullanıcılara daha sıkı mahremiyet önlemleri uygulanırken, yetişkinlerin kişisel bilgilerini yönetme konusunda daha fazla esneklik sağlanır. Örneğin, çocukların mahremiyet profilleri, sınırlı yetkiyle daha yüksek düzeyde koruma sağlarken, eř ve genç profilleri, kullanıcı-sistem güvenine dayalı olarak onay gerektiren etkileşimlerde daha fazla esneklik sunar. Bu yaklaşım, her bireyin mahremiyet risklerini anlama ve kontrol etme kapasitesine göre koruma düzeyini ayarlayan kullanıcı odaklı bir strateji ortaya koymaktadır.

Bu hedef doğrultusunda, risk deęerlendirme süreci farklı kullanıcı rollerine göre uyarlanmıştır. Rol bazlı mahremiyet profilleri oluşturulmakta ve her bir cihaz için elde edilen ifřa olasılığı ve ifřa etkisine dayalı mahremiyet risk deęerlendirmesi yapılmaktadır. Güven deęerlendirmesi, kullanıcının mahremiyet profiline göre özelleştirilmiştir.

Bir kullanıcı, bir cihazın işlevini kullanmak istediğinde, mahremiyet politikası, dięer benzer hizmetler aracılığıyla aynı işlevselliğin gerçekleştirilip gerçekleştirilemeyeceğini deęerlendirir. Örneğin, sesli asistan kullanarak veya lambalar için özel bir uygulama aracılığıyla ışıkları açmak mümkündür. Bu durumda, kullanıcıya hangi cihazı tercih etmesi gerektięi konusunda rehberlik etmek için birkaç parametre deęerlendirilir: i) seçilen cihazın işlevi için gereken hassas veri seti; ii) cihazın veri ifřa riski, ifřa olasılığıyla ölçülür; iii) verilerin ifřa edilmesi durumunda kullanıcının karşılaşacağı maliyet,

ifşa etkisiyle ölçülür; ve iv) kullanıcının mahremiyet profili. Eğer cihaz, farklı ifşa etkilerine sahip çeşitli bilgiler topluyorsa, en yüksek ifşa etkisi dikkate alınarak genel ifşa riski hesaplanır.

Akıllı ev ortamında, her kullanıcı rolü için ayrı mahremiyet profilleri tanımlanmıştır. Mahremiyet onay kararları bu profillere göre farklılık göstermektedir. Örneğin, ifşa olasılığı orta düzeyde ve ifşa etkisi düşük kritikse, eş profili "İzin Ver," çocuk profili "Reddet," ve misafir profili "Kullanıcıya Sor" olarak belirlenmiştir.

Cihaz d için kullanıcı rolünün mahremiyet riskini değerlendirmek amacıyla, açıklama olasılığı L ve açıklama etkisi I için dört puanlı bir Olasılık-Etki (Likelihood-Impact) matrisi kullanılmaktadır. Modelimizde, olasılık $L(d)$ ve etki $I(d)$, cihaz d ile değişiklik göstermektedir. Daha önce belirtildiği gibi, olasılık dört değerden birini alabilir: *Çok Düşük*, *Düşük*, *Orta* veya *Yüksek*. Benzer şekilde, etki *Kritiklik Yok*, *Düşük Kritiklik*, *Orta Kritiklik* veya *Yüksek Kritiklik* olarak kategorize edilebilir. Mahremiyet risk kararı D , hem $L(d)$ hem de $I(d)$ fonksiyonudur.

Tüm bu faktörleri dikkate alarak, beş farklı mahremiyet profili için tanımlanan mahremiyet onay kararlarının örnekleri Çizelge 4.4, 4.5, 4.6, 4.7 ve 4.8’de gösterilmiştir.

Çizelge 4.4: Çocuk Mahremiyet Profili için Mahremiyet Onay Kararları.

Mahremiyet Profili	Kritik Değil	Düşük Kritiklik	Orta Kritiklik	Yüksek Kritiklik
Çok Düşük	İzin Ver	İzin Ver	Reddet	Reddet
Düşük	İzin Ver	İzin Ver	Reddet	Reddet
Orta	İzin Ver	Reddet	Reddet	Reddet
Yüksek	İzin Ver	Reddet	Reddet	Reddet

Çizelge 4.5: Bakıcı Mahremiyet Profili için Mahremiyet Onay Kararları.

Mahremiyet Profili	Kritik Değil	Düşük Kritiklik	Orta Kritiklik	Yüksek Kritiklik
Çok Düşük	İzin Ver	İzin Ver	İzin Ver	Kullanıcıya Sor
Düşük	İzin Ver	İzin Ver	Kullanıcıya Sor	Kullanıcıya Sor
Orta	İzin Ver	Kullanıcıya Sor	Kullanıcıya Sor	Reddet
Yüksek	İzin Ver	Kullanıcıya Sor	Kullanıcıya Sor	Reddet

Çizelge 4.6: Misafir Mahremiyet Profili için Mahremiyet Onay Kararları.

Mahremiyet Profili	Kritik Değil	Düşük Kritiklik	Orta Kritiklik	Yüksek Kritiklik
Çok Düşük	İzin Ver	İzin Ver	İzin Ver	Kullanıcıya Sor
Düşük	İzin Ver	İzin Ver	İzin Ver	Reddet
Orta	İzin Ver	İzin Ver	Kullanıcıya Sor	Reddet
Yüksek	İzin Ver	Kullanıcıya Sor	Reddet	Reddet

Çizelge 4.7: Genç Mahremiyet Profili için Mahremiyet Onay Kararları.

Mahremiyet Profili	Kritik Değil	Düşük Kritiklik	Orta Kritiklik	Yüksek Kritiklik
Çok Düşük	İzin Ver	İzin Ver	İzin Ver	Kullanıcıya Sor
Düşük	İzin Ver	İzin Ver	Kullanıcıya Sor	Kullanıcıya Sor
Orta	İzin Ver	İzin Ver	Kullanıcıya Sor	Reddet
Yüksek	İzin Ver	Kullanıcıya Sor	Reddet	Reddet

Çizelge 4.8: Eş Mahremiyet Profili için Mahremiyet Onay Kararları.

Mahremiyet Profili	Kritik Değil	Düşük Kritiklik	Orta Kritiklik	Yüksek Kritiklik
Çok Düşük	İzin Ver	İzin Ver	İzin Ver	Kullanıcıya Sor
Düşük	İzin Ver	İzin Ver	Kullanıcıya Sor	Kullanıcıya Sor
Orta	İzin Ver	İzin Ver	Kullanıcıya Sor	Kullanıcıya Sor
Yüksek	İzin Ver	Kullanıcıya Sor	Kullanıcıya Sor	Reddet

Burada, satırlar, Çok Düşük'ten Yüksek'e kadar olan açıklama olasılığı değerlerini temsil etmektedir. Sütunlar ise, Kritik Değil'den Yüksek Kritik'e kadar değişen açıklama etki değerlerini göstermektedir. Örneğin, kullanıcı u (çocuk rolüne sahip) d cihazının işlevselliğini şu açıklama olasılığı ve etkisi ile kullanıyorsa:

$$L(d) = \text{Düşük}, \quad I(d) = \text{Orta Kritiklik}$$

O zaman, rolüne dayanarak cihaz d için mahremiyet onay kararı $D(L(d), I(d))$ şöyle olacaktır:

$$D(L(d), I(d)) = D(\text{Düşük}, \text{Orta Kritiklik}) = \text{Reddet}$$

Tablolardaki girişlerin tutarlı bir profil elde etmek için bağımsız olmadığını belirtmek gerekir. Bunun nedeni, hem satır hem de sütun değerlerinin sıralı olmasıdır. Örneğin, j sütunu için i satırındaki değer "Reddet" ise, bu durumda j sütunundaki diğer tüm satırların da "Reddet" olması beklenir. Benzer şekilde, i satırı için j sütunundaki değer "Reddet" ise, o zaman i satırındaki diğer tüm sütunların da "Reddet" olması gerekmektedir.

4.3.4 Birden Fazla Alternatif Cihazla Karar Alma

Kullanıcıların, cihazların işlevselliğini kullanırken mahremiyet onayı karmaşıklığıyla başa çıkmaları gerekmektedir. Kullanıcıların bilinçli kararlar alabilmesi ve mahremiyetlerinin korunması için tutarlı ve etkili bir mahremiyet politikası geliştirmek kritik öneme sahiptir. Bir kullanıcı, aynı işlevselliği birden fazla cihazla gerçekleştirebilir.

Talep edilen işlevselliği yerine getirebilen k cihazının bulunduğu varsayalım. Mahremiyet risk değerlendirmesi yapıldıktan sonra, her cihaz üç mahremiyet onay kararından birine sahip olacaktır: İzin Ver, Kullanıcıya Sor veya Reddet. Her bir k cihaz için onay kararlarını içeren bir mahremiyet karar vektörü oluşturulmaktadır. İşlemin devam edip

edemeyeceğine dair nihai karar, bu vektöre dayanarak belirlenmektedir.

