T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

AKILLI EV ORTAMLARINA YÖNELİK GDPR İLE UYUMLU HİBRİT DOĞRULAMA SİSTEMİ

Hisham Raad Jafer MERZEH

DOKTORA TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

Danışman

Prof. Dr. Hasan Hüseyin BALIK

Eş Danışman

Doç. Dr. Muhammed Ali AYDIN

Aralık, 2022

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

AKILLI EV ORTAMLARINA YÖNELİK GDPR İLE UYUMLU HİBRİT DOĞRULAMA SİSTEMİ

Hisham MERZEH tarafından hazırlanan tez çalışması 23.12.2022 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği Programı **DOKTORA TEZİ** olarak kabul edilmiştir.

Prof. Dr. Hasan Hüseyin BALIK Yıldız Teknik Üniversitesi Danışman	Doç. Dr. Muhammed Ali AYDIN İstanbul Üniversitesi-Cerrahpaşa Eş-Danışman

Jüri Üyeleri

Prof. Dr. Hasan Hüseyin BALIK, Danışman
Yıldız Teknik Üniversitesi _____

Prof. Dr. NİZAMETTİN AYDIN, Üye
Yıldız Teknik Üniversitesi _____

Prof. Dr. OĞUZ BAYAT, Üye
Altınbaş Üniversitesi _____

Prof. Dr. SIRMA YAVUZ, Üye
Yıldız Teknik Üni _____

Doç. Dr. CAN EYÜPOĞLU, Üye
Milli Savunma Üniversitesi _____

Danışmanım Prof. Dr. Hasan Hüseyin BALIK sorumluluğunda tarafımca hazırlanan GDPR Uyumlu IoT Akıllı Ev Kimlik Doğrulama Sistemi başlıklı çalışmada veri toplama ve veri kullanımında gerekli yasal izinleri aldığımı, diğer kaynaklardan aldığım bilgileri ana metin ve referanslarda eksiksiz gösterdiğimi, araştırma verilerine ve sonuçlarına ilişkin çarpıtma ve/veya sahtecilik yapmadığımı, çalışmam süresince bilimsel araştırma ve etik ilkelerine uygun davrandığımı beyan ederim. Beyanımın aksinin ispatı halinde her türlü yasal sonucu kabul ederim.

Hisham R. J. MERZEH

İmza

Babama

Anneme

ve

Biricik Eşime

TEŞEKKÜR

Words cannot express my gratitude to my supervisor Prof. Dr. Hasan Hüseyin BALIK for his dedicated support and guidance. He continuously provided encouragement and was always willing and enthusiastic to assist in any way he could throughout the Ph.D study. I cannot forget the extreme support that is provided by Doç. Dr. Muhammed Ali AYDIN and Dr. Mustafa KARA during the research period in all its stages, Special thanks to them. I am also grateful to my father and my mother for their support throughout my life. Their continued support is invaluable. My thanks and gratitude go to the dearest persons to my heart my wife and my daughters, for their continued support in the past, present and the future. Thank you for enduring all the hardships and standing by me through good times and hard times. Finally, I would like to mention all the friends and people who support and encouraged me to move forward.

Thank you all from the bottom of my heart…

Hisham MERZEH

İÇİNDEKİLER

SİMGE LİSTESİ vi

KISALTMA LİSTESİ ix

ŞEKİL LİSTESİ xi

TABLO LİSTESİ xii

ÖZET xiii

ABSTRACT xv

1 GİRİŞ 1

1.1 Giriş 1

1.2 Tezin Amacı 5

1.3 Orijinal Katkı 6

2 TEMEL TEKNİK ALTYAPI 7

2.1 Nesnelerin İnterneti (IoT) 7

2.2 QR kodu 12

2.3 Gizlilik ve Genel Veri Koruma Yönetmeliği (GDPR) 12

2.4 Bulanıklık Ayıklayıcı (Fuzzy Extractor) 15

2.5 Grup imzası 16

2.6 Kimlik Doğrulama 17

2.7 Blokzincir 21

2.8 Literatür Araştırması 22

3 METODOLOJİ 27

3.1 Akıllı Ev Sistemi Modeli 27

3.2 Çevrimdışı Doğrudan Mod için Önerilen Model 32

3.3 Çevrimiçi Mod için Önerilen Şeması 39

3.4 Sistem entegrasyonu 47

4 SONUÇ VE ANALİZ 49

4.1 Giriş 49

4.2 Güvenlik Analizi 49

4.3 AVISPA kullanarak Resmi Doğrulama 50

4.4 Deneysel Sonuçlar 51

4.5 Performans Değerlendirmesi 55

5 SONUÇ VE ÖNERİLER 59

KAYNAKÇA 63

TEZDEN ÜRETİLMİŞ YAYINLAR 71

SİMGE LİSTESİ

bi	Anahtar veri çıktıları
e()	Bilinear mapping function
GT	Bilinear pairing
Tmp	Bilineer haritalamanın yürütme süresi
Tbio	Biyo hash işleminin yürütme süresi
M	Biyometrik veri noktalarının sonlu bir metrik
PKd	Cihaz genel anahtarı
Didi,UIDi	Cihaz Kimliği
L	Çıktı dizisinin bit sayısı
g	EC üretim noktası
Gi,Gj	EC üzerinde nokta
Tex	ECC noktasının Modüler üstelinin yürütme süresi
Tmu	ECC noktasının skaler çarpımının yürütme süresi
address	Ethereum blok zinciri ortak anahtarı (genel adres)
HGW	Ev ağ geçidi
HGW PK	Ev ağ geçidi ortak anahtarı
HGW sk	Ev ağ geçidi özel anahtarı
AES()	Gelişmiş Şifreleme Standardı işlevi
PUK	Genel anahtar
pari	Genel çoğaltma parametresi
$C1, C2, c, w$	Grup imzası
Gsig	Grup imzası
gpk	Grup ortak anahtarı

gpk,(D, S ,U)	Grup ortak anahtarı
gsk[i]	Grup özel anahtarı
Tag_i	Grup üyesinin etiketi
q , P1, P2	Grup yöneticisi tarafından başlatma parametreleri
Gmsk	Grup yöneticisinin özel anahtarı
sk	Grup yöneticisinin özel anahtarı
fi	Gürültülü biyometrik bilgi
P1,P2	Hash değerleri
h(.)	Hash fonksiyonu
t	Hata toleransı
tk	İzleme anahtarı
Tki	Jeton(Token)
RGToken	Kayıt jetonu
Rtm	Kayıt zamanı
user PK	Kullanıcı ortak anahtarı
user sk	Kullanıcı özel anahtarı
M,MSG	Mesaj
Gen	Olasılık algoritması
s.key	Oturum anahtarı
G1, G2	Q mertebesindeki döngüsel gruplar
d, s, u, xi, k	Rastgele değerler
Ri,Rj	Rastgele değerler
RID	Rastgele kimlik
Ted	Simetrik şifreleme/şifre çözme yürütme süresi
PP	Sistem genel parametreleri
Pks	Sunucu genel anahtarı

xs	Sunucu gizli anahtarı
Sid	Sunucu kimliği
ps	Sunucu özel anahtarı
Th	Tek yönlü hash işlevinin yürütme süresi
Tx	XoR işleminin yürütme süresi

KISALTMA LİSTESİ

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AI	Yapay Zeka
ARPNET	İleri Araştırma Projeleri Ajans Ağı
AVISPA	İnternet Güvenliğine Duyarlı Protokollerin ve Uygulamaların Otomatik Doğrulaması
BLE	Bluetooth Düşük Enerji
CPU	Merkezi işlem birimi
DoS	Hizmet Reddi saldırısı
ECC	Eliptik Eğri Kriptografi
ECDH	Eliptik eğri Diffie Hellman
ECIES	Eliptik Eğri Entegre Şifreleme Şeması
GDPR	Genel Veri Koruma Yönetmeliğine
HLPSI	Üst düzey protokol belirtim dili
ICT	Bilişim ve İletişim Teknolojileri
ID	Kimlik
IIoT	Endüstriyel Nesnelerin İnterneti
IoT	Nesnelerin interneti
ISO/IEC	Uluslararası Standardizasyon Örgütü/Uluslararası Elektroteknik Komisyonu
KVKK	Kişisel Verilerin Korunması Kanun
M2M	Makineden Makineye
MAC	Medya Erişim Kontrolü adresi
MAC	mesaj doğrulama kodu
MITM	Ortadaki Adam
NGI	Yeni Nesil İnternete
NHS	Birleşik Krallık Ulusal Sağlık Servisi
O	O notasyonu
OOB	görsel Bant Dışı
OTP	Tek seferlik şifre
PC	kişisel bilgisayar
PUF	Fiziksel Klonlanamayan İşlev
PV	fotovoltaik

QR	Hızlı Yanıt Kodu
RFID	radyo frekans ile kimlik belirleme
SPAN	Güvenlik Protokolü Animatörü
TPM	Güvenilir Platform Modülünün
TRNG	Gerçek Rastgele Sayı Üreteci
TV	televizyon
UUID	evrensel benzersiz bir kimlik
WiFi	kablosuz iletişim
WWW	Dünya çapında Ağ

ŞEKİL LİSTESİ

Şekil 1.1 Tipik Akıllı Ev Bağlantısı 3
Şekil 2.1 Grup İmzası 17
Şekil 2.2 IoT Kimlik Doğrulama Şemalarının Taksonomisi..... 18
Şekil 2.3 Kimlik Doğrulama Protokolü Aşamaları 20
Şekil 3.1 Akıllı Ev Mimarisi..... 28
Şekil 3.2 Akıllı Ev İletişimi..... 31
Şekil 3.3 Akıllı Ev Kimlik Doğrulama Sistemi..... 32
Şekil 3.4 Kullanıcı Cihazı Kayıt Aşaması 35
Şekil 3.5 Akıllı Cihaz Kayıt Aşaması..... 35
Şekil 3.6 Kullanıcı Cihazı Kimlik Doğrulama Aşaması..... 37
Şekil 3.7 IoT Cihaz Girişi Kimlik Doğrulama Aşaması..... 38
Şekil 3.8 Akıllı sözleşme ile DHKE Kullanan Anahtar Değişim Mekanizması..... 40
Şekil 3.9 Anahtar Değişim Mekanizması ile Veri Aktarımının Zaman Çizgisi 45
Şekil 3.10 Çevrimiçi ve Çevrimdışı Kimlik Doğrulama ile Sistem Entegrasyonu 48
Şekil 4.1 AVISPA SPAN Protokolü Kontrol Sonucu..... 51
Şekil 4.2A Saniye Cinsinden RGToken İstek Süresi 52
Şekil 4.2B İstemci Token İstek Süresinin Normal Dağılımı..... 52
Şekil 4.3A Milisaniye Cinsinden Kayıt Süresi 52
Şekil 4.3B Müşteri Kayıt Süresinin Normal Dağılımı 52
Şekil 4.4A PK Gereksinimi Milisaniye Olarak 53
Şekil 4.4B İstemci PK Talep Süresinin Normal Dağılımı..... 53
Şekil 4.5A PK Değişimi Milisaniye Cinsinden 53
Şekil 4.5B İstemci PK'sinin Normal Dağılımı Değişim Zamanı..... 53
Şekil 4.6A Milisaniye Cinsinden Toplam talep/Yanıt (Req-Resp) Süresi 54
Şekil 4.6B Toplam Talep/Yanıt (Req-Resp) Normal Dağılımı..... 54
Şekil 4.7 İstek ve Yanıt İçin Toplam İşlem Süresi..... 55

TABLO LİSTESİ

Tablo 2.1 Farklı Kişisel Veri Türü..... 13
Tablo 4.1 Hesaplama Karmaşıklığı..... 56
Tablo 4.2 Güvenlik Özelliği 57
Tablo 4.3 Kimlik Doğrulama İçin Mesaj Boyutu ve İletişim Maliyeti 58

ÖZET

AKILLI EV ORTAMLARINA YÖNELİK GDPR İLE UYUMLU HİBRİT DOĞRULAMA SİSTEMİ

Hisham Raad Jafer MERZEH

Bilgisayar Mühendisliği Anabilim Dalı

Doktora Tezi

Danışman: Prof. Dr. Hasan Hüseyin BALIK

Eş-Danışman: Doç. Dr. Muhammed Ali AYDIN

Akıllı ev ortamlarındaki akıllı ekipmanlar günümüzde her alanda kullanılmaktadır ve geniş ölçüde birbirinden ayrılmıştır. Böylece akıllı nesneler, ağ üzerinden bağlantı kurulan, her yerden erişilebilen ve uzaktan kontrol edilebilir cihazlar haline getirilmiştir. Diğer taraftan internet üzerinden gerçekleştirilen iletişim kanalı sebebiyle akıllı nesneler bilgisayar korsanlığına, istismara ve yanlış bir şekilde uzlaşmaya karşı savunmasız hale gelmektedir ve güvenliğini garanti etmek geniş bir endişe kaynağı oluşturmaktadır. Literatür incelendiğinde birçok çalışma bu güvenlik sorunlarını tartışmakta ve bu sorunları çözmek için farklı çözümler önermektedir. Bununla birlikte, akıllı cihazların doğası ve daha fazla kaynağa olan ihtiyaç, güvenli bir mimari sağlamayı önemli ölçüde zorlaştırmaktadır. Ayrıca, bu sorunlara yönelik mevcut çözümlerin çoğu, gizlilik ve anonimlik konusunda zaafiyetler içeren tek sunucu mimarisine dayanmaktadır.

Bu tez, akıllı ev ortamında kullanıcıların ve cihazların kimliğinin doğrulanması ve mevcut yöntemlerin iyileştirilmesi için yeni bir kimlik doğrulama yaklaşımı önermektedir. Ayrıca, merkezi ve merkezi olmayan kimlik doğrulama

mekanizmalarını tek bir hibrit kimlik doğrulama sisteminde birleştirir. Merkezi kimlik doğrulama, akıllı ev cihazları ve ev içindeki yerel kullanıcılar için yerel kimlik doğrulama modeli olarak kullanılır. Yerel uç sunucusu, çevrimdışı mod adı verilen bağlantıyı, kontrol isteğini ve kimlik doğrulamayı yerel olarak yönetir. Bu yaklaşımda sözde rasgele kimlik algoritmasına ek olarak dinamik QR kodları ve akıllı kartlar gibi son teknolojiler kullanılmaktadır. Buna karşılık, merkezi olmayan kimlik doğrulama mekanizması, Çevrimiçi Mod adı verilen ev dışındaki uzak kullanıcıları yönetmek için kullanılır.

Bu tez çalışmasında, blok zinciri teknolojisindeki güvenlik altyapısı, biyometrik veriler ve grup imza yöntemi birleştirilerek bir arada kullanılmıştır. Sunulan yöntemde belirli bir kısım merkezi olmayan mimariye dayalı bir kimlik doğrulama mekanizması önermektedir. İlk olarak, kullanıcı cihazının meşru kullanıcısının kimliğini doğrulamak için bulanık çıkarıcı algoritması kullanarak biyometrik verileri kullanmaktadır. Ardından, kullanıcının cihazının kimliği, bir grup imzası yöntemi üzerinden akıllı evin bir üyesi olarak doğrulanır. Grup imzası yöntemi, bir grup üyesinin uzaktan erişim veya kontrol isteklerini imzalamasına izin veren blok zinciri tabanlı bir şemadır. Teklif, belirli bir grup üyesi yerine grup isteği olarak alınır. Her grup üyesinin, isteği imzalamak için kullandığı kendi özel anahtarı ve istek doğrulaması için kullandığı genel anahtarı vardır. Mevcut yaklaşımlarla karşılaştırıldığında, önerilen hibrit kimlik doğrulama yaklaşımı, güvenlik, güvenilirlik, performans, anonimlik ve mahremiyet hususları açısından merkezi ve merkezi olmayan mimari avantajlar sağlar. Ayrıca bu çalışma, kimlik doğrulama mekanizmasının güvenliğini ve güvenilirliğini artırmak için Dinamik QR Kodu, akıllı kart, sözde Rastgele Kimlik, biyometrik kullanıcı verileri, grup imzası, mesaj kimlik doğrulama kodu, eliptik eğri entegre şifreleme ve blok zinciri bir arada entegre etmektedir. Böylece önerilen şemanın güvenlik özelliklerini analiz ederek deneysel sonucunu literatürdeki mevcut şemalarla karşılaştırdık.

Anahtar Kelimeler: IoT, kimlik doğrulama, Blok zinciri, grup imzası.

ABSTRACT

HYBRID AUTHENTICATION SYSTEM FOR SMART HOME ENVIRONMENTS COMPLIES WITH GDPR

Hisham Raad Jafer MERZEH

Department of Computer Engineering

Doctor of Philosophy Thesis

Supervisor: Prof. Dr. Hasan Hüseyin BALIK

Co-supervisor: Assoc Prof. Dr. Muhammed Ali AYDIN

Smart equipment in smart home environments is ubiquitous and widely separated nowadays. Thus, smart things are connected through the network to make it accessible everywhere and remotely controlled. Nevertheless, connection to the internet made smart things vulnerable to hacking, exploitation, and compromised incorrectly, and guaranteeing its security has been a broad concern. Many research studies discuss these security problems and propose different solutions to solve these problems. However, the nature of smart devices and the lack of resources makes securing their significant challenges. Most of the existing solutions for these issues are based on single server architecture with low concern for privacy and anonymity. This thesis proposes a new authentication approach for authenticating users and devices in a smart home environment. This approach is an improvement on the existing methods. This study combines the centralized and de centralized authentication mechanism in one hybrid authentication system. The centralized authentication is utilized as a local authentication for Home Smart devices and local users inside home, the local edge server mange the connection, control request, and authentication locally named offline mode.

Resent technologies are used in this approach as dynamic QR code and smart card in addition to the pseudo random ID algorithm. While the decentralized authentication mechanism is utilized to manage the remote users outside home named Online Mode. This approach based on Blockchain techniques, biometric data and group signature scheme, they are utilized to propose an authentication mechanism based on decentralized architecture. First, we utilize the biometric data using a fuzzy extractor algorithm to authentic the legitimate user of the user device. Then, the user device is authenticated as a group member of the smart home using a group signature. The group signature is a Blockchain-based scheme that allows a group member to sign their request for remote access or control. The proposal is received as a group request instead of a specific group member. Every group member has their group private key used for signing the request and the group public key used for request verification. The proposed hybrid authentication approach provide the advantages of both centralized and decentralized architecture in term of security, reliability, performance, anonymity, and privacy consideration Compared with existing approaches. This research integrates Dynamic QR Code, smart card, pseudo Random ID, biometric user data, group signature, message authentication code, elliptic curve integrated encryption, and Blockchain to increase the security and reliability of the authentication mechanism. We analyze the security features and discussed the experimental result of the proposed scheme with the existing schemes.

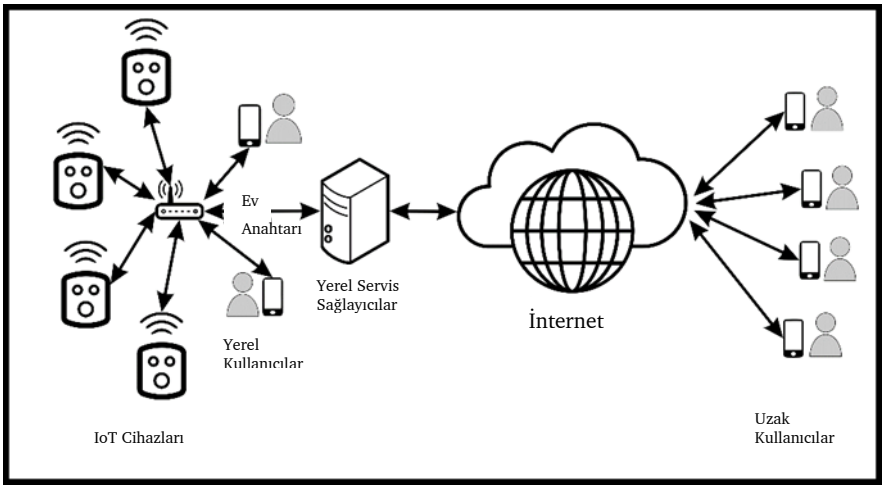
Keywords: IoT, authentication, Blockchain, group signature.

1
GİRİŞ

1.1 Giriş

Artan sayıda birbirine bağlı cihaz, Nesnelerin İnterneti olarak adlandırılan olguyu meydana getirir. Bu, sensörler ve aktüatörler gibi akıllı cihazları birbirine bağlayan geniş bir network ağıdır. Bu cihazlar akıllı şehirler [1], halk sağlığı[1], [2], akıllı evler [3], akıllı ulaşım [4], enerji yönetimi [5], akıllı şebekeler [6], tarım [7] ve atık yönetimi [8] gibi çeşitli alanlarda kullanılmaktadır. Her yerde var olan bu tür sistemler, insanların günlük yaşamına girmiş ve yaşamlarının güvenliğini ve kalitesini artırmak için kullanılmaktadır. Ancak, insanların günlük faaliyetleri hakkında bilgi toplayabilen bu tür sistemler, yaygın gözetim sistemleri haline gelebilir. Kullanıcıların günlük faaliyetlerini (örneğin günlük rutinler, seyahat rotaları, satın alma alışkanlıkları vb.) gösteren bilgiler birçok otorite tarafından özel olarak kabul edildiğinden, yaygın uygulama gereksinimlerinden birinin gizliliğin koruması olması şaşırtıcı olmayacaktır ve beklentileri karşılamayan uygulamalar kullanıcıların gizliliğini ihlal edeceği için yasaklanabilecektir. Bununla birlikte, yakın zamana kadar her yerde bulunan uygulama geliştiricileri, potansiyel olarak kullanılabilirliği ve potansiyel kullanıcılar tarafından kabul edilebilirliği sınırlayabilecek bir unsur olarak işlevselliğe odaklanmıştır [9]. Buna ek olarak, her yerde bulunan sistemlere bağlı cihazların kısıtları ve gereksinimleri, çok sayıda akıllı cihazın birbirleriyle veri alışverişinde bulunmaları için bağlantı sorunları ve nesnelerin interneti ağlarının saldırıya uğramasını önleme ihtiyacıyla ilgili güvenlik problemleri da dâhil olmak üzere çok farklı zorluk ortaya çıkarmaktadır. Aynı zamanda saldırı amaçlı kötüye kullanımdan korunma ihtiyacı vardır. Bu zorluklar, Nesnelerin İnterneti cihazlarının kaynak sınırlı özelliği ile de artmaktadır. Bu durum, geleneksel iletişim protokollerini ve güvenlik sistemlerini etkisiz hale getirmekte ve hatta Nesnelerin İnterneti için kullanımı imkânsız hale gelmektedir. IoT ile ilgili güvenlik sorunları daha endişe verici hale gelmiştir, çünkü IoT cihazları her yerde ve kritik uygulamalarda yer almaktadır. Herhangi bir güvenlik ihlalinin etkisi hayatı tehdit edecek ölçüde kötüleştirilmesi ve ağırlaştırılması sonucunu doğurabilir [10]. IoT ağ hizmetinin uygulandığı

uygulamaların niteliği güvenlik gereksinimlerini belirtir. Kimlik doğrulama, reddetmeme, kullanılabilirlik, gizlilik ve bütünlük ihtiyacı, güvenlik seviyesinin uygulama koşullarına bağlıdır. Özellikle kimlik doğrulama IoT için temel bir gerekliliktir. Bir IoT ağına bağlı cihazlara güvenmek, güvenilir ve güvenli bir ağ için temel bir ilkedir [11] [12]. Yalnızca tek bir enfekte düğüm kötücül olmaya yeter ve tüm sistemi çökertebilir veya yıkıcı bir etkiye neden olabilir [10]. Bu sorunları en aza indirmek için, veriler, bir düğümden diğerine güvenli bir şekilde gönderilebilmek için güvenli anahtar tabanlı algoritmalara dayanan şifreleme ve şifre çözme işlemi kullanılarak işlenmesi gerekir. Bu algoritmalar, şifreleme ve şifre çözme süresini etkili ve verimli bir şekilde azaltabilir, kırma girişimini de daha zor ve zaman alıcı hale getirebilir [13]. Tipik bir akıllı ev ortamı için iletişim mimarisi Şekil 1.1'de verilmiştir. Şekil 1.1'de görüldüğü gibi sistemde, konut kullanıcıları ev ağ geçidi vasıtasıyla İnternet üzerinden uzaktan iletişime geçmek için mobil cihaz (ör. Android ve iOS cihazları) kullanmaktadır. Ev ağ geçidi, kullanıcılardan erişim veya kontrol emri gibi mesajları aldıktan sonra, ilgili ev cihazlarıyla verilen görevleri yürütür. Bu nedenle, ev ağ geçidi sadece evdeki düğümlerle ağ bağlantısı sağlamakla kalmaz, aynı zamanda çeşitli ev cihazlarının (örneğin, ev cihazlarına takılan sensörler) oluşturduğu kablosuz sensör ağlarını birbirine bağlar. Cihazlar ve (kablosuz) iletişim kanalı hedef olabilir ve istismara maruz kalabilir. Cihazları ve iletişimleri güvence altına almanın zorlukları, kaynak kısıtlı cihazlarda (örneğin, akıllı anahtarlar) artar. Sonuçları hassas bilgilerin bu cihazlardan toplanması ve dışarıya sızdırılması içerir [14]. Herhangi bir cihazdan gelen bilgi hassas olarak kabul edilmeyebilir, ancak toplu olarak bu veriler son derece anlamlı olabilir. Örneğin, akıllı TV'nin hoparlörleri ve kamerası aracılığıyla gizlice toplanan sesler ve videolar, akıllı kilitler ve akıllı anahtarlardan elde edilen veriler, takip ve profil oluşturma gibi çeşitli amaçlarla kullanılabilir. Bu, aynı zamanda kaynak kısıtlı cihazlarda dağıtım için kullanılabilecek düzeyde yükü az güvenli uzaktan kullanıcı kimlik doğrulama sistemine sahip olmanın önemini vurgulamaktadır. Akıllı ev ağlarında düğümleri doğrulamak için tasarlanmış çözümler olsa da [14], sahip olduğu ksıtlar ve eksiklikler nedeni ile bu tez çalışmasında kullanıcılar ve ev ağ geçidi arasındaki güvenli (uzak) karşılıklı kimlik doğrulama sorununun çözümüne odaklanılmıştır.



Şekil 1.1 Tipik akıllı ev bağlantısı

Liretatürde bazı uzaktan kimlik doğrulama yaklaşımları bulunmaktadır. En basit ve en doğrudan yaklaşım şifre tabanlı kimlik doğrulamadır. Böyle bir yaklaşımın uygulanma maliyeti de azdır [15], ancak gizli, güvenli bir kanal kullanılmazsa doğrudan dinleme saldırılarına karşı koruma sağlamaz. İki faktörlü kimlik doğrulamada en popüler yöntemlerden biri olan tek kullanımlık parola (OTP) kimlik doğrulamasıdır [16] ve akıllı kartlara dayalı uzaktan kullanıcı kimlik doğrulama şemaları, verimlilik, kolaylık ve düşük hesaplama maliyeti nedeniyle uzaktan kullanıcı girişi, Web erişimi ve diğer çevrimiçi hizmetleri içeren uygulamalarda da yaygın olarak kullanılmaktadır [17] [18]. OTP bir takım basit saldırılara direniyor gibi görünebilir. Ancak, bir saldırgan meşru bir kullanıcının akıllı kartını aldıktan sonra, uzak sisteme erişmek için bu kullanıcının kimliğine bürünebilir [19]. Bu tür zaafları azaltmak için akıllı kartlar, akıllı ev cihazlarında güvenli erişim için güçlü bir şifre tabanlı yaklaşım uygulamak için kullanılır [20]. Ancak, bu daha yüksek bir hesaplama maliyeti demektir. Son zamanlarda, diğer uygulamalar için birkaç karşılıklı kimlik doğrulama protokolü tasarlanmıştır, ancak neredeyse hepsi tek sunucu mimarisi temellidir [21]. Tek sunucu mimarilerine dayanan mevcut uzaktan kimlik doğrulama yaklaşımları genellikle aşağıdaki sınırlamalara sahiptir.

• ***Gizlilik ve Anonimlik Eksikliği:*** Basit bir şifre doğrulama yaklaşımı, akıllı ev hizmetlerine ve cihazlarına eriştiklerinde kullanıcının gerçek kimliğini korumaz, çünkü kötücül veya gizliliği ortadan kalkmış bir ev ağ geçidi, kullanıcının günlük faaliyetlerini kolayca sızdırabilir.

- ***Bütünlük ve Gizlilik Zaafiyeti:*** Yerel bir veri tabanında, örneğin ana ağ geçidi tarafından saklanan kullanıcıların geçmiş erişim kayıtları, kullanıcının bilgisi olmadan değiştirilebilir ve bu da kullanıcı gizliliğinin sızmasına yol açabilir.

Bu sınırlamaları çözmek için, IoT senaryolarında, merkezsizleştirme, doğrulanabilirlik ve değişmezlik gibi özellikleri nedeniyle Blockchain teknolojisinin rolü öne çıkmaktadır. Bu özellikler, daha emin, güvenilir ve uygun IoT sistemleri oluşturmada faydalıdır [22]. Bu nedenle çözüm olarak anonimlik ve hatta gizlilik özelliği olan artan sayıda Blockchain tabanlı kimlik doğrulama önerilmiştir. Bununla birlikte, hala aşağıdaki listelene kritik sorunlar çözülmeyi beklemektedir. Blockchainin sağladığı doğal anonimlik, IoT ve akıllı evlerde kullanıcıları gizli tutmada uyuglanabilir, ancak bu sistemlerde kullanıcı davranışları etkili bir şekilde düzenlenemez. Başka bir deyişle, kötü niyetli istekleri gerçekleştiren kullanıcıları izlemek için etkili bir mekanizma yoktur. Daha da kötüsü, tüm talep işlemleri veya erişim politikası, kullanıcının günlük yaşamını istatistiksel olarak analiz etmek için toplanabilen ve böylece kullanıcı gizliliğini tehlikeye atan şifresiz belge halindedir. Bu sorunların üstesinden gelmek için, bu tez çalışmasında, kullanıcının bir web tarayıcısı veya mobil uygulama kullanarak sisteme erişmesi için bir kimlik doğrulama şeması ve ayrıca uzak kullanıcılar ile yerel (uç) sunucu arasında merkezi olmayan kimlik doğrulama mekanizması önermiştir. Önerilen bu şema, yerel kullanıcıların kimliğini doğrudan yerel uç sunucusunda doğrulamaya ek olarak, yerel sunucu ile IoT cihazları arasında M2M kimlik doğrulamasına sahiptir. Yerel bir ağ bağlantısı durumunda, kullanıcı akıllı cihazlara yerel uç sunucusu üzerinden doğrudan erişebilir. Tezde önerilen şema, kayıt için bir akıllı kart ve QR kodu ve karşılıklı kimlik doğrulama için güvenli bir jeton (belirteç) kullanarak kullanıcının kimliğini doğrulamak için çevrimdışı, yerel olarak üç yollu bir kimlik doğrulama modeli göstermektedir. Önerilen şema, akıllı ev cihazına erişimi doğrulamak için yerel Edge sunucusuna sahip uzak kullanıcılar için merkezi olmayan çevrimiçi kimlik doğrulamada Blockchain teknolojisini kullanmaktadır. Çevrimiçi kimlik doğrulama, ev kullanıcılarını doğrulamak, istek göndermek ve yanıt almak amacıyla güvenli bir kanal oluşturmak için grup imzası ve akıllı Diffie-Hellman anahtar değişimi kullanan Ethereum Blockchain'e dayanmaktadır. Ethereumun tercih edilmesinin ana sebebi, tercih edilen

mutabakat mekanizması ve düşük enerji tüketimi sayesinde sunduğu yüksek performanstır. Ethereum, dijital anlaşmalar sağlayan Akıllı Sözleşmeleri dağıtması için sisteme izin verir. Ethereum, merkezi olmayan otonom bir dijital sistem olması ve işlem kanıtı kurcalamaya karşı dayanıklı olması sayesinde önerilen mekanizmayı önemli ölçüde destekler. Buna ek olarak, Ethereum Blockchain, Ethereum'un işlem süresi üzerinde bir üst sınıra sahip olduğu için çok yüksek işlem hacmi ile çalışır, bu da fikir birliği mekanizmasının karmaşıklık seviyesini değiştirmekle elde edilir [23]. Bitcoin sistemi, gerçek yaşam senaryolarında önerilen mekanizma için merkezi olmayan kimlik doğrulama yapabilir. Ancak, İş Kanıtı olarak bilinen fikir birliği mekanizması nedeniyle Bitcoin Blockchain ağında bir blok oluşturma süresi yaklaşık 10 dakikadır. Ethereum'da ise blok oluşturma süresi yaklaşık 12 -14 saniyedir çünkü Ethereum, Hisse Kanıtı adı verilen bir fikir birliği mekanizması kullanır. Tezde önerilen bu şema yüksek verimlilik, güvenilirlik ve birçok güvenlik özelliği göstermektedir. Gizlilik değerlendirmesine ek olarak, Genel Veri Koruma Yönetmeliğine (GDPR) de uygundur.

1.2 Tezin Amacı

Yapılan tez çalışmasının açaşları aşağıda özet halinde listelenmiştir. Bunlar;

- Akıllı ev ortamındaki IoT cihazları için kimlik doğrulama protokollerine odaklanmak.
- Akıllı ev cihazlarına erişimi güvence altına almak için bir kimlik doğrulama sistemi önermek. Kullanıcı gizliliği açısından GDPR ile uyumu ve yerel ağlarda kullanılacak cihazlar için çevrimdışı kimlik doğrulama desteğini sağlamak.
- Kaynak kısıtlı cihazlar için uygun, yüksek performanslı ve düşük hesaplama maliyetli hafif bir model önermek. IoT cihazları genellikle sınırlı kaynaklardır, sınırlı bellek, iletişim ve hesaplama yetenekleri ve pil gücü vardır. Bundan farklı güvenlik saldırılarına karşı birçok güvenlik özelliğine sahiptir ve dirençli ancak hafif güvenlik vurgusu önemlidir.
- Homechain adlı kimlik doğrulama yaklaşımını geliştirmek.

- Tavsiye edilen kimlik doğrulama mekanizmasında yüksek hata toleransı sağlamak için Blockchain sistemine dayalı çevrimiçi Kimlik Doğrulama modu kullanmak.
- Akıllı ev sistemlerinde kullanılmak üzere hem çevrimdışı hem de çevrimiçi kimlik doğrulama yaklaşımlarını tek bir sistem modelinde birleştirmek.
- Önerilen şemaynın güçlü ve zayıf noktalarını bulmak için mevcut yaklaşımlarla karşılaştırmaktır

1.3 Orijinal Katkı

Bu çalışmada, akıllı ev sisteminde kullanılmak üzere iki farklı kimlik doğrulama yaklaşımına dayalı bir hibrit kimlik doğrulama modeli önerilmiştir. Çevrimdışı mod ile kullanılan yerel kimlik doğrulama, yerel kullanıcılara ve akıllı ev IoT cihazlarına güvenilir kimlik doğrulama sağlamıştır. Böylece, IoT cihazları gibi kaynak kısıtlı cihazlar için uygun bir ortam sağlanmıstır. Ek olarak, düşük güç tükemiti sağlayan algoritmalar ile gerçekleştirilen bir süreç üzerinden, yüksek güvenlik ve gizlilikle ilgili kimlik doğrulaması sağlanmıştır. Ayrıca bu çalışma internet bağlantısı üzerinden uzak kullanıcılarla kullanıldığında düşük hata toleransı sağlayan merkezi modele de dayanmaktadır. Bu nedenle, merkezi olmayan mekanizmaya dayalı yüksek hata toleransı sağlamak için çevrimiçi kimlik doğrulama yaklaşımı kullanılmıştır. Bu iki yaklaşımı tek bir akıllı ev sistemine entegre ederek, bu entegrasyon güvenilirlik, yüksek performans, yüksek hata toleransı, farklı tür saldırılara karşı koyabilen yüksek güvenlik ve kullanıcı gizliliğini koruyan GDPR uyumluluğu sağlandığını ve saldırıları engelleyebileceğini göstermiştir.

2
TEMEL TEKNİK ALTYAPI

2.1 Nesnelerin İnterneti (IoT)

Nesnelerin İnternetinin Tarihçesi ve Evrimi

ABD Savunma Bakanlığı projesi ARPNET de dahil olmak üzere bilgisayar ağlarının gelişimi, 1991'de belgeleri paylaşmak için bir araç olarak başlatılan WWW'ye kadar gider. İnternet ve WWW kombinasyonu, IoT evrimindeki en önemli kilometre taşıdır. Bilgisayarlar gibi İnternet de, kapalı bağlantı projelerinden bugün hepimizin bildiği ve kullandığı güçlü araçlara kadar 50 yıldan fazla bir süredir nispeten yavaş bir şekilde gelişmiştir [24].

2011 yılında Raspberry PI mikrodenetleyicisinin piyasaya sürülmesi, başka bir büyük IoT atılımıydı ve bir şekilde IoT teknolojisinin hızlı kabulüne yol açtı. Bu düşük maliyetli, çok yönlü mikrodenetleyici, birdenbire IoT'yi hobicilere ve son kullanıcılara açtı. Diğer mikrodenetleyiciler mevcuttu, ancak düşük maliyeti, basitliği ve nispeten büyük işlem gücü ve önemli miktarda ücretsiz çevrimiçi desteği nedeniyle IoT artık ticari projelerle sınırlı değildi. Değişim, IoT teknolojisinin, Nest'i alan Google, Apple Watch'u sunan Apple ve uygun fiyatlı bir akıllı ev başlangıç kiti ve yazılım platformu olan Smart Things'i sunan Siemens gibi şirketler tarafından geniş çapta tüketici pazarına sunulduğu 2014 yılına kadar devam etti. 2016 'da Amazon, Apple ve Google gibi büyük teknoloji şirketleri, sesli olarak etkinleştirilen kişisel asistanlarını piyasaya sürdü. Tüketici IoT'sine ek olarak, birçok endüstriyel sürecin otomasyonunu sağlayan Endüstriyel IoT (IIoT) mevcuttur. IoT kavramı da gelişmeye devam etmektedir; başlangıçta IoT sistemleri çok sayıda küçük kapalı ağdan oluşuyordu, fakat bu kavram daha fazla bağlantılı olan daha büyük ağları, söz gelimi akıllı ulaşım altyapılarına sahip akıllı şehirleri kapsayacak şekilde gelişti. Ancak büyük altyapı bu değişim yolculuğun sonu değildir, IoT kavramı günümüzde Yeni Nesil İnternete (NGI) dönüşmektedir. IoT'de zirve yapan ICT'nin (Bilişim ve İletişim Teknolojileri) evrimi. Bu NGI kavramları, yapay zeka, makine öğrenmesi, artırılmış gerçeklik ve sanal gerçeklik

gibi gelişmiş teknolojilerin eklenmesiyle mevcut ve yeni IoT sistemlerine entegre edilmektedir. Birçok alanda, NGI kavramları akıllı sürdürülebilir şehir kavramıyla uyuşur, temel fark NGI'nın sadece çevresel ve ekonomik refahı değil, insan refahı değerlerini içermesidir. Bu evrimsel yolculuğun yanı sıra, 2016 ve 17 'de, özellikle Mirai Dyn saldırısı [25] ve WannaCry NHS saldırısı [26] olmak üzere bir dizi çok önemli güvenlik saldırısı olmuştur. Bunun karşılığında, dünya çapındaki Hükümetler IoT güvenlik açıklarını azaltmak için stratejiler, girişimler ve bazı durumlarda yasalar geliştirmeye başladı. Yapay Zeka (AI), makine öğrenimi ve Blockchain gibi diğer teknolojiler, daha güçlü araçlar üretmek için IoT ile birleştirilmektedir. 1999'daki IoT'nin ilk versiyonlarından 2014 yılında IoT'nin tüketiciye sunulmasına kadar, IoT teknolojisi yaygın bir şekilde benimsenmiştir. IoT gelişim döngüsü sadece 15 -20 yıldır ve bu hızlı gelişimin bir sonucu olarak IoT, başta güvenlik açıkları olmak üzere büyük sorunlarla karşı karşıyadır. IoT güvenlik açıklarının büyüklüğünün nedeni, güvenliğin sonradan akla gelen konu olmasıdır. Dünya çapındaki tasarımcılar, geliştiriciler ve politika yapıcılar artık bu sorunu azaltmanın yollarını aramaktadır [24].