Özetle, aşağıdaki işlem sırası izlenir:

1. **Mahremiyet Onayı Değerlendirmesi:** k kümesindeki her cihaz için mahremiyet onayı değerlendirilerek, d_i 'nin cihaz i için kararı temsil ettiği $V = [d_1, d_2, \dots, d_k]$ şeklinde bir vektör elde edilir (İzin Ver, Kullanıcıya Sor, Reddet).

2. **Karar Seçimi:**

- Eğer V vektöründe en az bir "İzin Ver" varsa, kullanıcı ilgili cihazı kullanarak işlevselliği çalıştıracaktır.
- Eğer V içinde "İzin Ver" yoksa ama en az bir "Kullanıcıya Sor" varsa, kullanıcıdan ek bir onay istenecektir.
- Eğer tüm cihazlar "Reddet" yanıtı verirse, kullanıcının işlevselliği gerçekleştirilmesine izin verilmez.

Bu, mahremiyet kararlarını birden fazla cihaz girdisine dayalı olarak başarılı bir şekilde yönetilmesini sağlar ve her cihazın risk profilleri ve mahremiyet düzenlemeleri dikkate alınarak eylemlere uygun bir şekilde izin verilmesini sağlar.

4.4 Uygulama ve Kullanım Senaryoları

Tezin bu bölümünde, RBP-AeABAC yaklaşımı iki senaryo ile daha somut hale getirilmiştir.

4.4.1 Senaryo I

İlk senaryoda, Mary adında bir kullanıcının bakıcı rolünde olduğu ve Arc Speaker Sonos cihazı üzerinden müzik çalmak istediği varsayılmıştır. Mary'nin, müziği Samsung

SmartTV ve Google Home cihazları üzerinden de çalabileceği öngörülmüştür. Veri setine [19] dayanarak, Arc Speaker Sonos cihazının, çalışmak için kullanıcının "İsim, E-posta, Telefon ve Üçüncü Taraf Verileri" bilgilerini kullandığı tespit edilmiştir. Toplanan bilgilerin en yüksek ifşa etkisi, Çizelge 4.2'te sunulan değerlendirmeye göre "Düşük Kritiklik" olarak belirlenmiştir. Öte yandan, Mary'nin müziği Samsung SmartTV cihazı kullanarak çaldığında, "İsim, Adres, E-posta, Ülke, Telefon, Posta Kodu, Ürün Kullanımı, Ses, Üçüncü Taraf Verileri, Kredi Kartı Bilgileri, Fatura Bilgileri ve Konum" bilgilerinin kullanıldığı belirlenmiştir. Toplanan bilgilerin en yüksek ifşa etkisi "Yüksek Kritiklik" olarak tanımlanmıştır. Son olarak, Mary'nin müziği Google Home üzerinden çaldığında, Google Home cihazının "İsim, Telefon, Davranışsal Veri, Biyometrik Veri, Üçüncü Taraf Verileri, Fatura Bilgileri ve Konum" bilgilerini topladığı tespit edilmiştir. Bu durumun en yüksek ifşa etkisi de "Yüksek Kritiklik" olarak belirlenmiştir.

Değerlendirmenin ikinci bölümünde, ilişkili cihazların genel puanına dayanarak ifşa olasılığı veri setinden [5] elde edilmiştir. Çizelge 4.3'da görüldüğü üzere, hem Arc Speaker Sonos hem de Samsung SmartTV'nin genel puanı C, yani Orta düzey olarak belirlenmiştir. Son olarak, Google Home'un genel puanı ise B, yani Düşük olarak saptanmıştır. Mary'nin mahremiyet profili, Çizelge 4.5'da yer alan Bebek Bakıcısı kullanıcı profiline dayalı olarak mahremiyet riskinin değerlendirildiği ve üç cihaz için aşağıdaki olasılık, etki ve mahremiyet onay kararlarının elde edildiği ifade edilmiştir.

$$L(\text{Arc Speaker Sonos}) = \text{Orta},$$

$$I(\text{Arc Speaker Sonos}) = \text{Düşük Kritiklik},$$

$$D(\text{Arc Speaker Sonos}) = \text{Kullanıcıya Sor}$$

$$L(\text{Samsung SmartTV}) = \text{Orta},$$

$$I(\text{Samsung SmartTV}) = \text{Yüksek Kritik},$$

$$D(\text{Samsung SmartTV}) = \text{Reddet}$$

$L(\text{Google Home}) = \text{Düşük},$

$I(\text{Google Home}) = \text{Yüksek Kritik},$

$D(\text{Google Home}) = \text{Kullanıcıya Sor}$

Örnek akıllı evimiz için tanımlanmış mahremiyet politikasına göre, "İzin Ver" kararı bulunmadığında ancak "Kullanıcıya Sor" kararı mevcutsa, politika, işlemin gerçekleştirilmesinden önce kullanıcı onayını gerektirecektir. Bu nedenle, sistem Mary'den müziği ya Arc Speaker Sonos ya da Google Home üzerinden çalması için onay isteyecektir.

4.4.2 Senaryo II

İkinci senaryoda, Tom'un rolü "genç"tir ve Amazon Echo kullanarak ışıkları açmak istemektedir. Ayrıca bu işlemi Philips Hue Hub ve Samsung SmartThings Hub aracılığıyla da gerçekleştirebilir. Veri setine [19] göre, Amazon Echo, işlevselliğini sağlamak için "İsim, Adres, E-posta, Ülke, Takma Ad, Telefon, Davranışsal Veri, Hassas Veri, Posta Kodu, Kredi Kartı Bilgileri ve Konum" bilgilerini kullanıcıdan toplamaktadır. Değerlendirmemiz, Çizelge 4.2'ta belirtildiği üzere, bu bilgilerin en yüksek ifşa etkisinin "Yüksek Kritik" olduğunu göstermektedir. Philips Hue Hub kullanıldığında ise "İsim, E-posta, Ülke, Doğum Tarihi, Üçüncü Taraf Verileri, Dil ve Alışveriş Verileri" toplanmaktadır. Bu bilgilerin en yüksek ifşa etkisi "Orta Kritik" olarak değerlendirilmiştir. Son olarak, Samsung SmartThings Hub kullanıldığında "İsim, Adres, E-posta, Ülke, Telefon, Posta Kodu, Ürün Kullanımı, Ses, Üçüncü Taraf Verileri, Kredi Kartı Bilgileri, Fatura Bilgileri ve Konum" bilgileri gerekmektedir. Bu bilgilerin en yüksek ifşa etkisi de "Yüksek Kritik" olarak tanımlanmıştır.

Değerlendirmemizin ikinci aşamasında, ilişkili cihazların genel puanına dayanarak ifşa olasılığı değerlendirilmiştir [5]. Çizelge 4.3'da görülebileceği üzere, Samsung SmartThings Hub'ın genel puanı B (Düşük), Amazon Echo'nun genel puanı C (Orta) ve Philips Hue Hub'ın genel puanı A (Çok Düşük) olarak belirlenmiştir. Tom'un mahremiyet pro-

fili ve Çizelge 4.7’da belirtilen ergen kullanıcı profiline dayanarak mahremiyet riskini değerlendirirken, üç cihaz için aşağıdaki olasılık, etki ve mahremiyet onay kararları elde edilmiştir.

$L(\text{Amazon Echo}) = \text{Orta},$

$I(\text{Amazon Echo}) = \text{Yüksek Kritik},$

$D(\text{Amazon Echo}) = \text{Reddet}$

$L(\text{Samsung SmartThings Hub}) = \text{Düşük},$

$I(\text{Samsung SmartThings Hub}) = \text{Yüksek Kritik},$

$D(\text{Samsung SmartThings Hub}) = \text{Kullanıcıya Sor}$

$L(\text{Philips Hue Hub}) = \text{Çok Düşük},$

$I(\text{Philips Hue Hub}) = \text{Orta Kritik},$

$D(\text{Philips Hue Hub}) = \text{İzin Ver}$

Mahremiyet politikamıza göre, mevcut cihazlar arasında herhangi bir izin verilen mahremiyet onayı varsa, kullanıcı bu cihazla işlemi gerçekleştirecektir, bu durumda Tom ışıkları Philips Hue Hub aracılığıyla açmaktadır.