Nesnelerin İnterneti güvenliği

IoT cihazları Kaynak Kısıtlaması

IoT'yi oluşturan çoğu cihaz, sınırlı CPU, bellek ve güç kaynaklarına sahip kısıtlı cihazlardır (sensörler, akıllı nesneler veya akıllı cihazlar gibi). Bu cihazlar, verileri doğrudan internet üzerinden güvenli bir şekilde taşımak için gereken taşıma katmanı güvenlik mekanizmasını desteklemek için yeterli kaynağa sahip değildir [27].

IoT Güvenlik ve Gizlilik Sorunları

IoT, çeşitli heterojen nesneler arasında bir bağlantı kurar, bu nedenle esnek katmanlı bir mimariye ihtiyaç vardır. Tek tip bir IoT mimarisi yoktur, ancak temel IoT modeli, uygulama katmanı, ağ katmanı ve algılama katmanı dahil, 3 katmanlı mimariye sahiptir. Her IoT katmanı, bağlı olduğu işlev ve teknolojilere göre farklılaşır, bu yüzden her katmanın kendine has güvenlik sorunları vardır [28]. [28]'de verildiği gibi bu katmanların kısaca açıklanır ise;

• **Algı Katmanı:** Bu katman genellikle RFID'lere (radyo frekans ile kimlik belirleme) ve kablosuz sensör ağlarına sahip olan, bilgi sızıntısı, yeniden oynatma saldırıları, klonlama saldırıları ve ortadaki adam saldırıları gibi birçok güvenlik sorunu olan sensörlerden oluşur.

• **Ağ Katmanı**: Bu katman genellikle veri dinleme, DoS saldırıları, yasa dışı erişim, imha, virüs saldırısı, ortadaki adam saldırısı vb. için bir hedeftir. Saldırganlar, ağ gizliliğine saldırmak için trafiği ve dinlemeleri analiz edebilir. IoT'nin uzaktan erişim mekanizmaları ve veri alışverişi bu tür saldırıların ihtimalini artırmaktadır.

• **Uygulama Katmanı**: Uygulamalarda etkileşimi yöneten standartların olmaması ve uygulama geliştirme süreci nedeniyle uygulama güvenliğinde birçok sorun bulunmaktadır. Farklı kimlik doğrulama mekanizmalarına sahip uygulamaların kimlik doğrulama ve veri gizliliğini onaylaması zordur. Trafik yönetimi bu katmanın sorumluluğundadır, bu da onu DoS saldırısı için bir hedef haline getirmektedir.

IoT güvenliğine duyulan ihtiyaç

Birbirine bağlanan cihaz sayısı arttıkça, bunların hepsini güvence altına almak en büyük zorluk olacaktır. IoT nesnelerinin etkili bir şekilde çalışması için donanım, yazılım ve bağlantının güvenli olması gerekmektedir. IoT'un güvenliği olmaz ise, buzdolaplarından üretim robotlarına kadar herhangi bir bağlı nesne hacklenebilir. Hackerlar kontrolü ele geçirdikten sonra, nesnenin işlevselliğini gasp edebilir ve kullanıcının dijital verilerini çalabilirler. Endüstriyel IoT'yi güvence altına almak da ihmal edilmemelidir [29].

Güvenli İletişim

Nesnelerin İnterneti, günlük faaliyetlerin, rutinlerin ve davranışların çoğunu değiştirebilecek muazzam bir potansiyele sahiptir. Bilgi kaynaklarının yayılmacı doğası, hem kamu hem de özel olmak üzere insan faaliyetinin muhtemelen her yönüyle ilgili büyük miktarda verinin üretileceği, iletileceği, toplanacağı, depolanacağı ve işleneceği anlamına gelir. Sonuç olarak, iletilen verilerin bütünlüğü ve gizliliğinin yanı sıra bu verileri sunan hizmetlerin doğrulanması (ve güvenilmesi) çok önemlidir. Bu nedenle, güvenlik IoT için kritik bir işlevselliktir [30].

Güvenlik bileşeni, Saldırı, Tehditler ve Zaafiyet

Özellikle kablosuz veri ağları, dinleme, sahtecilik, hizmet reddi vb. gibi çok sayıda saldırıya açıktır. Eski İnternet sistemleri, bağlantı katmanına, ağ katmanına, taşıma katmanına veya uygulama katmanı şifrelemesine ve temel verilerin kimlik doğrulamasına dayanarak bu saldırıları azaltır. Bu çözümlerin bazıları IoT etki alanı için geçerli olsa da, IoT cihazlarının doğal olarak sınırlı işleme ve iletişim yetenekleri, tam teşekküllü güvenlik paketlerinin kullanımının önüne geçer [30].

Temel IoT güvenlik sorunları ve Önerilen Çözümler

Her IoT katmanı, pasif veya aktif güvenlik saldırılarına ve tehditlerine açıktır. Pasif saldırı, IoT ağ verilerini hizmetleri etkilemeden veya kesintiye uğratmadan takip eder. Aktif bir saldırı, hizmetleri tamamen durdururken, ağ performansını da kısıtlar. Ayrıca, tüm katmanlar, yaygın saldırılardan biri olan ve ağ kaynaklarını, cihazlarını ve hizmetlerini kullanan yetkili bir kullanıcı formunu önleyebilen Hizmet Reddi saldırılarına (DoS) karşı hassastır. [31]'da her bir IoT katmanında karşılaşılan güvenlik sorunlarının kapsamlı analizine verilmiş ve aşağıda özetlenmiştir;

- **Algılama Katmanı**

Bir IoT cihazının kimlik bilgilerinin tekrarlanması veya uyarılması veya taklit edilmesinden kaynaklanan "Yeniden Saldırı" gibi farklı saldırı türleri, bu katmanın gizliliğinden yararlanabilir. Buna ek olarak, saldırgan, Zamanlama Saldırısı olarak tanımlanan şifreleme anahtarını ele geçirmek amacıyla, şifrelemeyi gerçekleştirmek için gerekli zamanı analiz edebilir. Gizliliği hedef alan bir başka olası saldırı, saldırganın düğümü ele geçirdiği ve tüm veri ve bilgileri yakaladığı Düğüm Yakalama saldırısıdır. Ayrıca, saldırgan ağa veri bütünlüğünü etkileyen kötü amaçlı veriler gönderen başka bir düğüm ekleyebilir. DOS atağı, daha az talep edilen zamanlarda düğümlerin uyku moduna girmelerini önleyerek enerjilerinin tüketilmesi yoluyla da ortaya çıkabilir. Yukarıda bahsedilen Algı katmanının sorunları, kullanıcının önceki iletişimini tanımlamak için kullanılan şifreleme ve kimlik doğrulama çalışması olan şifrelemenin kullanılmasıyla aşılabilir [31].

• **Ağ katmanı**

İletim ortamının yayılmacı doğası ve sensör düğümünün ölçümlemesi ve güç sınırlaması, ağ katmanını DoS saldırılarına daha yatkın hale getirir. DoS saldırılarının yanı sıra, pasif izleme, trafik analizi ve dinleme saldırıları ile ağ katmanının gizliliği tehlikeye atılabilir. Bu saldırılar, bu katman tarafından sağlanan ana işlevler olan cihazlar ve uzaktan erişim mekanizmaları arasındaki veri alışverişinden kaynaklanmaktadır.

Bu katman gizlice dinleme yaşayabileceğinden, Ortadaki Adam Saldırısına maruz kalma olasılığı daha yüksektir. Anahtar değişim sürecinin güvence altına alınması, saldırganın anahtarlama malzemesini gizlice dinlemesini ve kimlik hırsızlığı yapmasını önleyebilir. IoT Nesneleri, ağ tehditlerini algılamak ve çeşitli ağ saldırılarına karşı gerekli korumayı sağlayan bir mekanizmaya sahip olmalıdır. Bu, güvenliği olumsuz etkileyebilecek beklenmedik bir duruma karşı cihazın anında tepki vermesine izin verebilecek yazılım ve protokoller tasarlayarak gerçekleştirilebilir. Şifreleme mekanizmaları, kimlik doğrulama, anahtar yönetimi ve güvenli yönlendirme protokolleri de kullanılabilir. Ancak, kaynak kısıtı nedeniyle, güvenlik ve güç tüketimi arasında denge kurmak amacıyla, sadece hafif algoritmalar kullanılabilir [31].

• **Uygulama Katmanı**

Uygulama katmanının, IoT'nin farklı uygulamalar arasındaki gelişimi ve etkileşimi kontrol eden standartlardan ve küresel politikalardan yoksun olması nedeniyle birçok güvenlik sorunu barındırır. Uygulamalar tarafından kullanılan farklı kimlik doğrulama mekanizmaları, kimlik doğrulama ve veri gizliliğini aynı anda sağlarken, aralarındaki entegrasyonu zorlaştırır. Bağlı cihazlar tarafından paylaşılan büyük miktardaki veri, verileri analiz eden uygulamalarda büyük bir ek yüke neden olabilir ve bu da hizmetlerin kullanılabilirliği üzerinde büyük bir etkiye yol açabilir. Paylaşılacak veri miktarı, çeşitli kullanıcılar ve farklı uygulamalar arasındaki etkileşim doğası ve uygulama yönetimi, IoT'de uygulamalar tasarlanırken akılda tutulması gereken hususlardır. Bazı araçlar, kullanıcıların veri ifşası üzerinde kontrol sahibi olmalarına ve diğer iletişim taraflarını doğrulamalarına izin verecek şekilde tasarlanmalıdır [31].

2.2 QR kodu

QR Kod (Hızlı Yanıt Kodu), ilk olarak 1994 yılında bir Japon şirketi olan Denso tarafından önerilen iki boyutlu bir kod standardıdır [32]. 2000 yılında başarılı bir şekilde ISO Uluslararası Standardı (ISO/IEC 18004:2000) haline gelmiştir. Başlangıçta QR Kod, otomatik üretim süreçlerinin ve tasarımının kontrolünde uygulanmak üzere tasarlanmıştır, ancak daha sonra diğer birçok alanda yaygın olarak kullanılmıştır. QR Kod, yüksek veri kapasitesi, yüksek hızlı veri toplama, yüksek yoğunluklu veri yazdırma ve diğer özelliklere sahip bir matris sembolüdür. Doğrusal tek boyutlu bir koda kıyasla, iki boyutlu kod daha fazla veri depolayabilir ve verileri okumak ve işlemek için nispeten daha uzun bir süre gerektirir. Giderek daha fazla insan bu kadar küçük iki boyutlu bir kod hakkında endişelenmeye başlıyor, çünkü gerçekten kullanışlı, insanlar arkadaş ekleyebilir, bir web sitesinde oturum açabilir ve hatta onu tarayarak ödemeyi tamamlayabilir. Sosyal ağ ve ticari amaçla zaten her yerde kullanılmaktadır ve bazı araştırmacılar kimlik doğrulayı buna adapte etme konusunda çalışmalar yapmaktadır [33] [34] [35].

2.3 Gizlilik ve Genel Veri Koruma Yönetmeliği (GDPR)

Genel Veri Koruma Yönetmeliği (AB) 2016/679 (“GDPR”) Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihinde kabul edilmiş ve 25 Mayıs 2018 tarihinde yürürlüğe girmiş ve verilerin serbest dolaşımı (" Yönetmelik") ile ilgili olarak bireylerin korunmasına ilişkin 95/46/EC sayılı Veri Koruma Yönetmeliğini yürürlükten kaldırmıştır [36], [37]. GDPR bireyin veri gizliliğini ve veri haklarını arttırır ve veri denetleyicilerinin yükümlülükleri ve sorumluluklarını çoğaltır. Kişisel veriler, Kimliği belirli veya belirlenebilir yaşayan bir kişiye ilişkin her türlü bilgi olarak tanımlanmaktadır. Tanımlanabilir yaşayan bir kişi, birinin doğrudan veya dolaylı olarak tanımlayabileceği bir kişidir [38]. AB'de ikamet edenlerin kişisel verilerini işleyen veya veri sahiplerinin AB içindeki davranışlarını izleyen tüm şirketler, nerede bulunduklarına bakılmaksızın GDPR'ye tabidir [39].

GDPR, ek yollarla korunması gereken *özel kişisel veri kategorilerini* (hassas veriler) tanımlar ve açık rıza, iyi bir neden veya birkaç başka istisna olmadan toplanmasına izin vermez. Bu veriler: Irk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar, sendika üyeliği, genetik veriler, biyometrik veriler, sağlık

verileri, cinsel yaşam ve cinsel yönelimdir [40] [41]. Diğer kişisel veri türleri Tablo-2.1 'de gösterilmiştir.

Tablo-2.1 Farklı kişisel veri türü [42]

Kişisel Olmayan Veriler	**Kişisel Bilgiler**	**Hassas kişisel veriler**
İsimsiz adres	İsim ve Adres	Irksal veya etnik köken
info@web.com gibi genel bir e-posta adresi	Kişisel e-posta adresi Kişisel Telefon Numarası.	Siyasi görüşler
Tarih, saat, kredi kartı numarasının son 4 hanesini içeren ancak adı veya e - posta adresi olmayan bir makbuz	Kredi kartı numarasının adı ve son 4 hanesi	Dini inançlar
Özet bordro verilerine sahip kurumsal hesaplar	adı olmasa bile cinsiyet ve yaş ile ödeme kayıtları	Cinsel Tercihler
Şirket adı ve web sitesi	Bir web çerezi	Biyometrik bilgiler

GDPR ve anonim bilgiler, GDPR'nin 26. Maddesinde “veri koruma ilkeleri, anonim bilgiler, yani kimliği belirli veya belirlenebilir bir gerçek kişiyle ilgili olmayan bilgiler veya veri sahibini tanımlanamayan veya artık tanımlanamayacak şekilde anonim hale getirilen kişisel veriler için geçerli olmamalıdır” şeklinde tanımlanmıştır. Bu nedenle bu Yönetmelik, istatistiksel veya araştırma amaçları da dahil olmak üzere bu tür anonim bilgilerin işlenmesi ile ilgili değildir [43].

Olası bir ihlal durumunda öngörülen yaptırımlar açısından GDPR ile KVKK arasındaki en önemli fark, GDPR kapsamında belirlenen idari para cezalarının KVKK'dan çok daha fazla olmasıdır. Başka bir deyişle, KVK kapsamındaki idari para cezaları 5.000 TL'den 1.000.000 TL'ye kadar değişirken, GDPR, 10.000.00 EUR'ya kadar idari para cezalarını veya bir teşebbüs durumunda, 20.000.000 EUR'ya kadar bazı ihlaller ve para cezaları için önceki mali yılın toplam dünya

çapındaki yıllık cirosunun % 2' sine kadar (hangisi daha yüksekse) idari para cezalarını şart koşmaktadır [36]. Türkiye'deki ulusal yasal düzenlemelere bakıldığında, kişisel verilerin korunmasına ilişkin ana mevzuatın 6698 sayılı Kişisel Verilerin Korunması Kanunu (“ KVKK ”) olduğu ve buna ilişkin ikincil mevzuatın Kişisel Verileri Koruma Kurulu kararları ile birlikte KVKK'nın yorumlanmasında ve uygulanmasında yol gösterici nitelikte olduğu anlaşılmaktadır. Nitekim KVKK, AB mevzuatından kopyalandığı şekliyle bir çerçeve mevzuattır. Ancak KVKK'nın uygulanmasına ilişkin hukuki ve teknik detaylar, Kurulun tebliğ ve yönetmelikleri ile çeşitli kararları gibi ikincil mevzuatla şekillenmiş ve şekillenecektir. Bu noktada dikkat çekici olan, ikincil mevzuatın ve Kurul kararlarının GDPR ve AB'nin GDPR uygulaması ile uyumlu olmasıdır [36]. GDPR ve KVKK arasında genel bir karşılaştırmada, en önemli farklar.

- Kişisel Verilerin Tanımı açısından GDPR ad, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı veya fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğe özgü bir veya daha fazla faktöre sahiptir. KVKK'da ise ad, kimlik numarası veya kültürel veya sosyal kimliğe özgü faktörler vardır.
- Kişisel Verilerin İşlenmesi GDPR, toplama, kaydetme, organizasyon, yapılandırma, depolama, uyarlama veya değiştirme, geri alma, danışma, kullanım, iletim, yayma veya başka bir şekilde kullanılabilir hale getirme, hizalama veya birleştirme, kısıtlama, silme veya imha etme işlemlerine sahiptir. KVKK, toplama, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, geri alma, danışma, kullanma, iletim, yayma veya başka bir şekilde kullanılabilir hale getirme, hizalama veya birleştirme, kısıtlama, silme veya imha etme işlemlerine sahiptir.
- Veri Kayıt Sistemi: GDPR hem elektronik hem de fiziksel ortamda oluşturulabilir. KVKK hem elektronik hem de fiziksel ortamda oluşturulabilir.
- Açık Rıza “belirli bir konuya ilişkin olarak özgürce verilmiş, bilgilendirilmiş rıza” dır. GDPR'da, veri sahibinin, bir açıklama veya açık bir onaylayıcı eylemle, kendisiyle ilgili kişisel verilerin işlenmesine ilişkin anlaşmayı ifade ettiği taleplerinin, hür iradesiyle verilmiş, net, bilgilendirilmiş ve açık bir göstergesi olarak tanımlanır. KVKK'da, veri sahibinin kişisel verilerinin işlenmesine ilişkin

yeterli bilgiye dayalı, açık ve belirli bir konu ile sınırlı olarak özgürce verdiği onay beyanı kastedilmektedir.

• GDPR'de “Anonimleştirme” terimi, bir kişinin kimliğinin bilinmediği veya kasıtlı olarak gizlendiği bir durumu ifade eder. KVKK'da “Takma adlandırma” terimi, kişiye özgü verilerin şifrelenmiş verilerle belirli bir algoritma tarafından değiştirildiği teknik bir yöntemi ifade eder.

• Yükümlülükler ve İdari Cezalar, GDPR'de 10.000.00-EUR'a kadar veya bir teşebbüs durumunda, bir önceki mali yılın toplam dünya çapındaki yıllık cirosunun % 2 'sine kadar, hangisi daha yüksekse, 20.000.000.-EUR'a kadar bazı ihlaller ve para cezaları için veya bir teşebbüs durumunda, diğer ihlaller için bir önceki mali yılın dünya çapındaki yıllık cirosunun % 4' üne kadar, hangisi daha yüksekse şeklindedir. KVKK'da 5.000-TL ile 1.000.000-TL arasındadır.

• Veri Taşınabilirliği ve Etki Değerlendirmesi: GDPR “veri koruma görevlisine” sahiptir. Kontrolörün veya işlemcinin temel faaliyetleri, doğası gereği veri sahiplerinin büyük ölçekte düzenli ve sistematik olarak izlenmesini gerektiren işleme aktivitelerinden veya kontrolörün veya işlemcinin temel faaliyetlerinden oluşur ve KVKK'da “veri koruma görevlisi” buna dahil değildir.

2.4 Bulanıklık Ayıklayıcı (Fuzzy Extractor)

Bulanıklık ayıklayıcılar, kullanıcının biyometrik verilerinden oluşturulan bir şablonu anahtar olarak kullanarak, kullanıcı kimlik doğrulamasına izin veren bir biyometrik araçtır. İlgili cihaz üzerinden gürültülü bir ortamdan güvenilir bir şekilde kriptografik anahtarlar elde etmek için tasarlanmış bir kriptografik yöntemdir [44]. Bir karma algoritma kullanır ve çok küçük farklarla bile farklı sonuçlar üretir [45]. Gerçek biyometrik verilerin çoğaltılması genel uygulamada çok zordur ve veri toplama sırasında ortamdaki gürültüden etkilenir. Bu etkiyi önlemek için, belirli bir hata toleransına (t) sahip biyometrik şablondan rastgele bir dize ve genel bilgiler ayıklayabilen bir bulanıklık ayıklama yöntemi tercih edilir. Cihazın biyometrik doğrulama için veri üretme sürecinde, bulanık çıkarıcı genel bilgi ve hata toleransı (t) kullanarak sahip olduğu biyometrik verilerden gürültüyü süzer ve gerekli yöntemlerle orijinal biyometrik anahtar verilerini elde eder.

M'nin M ={0,1}m biyometrik veri noktalarının sonlu bir m - boyutlu metrik uzay olduğunu varsayalım, d: M × M = → Z+, seçilen metriğe göre iki nokta arasındaki mesafeyi hesaplamak için kullanılan bir mesafe fonksiyonudur; L, çıktı dizesinin bit sayısı ve t, Z+ 'nın tüm pozitif tamsayıların kümesi olduğu hata toleransıdır [46].

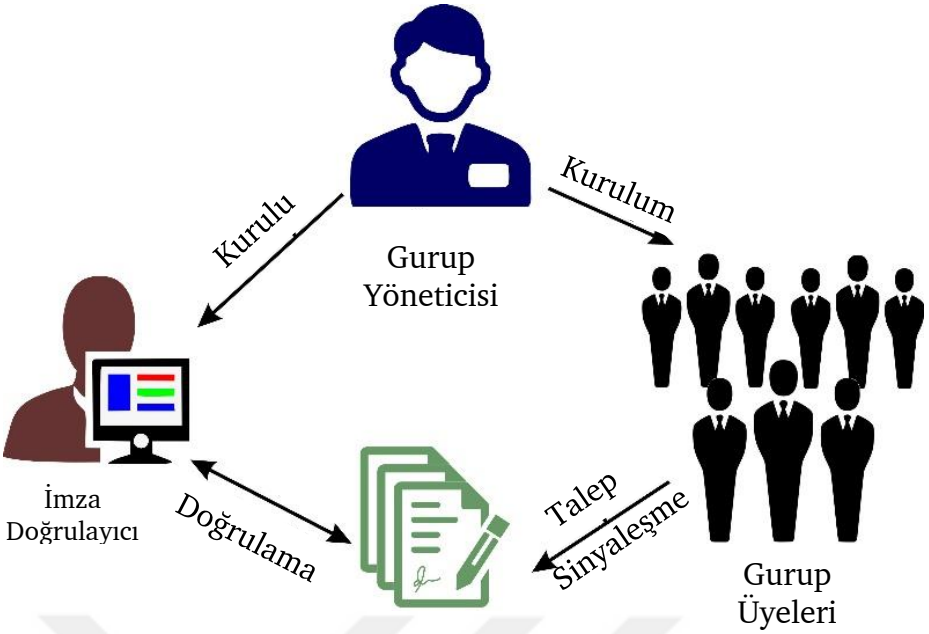
Bulanıklık ayıklayıcı (M, L, t) aşağıdaki iki algoritma ile tanımlanır:

Gen: Bu, girdi olarak bir biyometrik bilgi alan fi ∈M olasılıksal bir algoritmadır ve çıktı olarak bir anahtar veri bi ∈ {0, 1} ve bir genel çoğaltma parametresi pari'yi verir. Başka bir deyişle, Gen(fi) = {bi, pari }.

Rep: Bu, gürültülü bir biyometrik bilgi fi′ ∈ M alan ve fi ile ilgili genel bir parametre pari ve daha sonra biyometrik anahtar verileri, yani bi değerini üreten deterministik bir algoritmadır. Başka bir deyişle, d (fi, fi') ≤ t koşulunu yerine getiren Rep (fi′, pari) = bi sonucu verir.

2.5 Grup imzası

Bir grup imza şeması, grup üyelerinin Şekil 2.1 'de gösterildiği gibi tüm grup adına mesajları imzalamasına izin verir. Mevcut grup imza teknolojisi, Lin, Chao ve diğerleri tarafından önerilen verimli grup imza şemasına dayanmaktadır [14]. Bir grup imzası, daha verimli olan yalnızca tek bir grup ortak anahtarı ile doğrulanabilir. Ayrıca, grup dışındaki kullanıcılar imzalayan kişinin özel kimliğini bilemezler. Bu nedenle, grup imza şeması kamu kaynakları yönetimi, kritik bilgi verilmesi ve sözleşme imzalanmasında uygulanabilir. Blockchain tabanlı bir sistem [14] olan grup imza şemasında, grup üyelerinin uzaktan erişim veya kontrol taleplerini imzalamak için bir algoritma kullanılmıştır. Bu, sisteme anonim erişime imkân verir [47] [48]. Talep, bireysel bir grup üyesi yerine bir grup talebi olarak kabul edilir. Herhangi bir şüpheli davranış durumunda, şema, grup yöneticisinin soruşturma amacıyla belirli bir talebi olan grup üyesini tanımlamasına izin veren izlemesine imkân verebilir. Grup imzasının kısa haline sahip olan şema, iletişim yükünü azaltabilir ve hafif bir işlem sağlayabilir. Bu nedenle IoT doğrulama sistemi için uygundur.



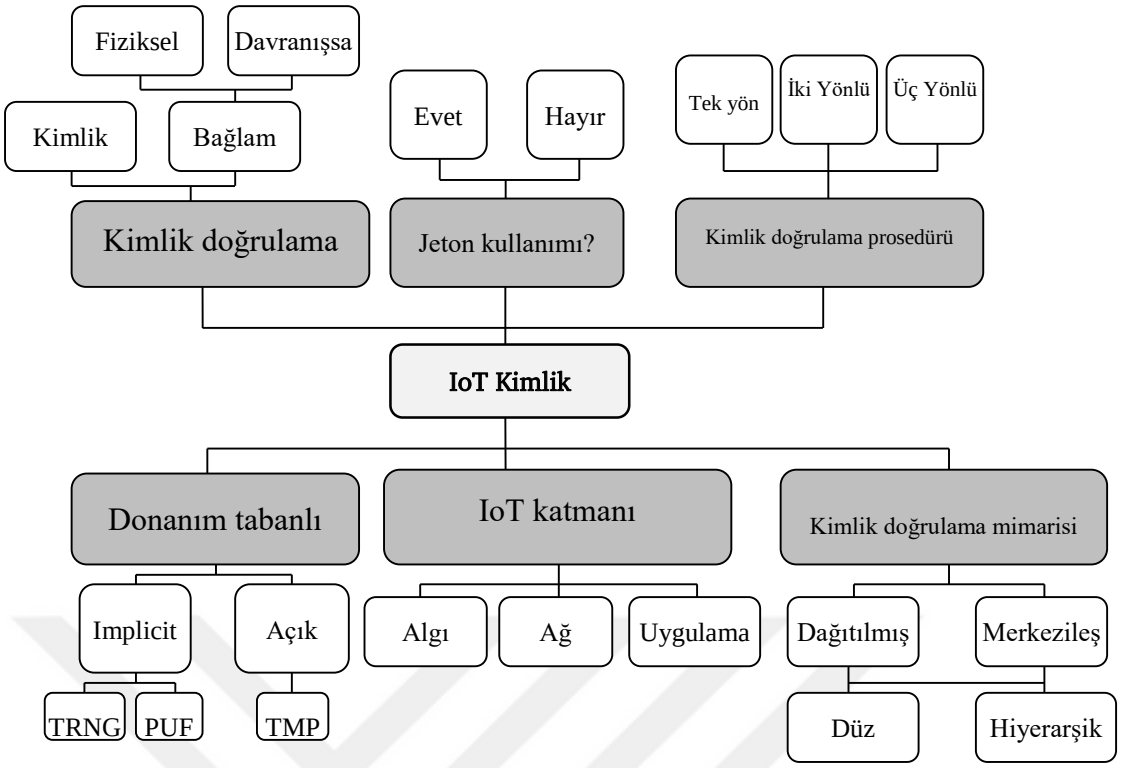
Şekil 2.1 Grup imzası

2.6 Kimlik Doğrulama

IoT'de güvenliğin önemi ve kullanıcının verilerinin gizliliğinin güvence altına alınması gerektiği için, bağlı cihazlar arasında kimlik doğrulama protokolünün uygulanması zorunludur. Ayrıca, kimlik doğrulama sürecini güçlendirmek için, birçok uzman tarafından çeşitli şifreleme teknikleri ve algoritmalarına dayalı farklı kimlik doğrulama protokol modelleri önerilmiştir.

2.6.1 Kimlik Doğrulama Şemalarının Taksonomisi

Bu bölüm, benzerliklere ve bu şemaların ana özelliklerine dayanarak seçilen çeşitli kriterleri kullanarak IoT kimlik doğrulama şemalarının taksonomisini sunar. Daha önce de belirtildiği gibi, kimlik doğrulama, kimlik doğrulama tekniklerinin çeşitliliğini sağlayan IoT mimarisinin üç katmanının her birine uygulanabilir. Bu kriterler Şekil 2.2 'de gösterilmiş ve takip eden bölümlerde özetlenmiştir.



Şekil 2.2 IoT kimlik doğrulama şemalarının taksonomisi [49]

2.6.2 Kimlik doğrulama faktörü

• **Kimlik**: Bir tarafın kendisini doğrulamak için diğerine verdiği bilgilerdir. Kimlik tabanlı kimlik doğrulama şemaları, karma, simetrik veya asimetrik kriptografik algoritmaların birini (veya bir kombinasyonunu) kullanabilir.

• **Bağlam**: ***Fiziksel***: Bir bireyin fiziksel özelliklerine dayanan biyometrik bilgiler, örneğin parmak izleri, el geometrisi, retina taramaları vb. ***Davranışsal***: Bir bireyin davranışsal özelliklerine dayalı biyometrik, örneğin, tuş vuruşu dinamikleri (bir kişi yazdığında oluşturulan ritim ve zamanlama modeli), yürüyüş analizi (yürüme veya koşma şeklimizi değerlendirmek için kullanılan yöntem), ses kimliği (ses izi kullanan ses doğrulaması), vb [49].

2.6.3 Belirteç (Jeton) kullanımı

• **Belirteç (Jeton) Tabanlı** Kimlik Doğrulama: OAuth2 protokolü [50] veya açık kimlik gibi bir sunucu tarafından oluşturulan bir tanımlama jetonuna (veri parçası) dayalı olarak bir kullanıcıyı/cihazı doğrular.

• **Belirteç (Jeton) tabanlı olmayan kimlik doğrulama**: Veri alışverişine her ihtiyaç duyulduğunda kimlik bilgilerinin (kullanıcı adı/şifre) kullanılmasını içerir [49].

2.6.4 Kimlik doğrulama prosedürü

• **Tek yönlü kimlik doğrulama:** Birbirleriyle iletişim kurmak isteyen iki taraflı senaryoda, yalnızca bir taraf diğerine kimliğini doğrularken diğeri kimlik doğrulaması yapmaz.

• **İki yönlü kimlik doğrulama:** Her iki varlığın da birbirini doğruladığı karşılıklı kimlik doğrulama olarak da adlandırılır.

• **Üç yönlü kimlik doğrulama:** Merkezi bir otoritenin iki tarafı doğruladığı ve karşılıklı olarak kendilerini doğrulamalarına yardımcı olduğu durumdur [49].

2.6.5 Kimlik doğrulama mimarisi

Dağıtılmış: İletişim kuran taraflar arasında dağıtılmış bir düz kimlik doğrulama yöntemi kullanmadır. **Merkezi**: Kimlik doğrulama için kullanılan kimlik bilgilerini dağıtmak ve yönetmek için merkezi bir sunucu veya güvenilir bir üçüncü taraf kullanmadır. İster merkezi ister dağıtılmış olsun, kimlik doğrulama şeması mimarisi iki şekilde olabilir: **Hiyerarşik**: Kimlik doğrulama prosedürünü işlemek için çok seviyeli bir mimari kullanır. **Düz**: Kimlik doğrulama prosedürünü uygulamak için hiyerarşik mimari kullanılmaz [49].

2.6.6 IoT katmanları

Kimlik doğrulama prosedürünün uygulandığı katmanı gösterir.

• **Algı katmanı:** IoT platformundaki son düğümler tarafından algılanan verilerin toplanmasından, işlenmesinden ve sayısallaştırılmasından sorumludur.

• **Ağ katmanı:** Algılanan verilerin algı katmanından alınmasından ve işlenmesinden sorumludur.

• **Uygulama katmanı:** Ağ katmanından veri almaktan ve ardından kullanıcılar tarafından talep edilen hizmetleri vermekten sorumludur [49].

2.6.7 Donanım tabanlı:

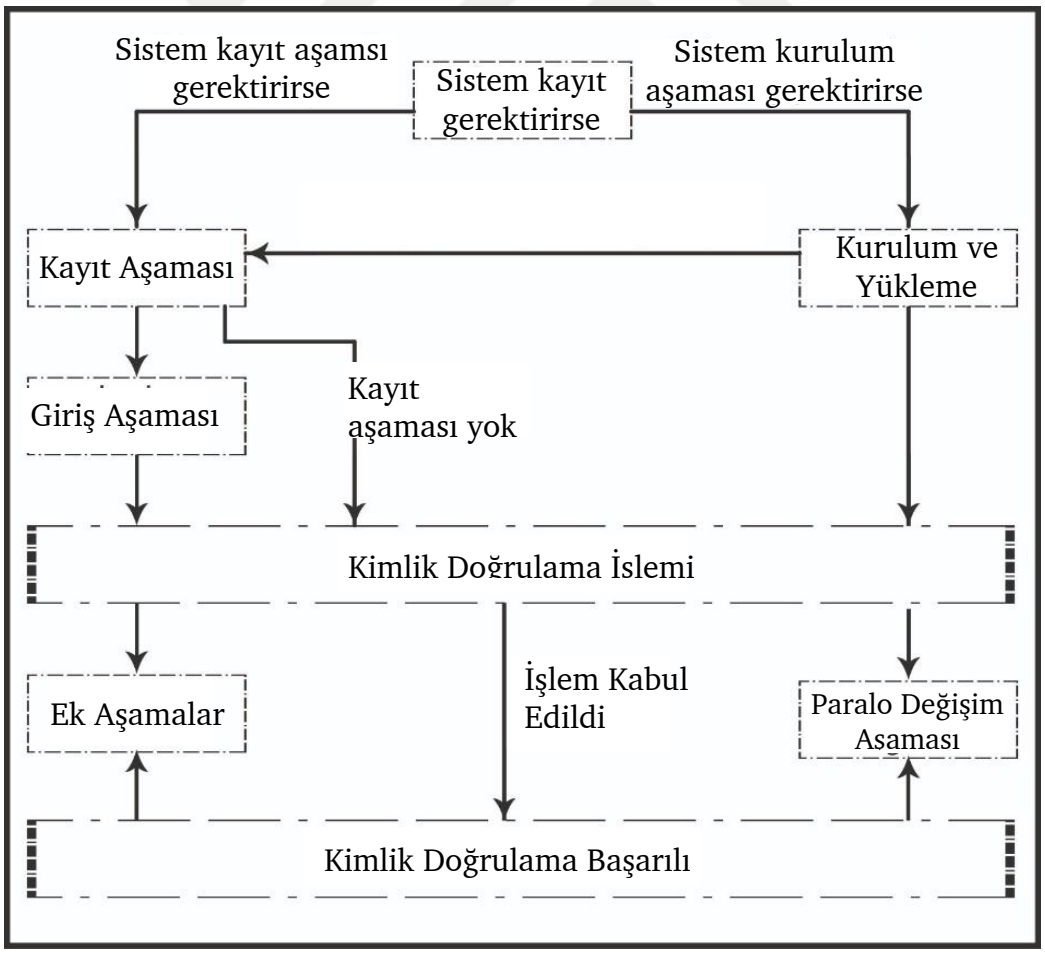
Kimlik doğrulama işlemi, donanımın fiziksel özelliklerinin veya donanımın kendisinin kullanılmasını gerektirebilir. İki tür donanım tabanlı kimlik doğrulama bulunmaktadır. Bunlar;

• **Örtük donanım tabanlı**: Fiziksel Klonlanamayan İşlev (PUF) veya Gerçek Rastgele Sayı Üreteci (TRNG) gibi kimlik doğrulamasını geliştirmek için donanımın fiziksel özelliklerini kullanır.

• **Açık donanım tabanlı:** Bazı kimlik doğrulama şemaları, donanım kimlik doğrulaması için kullanılan anahtarları depolayan ve işleyen bir çip (donanım) olan Güvenilir Platform Modülünün (TPM) kullanımına dayanır [49].

2.6.8 Kimlik Doğrulama Aşamaları

Kimlik doğrulama planlarında birçok faz bulunmaktadır. Bu fazlardan bazıları zorunludur ve bazıları Şekil 2.3 'te gösterildiği gibi başka bir fazla değiştirilebilir. Başlangıçta, kurulum aşaması veya ön hesaplama aşaması diye adlandırılan bir kurulum aşaması vardır. Bu aşama, gizli anahtarları, kimlikler, bazı parametrelerin başlangıç değerlerini oluşturmak için kullanılır ve bu aşamada da önceden paylaşılmış bir anahtar kullanılabilir. Kayıt aşaması, kullanıcıyı veya cihazı sunucu veri tabanına kaydetmek ve kimlik doğrulama için kullanmak üzere kimlik verilerini ilk kez depolamak için kullanılır. Oturum açma aşaması, kullanıcının veya cihazın sisteme erişmek için talep ettiği aşamadır ve sunucu kimlik doğrulama aşamasını başlatmak için bu talebi alır.



Şekil 2.3 Kimlik doğrulama protokolü aşamaları

Kimlik doğrulama aşaması, kullanıcının kimlik doğrulama faktörünü sunucu tarafından kontrol edilmesini ve kimlik doğrulamasını sağladığı aşamadır. Bazı şemalar bu iki fazı bir fazda birleştirir. Kimlik doğrulama aşaması onaylandıktan sonra, parola değiştirme aşaması, bazı şemalarda önerilen parolanın sona erme süresine göre parola değiştirmek için kullanılabilir. Ayrıca, kimlik doğrulama sisteminin işlevselliğini tamamlamak için birçok planda ek aşamalara ihtiyaç vardır. Örneğin, İptal ve yeniden kayıt aşaması, çıkış aşaması, ana ağ geçidi ağ aşamasına yeniden katılma vb aşamalarıdır.