4.4.3 Senaryo I için XACML Uygulaması

RBP-AeABAC yaklaşımında, akıllı ev cihazları için mahremiyet politikalarının uygulanması ve yönetilmesi amacıyla Genişletilebilir Erişim Kontrol İşaretleme Dili (XACML) kullanılmaktadır. XACML, niteliğe dayalı erişim kontrolü yetenekleri ile bilinip, kullanıcı öznitelikleri, kaynak öznitelikleri, çevre öznitelikleri ve eylemler temelinde dinamik olarak değişen ayrıntılı politikaların tanımlanmasına olanak tanır. Önceki bölümde yapılan geliştirmeye [14] dayanılarak, mahremiyet kararları ile birlikte ifşa etkisi ve ifşa olasılığının başka bir kaynak özniteliği olarak tanımlanarak akıllı ev ortamında gü-

venlik ve mahremiyet sağlanmaktadır. Politika bileşenlerinin, eş, çocuk, genç, bakıcı ve misafir gibi çeşitli kullanıcı profillerini, cihaz özniteliklerini ve kullanıcı özniteliklerini içerdiği ifade edilmektedir. Senaryoların XACML'de uygulanması için Security Policy Tool kullanılmaktadır. Mahremiyet kararları esas olarak kullanıcı rolleri, cihaz işlevsellikleri, ifşa etkisi ve ifşa olasılığına dayanmaktadır. Senaryoda, farklı profillere sahip kullanıcıların, müzik çalma gibi işlevlerin kontrol edildiği Google Home ve Arc Speaker Sonos gibi çeşitli cihazlarla etkileşimde bulunduğu belirtilir. XACML politikaları, ifşa etkisi ve ifşa olasılığı gibi faktörler dahil edilerek erişim kararlarının güvenliği ve kullanıcı iznini dikkate alacak şekilde oluşturulur. Ayrıca, XACML'deki "Yükümlülükler" (Obligations) bileşen kullanılarak, ifşa etkisi ve ifşa olasılığına bağlı olarak bir cihazın işlevselliğinin mahremiyet endişeleri doğurması durumunda kullanıcı onayının dinamik olarak elde edilir.

Senaryo I'de, Mary müzik çalmak istemekte ve bunu üç cihazdan biri olan Arc Speaker Sonos, Samsung SmartTV ve Google Home kullanarak gerçekleştirebilmektedir. Politika bileşenleri, Kullanıcı, Kaynak, Çevresel ve Eylemler şu şekilde tanımlanmıştır:

- Kullanıcı: Cihazlara erişim sağlamaya çalışan kullanıcılar (örneğin, bebek bakıcıları).
- Kaynak: Cihazların kendisi (Arc Speaker Sonos, Samsung SmartTV, Google Home).
- Çevresel: Erişim isteği ile ilgili bağlamsal bilgiler (örneğin, günün saati, konum).
- Eylemler: Cihazlarda gerçekleştirilebilecek işlemler (örneğin, müzik çalma, ışıkları açma/kapatma).

Politika, her cihaz için erişim sağlarken mahremiyet risklerini değerlendirmek amacıyla ifşa etkisi ve ifşa olasılığını açıkça içermektedir. Bunlar, tam sayı türünde kaynak nitelikleri olarak tanımlanmıştır ve her biri çok düşük (1) ile yüksek (4) arasında değişmektedir. Her bir ifşa etkisi ve olasılık düzeyi ile ilgili izin verme ve reddetme kurallarına

yönelik politikalar, modülerlik sağlamak amacıyla farklı alt bölümlerde ifade edilmiştir. Tanımlanan bileşenlerle, Senaryo I'ye yansıyan üç kural içeren örnek bir XACML politika spesifikasyonu Ek 3'te sunulmuştur. Örnek politika aşağıdaki kuralları içermektedir:

- Arc Speaker Sonos için Kullanıcıya Sor Kuralı: Bakıcı rolündeki bir kullanıcıya Arc Speaker Sonos'a erişim izni verir, ancak kullanıcının onay için yönlendirilmesini gerektirir; bu durum XACML'deki 'Yükümlülükler' yapısı aracılığıyla uygulanmaktadır.
- Samsung SmartTV için Reddetme Kuralı: Bu kural, ifşa etkisi yüksek (4) ve ifşa olasılığı orta (3) olduğunda bakıcının cihaza erişemeyeceğini belirtmektedir.
- Google Home için Kullanıcıya Sor Kuralı: Bu kural, Google Home'a erişime izin verir, ancak ilk kuralda olduğu gibi kullanıcının onay için yönlendirilmesini gerektirmektedir.

4.4.4 Akıllı ev ortamına yeni bir cihaz eklenmesi

Akıllı ev ortamına yeni bir cihaz eklemek, hem kullanıcı mahremiyetini korumak hem de bu ortamın güvenliğini devam ettirmek açısından dikkatle yönetilmesi gereken bir süreçtir. Bu süreç, cihazın özelliklerinin, topladığı verilerin ve güvenlik açıklarının detaylı bir şekilde değerlendirilmesini gerektirir. Özellikle IoT ekosisteminde her cihaz, ortamın genel güvenliğine ve kullanıcıların kişisel veri mahremiyetine doğrudan etki edebilir. Aşağıdaki rehber, akıllı ev ortamına veri setimizde bulunmayan yeni bir cihaz eklendiğinde izlenmesi gereken adımları ve bu süreçte dikkat edilmesi gereken kritik noktaları açıklamaktadır.

- **Cihazın Temel Bilgilerinin Toplanması:** Ortama yeni bir cihaz eklenirken ilk yapılması gereken işlem, cihazla ilgili temel bilgileri toplamaktır. Bu bilgiler ge-

nellikle cihazın kutusundaki teknik dokümantasyondan, cihazın mobil uygulamasından ya da üretici web sitesinden elde edilebilir. Bu bilgiler en az şunları içermelidir:

- **Üretici Bilgileri:** Cihazın markası, modeli, üretici firma bilgileri.
- **Yazılım/Donanım Versiyonu:** Cihazın yazılım sürümü, donanım özellikleri, güncelleme destek durumu.
- **Bağlantı Protokolü:** Cihazın kullandığı kablosuz bağlantı protokolü (Wi-Fi, Zigbee, Bluetooth vb.).
- **Cihazın Güvenlik Puanının Belirlenmesi:** Cihazın güvenlik risklerinin değerlendirilmesi için bir güvenlik skoru oluşturulmalıdır. Bu tez kapsamında kullanılan YourThings projesine ek olarak IoT Security Foundation, Mozilla’s Privacy Not Included, Consumers Reports ve OWASP IoT Project gibi platformlar da cihazların güvenliğini değerlendirmektedir. Bu platformlar ve cihazların teknik dokümantasyonları kullanılarak aşağıdaki veriler toplanabilir:
 - **Şifreleme Yöntemleri:** Cihazın veri iletiminde hangi şifreleme protokollerini kullandığı (örneğin, AES-256, TLS 1.3), cihaz-uygulama, uygulama-bulut ve cihaz-bulut arasındaki veri iletiminin şifreli olup olmadığı
 - **Konfigürasyon Yöntemi** Cihazın varsayılan güvenlik ayarlarıyla kullanılıp kullanılmadığı, daha güvenli bir konfigürasyonu zorunlu hale getirip getirmediği
 - **Yazılım Güncelleme Sıklığı:** Üreticinin cihaz için güvenlik güncellemelerini ne sıklıkla sağladığı, bu güncellemelerin otomatik veya manuel yapıldığı
 - **Varsayılan Parola Durumu:** Cihazın varsayılan bir parolaya sahip olup olmadığı ve bu parolanın değiştirilebilir olup olmadığı
 - **Bilinen Güvenlik Açıkları:** Cihazın geçmişte bilinen güvenlik açıklarına sahip olup olmadığı ve bu açıkların nasıl ele alındığı

- **Mobil Uygulama Güvenliđi:** MobSF (Mobile Security Framework) veya IoT Inspector gibi güvenlik analiz araçlarının analiz sonuçları
- **Bulut Güvenliđi:** Cihazın bulut servis sağlayıcısının güvenlik sertifikasyonları, veri şifreleme yöntemleri ve üçüncü taraf erişim politikaları

gözden geçirilmelidir. Bu incelemeler sonucunda cihazın güvenlik durumu ile ilgili bilgi edinilmiş olur.

- **Cihazın Topladığı Verilerin Tespiti:** Cihazın hangi tür verileri topladığı (örneğin, ses verileri, video görüntüleri, konum bilgisi, biyometrik veriler) cihazın kullanıcı kılavuzlarından ve üreticinin mahremiyet politikalarından öğrenilir.

Yukarıda listelenen yöntemler sonucunda cihazın güvenlik durumu ile ilgili edinilen bilgiler ve cihazın topladığı veriler RBP-AeABAC modelindeki ifşa etkisi ve ifşa olasılık hesaplamalarına girdi olarak kullanılır. Daha sonra RBP-AeABAC modeli kapsamında oluşturulan mahremiyet profilleri ve politikalarına göre kullanıcı mahremiyet onay mekanizması işler.

5. SONUÇ VE ÖNERİLER

Tez kapsamında, nesnelerin interneti ve daha spesifik olarak akıllı evler için üç aşamada genişletilmiş bir AeABAC modeli önerilmiştir. İlk aşamada, literatürdeki çalışmalardan farklı olarak, kullanıcıların biyometrik sistemlerde kimlik doğrulaması sırasında elde ettikleri kimlik doğrulama eşleşme puanına (AMS) dayalı bir kimlik doğrulama güvence düzeyi belirlenmiştir. Bu puan, tanımlanmış eşik değerleri ile karşılaştırılarak kullanıcıya, rolüne ve kimlik doğrulama güvence düzeyine göre erişim kararları sunan ince taneli bir erişim kontrol modeli geliştirilmiştir.

İkinci aşamada, kimlik doğrulama puanının ölçümünde kullanılacak performans metrikleri incelenmiştir. Geleneksel olarak eşik değerlerine dayanan bu metrikler, AeABAC modelinde eşleştirme puanlarının fonksiyonları olarak kullanılmıştır. Kimlik doğrulama eşleşme puanlarının Yanlış Eşleşme Oranı (FMR) hesaplanmış ve sonuç Erişim Kararı Belirsizlik Puanı (ADUS) olarak tanımlanmıştır. Cihaz işlevselliği, kritiklik seviyesi açısından temel, önemli ve kritik olarak sınıflandırılarak, erişim kontrol politikaları ADUS, kullanıcı rolü ve talep edilen işlevin kategorisine göre oluşturulmuştur. Bu aşama, biyometrik kimlik doğrulamanın kullanıldığı IoT uygulamaları için daha uygun bir model sunarak AeABAC'ın uygulanabilirliğini göstermiştir.

Son aşamada, Risk Temelli Mahremiyet Yaklaşımı ile AeABAC modeli, RBP-AeABAC olarak genişletilmiştir. Önceki aşamalarda kimlik doğrulama ve yetkilendirilme ile sistemin kullanıcıya güveni üzerine odaklanılmıştır. Bu aşamada ise kullanıcının sisteme güveni ele alınmıştır. Kullanıcının yetkilendirildiği cihaz üzerindeki işlevi gerçekleştirirken cihazın kullanıcının hangi verilerini kullanacağını bilmesi ve mahremiyet risklerini anlaması önemlidir. Akıllı ev ekosistemlerinin karmaşıklığının artmasıyla birlikte kullanıcı mahremiyetini korumanın gerekliliği ön plana çıkmış, sistem ve kullanıcı arasında çift yönlü güvenin sağlanması kritik hale gelmiştir. Bu model, kimlik doğrulama ve yetkilendirme süreçlerinde kullanıcıya şeffaf ve bilgilendirici risk değerlendirmeleri

sunarak, çift yönlü güveni tesis etmektedir. RBP-AeABAC modeli, akıllı ev ortamındaki verilerin ifşa risklerini değerlendirirken, bu risklerin kullanıcılara olası zararlarını analiz etmeye odaklanmıştır. Mahremiyet tercihleri ve onay mekanizmaları ile kullanıcıların verilerinin güvenliğini sağlamak hedeflenmiştir.

Sonuç olarak, ifşa olasılığı ve ifşa etkisine odaklanan RBP-AeABAC modeli, kullanıcıların veri mahremiyeti ile ilgili daha bilinçli kararlar almasına yardımcı olmaktadır. Bu yenilikçi model, mahremiyet risklerini kullanıcı tanımlı profiller aracılığıyla değerlendirerek özelleştirilmiş mahremiyet koruması sunmakta ve kullanıcı güvenliğini artırmaktadır. Modelin akıllı ev senaryolarında uygulanması, kullanıcıların farklı cihazlarla ilgili mahremiyet risklerini daha iyi anlamalarını ve bu risklere göre bilinçli seçimler yapmalarını sağlamıştır. Böylelikle, kullanıcıların veri mahremiyeti ve hizmetleri kullanırken olası sonuçları hakkında farkındalıkları artırılmıştır.

Tez kapsamında sunulan bu çözümler, gelecekte daha büyük ölçekli IoT ortamlarında uygulanabilirlik açısından geliştirilerek incelenebilir.

KAYNAKLAR

- [1] **GDPR**, 2024.
- [2] **A BROADBAND INTERNET TECHNICAL ADVISORY GROUP**. Internet of Things (IoT) Security and Privacy Recommendations. Tech. Rep. November, 2016.
- [3] **ABRAHAM, A.** Mobile-Security-Framework-MobSF:README, 2016.
- [4] **AGHILI, S. F., SEDAGHAT, M., SINGELÉE, D., AND GUPTA, M.** MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme. *Future Generation Computer Systems* 131, January (2022), 75–90.
- [5] **ALRAWI, O., FAULKENBERRY, A., AND MONROSE, F.** *YourThings: A Comprehensive Annotated Dataset of Network Traffic from Deployed Home-based IoT Devices*, vol. 1. Association for Computing Machinery, 2022.
- [6] **AMEER, S., AND SANDHU, R.** The HABAC Model for Smart Home IoT and Comparison to EGRBAC. *SAT-CPS 2021 - Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems* (2021), 39–48.
- [7] **AMRAOUI, N., BESROUR, A., KSANTINI, R., AND ZOUARI, B.** Implicit and Continuous Authentication of Smart Home Users. *International Conference on Advanced Information Networking and Applications*, 1 (2019), 834–845.
- [8] **APTHORPE, N., SHVARTZSHNAIDER, Y., MATHUR, A., REISMAN, D., AND FEAMSTER, N.** Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (2018), 1–23.
- [9] **BAHIZAD, S.** Risks of Increase in the IoT Devices. *Proceedings - 2020 7th IEEE International Conference on Cyber Security and Cloud Computing and 2020 6th IEEE International Conference on Edge Computing and Scalable Cloud, CSCloud-EdgeCom 2020* (2020), 178–181.
- [10] **BARBOSA, N. M., ZHANG, Z., AND WANG, Y.** Do privacy and security matter to everyone? Quantifying and clustering user-centric considerations about smartll

home device adoption. *Proceedings of the 16th Symposium on Usable Privacy and Security, SOUPS 2020* (2020), 417–436.

- [11] **BERND, J., ABU-SALMA, R., AND FRIK, A.** Bystanders’ privacy: The perspectives of nannies on smart home surveillance. *FOCI 2020 - 10th USENIX Workshop on Free and Open Communications on the Internet, co-located with USENIX Security 2020* (2020).
- [12] **BEZAWADA, B., HAEFNER, K., AND RAY, I.** Securing Home IoT Environments with Attribute-Based Access Control. *Proceedings of the 3rd ACM Workshop on Attribute-Based Access Control, Co-located with CODASPY 2018* (2018), 43–53.
- [13] **BUGEJA, J., JACOBSSON, A., AND DAVIDSSON, P.** PRASH: A framework for privacy risk analysis of smart homes. *Sensors* 21, 19 (2021).
- [14] **BURAKGAZI BİLGİN, M., ABUL, O., AND BİCAKCI, K.** Authentication-enabled attribute-based access control for smart homes. *International Journal of Information Security* 22, 2 (2023), 479–495.
- [15] **BURAKGAZI BİLGİN, M., AND BİCAKCI, K.** Extending Attribute-Based Access Control Model with Authentication Information for Internet of Things. *2020 International Conference on Information Security and Cryptology, ISCTURKEY 2020 - Proceedings* (2020), 48–55.
- [16] **CATHEY, G., BENSON, J., GUPTA, M., AND SANDHU, R.** Edge Centric Secure Data Sharing with Digital Twins in Smart Ecosystems. *Proceedings - 2021 3rd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2021* (2021), 70–79.
- [17] **CHALHOUB, G., FLECHAIS, I., NTHALA, N., AND ABU-SALMA, R.** Innovation inaction or in action? The role of user experience in the security and privacy design of smart home cameras. *Proceedings of the 16th Symposium on Usable Privacy and Security, SOUPS 2020* (2020), 185–204.
- [18] **CHANG, S., AND NAM, K.** Smart home adoption: The impact of user characteristics and differences in perception of benefits. *Buildings* 11, 9 (2021).
- [19] **COLETI, T. A., BALANCIERI, R., MENOLLI, A., MAHMOUD, O. A., SOTTI, V. H., YVANO, M., AND MORANDINI, M.** Handling of Personal Data by Smart Home Equipment: an Exploratory Analysis in the Context of LGPD. *Journal on Interactive Systems* 15, 1 (2024), 311–322.
- [20] **COMMISSION, F. T.** FTC and DOJ Charge Amazon with Violating Children’s Privacy Law by Keeping Kids’ Alexa Voice Records, 2023.