2.7 Blokzincir

Blokzincir, işlem verilerinin kalıcı ve kurcalamaya dayanıklı bir kaydını tutan dağıtılmış bir veritabanı (muhasebe defteri) olarak tanımlanır. Bir Blokzincir, bir uçtan uca ağ sayesinde tamamen merkezsizleştirilmiştir. Daha doğrusu, ağın her bir düğümü, tek bir arıza noktasını engellemek için defterin bir kopyasını tutar. Tüm kopyalar aynı anda güncellenir ve doğrulanır. Kripto para biriminde çift harcama sorununu çözmek için mevcut Blokzincir işleyişi oluşturulmuştur. Bununla birlikte, şu anda çok sayıda çalışma, çoklu kullanım durumlarında Blokzincir uygulamalarını araştırmakta ve bunları dağıtılmış bir veritabanı oluşturmak ve yönetmek ve her tür dijital işlemde kayıtlarını tutmak için güvenli bir yol olarak kullanmaktadır. Bir blokzincir, verileri güvende tutan iki seviyeli şifreleme kullanır. Bunlardan ilki anahtar şifreleme yöntemi, diğeri ise karma fonksiyonlardır. Bir tür harici koruma katmanı olan anahtar şifreleme, düğümler arasında güvenli işlem iletimi sağlar. Blokzincir kriptografik yöntemleri, bir blokta geri döndürülemez veri şifreleme prosedürü olan özet (hash) işlevlerdir. Bloktaki tüm veriler, geri dönüşü olmayan SHA256 özet algoritması ile şifrelenir. Bu nedenle, bir Blokzincirde iki seviyeli kriptografi kullanmak sistemi daha güvenilir yapar. Blokzincir defteri birden fazla bloktan oluşur, her blok iki bölümden oluşur. Birincisi, parasal işlemler, sağlık verileri, sistem günlükleri, trafik bilgileri vb. gibi herhangi bir türde olabilecek işlemleri veya olguları (veritabanının saklaması gereken) temsil eder. İkincisi başlık olarak adlandırılır ve kendi bloğu hakkında bilgi içerir, örneğin zaman damgası, kendi işleminin karması, vb. aynı zamanda

bir önceki bloğun karması. Böylece, mevcut blokların kümesi, bağlantılı ve sıralı bloklar zinciri oluşturur. Zincir ne kadar uzunsa, onu bozmak o kadar zordur. Gerçekten de, kötü niyetli bir kullanıcı bir bloktaki bir işlemi bozmak veya değiştirmek isterse, hash'leriyle bağlantılı oldukları için aşağıdaki tüm blokları değiştirmelidir. Ardından, her katılımcı düğümün depoladığı blok zincirinin sürümünü değiştirmelidir [51]. Blok zincirinde tipik olarak iki tür düğüm vardır. İlki, blok verilerini depolamaktan ve okumaktan sorumlu aktif olmayan bir düğümdür. Etkin olmayan düğümler yeni bir blok oluşturamaz veya bir işlem başlatamaz. İkincisi, bir blok oluşturan ve işlemleri doğrulayan madenci düğümdür. Blokzincir türlerine göre, sistem, madencileri ağa katılmaları, konsensüs mekanizmasını yürütmeleri ve dağıtılmış defteri korumaları için seçer. Madencilerin seçimi, farklı Blokzincir türlerine göre değişir. Örneğin, Kamu Blok Zincirinde, herhangi bir düğüm dâhil olabilir ve sistem madenciler olarak katılan katılımcıları destekler. Öte yandan, Özel Blokzincirde, özel dağıtım farklı fikir birliği mekanizmalarını seçer ve genellikle katılımcıları teşvik etmesi gerekmez. Hem kamu hem de özel Blockchain içeren ve melez Blockchain olarak adlandırılan başka bir Blockchain türü daha vardır, sistem tüm katılımcıların bir madenci olarak katılmasına izin verir. Ancak Blokzincir ağına katılımda kısıtlamalar vardır.

2.8 Literatür Araştırması

Akıllı cihazların ve nesnelerin internetinin günlük yaşamın çeşitli alanlarında yaygınlaşması, başta gizlilik endişeleri olmak üzere çeşitli yeni güvenlik sorunlarının ortaya çıkmasına yol açmıştır. Ne yazık ki, bu cihazları yönetmekten sorumlu sistemlerin çoğu hassas bilgileri korumak için gerekli yetkinlikten yoksun olabilir ve bu kaynak, maliyet veya tasarım kısıtlamalarından kaynaklanabilir. Bu nedenle, kullanıcıyı ve akıllı IoT cihazlarını yönetebilecek ve güvenliği ihlal, hassas bilgileri ifşa ve kullanıcının gizliliğini ihlal etme girişimlerinden koruyabilecek mekanizmalara ihtiyaç duyulmaktadır. Göz önünde bulundurulması ve dikkat edilmesi gereken en önemli hususlardan biri, kullanıcının kimliğini doğru tespit etmek ve sisteme bağlı cihazları güvenceye almaktır. Bu nedenle, bu güvenlik sorunlarını çözmeye veya risklerini azaltmaya yönelik literatürde birçok çalışma bulunmaktadır. [52], [53], [54], [55]'deki yazarlar güvenli bir kimlik doğrulama

protokolü tasarlamak ve gömülü cihazlar ile bulut sunucuları arasındaki iletişimi güvence altına almak için ECC (Eliptik Eğri Kriptografi) yi kullanmıştır. Ayrıca, IoT uygulama katmanında iki yönlü bir kimlik doğrulama prosedürüne dayanırlar, merkezi ve düz kimlik doğrulama mimarisi kullanılır ve belirteç (jeton) tabanlı protokol kullanılır. [54], [55] dışında bu yöntemlerde kurulum aşaması dikkate alınırken, kayıt, oturum açma ve kimlik doğrulama gibi diğer aşamalar kullanılır. Bu önerilen şemalarda şifre değişikliği ve herhangi bir ek aşama dikkate alınmaz. Ne yazık ki, [52]'de karşılıklı kimlik doğrulama zafiyeti, oturum anahtarı belirsizliği ve şifre saldırısını tahmin etme gibi bazı zayıf yönleri vardır. MITM, tekrar eden saldırılar gibi bazı saldırı türlerine karşı dayanıklıdırlar, ancak zamanlama saldırıları, sahtecilik saldırıları ve DoS gibi saldırıların bazılarına karşı zayıf kalır. [56], [57], [58], [59]'de yazarlar uzaktan kimlik doğrulama şeması önermiştir. Kimliği üç yönlü bir kimlik doğrulama prosedürü sayesinde bir kimlik doğrulama faktörü olarak kullanırlar; uygulama katmanı bu şemalardaki kimlik doğrulamasından sorumludur. Düz ve merkezi mimari tarzı bir kimlik doğrulama sistemi kullanılmıştır. Kurulum, kayıt, giriş ve kimlik doğrulama gibi farklı kimlik doğrulama aşamaları kullanılır ve [57], dışında şifre değişikliği aşamaları kullanılmaz. [56], [58]'deki yaklaşımlar kayıt için güvenli bir kanala ihtiyaç duyar ve bunlar ECC şifrelemesine dayanır. [57], [59]'deki yaklaşımlar şifreleme ve kayıt için önceden paylaşılan anahtar olarak kullanılırken, şifreleme ve kayıt için de önceden paylaşılan anahtar olarak kullanılır ve ayrıca XOR işlemine ve tek yönlü karma işlevine dayanır. Bu şemalar bazı saldırı türlerine karşı dayanıklıdır, ancak DoS saldırısına karşı zayıf kalır. Bu yöntemlerden bazıları daha yüksek hesaplama ve iletişim maliyetlerine sahiptir. [60], [61], [62]'de akıllı ev ve makineden makineye sistemler için ECC şifrelemesine dayanan güvenli kimlik doğrulama ve iletişim şeması önermişlerdir. ECDH anahtar değişimi [61], [62]'de kullanılır. [60], [62]'de kayıt için güvenli kanal gereklidir. Bu planlar birçok güvenlik saldırısına karşı dayanıklıdır. Bununla birlikte, [60], [62]'de DoS saldırısı gibi bazı dezavantajlar vardır. [63]'de yazarlar, Biyo Kimliğe, Akıllı karta ve Parolalara ek olarak benzersiz adresleme ve tanımlama için IPv6 başlıklarına dayanan bir kimlik doğrulama şeması önermiştir. Kimlik doğrulama için, Simetrik şifreleme, Bio özet (hash) ve tek yönlü özet fonksiyonuna dayanır. Daha önce listelenen tüm

çalışmalarda, akıllı bir ev için çevrimdışı ortamda kimlik doğrulama sistemi modelinden bahsedilmediğini gördük. Bu, listelenen modelleri internet hizmeti olmadan kullanamayacağınız anlamına gelir. İnternet hizmetine ihtiyaç duymadan akıllı ev içinden kullanılabilen kimlik doğrulama ve güvenli iletişim sistemi için alternatif bir yol bulunmamaktadır. Bu tez çalışmasında, yalnızca yerel bir ağ kullanarak çevrimdışı ortamda kimlik doğrulama ve güvenli iletişim için kullanılabilecek bazı çözümler önerilmiştir. Tezde sunulan çalışmalar son dönemdeki benzer çalışmalarla karşılaştırılmış ve eksiklerini iyileştiren yeni bir model önerilmiştir. Burada her bir benzer çalışmanın avantaj ve dezavantajlarını gösteren temel özellikleri ele alınmıştır. 2017'de yayınlanan Wang ve ark.'nın Şeması [54], modelleri kayıt ve Kimlik Doğrulama aşamasını içerir. Kayıt ve Kimlik Doğrulama için gerçek cihaz kimliği kullandı. Kayıt için güvenli bir kanala ihtiyacı vardır. ECC tuş çiftlerine, ECC noktasının skaler çarpımına, hash fonksiyonuna, XoR işlemine dayanır. Hesaplama karmaşıklığı 209.0221 ms'ye mal olur. Toplam boyutu 1568 bit olan kimlik doğrulama için 3 mesaj kullanır. Bazı güvenlik tehditlerine karşı koyabilir, ancak Hizmet Reddi (DoS) saldırısı, Gizlice Dinleme Saldırıları ve İleri Gizlilik saldırısı için güvensizdir. Veri Gizliliği ve Güvenilirliği, Anonimlik, Gizlilik ve GDPR Uyumluluğu dikkate alınmaz. 2020'de yayınlanan Wang ve ark.'nın Şeması [55], modelleri kayıt ve Kimlik Doğrulama aşamasını içerir. Kayıt için gerçek cihaz kimliği, Kimlik Doğrulama için sahte kimlik kullandı. Kayıt için güvenli bir kanala ihtiyacı vardır. ECC tuş çiftlerine, ECC noktasının modüler üsteline, çift doğrusal haritalamaya, ECC noktasının skaler çarpımına, hash fonksiyonuna ve XoR işlemine dayanır. Hesaplama karmaşıklığı 164.5702ms'ye mal olur. Toplam boyutu 1404 bit olan kimlik doğrulama için 3 mesaj kullanır. Bazı güvenlik tehditlerine karşı koyabilir, ancak Hizmet Reddi (DoS) saldırısı ve İleri Gizlilik saldırısı için güvensizdir. Veri Gizliliği ve Güvenilirliği, Anonimlik, Gizlilik ve GDPR Uyumluluğu dikkate alınmaz. 2020'de yayınlanan Kumar vd.' nin Şeması [63], modelleri Başlangıç, Adresleme, kayıt, Kimlik Doğrulama, Oturum Anlaşması ve Şifre Güncelleme aşamasını içerir. IPv6 adresleme şemalarına dayanmaktadır. Kimlik Doğrulama için bir akıllı kart, şifre ve kullanıcı biyometrik kimliği kullanır. Biyometrik karma, simetrik şifreleme/şifre çözme ve karma işlevini kullanır. Hesaplama karmaşıklığı 209.0221ms'ye mal

olur. Toplam boyutu 959 bit olan kimlik doğrulama için 5 mesaj kullanır. Bazı güvenlik tehditlerine karşı koyabilir. Gizlilik ve GDPR Uyumluluğu dikkate alınmaz. Güvenlik ve gizlilik sağlamakla ilgili merkezi olmayan kimlik doğrulama şeması. Zhihua Cui *ve ark*. [64] çoklu kümeler, küme kafaları (clusters heads) ve baz istasyonlarından oluşan IoT sistemleri için kullanılabilecek bir kimlik doğrulama şeması önerdi. Her bir baz istasyonu için yerel Blokzincire dayanır ve tüm baz istasyonlarını genel Blokzincir ile birleştirir. Ma Zhaofeng *ve ark.* [65]*,* IoT ortamında merkezi olmayan bir kimlik doğrulama olan BlockAuth'u önermiştir. Bu çalışma, tek taraflı ve hata toleransı zayıf olan merkezi, geleneksel kimlik doğrulama modellerine göre, merkezi olmayan bir Blokzincir tabanlı model kullanarak hata toleransını artırabilecek bir model önermiştir. A. Patwary *ve arkadaşları* [66] kimlik doğrulama mekanizmasını geliştirmek için cihaz konum bilgilerine dayanan bir Blokzincir kimlik doğrulama modeli önermişlerdir. Tüm cihazların üzerinde anlaşmaya varılabileceğini ve güvenilir konum bilgileri sağlayabileceğini varsayarlar. Chao Lin *ve diğerleri* [14] HomeChain adlı bir IoT ortamında Blokzincir kullanarak grup imzasına dayalı merkezi olmayan bir kimlik doğrulama şeması önermişler ve grup isteği doğrulaması yapmak için grup imzasını kullanmışlardır. Tüm kontrol talepleri ve yanıtları Blokzincirde bir blokta saklanır. Bu yaklaşım yüksek bir güvenlik düzeyi sağlasa da, süreç için para maliyetine ek olarak, madencilik için blok oluşturma ihtiyacından dolayı zaman alıcıdır. Bu yaklaşımda kullanılacak net bir anahtar değişim mekanizması bulunmamaktadır. Kuruluşlar ve ana ağ geçitleri arasında doğrudan bir kanal yoktur, bu nedenle istekler ve yanıtlar gönderen kuruluşlardan alıcı kuruluşlara herhangi bir bildirim yapılmadan akıllı sözleşme aracılığıyla dolaylı olarak alınacağından bir senkronizasyon sorunu ortaya çıkacaktır. Hammi *ve arkadaşları* [51] cihazların tanımlanmasını ve kimlik doğrulamasını sağlayan Güven Kabarcıkları (Bubbles of Trust) adı verilen merkezi olmayan bir sistem önermektedir. Ayrıca bu, veri bütünlüğünü ve kullanılabilirliğini korur. Böyle bir hedefe ulaşmak için önerilen yaklaşım Blokzincirler tarafından sağlanan güvenlik avantajları sayesinde, şeylerin birbirini tanımlayabileceği ve güvenebileceği güvenli sanal bölgeler (baloncuklar) yaratmaya yardımcı olur. Zhang *ve ark.* [67] Blokzincir tabanlı mobil- kenar bilgi işlem için bir kimlik doğrulama şeması

önermiştir. Blokzincir ile oluşturulan bloğu doğrulamak için bir grup imzası kullandılar. Blok validasyonu imzaya göre uygulanır. Blok, onu oluşturan gruba aittir. Jiang *ve ark.* [68] taşıt geçici ağları için kullanılan bir kimlik doğrulama yaklaşımı önermiştir. Koşullu gizlilik ve anonimlik elde etmek için güvenilir bölge otoritesine ek olarak kimlik doğrulama için grup imzasını kabul etmişlerdir. Zhang *ve diğerleri* [69] hesaplama verimliliği elde etmek için Grup Oturumu Anahtarını toplu grup imzasıyla birlikte kullanarak Araç Geçici Ağları için bir kimlik doğrulama şeması önermiştir.

Bu çalışma çoklu bir grup modeli önermektedir ve her grup, tüm grup üyelerinin işlemleri imzalamak ve diğer uzak cihazlarla anonim olarak iletişim kurmak için kullanabileceği bir grup imzası oluşturur. Bununla birlikte, önceki literatür çalışmaları güvenlik ve gizlilik sorunlarını azaltabilir. Yine de, aşılması gereken kritik zorluklar vardır. Benzer çalışmaların bu özelliklerine kıyasla, tez çalışmasında önerilen şema daha yüksek performans, düşük hesaplama maliyeti ve daha fazla güvenlik tehdidine karşı direnç göstermektedir. Karşılaştırma ve performans değerlendirmesi 4. Bölüm'de ayrıntılı olarak açıklanmıştır.

3
METODOLOJİ

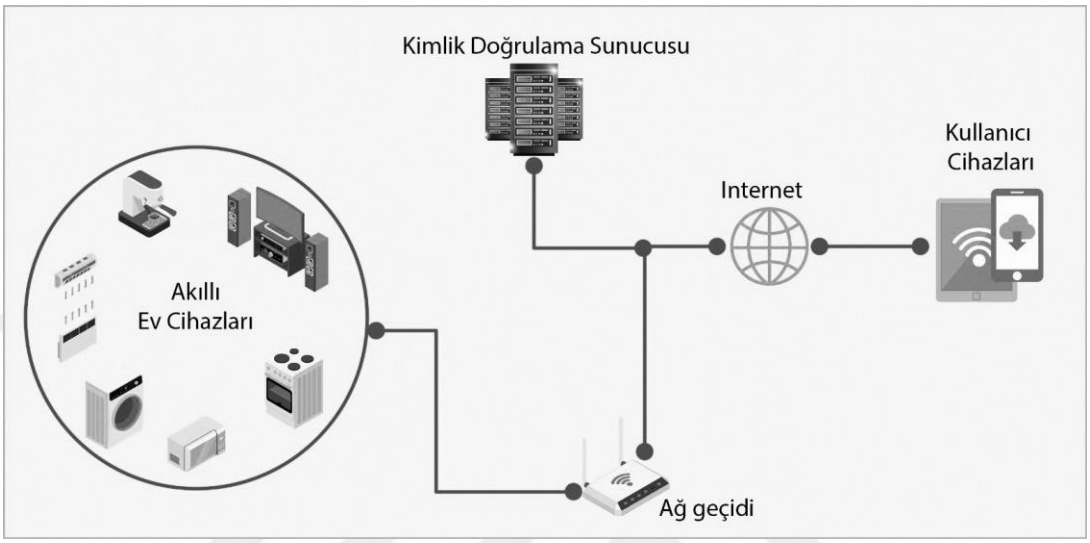
Akıllı ev ortamı için önerilen kimlik doğrulama mekanizması iki ana duruma dayanmaktadır. İlk durum, çevrimdışı doğrudan kimlik doğrulama modu olarak adlandırdığımız ev kaçamağı aracılığıyla doğrudan yerel sunucuya bağlanan akıllı IoT cihazlarının ve kullanıcı cihazlarının kimliğini doğrulamaktır. İkinci durum ise çevrimiçi kimlik doğrulama modu dediğimiz internet üzerinden akıllı eve uzaktan bağlanan kullanıcılardır.