- [21] DEWI, C., KENCANA, P., RIIS, H., AND VERSION, D. Modelling and Analysing Access Control Policies in XACML 3.0 Carroline. *Technical University of Denmark* (2015).
- [22] DHIR, V., SINGH, A., KUMAR, R., AND SINGH, G. Biometric Recognition: A Modern Era For Security. *International Journal of Engineering Science and Technology* 2, 8 (2010), 3364–3380.
- [23] DONG, Y., WAN, K., HUANG, X., AND YUE, Y. Contexts-States-Aware Access Control for Internet of Things. *Proceedings of the 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design, CSCWD 2018* (2018), 271–276.
- [24] DORIZZI, B., CAPPELLI, R., FERRARA, M., MAIO, D., MALTONI, D., HOMANI, N., GARCIA-SALICETTI, S., AND MAYOUE, A. Fingerprint and on-line signature verification competitions at icb 2009. *Proceedings International Conference on Biometrics (ICB) 5558 LNCS* (2009), 725–732.
- [25] DUNSTONE, T., AND YAGER, N. *Biometric System and Data Analysis Design, Evaluation, and Data Mining*. Springer, 2008.
- [26] EARP, J. B., ANTÓN, A. Í., AÍMAN-SMITH, L., AND STUFFLEBEAM, W. H. Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management* 52, 2 (2005), 227–237.
- [27] EMAMI-NAEINI, P., DIXON, H., AGARWAL, Y., AND CRANOR, L. F. Exploring how privacy and security factor into IoT device purchase behavior. *Conference on Human Factors in Computing Systems - Proceedings* (2019), 1–12.
- [28] FERNANDES, E., RAHMATI, A., EYKHOLT, K., AND PRAKASH, A. Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges? *IEEE Security and Privacy* 15, 4 (2017), 79–84.
- [29] FERRAILOLO, D., CHANDRAMOULI, R., KUHN, R., AND HU, V. Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). In *2016 ACM International Workshop* (New York, New York, USA, 2016), ACM Press, pp. 13–24.
- [30] FORCE, J. T. Risk Management Framework. 229–270.
- [31] GOYAL, G., LIU, P., AND SURAL, S. *Securing Smart Home IoT Systems with Attribute-Based Access Control*, vol. 1. Association for Computing Machinery, 2022.
- [32] GUPTA, M., AND SANDHU, R. *Towards activity-centric access control for smart collaborative ecosystems*, vol. 1. Association for Computing Machinery, 2021.

- [33] HANEY, J. M., FURMAN, S. M., AND ACAR, Y. Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 12210 LNCS (2020), 393–411.
- [34] HE, W., PADHI, R., OFEK, J., GOLLA, M., DÜRMUTH, M., FERNANDES, E., AND UR, B. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). *Usenix Sec* (2018).
- [35] HE, Y., BAHIRAT, P., KNIJNENBURG, B. P., AND MENON, A. A Data-Driven Approach to Designing for Privacy in Household IoT. *ACM Transactions on Interactive Intelligent Systems* 10, 1 (2020), 1–47.
- [36] [HTTPS://BIOLAB.CSR.UNIBO.IT/FVCONGOING/UI/FORM/PUBLISHEDALGS.ASPX](https://biolab.csr.unibo.it/FVCongoing/UI/Form/PublishedALGS.aspx). FVC-onGoing, 2022.
- [37] HU, V. C., FERRAILOLO, D., KUHN, R., SCHNITZER, A., SANDLIN, K., MILLER, R., AND SCARFONE, K. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. *NIST Special Publication* (2014).
- [38] HUAN1, K., ZHOU, Y. T., ZHANG, K., XU, J., CHEN, J., TANG, D., AND ZHANG, K. HOMESPY: The Invisible Sniffer of Infrared Remote Control of Smart TVs. *32nd USENIX Security Symposium, USENIX Security 2023* 7 (2023), 4553–4570.
- [39] KELLEY, P. G., CRANOR, L. F., AND SADEH, N. Privacy as part of the app decision-making process. *Conference on Human Factors in Computing Systems - Proceedings* (2013), 3393–3402.
- [40] KIRCHBUCHNER, F., GROSSE-PUPPENDAHL, T., HASTALL, M. R., DISTLER, M., AND KUIJPER, A. Ambient intelligence from senior citizens’ perspectives: Understanding privacy concerns, technology acceptance, and expectations. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9425, November (2015), 48–59.
- [41] KVK. Resmî Gazete. *Resmi Gazete*, 1 (2018), 30356.
- [42] LEE, H., AND KOBSA, A. Understanding user privacy in Internet of Things environments. *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016* (2016), 407–412.
- [43] LEE, S., KIM, J., LEE, S., TECH, G., KIM, H., AND KIM, J. FACT: Functionality-centric Access Control System for IoT Programming Frameworks. *SACMAT’17* (2017), 43–54.

- [44] **LI, J., ZONG, B., CHENG, T., LI, Y., MYNATT, E. D., AND DHEKNE, A.** Privacy vs. Awareness: Relieving the Tension between Older Adults and Adult Children When Sharing In-home Activity Data. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW2 (2023).
- [45] **LINKEDIN, Q.** linkedin/qark: Tool to look for several security related Android application vulnerabilities, 2019.
- [46] **MAIO, D., MALTONI, D., CAPPELLI, R., WAYMAN, J. L., AND JAIN, A. K.** FVC2002: Second fingerprint verification competition. *Proceedings - International Conference on Pattern Recognition* 16, 3 (2002), 811–814.
- [47] **MALKIN, N., WAGNER, D., AND EGELMAN, S.** Runtime Permissions for Privacy in Proactive Intelligent Assistants. *Proceedings of the 18th Symposium on Usable Privacy and Security, SOUPS 2022*, Soups (2022), 633–651.
- [48] **MANANDHAR, S., KAFLE, K., ANDOW, B., SINGH, K., AND NADKARNI, A.** Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage. *Proceedings of the 31st USENIX Security Symposium, Security 2022* (2022), 3521–3538.
- [49] **MAWLA, T., GUPTA, M., AND SANDHU, R.** *BlueSky: Activity Control: A Vision for "active" Security Models for Smart Collaborative Systems*, vol. 1. Association for Computing Machinery, 2022.
- [50] **MELL, P., SCARFONE, K., AND ROMANOSKY, S.** Common vulnerability scoring system, 2006.
- [51] **NAEINI, P. E., BHAGAVATULA, S., HABIB, H., DEGELING, M., BAUER, L., CRANOR, L., SADEH, N., CLARA, S., EMAMI-NAEINI, P., BHAGAVATULA, S., HABIB, H., DEGELING, M., BAUER, L., CRANOR, L. F., AND SADEH, N.** The Proceedings of the Privacy Expectations and Preferences in an IoT World. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, Soups (2017).
- [52] **NAIK, S., AND MARAL, V.** Cyber security - IoT. *RTEICT 2017 - 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, Proceedings 2018-Janua* (2018), 764–767.
- [53] **NUMBER OF INTERNET OF THINGS (IoT) CONNECTED DEVICES WITH FORECASTS FROM 2022 TO 2030.** Statista, 2024.
- [54] **OASIS.** eXtensible Access Control Markup Language. *OASIS Standard*, January (2013), 154.

- [55] OUADDAH, A., MOUSANNIF, H., ABOU ELKALAM, A., AND AÏT OUAHMAN, A. Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks* 112 (2017), 237–262.
- [56] PRIEBE, T., DOBMEIER, W., SCHLÄGER, C., AND KAMPRATH, N. Supporting attribute-based access control in authorization and authentication infrastructures with ontologies. *Journal of Software* 2, 1 (2007), 27–38.
- [57] RATH, A. T., AND COLIN, J. N. Strengthening access control in case of compromised accounts in smart home. *International Conference on Wireless and Mobile Computing, Networking and Communications 2017-Octob* (2017), 1–8.
- [58] RATH, T. A., AND COLIN, J. N. Adaptive Risk-Aware Access Control Model for Internet of Things. In *Proceedings - 2017 International Workshop on Secure Internet of Things* (2018), SIoT 2017 (2018), pp. 40–49.
- [59] RISTO, J. What is CVSS - Common Vulnerability Scoring System, 2023.
- [60] SIKDER, A. K., BABUN, L., CELİK, Z. B., AKSU, H., MCDANIEL, P., KIRDA, E., AND ULUAGAC, A. S. Who’s Controlling My Device? Multi-User Multi-Device-Aware Access Control System for Shared Smart Home Environment. *ACM Transactions on Internet of Things* 3, 4 (2022).
- [61] SINGH, D., PSYCHOULA, İ., KROPE, J., HANKE, S., AND HOLZINGER, A. Users’ perceptions and attitudes towards smart home technologies. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10898 LNCS, June (2018), 203–214.
- [62] SONG, L., LI, M., ZHU, Z., YUAN, P., AND HE, Y. Attribute-Based Access Control Using Smart Contracts for the Internet of Things. *Procedia Computer Science* 174, 2019 (2020), 231–242.
- [63] STURGESS, J., NURSE, J. R., AND ZHAO, J. A capability-oriented approach to assessing privacy risk in smart home ecosystems. *IET Conference Publications* 2018, CP740 (2018), 1–8.
- [64] SUGRIM, S., LIU, C., MCLEAN, M., AND LINDQVIST, J. Robust Performance Metrics for Authentication Systems. *Network and Distributed Systems Security (NDSS) Symposium 2019*, February (2019).
- [65] SUN, K., AND YIN, L. Attribute-Role-Based Hybrid Access Control. *APWeb 2014 Workshops*, 61100181 (2014), 333–343.
- [66] SUN, P., SHEN, S., WAN, Y., WU, Z., FANG, Z., AND ZHI GAO, X. A Survey of IoT Privacy Security: Architecture, Technology, Challenges, and Trends. *IEEE Internet of Things Journal PP*, X (2024), 1.

- [67] VAN OORSCHOT, P. C. Internet of things security: Is Anything New? *IEEE Security and Privacy* 16, 5 (2018), 3–5.
- [68] VETRIVEL, S., VAN HARTEN, V., GAÑÁN, C. H., VAN EETEN, M., AND PARKIN, S. Examining Consumer Reviews to Understand Security and Privacy Issues in the Market of Smart Home Devices. *32nd USENIX Security Symposium, USENIX Security 2023* 3 (2023), 1523–1540.
- [69] YALCINKAYA, E., MAFFEI, A., AND ONORI, M. Application of Attribute Based Access Control Model for Industrial Control Systems. *International Journal of Computer Network and Information Security* 9, 2 (2017), 12–21.
- [70] YASSINE, I., HALABI, T., AND BELLAÏCHE, M. Security Risk Assessment Methodologies in The Internet of Things: Survey and Taxonomy. *Proceedings - 2021 21st International Conference on Software Quality, Reliability and Security Companion, QRS-C 2021* (2021), 668–675.
- [71] YE, N., ZHU, Y., WANG, R. C., MALEKIAN, R., AND LIN, Q. M. An efficient authentication and access control scheme for perception layer of internet of things. *Applied Mathematics and Information Sciences* 8, 4 (2014), 1617–1624.
- [72] ZANG, J., DUMMIT, K., GRAVES, J., LISKER, P., AND SWEENEY, L. Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps. *Technology Science 2015103001* (2015).
- [73] ZENG, E., MARE, S., ROESNER, F., CLARA, S., ZENG, E., MARE, S., AND ROESNER, F. End User Security and Privacy Concerns with Smart Homes T. *Thirteenth Symposium on Usable Privacy and Security (SOUPS)*, Soups (2017), 65–80.
- [74] ZENG, E., AND ROESNER, F. Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. *Proceedings of the 28th USENIX Security Symposium* (2019), 159–176.
- [75] ZHANG, Y., AND WU, X. Access Control in Internet of Things: A Survey. *DEStech Transactions on Engineering and Technology Research*, apetc (2018).
- [76] ZHAO, Y., YAO, Y., FU, J., AND ZHOU, N. If sighted people know, I should be able to know:" Privacy Perceptions of Bystanders with Visual Impairments around Camera-based Technology. *32nd USENIX Security Symposium, USENIX Security 2023* 7 (2023), 4661–4678.
- [77] ZIMMERMANN, V., GERBER, P., MARKY, K., BÖCK, L., AND KIRCHBUCHNER, F. Assessing users' privacy and security concerns of smart home technologies. *I-Com* 18, 3 (2020), 197–216.

EKLER

EK 1 Kritik işlevlere yansıtılmış dört izin kuralını içeren örnek bir politika belirtimi

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="
  urn:infobeyondtech:securitypolicytool:smartHome.
  spt:ABAC:CriticalPermitsPolicy" RuleCombiningAlgId="
  urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:ordered-deny-
  overrides" Version="1.0">
  <Target></Target>
  <Rule Effect="Permit" RuleId="rule_1">
    <Target>
      <AnyOf>
        <AllOf>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
            w3.org/2001/xmlschema#string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
              string">Spouse</AttributeValue>
            <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
              ::subjectcategory:accesssubject" AttributeId="
              urn:oasis:names:tc:xacml:1.0:subject:Role" DataType="http://
              www.w3.org/2001/XMLSchema#string" MustBePresent="true"></
              AttributeDesignator>
          </Match>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
            w3.org/2001/xmlschema#string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
              string">Xiaomi Mi Home Security Camera</AttributeValue>
            <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
              ::attributecategory:resource" AttributeId="
              urn:oasis:names:tc:xacml:1.0:resource:SecurityCamera"
              DataType="http://www.w3.org/2001/XMLSchema#string"
              MustBePresent="true"></AttributeDesignator>
          </Match>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
            w3.org/2001/xmlschema#string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
              string">Camera ON/OFF</AttributeValue>
            <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
              ::attributecategory:action" AttributeId="
              urn:oasis:names:tc:xacml:1.0:action:Critical Functionalities
              " DataType="http://www.w3.org/2001/XMLSchema#string"
              MustBePresent="true"></AttributeDesignator>
          </Match>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
            w3.org/2001/xmlschema#string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
              string">Strong FMR</AttributeValue>
            <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
              ::attributecategory:environment" AttributeId="
              urn:oasis:names:tc:xacml:1.0:environment:Access Decision
```

```

        Score" DataType="http://www.w3.org/2001/XMLSchema#string"
        MustBePresent="true"></AttributeDesignator>
    </Match>
    <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
        w3.org/2001/xmlschema#string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
            string">At Home</AttributeValue>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
            ::attributecategory:environment" AttributeId="
            urn:oasis:names:tc:xacml:1.0:environment:Location" DataType=
            "http://www.w3.org/2001/XMLSchema#string" MustBePresent="
            true"></AttributeDesignator>
    </Match>
</AllOf>
</AnyOf>
</Target>
</Rule>
<Rule Effect="Permit" RuleId="rule_2">
    <Target>
        <AnyOf>
            <AllOf>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
                    w3.org/2001/xmlschema#string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                        string">Teenage</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
                        ::subjectcategory:accesssubject" AttributeId="
                        urn:oasis:names:tc:xacml:1.0:subject:Role" DataType="http://
                        www.w3.org/2001/XMLSchema#string" MustBePresent="true"></
                        AttributeDesignator>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
                    w3.org/2001/xmlschema#string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                        string">Xiaomi Mi Home Security Camera</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
                        ::attributecategory:resource" AttributeId="
                        urn:oasis:names:tc:xacml:1.0:resource:SecurityCamera"
                        DataType="http://www.w3.org/2001/XMLSchema#string"
                        MustBePresent="true"></AttributeDesignator>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
                    w3.org/2001/xmlschema#string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                        string">Camera ON/OFF</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
                        ::attributecategory:action" AttributeId="
                        urn:oasis:names:tc:xacml:1.0:action:Critical Functionalities
                        " DataType="http://www.w3.org/2001/XMLSchema#string"
                        MustBePresent="true"></AttributeDesignator>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
                    w3.org/2001/xmlschema#string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                        string">Strong FMR</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
                        ::attributecategory:environment" AttributeId="
                        urn:oasis:names:tc:xacml:1.0:environment:Access Decision

```

```

        Score" DataType="http://www.w3.org/2001/XMLSchema#string"
        MustBePresent="true"></AttributeDesignator>
    </Match>
    <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
        w3.org/2001/xmlschema#string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
            string">At Home</AttributeValue>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
            ::attributecategory:environment" AttributeId="
            urn:oasis:names:tc:xacml:1.0:environment:Location" DataType=
            "http://www.w3.org/2001/XMLSchema#string" MustBePresent="
            true"></AttributeDesignator>
    </Match>
</AllOf>
</AnyOf>
</Target>
</Rule>
<Rule Effect="Permit" RuleId="rule_3">
    <Target>
        <AnyOf>
            <AllOf>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
                    w3.org/2001/xmlschema#string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                        string">Teenage</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
                        ::subjectcategory:accesssubject" AttributeId="
                        urn:oasis:names:tc:xacml:1.0:subject:Role" DataType="http://
                        www.w3.org/2001/XMLSchema#string" MustBePresent="true"></
                        AttributeDesignator>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
                    w3.org/2001/xmlschema#string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                        string">Google Home</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
                        ::attributecategory:resource" AttributeId="
                        urn:oasis:names:tc:xacml:1.0:resource:VoiceAssistant"
                        DataType="http://www.w3.org/2001/XMLSchema#string"
                        MustBePresent="true"></AttributeDesignator>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
                    w3.org/2001/xmlschema#string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                        string">Online Shopping</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
                        ::attributecategory:action" AttributeId="
                        urn:oasis:names:tc:xacml:1.0:action:Critical Functionalities
                        " DataType="http://www.w3.org/2001/XMLSchema#string"
                        MustBePresent="true"></AttributeDesignator>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
                    w3.org/2001/xmlschema#string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                        string">At Home</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
                        ::attributecategory:environment" AttributeId="
                        urn:oasis:names:tc:xacml:1.0:environment:Location" DataType=

```