Çevrimdışı doğrudan kimlik doğrulama modunda, şu anda popüler olan çeşitli teknolojilerden faydalanılmıştır. Geliştirilen program, kayıt için benzersiz kimliği göndermek için görsel bir kanal, akıllı kart olarak QR Kodunu kullanmaktadır. Ayrıca, kimlik doğrulama için sahte rastgele kimlik ve gizli belirteç (token) de kullanılır. Çevrimiçi kimlik doğrulama modunda, uzaktan kullanıcı kimlik doğrulaması için Blokzincir tarafından kullanılan bulanık çıkarıcı algoritması ve grup imzası tekniğini kullanarak biyometrik verileri temel aldık. Her durum için farklı kimlik doğrulama teknikleri önerdik. Bu iki tekniği tek bir kimlik doğrulama sisteminde birleştirmek, performans verimliliğini, güvenilirliği, güvenliği, kullanıcı gizliliğini artırır ve işletme maliyetini azaltır.

3.1 Akıllı Ev Sistemi Modeli

Kablosuz iletişim için arayüzlerle donatılmış tüm ev cihazları, ev ağını oluşturur. Her evin bir kablolu (veya/ve) kablosuz iletişim ağı vardır ve her cihazdan algılanan veriler, ev havuzu veya ev merkezi olarak adlandırdığımız bir merkezi istasyona iletilir. Ev ağındaki her düğüm akıllı bir cihaz olarak kabul edilir ve orta düzeyde hesaplama ve iletişim yeteneklerine sahiptir. Ev merkezi, bir miktar veri depolama kapasitesine sahip, yerel işlem yapabilen ve ev ağı dışındaki cihazlarla iletişim kurabilen herhangi bir cihaz (akıllı sayaç, PC, tablet veya akıllı telefon) olabilir. Akıllı konut kompleksleri veya akıllı binalar söz konusu olduğunda, ana merkezin karşılığı konut havuzu veya konut merkezi olarak tanımlanır. Konut merkezinin, ana merkeze kıyasla ek bir özelliğe sahip olması gerekir, bu, paylaşılan dağıtılmış üretim kaynaklarına/kaynaklardan gelen verileri yönetmekten sorumludur. Yenilenebilir kaynaklar genellikle tüketiciler arasında

paylaşıldığı için bu oldukça önemlidir, bir örnek, binadaki tüm hanelerin PV sistemini kullandığı çatıda güneş fotovoltaik PV sistemine sahip bir konut binasıdır. Bu çerçevede, dağıtılan her bir yenilenebilir enerji kaynağı akıllı cihaz olarak kabul edilmektedir. [70] Şekil 3.1 'de akıllı ev genel mimarisi gösterilmektedir.



Şekil 3.1 Akıllı ev mimarisi

IoT sistemlerindeki akıllı cihazlara iddia ettikleri gibi güvenilebileceğini garanti etmek için güçlü IoT cihazı kimlik doğrulaması gereklidir. Sonuç olarak, her bir IoT cihazı, bir ağ geçidine veya merkezi sunucuya bağlanmaya çalıştığında doğrulanabilen farklı bir kimliğe ihtiyaç duyar. IoT sistem yöneticileri, her cihazı varlığı boyunca takip edebilir, onunla güvenli bir şekilde iletişim kurabilir ve bu benzersiz kimlik yerinde iken tehlikeli işlemler yapmasını yasaklayabilir. Yöneticiler, olağandışı davranışlar sergileyen bir cihazın ayrıcalıklarını kolayca geri çekebilir. Akıllı ev sisteminde, bu cihazlara erişimi kontrol eden yerel bir sunucu kullanarak bir araya gelmek üzere bağlanan kullanıcıya çeşitli hizmetler sunan farklı IoT cihazlarımız bulunmaktadır. Kullanıcılar bu IoT cihazlarına evin içinden veya dışından erişebilir ve kontrol edebilir. Bu durumda aşağıda açıklayacağımız iki senaryomuz vardır. Aşağıdaki bölümlerde ayrıntılı bir şekilde açıklanacaktır.

3.1.1 Akıllı Sistem Erişim Senaryoları

İlk senaryo, kullanıcının yerel ağı kullanarak IoT cihazına evin içinden erişmek istemesidir. Bu nedenle, akıllı ev sistemine bağlanmak ve erişmek için çevrimdışı bir kimlik doğrulama sistemine ihtiyaç vardır. İkinci senaryo, kullanıcının internet bağlantısını kullanarak ev dışından IoT cihazına erişmek istemesidir. Bu durumda, kullanıcıların akıllı ev sistemine erişmelerine ve IoT cihazlarını kontrol etmelerine izin vermek için çevrimiçi kimlik doğrulamaya ihtiyaç vardır. Her iki senaryoda da kullanıcı gizliliği dikkate alınmalıdır. Kullanıcı gizliliğini göz önünde bulundurmak ve GDPR'ye uymak için anonim erişim uygulanmalıdır.

3.1.2 Varsayım

Her Akıllı ev cihazının bir akıllı kartı vardır ve bu kart kayıt için karta yerleştirilmiş bir genel anahtara sahip evrensel benzersiz bir kimlik içerir. Bu kart üretim zamanında verilir. Her kullanıcı cihazının ayrıca evrensel olarak benzersiz bir kimlik içeren bir akıllı karta ihtiyacı vardır, bu kimlik kullanıcı cihazı tarafından oluşturulur ve akıllı kartta saklanır. Kullanıcı cihazları, akıllı ev cihazları ve yerel (Edge) kimlik doğrulama sunucusu arasındaki iletişim için kullanılabilecek kablolu veya kablosuz yerel bir ağ ardır. Grup aile üyelerinden oluşmaktadır. Buna ek olarak, grup yöneticisi aile üyelerinden biridir (örneğin ebeveynlerden biri).

3.1.3 Sistem Mimarisi

Herhangi bir akıllı ev sisteminde, birkaç IoT cihazı, yetkili kullanıcılar tarafından bu cihazlara erişimi kontrol eden ana sunucuya bağlı akıllı ev cihazları olarak işlev görür. IoT cihazları, yerel bir ağ geçidi veya Edge sunucusu kullanarak yönetim sunucusuna bağlanabilir. Kullanıcı akıllı ev hizmetine dışarıdan veya evin içinden erişebilir. Akıllı ev sistemindeki IoT cihazı, bellek ve işlemedeki kaynak sınırlamasına göre hafif kimlik doğrulama kullanan güvenli bir erişim mekanizmasına ihtiyaç duyar. Kimlik doğrulama sistemleri kullanıcı gizliliği ile ilgili olmalı ve GDPR ile uyumlu olmalıdır. Verimlidir ve güvenlik saldırılarına karşı bağışıklığı vardır. Tüm bu gerekli özelliklere göre, Şekil 3.2 'deki sisteme göre tasarlanmış bir model önerdik. Şekil 3.3'te gösterildiği gibi, bu model çevrimiçi ve çevrimdışı senaryolarda kullanılabilecek bir kimlik doğrulama yöntemi sağlar. Bu sistem aşağıdakilerden oluşur:

Kimlik Doğrulama Seviyesi

Bu sistem, üç kimlik doğrulama seviyesi içerir

- **Kullanıcı Kimlik Doğrulaması:** Bu kimlik doğrulama, cihaz sahibinin bulanık çıkarıcı üzerinde biyometrik doğrulama tabanını kullanmasını sağlamak için kullanıcı ve kullanıcı cihazı arasındaki doğrulamadır.
- **Kullanıcı cihazı Kimlik Doğrulaması:** Mobil Uygulama veya Web sayfası kullanan kullanıcı cihazı ile yerel sunucu arasındaki bu kimlik doğrulama, ev erişim bağlantı türüne (Yerel veya Uzak) dayanmaktadır.
- **M2M Kimlik Doğrulaması:** Akıllı ev cihazlarını (IoT cihazları) ev yerel sunucusu (Edge sunucusu) ile doğrulamak için kullanılır.

Kimlik Doğrulama Modu

Bu sistemin iki modu vardır

- **Çevrimiçi mod:** Akıllı ev cihazlarını bağlamak ve kontrol etmek için kullanıcının kimliğini doğrulama amasıyla uzaktan kimlik doğrulamayı kullanmadır.
- **Çevrimdışı mod:** İnternet bağlantısı olmaması ve çevrimdışı ortam olması durumunda yerel kullanıcıya ek olarak yerel IoT cihazlarının kimliğini doğrulamak için kullanılır.

Cihaz düzeyinde

Dört cihaz seviyesi vardır

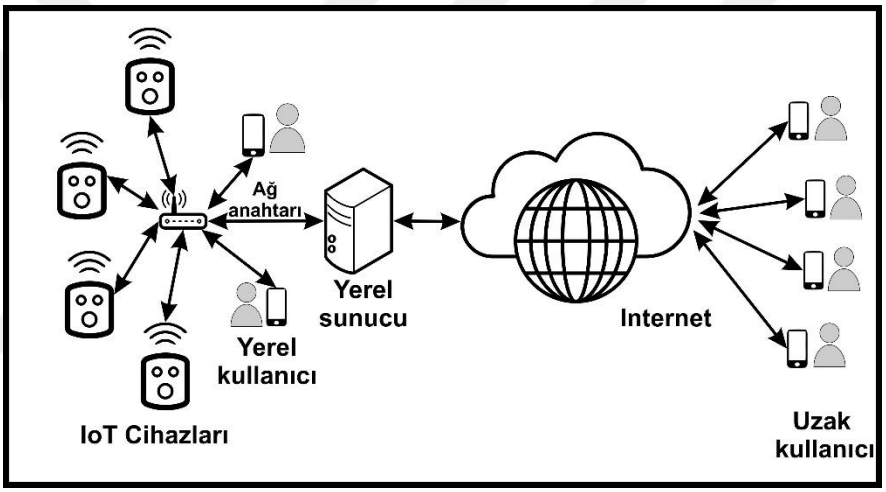
- **Kullanıcı cihazı:** Kullanıcı tarafından kullanıcı arayüzünü kullanmak için kullanılan cihaz (mobil, PC, vb.).
- **Yerel (uç) sunucu**: IoT cihazlarını bağlamak ve yönetmek için sunucu olarak kullanılan yerel cihaz.
- **IoT cihazları**: Yerel sunucuya bağlı akıllı ev cihazları.
- **Blokzincir ağı**: Blok zincirindeki yeni bloklar için akıllı sözleşmeleri ve madenciliği dağıtmaya dahil olan tüm düğümlerden oluşur.

Kimlik doğrulama mekanizması

- **Uzaktan Kimlik Doğrulama Mekanizması:** Ağdaki kullanıcıların kimliğini doğrulamak için Blockchain ile Grup imzasına dayanır. Bu mekanizma bir

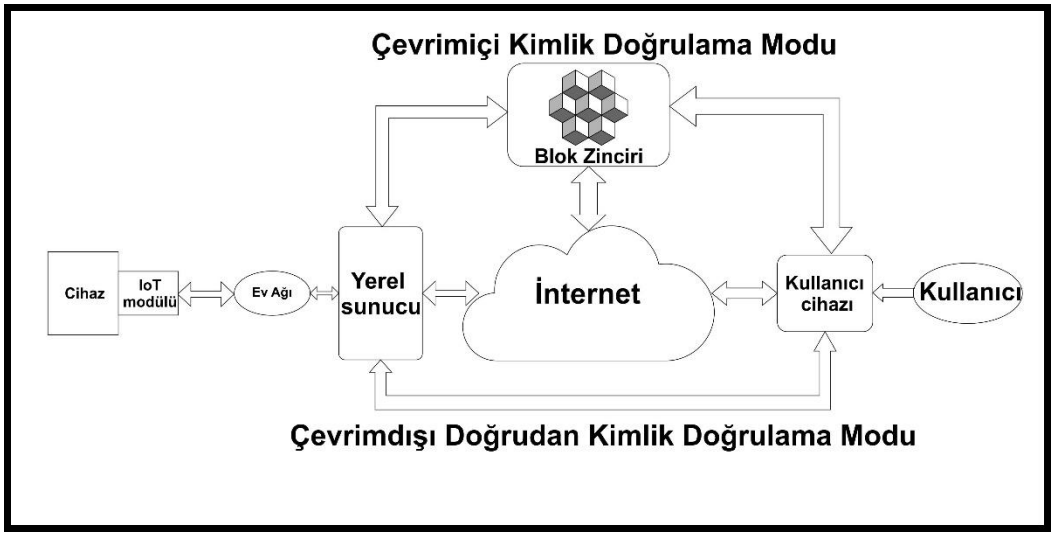
internet erişimine ihtiyaç duyar ve uygulama için Blockchain ile akıllı bir sözleşme dağıtır, bu mekanizma çevrimiçi modda kullanılır.

- **Yerel Kimlik Doğrulama Mekanizması**: Kullanıcılar ve cihazlar, yalnızca yerel ağ ve uç sunucu kullanılarak, internet erişimi olmadan yerel olarak doğrulanabilir. Bu mekanizma çevrimdışı modda kullanılır. Tüm bu gerekli özelliklere göre, Şekil 3.2 'de genel hatları ile sistem tasarlanmış ve bir model olarak resmedilmiştir. Bu model akıllı ev iletişiminin genel bir özeti şeklindedir. IoT cihazları üzerinden kullanıcılar yerel sunuculara yerel sunucuya bağlanır. Uzak bağlantı yapacak kullanıcılar ile iletişim bu şekilde sağlanmaktadır.Yerel sunucu üzerinden sağlanan merkezi kimlik doğrulama, akıllı ev cihazları ve ev içindeki yerel kullanıcılar için yerel kimlik doğrulama modeli olarak kullanılır.



Şekil 3.2 Akıllı ev iletişimi

Bu akıllı ev, yerel sunucuya bağlı yerel kullanıcılar ve akıllı ev cihazlarından oluşur, internet üzerinden akıllı eve bağlanan uzak kullanıcılara ek olarak, ev ağ geçidi yerel ağ üzerinden bağlanan ev cihazlarını yönetir.



Şekil 3.3 Akıllı ev kimlik doğrulama sistemi

Şekil 3.3, hem çevrimiçi hem de çevrimdışı modlar için kimlik doğrulamayı gösterir; çevrimdışı kimlik doğrulama, yerel kullanıcıların ve ev cihazlarının kimliğini doğrulamak için yerel sunucuyu kullanır. Çevrimiçi mod, Blokzincir kullanarak internet üzerinden uzaktaki kullanıcıların kimliğini doğrulamak için kullanılır.

3.2 Çevrimdışı Doğrudan Mod için Önerilen Model

Bu çalışma, Wu ve diğerleri [37] tarafından 2020'de önerilen protokolde bir iyileştirme önermiştir. Orijinal protokolün kayıt aşaması için güvenli bir kanala ihtiyacı vardır ve çevrimdışı ortamda kimlik doğrulama için alternatif bir yol yoktur. Şemamız, yerel ağda kullanıcının kimliğini doğrulamak için yerel sunucu ile geliştirilmiş protokoldür.

3.2.1 Önerilen Algoritma

Bu çalışmada, Algo.1'de (kullanıcı/IoT) cihaz tarafı ve Algo.2'de yerel sunucu tarafı için sözde kod kullanılarak kimlik doğrulama algoritması önerilmiştir.

Algoritma 1: Cihaz Tarafı

Başlatma:
Ri←rastgele ()←
Girdi:
Saklanan veriler Tki, Did, Ex, Pks'yi okur
Gi←ECC.g*Ri←
RID←karma (Gi) ⊕(Tki+Did+Ex)←
M←ECC_encrypt(Gi,Pks)←
Çıktı:
Gönder(M,RID)
(! Alındığı zaman (Gj, P1))
Bekle()
P1'←karma(Gi+Gj)←
Eğer P1 ≠P1' ise
Bağlantıyı sonlandırır
Dönüş(0)
Başka
P2←karma(P1+(Gj*Ri))←
Gönder (P2)
Session_Key←karma (Did+(Gj*Ri))←
Dönüş (Oturum_Anahtarı)
Son:

Algoritma 2: Sunucu Tarafı

Başlatma:
Rj ← Rastgele ()
Girdi:
Depolanan veriler pks, xs'yi okur
(! Alındığı zaman (M,RID))
Bekle()
Gi←ECC_şifresini çözer(M,pks)←
Tki,Did,Ex ←karma(Gi) ⊕RID←
Tki'←karma(karma(xs)+Did+Rtm)←
Çıktı:
Eğer Tki'≠Tki ise
Bağlantıyı sonlandırır
Dönüş(0)
Başka
Gj ← ECC.g*Rj
P1 ← karma(Gi+Gj)
Gönder(Gj,P1)
(! Alındığı Zaman (P2))
Bekle()
P2'←karma(P1+(Gi*Rj))
P2 ≠P2' ise
Bağlantıyı sonlandır
Dönüş(0)
Başka
Oturum_anahtar←karma (Did+(Gi*Rj))
Dönüş (Oturum_Anahtarı)
Son:

3.2.2 Kurulum Aşaması

Bu sistemdeki her cihaza (akıllı cihaz, kullanıcı cihazı veya sunucu) RFC 4122 [71] [72] ile uyumlu 128 bit uzunluğunda evrensel benzersiz bir kimlik (UUID) atanmıştır. Bu UUID, bir ad alanının (ISO nesne kimliği) SHA-1'i ve ağ MAC adresinin SHA-1'i temelinde oluşturulur. Sunucu, brainpoolP256r1 256-bit asal alan Weierstrass eğrisi [73] [74] ve 256-bit uzunluğunda uzun vadeli bir gizli anahtar (x) kullanarak ECC anahtar çifti (Privet, Public) üretir. Kayıt Aşaması Önerilen şemamızda, kullanıcı cihazı ve IoT cihazı için kayıt aşaması deyatları ile verilmiştir.

Kullanıcı cihazı Kayıt Aşaması

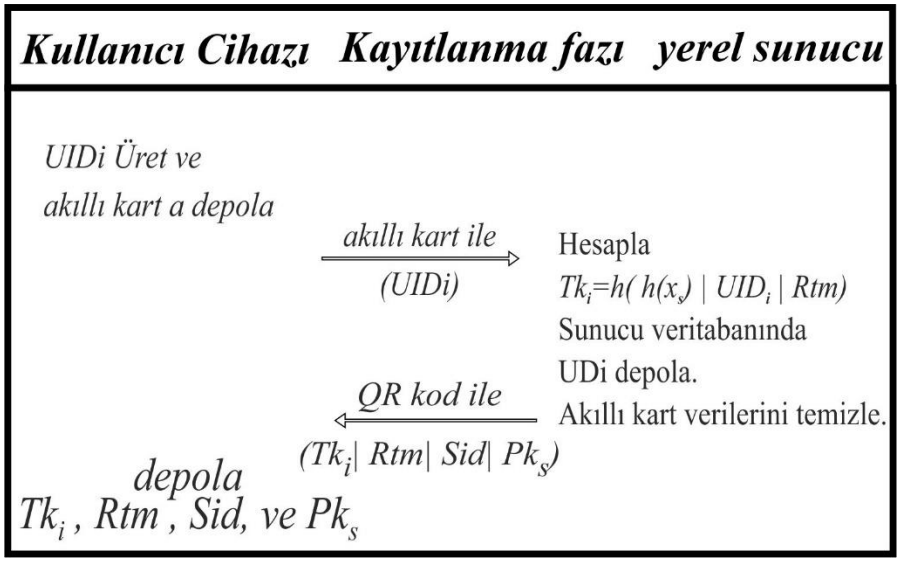
Bu aşamada kullanıcı, UID'yi içeren akıllı kartı sunucuya sunarak kayıt talebinde bulunur. Sunucu, gizli belirteci (token) içeren QR kodunu da görüntüler. Ardından kullanıcı cihazı, yerleşik kamerayı kullanarak bu QR kodunu okur. QR kodu 45x45 piksel boyutunda sürüm 7'dir, sınırlı bir süre için gösterilir ve yerel sunucu akıllı kart verilerini temizler. Adımlar Şekil 3.4'te gösteirlmiş detayları aşağıda verilmiştir.

Adım 1: kullanıcı UIDi'yi akıllı kart ile yerel sunucuya gönderir.