```

        "http://www.w3.org/2001/XMLSchema#string" MustBePresent="
        true"></AttributeDesignator>
    </Match>
    <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
        w3.org/2001/xmlschema#string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
            string">Strong FMR</AttributeValue>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
            ::attributecategory:environment" AttributeId="
            urn:oasis:names:tc:xacml:1.0:environment:Access Decision
            Score" DataType="http://www.w3.org/2001/XMLSchema#string"
            MustBePresent="true"></AttributeDesignator>
    </Match>
</AllOf>
</AnyOf>
</Target>
</Rule>
<Rule Effect="Permit" RuleId="rule_4">
    <Target>
        <AnyOf>
            <AllOf>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
                    w3.org/2001/xmlschema#string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                        string">Spouse</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
                        ::subjectcategory:accesssubject" AttributeId="
                        urn:oasis:names:tc:xacml:1.0:subject:Role" DataType="http://
                        www.w3.org/2001/XMLSchema#string" MustBePresent="true"></
                        AttributeDesignator>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
                    w3.org/2001/xmlschema#string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                        string">Google Home</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
                        ::attributecategory:resource" AttributeId="
                        urn:oasis:names:tc:xacml:1.0:resource:VoiceAssistant"
                        DataType="http://www.w3.org/2001/XMLSchema#string"
                        MustBePresent="true"></AttributeDesignator>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
                    w3.org/2001/xmlschema#string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                        string">Online Shopping</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
                        ::attributecategory:action" AttributeId="
                        urn:oasis:names:tc:xacml:1.0:action:Critical Functionalities
                        " DataType="http://www.w3.org/2001/XMLSchema#string"
                        MustBePresent="true"></AttributeDesignator>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
                    w3.org/2001/xmlschema#string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
                        string">At Home</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
                        ::attributecategory:environment" AttributeId="
                        urn:oasis:names:tc:xacml:1.0:environment:Location" DataType=

```

```

        " http://www.w3.org/2001/XMLSchema#string" MustBePresent="
        true"></AttributeDesignator>
    </Match>
    <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:http://www.
        w3.org/2001/xmlschema#string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#
            string">Strong FMR</AttributeValue>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0
            ::attributecategory:environment" AttributeId="
            urn:oasis:names:tc:xacml:1.0:environment:Access Decision
            Score" DataType="http://www.w3.org/2001/XMLSchema#string"
            MustBePresent="true"></AttributeDesignator>
    </Match>
</AllOf>
</AnyOf>
</Target>
</Rule>
</Policy>

```



EK 2:

Senaryo 1 için örnek bir politikanın XACML'de belirtimi

```
<?xml version="1.0" encoding="UTF-8"?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
  PolicySetId="urn:infobeyondtech:securitypolicytool:SmartHome:Scenario1"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable"
  Version="1.0">

  <Description>This PolicySet governs the access permissions for the babysitter role to various
    devices in a smart home setup.</Description>

  <PolicyIssuer>
    <Attribute AttributeId="issuer" IncludeInResult="false">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">SmartHomePrivacy</
        AttributeValue>
    </Attribute>
  </PolicyIssuer>

  <PolicySetDefaults>
    <XPathVersion>http://www.w3.org/2001/XMLSchema#XPath</XPathVersion>
  </PolicySetDefaults>

  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Babysitter</
            AttributeValue>
          <AttributeDesignator AttributeId="subject:role"
            Category="urn:oasis:names:tc:xacml:1.0:subject-
              category:access-subject"
            DataType="http://www.w3.org/2001/XMLSchema#string"
            MustBePresent="true"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>

  <!-- Policy for the babysitter role for playing music -->
  <Policy PolicyId="babysitter-role-policy"
    Version="1.0"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
      overrides">

    <Target>
      <AnyOf>
        <AllOf>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              Babysitter</AttributeValue>
            <AttributeDesignator AttributeId="subject:role"
              Category="urn:oasis:names:tc:xacml:1.0:subject-
                category:access-subject"
              DataType="http://www.w3.org/2001/XMLSchema#string"
              MustBePresent="true"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Policy>
</PolicySet>
```

```

    </AnyOf>
</Target>

<!-- Rule for Arc Speaker Sonos -->
<Rule Effect="Permit" RuleId="rule_arc_speaker_sonos">
    <Target>
        <AnyOf>
            <AllOf>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        Babysitter</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:subject-
                        category:access-subject"
                        AttributeId="urn:oasis:names:tc:xacml:1.0
                            :subject:Role"
                        DataType="http://www.w3.org/2001/XMLSchema#string"
                        MustBePresent="true"/>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Arc
                        Speaker Sonos</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:resource"
                        AttributeId="urn:oasis:names:tc:xacml:1.0
                            :resource:Device"
                        DataType="http://www.w3.org/2001/XMLSchema#string"
                        MustBePresent="true"/>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        Playing Music</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:resource"
                        AttributeId="urn:oasis:names:tc:xacml:1.0
                            :resource:Functionality"
                        DataType="http://www.w3.org/2001/XMLSchema#string"
                        MustBePresent="true"/>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">2</
                        AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:resource"
                        AttributeId="urn:oasis:names:tc:xacml:1.0
                            :resource:DisclosureImpact"
                        DataType="http://www.w3.org/2001/XMLSchema#integer
                            "
                        MustBePresent="true"/>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">3</
                        AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:resource"
                        AttributeId="urn:oasis:names:tc:xacml:1.0
                            :resource:DisclosureLikelihood"
                        DataType="http://www.w3.org/2001/XMLSchema#integer
                            "

```

```

MustBePresent=" true " />
    </Match>
  </AllOf>
</AnyOf>
</Target>

<!-- Ask the User -->
<ObligationExpressions>
  <ObligationExpression ObligationId="urn:oasis:names:tc:xacml:obligation:request -
    user-consent" FulfillOn="Permit">
    <!-- Set the "consent-required" attribute to "true" -->
    <AttributeAssignmentExpression AttributeId="
      urn:oasis:names:tc:xacml:attribute:consent-required">
      <AttributeValue DataType=" http://www.w3.org/2001/XMLSchema#string "
        >true</ AttributeValue>
    </ AttributeAssignmentExpression>
  </ObligationExpression>
</ObligationExpressions>
</Rule>

<!-- Rule for Samsung SmartTV -->
<Rule Effect="Deny" RuleId="rule_samsung_smarttv">
  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType=" http://www.w3.org/2001/XMLSchema#string ">
            Babysitter</ AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:subject -
            category:access-subject"
            AttributeId="urn:oasis:names:tc:xacml:1.0
              :subject:Role "
            DataType=" http://www.w3.org/2001/XMLSchema#string "
            MustBePresent=" true " />
        </Match>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType=" http://www.w3.org/2001/XMLSchema#string ">
            Samsung SmartTV</ AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute -
            category:resource"
            AttributeId="urn:oasis:names:tc:xacml:1.0
              :resource:Device "
            DataType=" http://www.w3.org/2001/XMLSchema#string "
            MustBePresent=" true " />
        </Match>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType=" http://www.w3.org/2001/XMLSchema#string ">
            Playing Music</ AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute -
            category:resource"
            AttributeId="urn:oasis:names:tc:xacml:1.0
              :resource:Functionality "
            DataType=" http://www.w3.org/2001/XMLSchema#string "
            MustBePresent=" true " />
        </Match>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-equal">
          <AttributeValue DataType=" http://www.w3.org/2001/XMLSchema#integer ">4</
            AttributeValue>

```

```

        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute -
            category:resource"
                AttributeId="urn:oasis:names:tc:xacml:1.0
                    :resource:DisclosureImpact"
                DataType="http://www.w3.org/2001/XMLSchema#integer"
                MustBePresent="true"/>
    </Match>
    <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">3</
            AttributeValue>
        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute -
            category:resource"
                AttributeId="urn:oasis:names:tc:xacml:1.0
                    :resource:DisclosureLikelihood"
                DataType="http://www.w3.org/2001/XMLSchema#integer"
                MustBePresent="true"/>
    </Match>
</AllOf>
</AnyOf>
</Target>
</Rule>

<!-- Rule for Google Home Playing Music-->
<Rule Effect="Permit" RuleId="rule_google_home">
    <Target>
        <AnyOf>
            <AllOf>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        Babysitter</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:subject -
                        category:access-subject"
                            AttributeId="urn:oasis:names:tc:xacml:1.0
                                :subject:Role"
                            DataType="http://www.w3.org/2001/XMLSchema#string"
                            MustBePresent="true"/>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        Google Home</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute -
                        category:resource"
                            AttributeId="urn:oasis:names:tc:xacml:1.0
                                :resource:Device"
                            DataType="http://www.w3.org/2001/XMLSchema#string"
                            MustBePresent="true"/>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                        Playing Music</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute -
                        category:resource"
                            AttributeId="urn:oasis:names:tc:xacml:1.0
                                :resource:Functionality"
                            DataType="http://www.w3.org/2001/XMLSchema#string"
                            MustBePresent="true"/>
                </Match>
            </AllOf>
        </AnyOf>
    </Target>
</Rule>

```

```

    </Match>
    <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">4</
        AttributeValue>
      <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-
        category:resource"
        AttributeId="urn:oasis:names:tc:xacml:1.0
          :resource:DisclosureImpact"
        DataType="http://www.w3.org/2001/XMLSchema#integer"
        MustBePresent="true"/>
    </Match>
    <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:integer-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">2</
        AttributeValue>
      <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-
        category:resource"
        AttributeId="urn:oasis:names:tc:xacml:1.0
          :resource:DisclosureLikelihood"
        DataType="http://www.w3.org/2001/XMLSchema#integer"
        MustBePresent="true"/>
    </Match>
  </AllOf>
</AnyOf>
</Target>

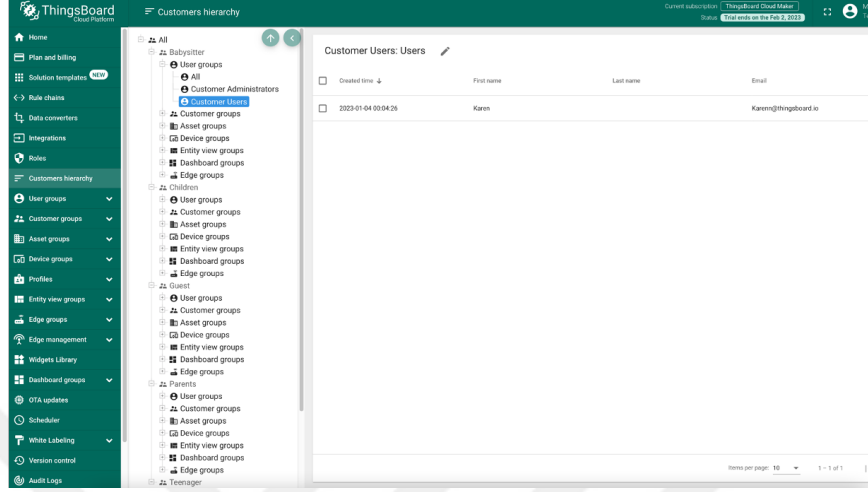
<!-- Ask the User -->
<ObligationExpressions>
  <ObligationExpression ObligationId="urn:oasis:names:tc:xacml:obligation:request-
    user-consent" FulfillOn="Permit">
    <!-- Set the "consent-required" attribute to "true" -->
    <AttributeAssignmentExpression AttributeId="
      urn:oasis:names:tc:xacml:attribute:consent-required">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
        >true</AttributeValue>
    </AttributeAssignmentExpression>
  </ObligationExpression>
</ObligationExpressions>

</Rule>
</Policy>
</PolicySet>

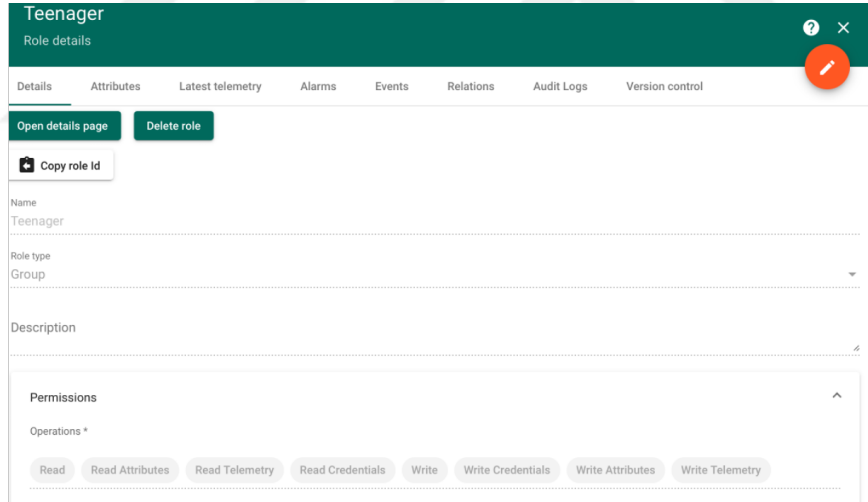
```

EK 3:

Yetişkin, eş ve çocuk rolündeki kullanıcıların ThingsBoard platformu üzerinde gösterge panelleri oluşturulmuştur. Eş rolündeki kullanıcıların bütün cihaz işlevlerine, bebek bakıcısının önemli ve temel işlevlere, çocukların temel işlevlere eriştiğini gösteren ilgili gösterge panelleri aşağıda sunulmuştur.



Şekil EK 3.1: ThingsBoard Ortam Bileşenleri



Şekil EK 3.2: Yetişkin Rolü Yetkilendirme

Parent

Role details

?

×

✎

Details

Attributes

Latest telemetry

Alarms

Events

Relations

Audit Logs

Version control

Open details page

Delete role

✎ Copy role Id

Name

Parent

Role type

Group

Description

Permissions

Operations *

All

Şekil EK 3.3: Eş Rolü Yetkilendirme

Child

Role details

?

×

✎

Details

Attributes

Latest telemetry

Alarms

Events

Relations

Audit Logs

Version control

Open details page

Delete role

✎ Copy role Id

Name

Child

Role type

Group

Description

Permissions

Operations *

Read

Read Attributes

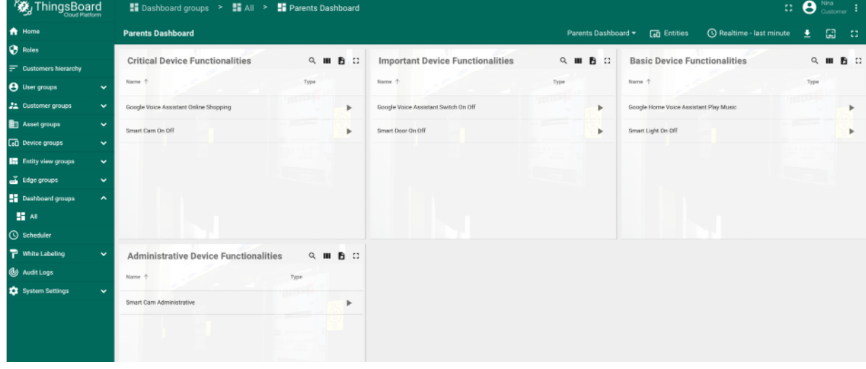
Read Credentials

Read Telemetry

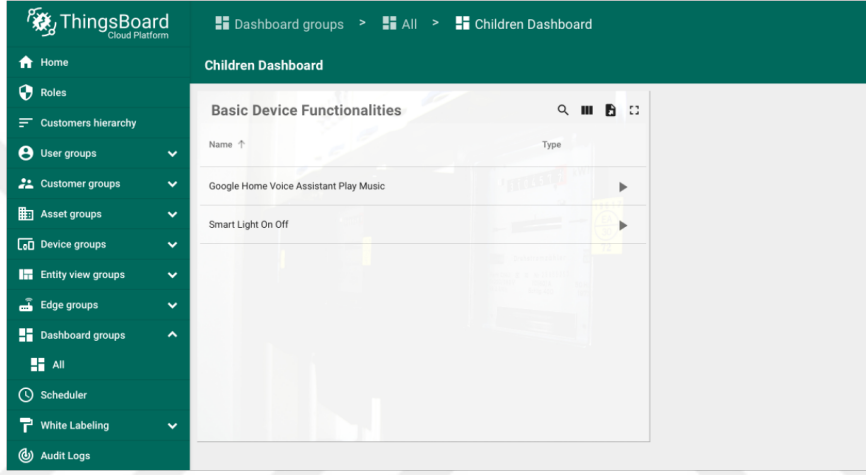
Şekil EK 3.4: Çocuk Rolü Yetkilendirme

Shared Devices: Devices ✎		
☐	Created time ↓	Device profile
☐	2023-01-03 23:57:58	Smart Light On Off
☐	2023-01-03 23:57:26	Smart Door On Off
☐	2023-01-03 23:55:30	Google Home Voice Assistant Play Music
☐	2023-01-03 23:54:30	Smart Cam Administrative
☐	2023-01-03 23:54:13	Smart Cam On Off
☐	2023-01-03 23:53:13	Google Voice Assistant Switch On Off
☐	2023-01-03 23:52:44	Google Voice Assistant Online Shopping

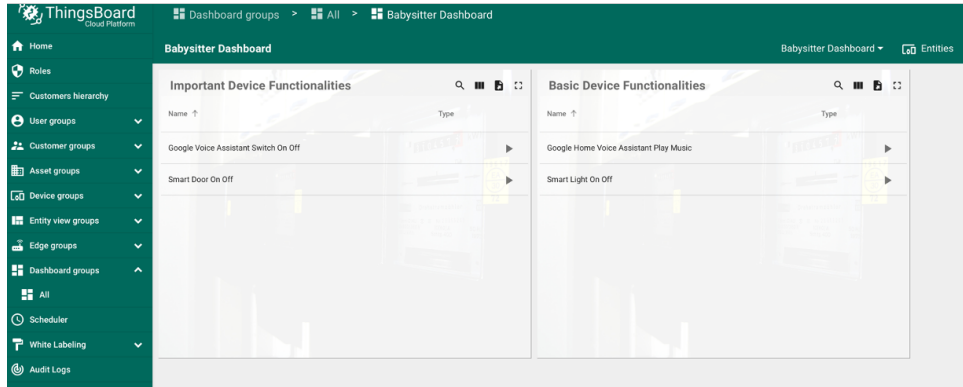
Şekil EK 3.5: Akıllı Cihaz İşlevleri ve Kritiklik Seviyeleri



Şekil EK 3.6: Eş Rolü Gösterge Paneli



Şekil EK 3.7: Çocuk Rolü Gösterge Paneli



Şekil EK 3.8: Bebek Bakıcı Rolü Gösterge Paneli