Adım 2: yerel sunucu, $Tk_i = h(\, h(x_s) \mid UID_i \mid Rtm)$ denklemiyle bir sona erme tarihi olan gizli belirteci (token) hesaplar. Ayrıca, UIDi'yi sunucu veritabanında saklar.

Adım 3: Gizli belirteç Tk_i (token), son kullanma tarihi Ex ve genel anahtar Pks içeren QR kodu oluşturur. ardından ekranda QR kodunu gösterir.

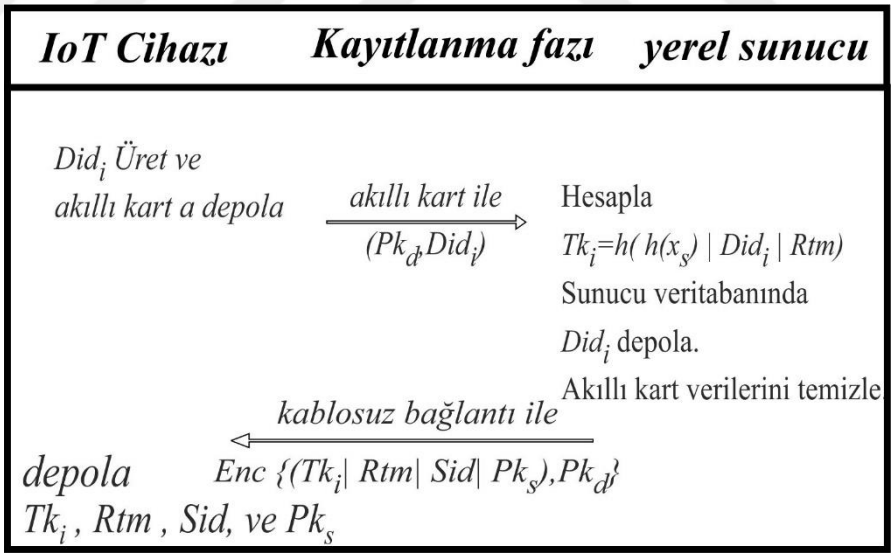
Adım 4: kullanıcı cihazı QR kodunu okur ve oturum açma kimlik doğrulaması için kullanılacak Tki, Rtm ve Pks'yi kaydeder.



Şekil 3.4 Kullanıcı cihazı kayıt aşaması

IoT Akıllı Cihaz Kayıt Aşaması

Bu aşamada Akıllı Cihaz, ve Did ve Cihaz genel anahtarını içeren akıllı kartın kaydedilmesini ve sunucuya sunulmasını talep eder. Sunucu, Aygıt genel anahtarıyla şifrelenmiş gizli simgeyi (token) oluşturur. Ardından akıllı cihaz, simgeyi (token) Wi-Fi veya BLE kanalıyla alır.Adımlar şekil 3.5'te gösterilmiştir.



Şekil 3.5 IoT akıllı cihaz kayıt aşaması

Adım 1: IoT Cihazı, akıllı kart ile Uidi, Pkd'yi yerel sunucuya gönderir.

Adım 2: yerel sunucu, bu denklemle bir sona erme tarihi olan gizli belirteci (token) hesaplar.

Tki=h(h(xs) | Didi | Rtm). Ayrıca Didi ve Pkd'yi sunucu veritabanında saklar.

Adım 3: gizli belirteç Tki (token), son kullanma tarihi Ex, Server Sid ve genel anahtar Pks'yi içeren bir mesaj oluşturur. IoT cihazı genel anahtarı Pkd ile şifrelenir, ardından mesajı BLE veya WiFi Kanalı üzerinden IoT cihazına gönderir.
Adım 4: IoT cihazı şifreli mesajı alır ve şifresini çözdükten sonra oturum açma kimlik doğrulaması için kullanılmak üzere Tki, Rtm ve Pks'yi depolar.

3.2.3 Kimlik Doğrulama Aşaması

Bu tez çalışmasında önerilen şemada, kullanıcı cihazı ve IoT cihazı için kimlik doğrulama aşaması aşağıda verilmiştir.

Kullanıcı Cihazı Kimlik Doğrulama Aşaması

Bu aşamada, kullanıcı cihazı, gizli belirteç (token) Tki'yi, jeton Rtm'nin son kullanma tarihini ve sunucu Pks'nin ortak anahtarını depolar. Aşağıdaki adımlar, oturum açma kimlik doğrulamasını ve oturum anahtarı oluşturmayı açıklar. Şekil 3.6'da gösterildiği gibi;

Adım 1: kullanıcı cihazı, Gi=g*Ri ve RIDi =h(Gi) ⊕ (Tki | UIDi |Rtm) hesaplamak için rasgele Ri sayısını seçer.

Adım 2: kullanıcı cihazı, sunucu genel anahtarı Pks tarafından şifrelenmiş Gi ve sunucuya RIDi ile bir mesaj oluşturur

Adım 3: sunucu ps özel anahtarını kullanarak Gi'nin şifresini çözer ve ardından (Tki | UIDi |Rtm) = h(Gi) ⊕RIDi'yi hesaplar

Veritabanındaki UIDi'yi kontrol eder, ardından Tki`=h(h(xs) | UIDi | Rtm) hesaplar.

Tki=Tki`yi Kontrol edin ?, eğer Tki`≠ Tki ise, doğrulama işlemi sona erecektir, aksi takdirde

Rastgele sayı seç Rj, Hesapla Gj=g*Rj , P1=h(Gi | Gj). Ve Gj, P1'i kullanıcı cihazına gönderir.

Adım 4: kullanıcı cihazı Gj, P1'i alır ve P1`=h(Gi|Gj) değerini hesaplar.

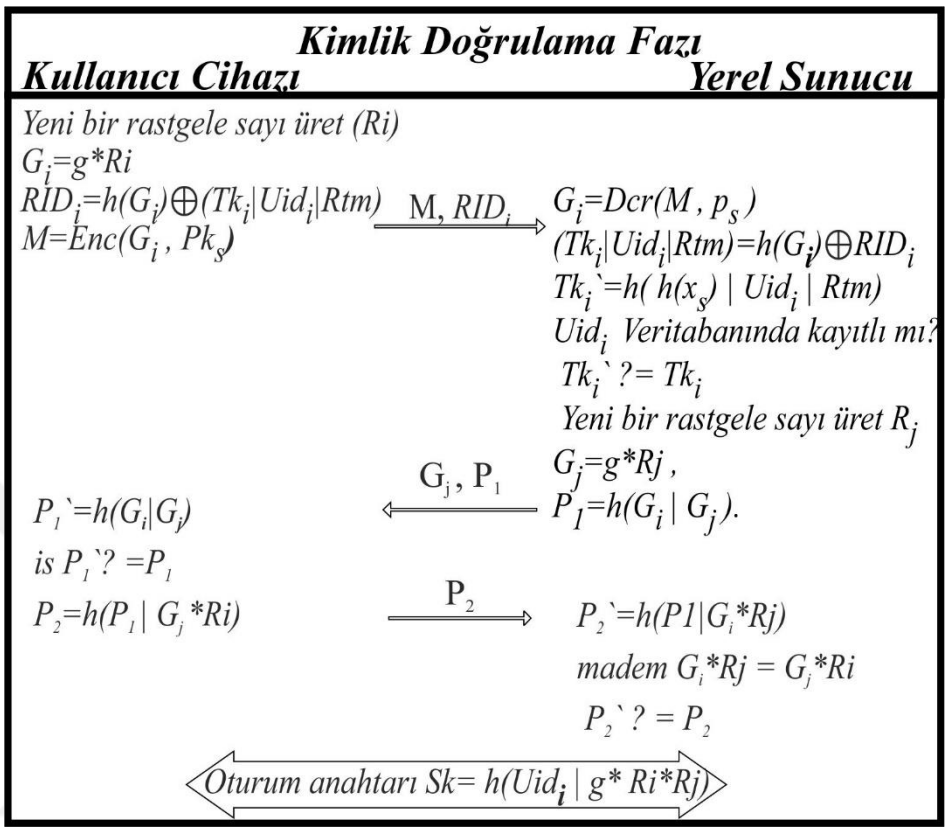
P1=P1`'i kontrol edin?, eğer P1`≠P1 ise, doğrulama işlemi sona erecektir, aksi takdirde

P2=h(P1 | Gj*Ri) hesaplar, ardından P2'yi yerel sunucuya gönderir.

Adım 5: yerel sunucu P2'yi alır ve Gi*Rj = Gj*Ri = g*Ri*Rj olduğundan P2`=h(P1|Gi*Rj) değerini hesaplar.

P2=P2'yi kontrol edin? eğer P2` ≠P2 ise, o zaman kimlik doğrulama işlemi sona erecektir, aksi takdirde

Karşılıklı Kimlik Doğrulama kurulur ve oturum anahtarı Sk= h(UIDi| g*Ri*Rj)'dir.



Şekil 3.6 Kullanıcı cihazı kimlik doğrulama aşaması

IoT Cihaz Girişi Kimlik Doğrulama aşaması

Bu aşamada, kullanıcı cihazı, simge belirteç Tki'yi (token), simge Ex'in sona erme tarihini ve sunucu Pks'nin ortak anahtarını depolar. Aşağıdaki adımlar, oturum açma kimlik doğrulamasını ve oturum anahtarı oluşturmayı açıklar. Şekil 3.7'de gösterildiği gibi;

Adım 1: IoT cihazı, Gi=g*Ri ve RIDi =h(Gi) ⊕(Tki | UIDi |Rtm) hesaplamak için rasgele bir Ri sayısı seçer.

Adım 2: IoT cihazı, sunucu genel anahtarı Pks tarafından şifrelenmiş Gi ve sunucuya RIDi ile bir mesaj oluşturur

Adım 3: Yerel sunucu, özel anahtar ps kullanarak Gi'nin şifresini çözer ve ardından (Tki | UIDi |Rtm) = h(Gi) ⊕RIDi'yi hesaplar

Veritabanındaki UIDi'yi kontrol eder, ardından Tki`=h(h(xs) | UIDi | Rtm) hesaplar

Tki`?= Tki'yi kontrol *eder, eğer Tki`≠ Tki ise, kimlik doğrulama işlemi sona erecektir, aksi takdirde Rastgele sayı Rj seçer, Gj=gRj, P1=h(Gi | Gj)'yi hesaplar.* Ve Gj, P1'i akıllı cihaza gönderir.

Adım 4: IoT akıllı cihazı Gj, P1'i alır ve P1`=h(Gi|Gj) değerini hesaplar

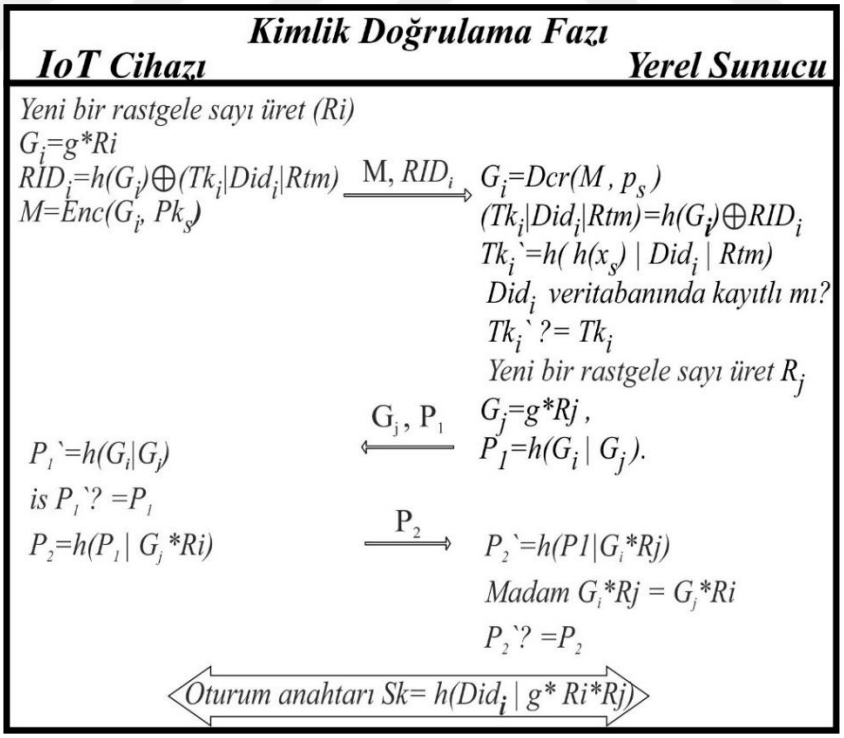
P1`?= P1'i kontrol *eder, eğer P1`≠ P1 ise, doğrulama işlemi sona erecektir, aksi takdirde*

P2=h(P1 | Gj*Ri) hesaplar, ardından P2'yi yerel sunucuya gönderir.

Adım 5: yerel sunucu P2'yi alır ve Gi*Rj = Gj*Ri = g*Ri*Rj olduğundan P2`=h(P1|Gi*Rj) değerini hesaplar.

P2`?=P2'yi kontrol *eder, P2`≠P2 ise o zaman kimlik doğrulama işlemi sona erecektir, aksi takdirde*

Karşılıklı Kimlik Doğrulama kurulur ve oturum anahtarı Sk= h(UIDi| g*Ri*Rj)'dir.



Şekil 3.7 IoT cihaz girişi kimlik doğrulama aşaması

3.3 Çevrimiçi Mod için Önerilen Şeması

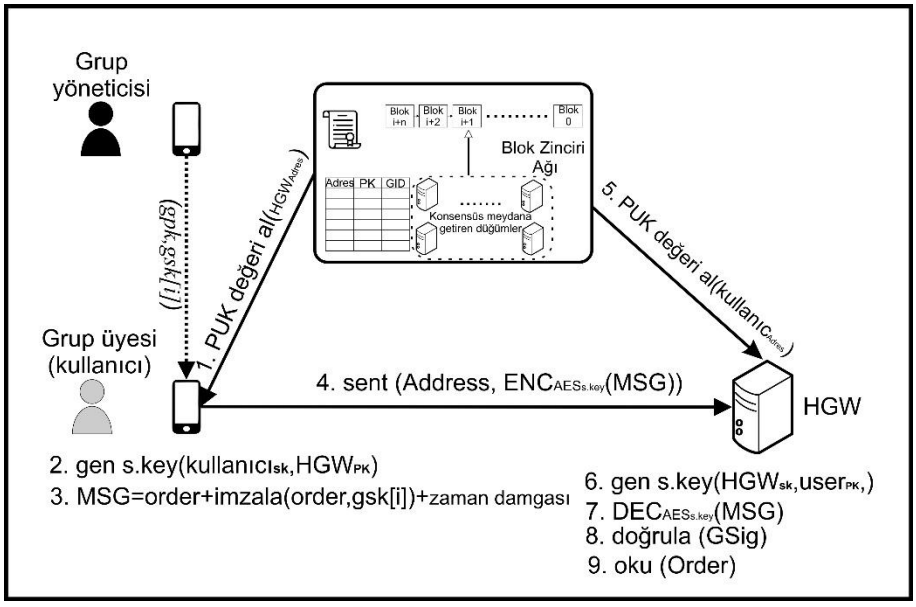
3.3.1 Sistem Kurulum Aşaması

IoT'deki bağlı cihazların iddia ettikleri gibi olduklarına güvenilebilmesi için güçlü IoT cihaz kimlik doğrulaması gerekir. Sonuç olarak, her IoT cihazının, cihaz bir ağ geçidine veya merkezi sunucuya bağlanmaya çalıştığında, doğrulanabilecek benzersiz bir kimliğe ihtiyacı vardır. Bu benzersiz kimlik ile BT sistem yöneticileri, yaşam döngüsü boyunca her cihazı izleyebilir, onunla güvenli bir şekilde iletişim kurabilir ve zararlı işlemler yürütmesini önleyebilir. Bir cihaz beklenmeyen bir davranış sergilerse, yöneticiler basitçe onun ayrıcalıklarını iptal edebilir. Şekil 3.8'de gösterilen kimlik doğrulama adımları.

• Grubun aile üyelerinden oluştuğunu varsayıyoruz. Ayrıca grup yöneticisi, aile üyelerinden birinden (örneğin ebeveynlerden biri) seçilir.

• Başlangıçta yönetici dahil tüm grup üyelerinin biyometrik bilgileri bulanık çıkarıcı kimlik doğrulama yöntemi kullanılarak kaydedilir. Bu yöntem, biyometrik bilgileri fi alır, ardından anahtar verisi bi ve genel bir çoğaltma parametresi pari üretir. Gen(fi) = {bi, pari }.

Kullanıcıyı doğrulamak için bulanık çıkarıcı yöntemini kullanma. Tanımlamanın yüksek doğruluğu ve kişisel cihazlarda yaygın olarak kullanılması nedeniyle diğer metodoloji yerine parmak izi kullandık. d (fi, fi′) ≤ t koşulunu sağlamak sonucu verir Temsilci (fi ′, pari) = bi.



Şekil 3.8 Akıllı sözleşme ile DHKE kullanan anahtar değişim mekanizması

Bu şekil, kullanıcı cihazı ve ev ağ geçidi arasında anahtar alışverişi uygulamak için iletişim mimarisini açıklamaktadır.

3.3.2 Başlatma

Grup yöneticisi, grup özel anahtarları gski ve grup genel anahtarı gpk'yi almak için Alog.3 ve Enroll Algo.4 başlatma algoritmasını çağırarak ana ağ geçidinde parametreleri başlatır. Grup özel anahtarı gpki, grup yöneticisi tarafından her üye için işlemlerini imzalamak için tahsis edilir. Grup ortak anahtarı, işlemleri doğrulamak için kullanılır, bu anahtar ana ağ geçidinde saklanır. Grup yöneticisi ayrıca genel parametreyi almak için genel parametre oluşturmayı da çağırır. Bu, eliptik eğri entegre şifreleme şeması (ECIES) ile birlikte kullanılır [75].

Algoritma 3, sistem genel parametrelerini, grup yöneticisinin özel anahtarını, izleme anahtarını ve grup ortak anahtarını oluşturmak için grup yönetimi tarafından parametreleri başlatmak için kullanılır.

Algoritma 3 başlatma

Girdiler : q , P1, P2 ; grup yöneticisi tarafından başlatma parametreleri

Çıktı : (PP, sk, tk, gpk) // sistem genel parametreleri , grup yöneticisinin özel anahtarı , izleme anahtarı , grup genel anahtarı

Başlatma:

d, s, u = rastgele()

hesaplanır:

G1, G2, GT = q sıralı döngüsel gruplar // GT bir çift doğrusal eşleştirmedir

D=d . P1

S=s . P2

U=u . P1

sk = (d, s) // grup yöneticisinin özel anahtarı

tk=u // izleme anahtarı

gpk = (D, S ,U) // grup ortak anahtarı

PP = (q,G1,G2,GT , e, P1, P2,H(·)), // sistem genel parametreleri

Algoritma 4 kayıt için kullanılır, sistem genel parametresini, grup üyesinin etiketini oluşturmak için grup yöneticisinin özel anahtarını ve grup üyesinin özel anahtarını alır

Algoritma 4 Kayıt

Girdiler: PP, sk , IDi ,GUi // sistem genel parametreleri , grup yöneticisinin özel anahtarı

Çıktı etiketi i **,** gsk_i

Başlat:

x_i= rastgele()

(q,G1,G2,GT , e, P1, P2,H(·)) = PP //parametreleri PP'den çıkarır

(d,s) = sk //parametreleri sk'den çıkar

Hesapla:

$Z_i = (d - xi)(s.\ xi)^{-1} . P1$

$Etiket_i = H(x_i \cdot Z_i)$ // grup üyesinin etiketi

$gsk_i = (x_i, Z_i)$ // grup üyesinin özel anahtarı

3.3.3 Kayıt

Bu aşamada grup üyelerinin ve ana ağ geçidinin kaydını içerir. Her kullanıcı cihazı için grup imzası özel anahtarının oluşturulur. Her cihaz yeni EC anahtar çifti

(genel ve özel) oluşturur. Özel anahtar güvenli bir şekilde saklanmalıdır ve ortak anahtar, Ethereum Adresi ile eşlenmiş blok zincirinde saklanır. Grup üyesi, grup yöneticisinden kayıt jetonu (token) ister. Grup üyesi bize blok zinciri adresini, grup yöneticisi tarafından belirlenen Üye Kimliği ve Grup Kimliğini ve üye EC ortak anahtarını verir. Grup yöneticisi, 1 numaralı denklemi kullanarak kayıt jetonunu (token) imzalamak için bize imzasını verir.

$$RGToken = sign_{Gmsk}(adres,Id,Gid,PK) \quad (3.1)$$

$$RG\_Req = address,Id,Gid,PK, RGToken \quad (3.2)$$

Grup üyesi, kayıt jetonunu (token) ve grup imzasını grup yöneticisinden alır

Grup üyesi, kayıt jetonu (token) ile bilgilerini (adres,Id, Gid,PK) kayıt için akıllı sözleşmeye gönderir

Akıllı sözleşme, bilgileri kontrol eder ve kayıt talebini onaylamak ve blok zinciri adresini üye genel anahtarı ve grup kimliği ile eşleştirmek için kayıt jetonunu (token) doğrular.

3.3.4 Kimlik doğrulama ve anahtar teslimi

- Kullanıcı, ortak anahtarı isteyen akıllı sözleşmeye ev ağ geçidi Eth adresini içeren bir istek gönderir. Akıllı sözleşme, genel anahtarı almak ve kullanıcıya geri göndermek için adresi tabloyla eşleştirir.
- Ev ağ geçidinin genel anahtarını aldıktan sonra, kullanıcı cihazı paylaşılan anahtarı hesaplar.

$$s.key = skuser.PK_{HGW} \quad (3.3)$$

Ardından, algoritma 5'te grup imzasıyla imzalanan kontrol emrini ve zaman damgasını içeren Mesajı oluşturur.

$$M = sipariş + imza(sipariş, gsk_{kullanıcısı}) + zaman\ damgası \quad (3.4)$$

Algoritma 5, sistem genel parametreleri, grup üyesinin özel anahtarı, grup genel anahtarı ve mesajı kullanarak grup imzalı mesajı imzalamak için kullanılır. Ardından mesaj imzası oluşturur.

Algoritma 5 Grup imzalama

Girdiler: PP, *gski, gpk,* msg // sistem genel parametreleri, grup üyesinin özel anahtarı, grup genel anahtarı, mesaj
Çıktılar: imza *(C1,C2, c,w)*
Başlatma:
k= rastgele ()
(q,G1,G2,GT , e, P1, P2,H(·)) = PP //parametreleri PP'den çıkarır
(D, S,U) = gpk // gpk dan parametreleri ayıklar
$(x_i, Z_i) = _{gsk\ i}$ // gsk $_{i'den}$parametreleri çıkarır
Hesaplar:
$C1 = k \cdot P1$
$C2 = xi \cdot Zi + k \cdot U$
$Q = e(U, S)k.$
özet = *H(*msg*)*
c = H(C1,C2,Q, özet*)*
w = kc + xi
imza = *(C1,C2, c,w)*

- Mesajı paylaşılan anahtarla şifreler, şifreli mesajı Eth kullanıcısıyla gönderir. Ev ağ geçidinin adresi.
- Ev ağ geçidi tarafından şifreli mesajı ve kullanıcının Eth adresini aldıktan sonra. Ev ağ geçidi, kullanıcı ortak anahtarını isteyen akıllı sözleşmeye kullanıcı Eth adresini içeren bir istek gönderir.
- Akıllı sözleşme, adresi tablo ile eşleştirir, adresle eşleşen bir ortak anahtar varsa, ortak anahtar ev ağ geçidine geri gönderir.
- Ev ağ geçidi, kendi özel anahtarını ve kullanıcı genel anahtarını kullanarak paylaşılan anahtarı hesaplar.

$$s.key = sk_{HGW.PK\ kullanıcısı} \tag{3.5}$$

Paylaşılan anahtarı kullanarak şifreli mesajın şifresini çözme

$$M = DEC_{AES}^{s.key}(MSG) \tag{3.6}$$

Grup imzasını ve zaman damgasını doğrular. Doğrulama geçerse, sipariş kabul edilebilir.

- Sipariş, yürütülmek üzere IoT cihazına gönderilir. IoT cihazı siparişi alır ve yürütür

- Siparişi yürüttükten sonra, IoT cihazı yeni durumunu ev ağ geçidine geri bildirim olarak gönderir.
- Ana ağ geçidi geri bildirim alır ve kullanıcıya geri bildirim , zaman damgası ve geri bildirimin MAC'İNİ içeren yeni bir mesaj oluşturur

$$M = geribildirim + zamanDamgası + MACsk.HGW(geribildirim) \quad (3.7)$$

- İletiyi paylaşılan anahtarla şifreler ve ilgili kullanıcı cihazına geri gönderir.
- Kullanıcı, ana ağ geçidinden geri bildirim mesajını alır

Paylaşılan anahtarı kullanarak şifresini çözer

$$M = DEC_{AES}^{s.key}(MSG) \quad (3.8)$$

MAC'İ ve zaman damgasını doğrular, doğrulanırsa geri bildirim kabul edilecektir.

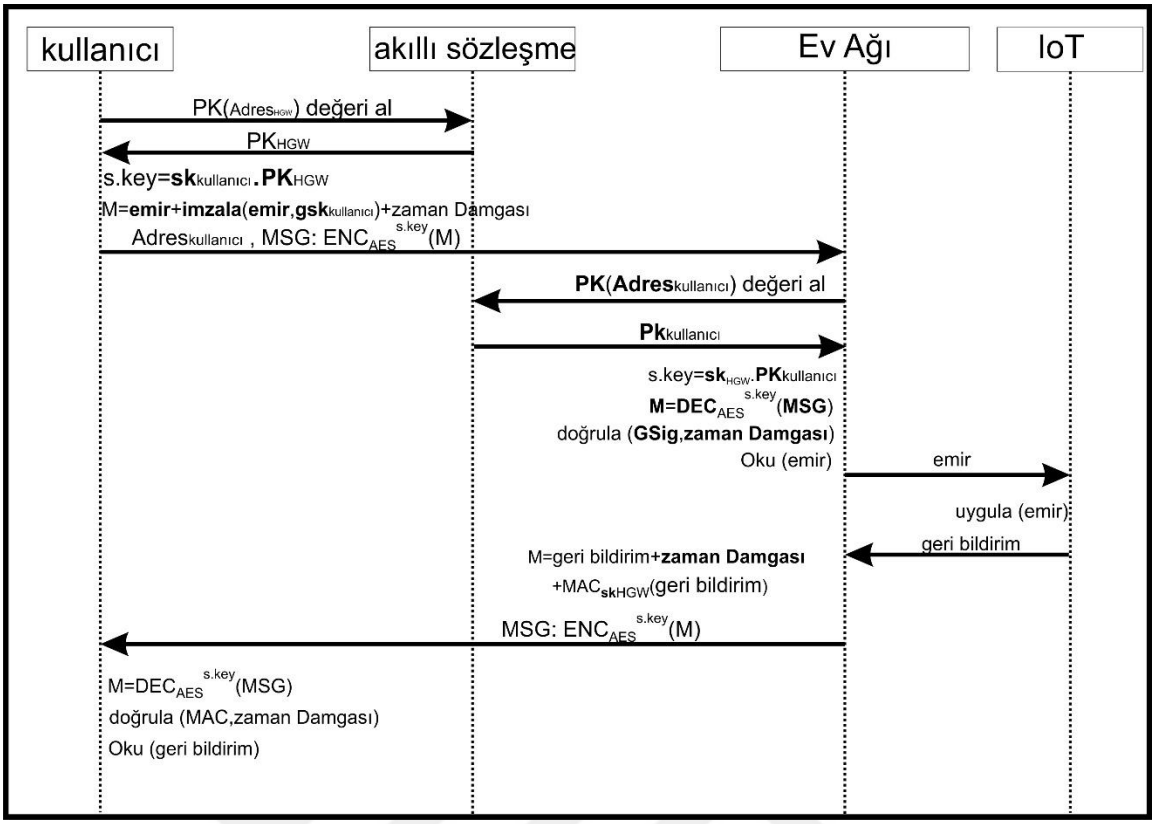
3.3.5 Genel Anahtar Güncellemesi

Tüm kayıtlı üyeler ve ev ağ geçitleri, genel anahtarın sona erme süresinin sona ermesinden sonra ortak anahtarlarını periyodik olarak güncelleyebilir. Bu işlem, cihaz imzası ile imzalanmış yeni ortak anahtarın zaman damgası ile gönderilmesiyle güvenli bir şekilde uygulanabilir.

$$update\_public\_key\_request = adres, kimlik, gid, new\_pk, zaman\ damgası, imza \quad (3.9)$$

Akıllı sözleşme, kayıtlı üyelerdeki adresi ve kimliği kontrol eder ve ardından ortak anahtarı güncellemek için imzayı doğrular.

Sistem bileşenleri arasındaki iletişim ve veri aktarımının zaman çizgisi Şekil 3.9 'da açıklanmıştır. Mesajları şifrelemek ve şifresini çözmek için akıllı kontak kullanan DHKE uygulamasını gösterir.



Şekil 3.9 Anahtar değişim mekanizması ile veri aktarımının zaman çizgisi

Önerilen mimaride, Blokzincir üzerinde olmayan kullanıcı cihazları kimlik doğrulaması yapamaz. Bu sayede kötü niyetli cihazlar engellenmiş olacaktır. Ancak saldırının ilk aşaması olarak Blockchain sisteminde kayıtlı bir kullanıcı cihazına bir şekilde erişim sağlayan kötü niyetli kullanıcı bu cihaz ile bir kontrol yapmak isterse ilgili cihaz üzerinde biyometrik doğrulama yapılacaktır. Biyometrik doğrulaması kullanıcı cihaz tarafından onaylanan kişi ilgili cihazdan erişim talebinde bulunabilecektir. Böylece sadece cihaz sahibi olduğu teyit edilen kişi cihaz doğrulama işlemini başlatabilecektir.

Kullanıcı, kullanıcı cihazına sırasıyla Parola ve Biyometrik bilgilerini sağlar. Biyometrik veriler (örneğin, parmak izi, iris, yüz tanıma) cihaz tarafından bulanık çıkarıcı işlevinin Gen işlevi aracılığıyla oluşturulur. Biyometrik veriler, SHA -256 karma algoritması ile kullanıcı telefon cihazı tarafından sindirilir ve saklanır. Ayrıca, birden fazla hata girildiğinde doğrulama için bir değer oluşturulur. Kişinin şifresi ile biyometrik özet değerine XOR fonksiyonu uygulandıktan sonra oluşturulan çıkış değeri şifrelenir ve telefon cihazında (Key Value) saklanır. Kişi kimlik doğrulamasının amacı, belirli bir biyometrik veri akışının özelliklerine karşı

bir kullanıcının kimlik doğrulaması sürecidir. Kullanıcının ilgili cihazın arayüzünden telefonu kullanmaya çalışması ve biyometrik kimlik doğrulaması. Varlık iletişim cihazının kilidini her açtığında, cihaz sensörü varlığı doğru verilerle tanır (Biyometrik Hash = Biyometrik Hash´). Sensör ile elde edilen biyometrik veriler kimlik doğrulama için depolanan matematiksel model ile eşleştirilir. Yöntem, çeşitli tekniklerle hileli kilit açma girişimlerine karşı koruma sağlamak için tasarlanmıştır. Önerilen şemanın ilk doğrulama adımı olan varlık doğrulama ile erişim talebinden önce sistem içerisinde mahremiyete dayalı erişilebilirlik sağlanmaktadır. Birden fazla denemeden sonra biyometrik doğrulama sağlanamazsa, biyometrik veriler baştan girilir ve kayıt sırasında girilen şifre kullanıcı telefon cihazı tarafından istenir. Yeni bir anahtar değer oluşturulur ve eski oluşturulan değerle karşılaştırılır. Karşılaştırma sonucunda farklı değerler çıkarsa cihaz açılmayacaktır. Ayrıca biyometrik kimlik doğrulama sistemine ek olarak şifre eklendiğinden belirli durumlarda şifre sistemi ile ek güvenlik sağlanmakta ve doğrulama işlemi desteklenmektedir.

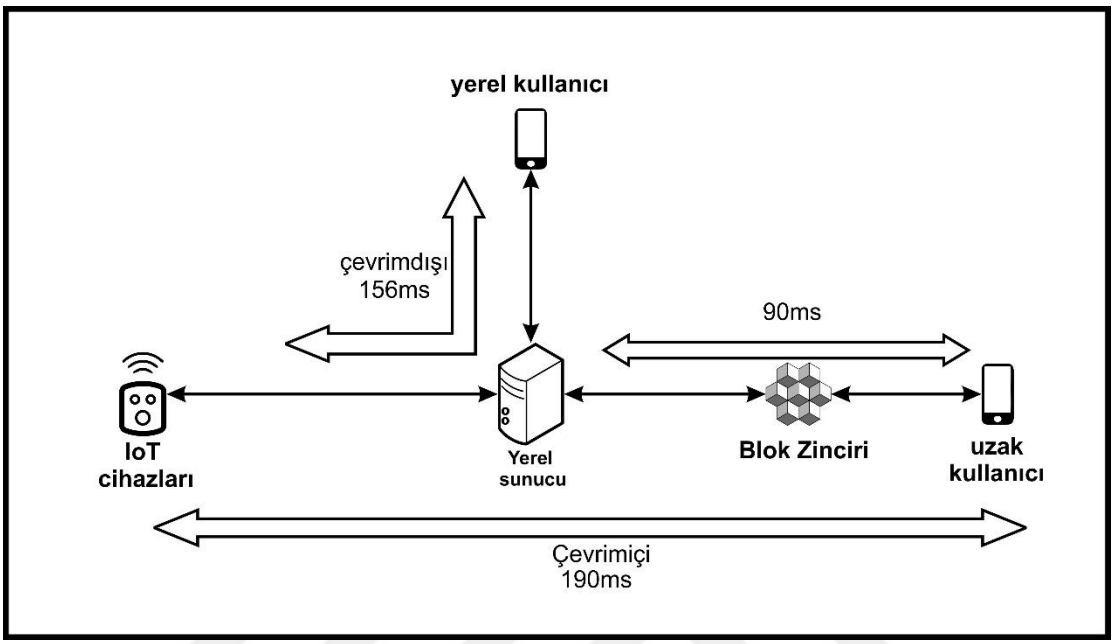
- Kullanıcı cihazı, 48 saatten fazla kullanılmamışsa
- Cihaza son 3 gün içinde şifre ve son 4 saat içinde biyometrik veriler kullanılarak giriş yapılmadıysa
- Kullanıcı telefon cihazı bir uzaktan kilitleme komutu aldıysa
- Üç başarısız biyometrik kimlik doğrulama denemesinden sonra parola girişi zorunludur.

Bu bölüm, IoT cihazlarının ve kullanıcıların kimliğini doğrulamak için bir akıllı ev kimlik doğrulama modelini açıklar. Önerilen şema, varlıkların kimliğini doğrulamak için yerel olarak ve uzaktan kullanılır. Yerel kullanıcılar ve cihazlar, ev ağ geçidi aracılığıyla yerel ağa bağlanır ve kimlik doğrulama için yerel sunucu tarafından yönetilir. Uzak kullanıcılar, biyometrik kullanıcı verilerine ek olarak Blockchain ve grup imzası kullanılarak doğrulanırken, Önerilen şema internet bağlantısı olmasa bile farklı ortamlarda uygulanabilmektedir.

3.4 Sistem entegrasyonu

Bu bölümde, akıllı ev sisteminde kullanılmak üzere iki farklı kimlik doğrulama yaklaşımına dayalı bir hibrit kimlik doğrulama modeli önerilmiştir. Bu iki yaklaşım, Şekil 3.10'da gösterildiği gibi kullanıcı durumuna bağlı olarak aynı ev sisteminde birlikte kullanılır. Çevrimdışı mod ile kullanılan yerel kimlik doğrulama, yerel kullanıcılara ve akıllı ev IoT cihazlarına güvenilir kimlik doğrulama sağlayabilir, bu yaklaşım, yerel karşılıklı kimlik doğrulama için ortalama 156 ms süren IoT cihazları gibi kaynak kısıtlı cihazlar için uygundur. Ek olarak, hafif bir süreç, yüksek güvenlik ve gizlilikle ilgili kimlik doğrulaması sağlar. Ancak internet bağlantısı üzerinden uzak kullanıcılarla kullanıldığında düşük hata toleransı sağlayan merkezi modele dayanmaktadır. Bu nedenle, merkezi olmayan mekanizmaya dayalı yüksek hata toleransı sağlamak için çevrimiçi kimlik doğrulama yaklaşımı kullanılır. Deneysel sonuca göre, Blockchain aracılığıyla uzak kullanıcılar ve yerel uç sunucu arasındaki karşılıklı kimlik doğrulaması ortalama 90 ms ve kaynakları kısıtlı IoT cihazları arasındaki kimlik doğrulaması ortalama 100 ms sürer, bu nedenle kullanıcılar ve IoT Cihazları arasındaki çevrimiçi karşılıklı kimlik doğrulama için toplam süre yerel uç sunucu aracılığıyla ortalama 190 ms sürer. Bu kimlik doğrulama yaklaşımı bile, yerel çevrimdışı kimlik doğrulama yaklaşımıyla karşılaştırıldığında zaman ve para tüketir. Ancak güvenilirlik yüksek güvenlik sağlayabilir ve her yerde ev cihazlarını kontrol etmek için kullanılabilir. Akıllı ev IoT cihazı, ev ağ geçidine yerel olarak bağlı olduğundan, yerel kimlik doğrulama yaklaşımı (Çevrimdışı mod) kullanılarak ev ağ geçidi ile yerel olarak doğrulanır. Kullanıcılar konumlarına göre her iki yaklaşımı da kullanabilirler. Kullanıcı iç mekandaysa ve yerel ağ bağlantısı kullanarak ev sistemine yerel olarak bağlıysa, kullanıcı hızlı kontrol için çevrimdışı modu kullanarak ve hatta internet bağlantısına gerek duymadan kimlik doğrulaması yapabilir. Kullanıcı dışarıdaysa ve ev cihazlarını kontrol etmesi gerekiyorsa, kullanıcı akıllı eve bağlanabilir ve çevrimiçi kimlik doğrulama modunu kullanarak uzaktan kimlik doğrulaması yapabilir. Bu yaklaşım, kullanıcının internet bağlantısı üzerinden ev ağ geçidine güvenli bir şekilde bağlanmasını sağlar. Bu yaklaşım, kontrol emri göndermek ve yanıtı almak için ev ağ geçidi aracılığıyla kullanıcı ve IoT cihazları arasında güvenli bir kanal başlatır.

Dolayısıyla bu iki yaklaşımı tek bir akıllı ev sistemine entegre ediyoruz, bu entegrasyon güvenilirlik, yüksek performans, yüksek hata toleransı, farklı tür saldırılara karşı koyabilen yüksek güvenlik ve kullanıcı gizliliğini koruyan GDPR uyumluluğu sağlayabilir.



Şekil 3.10 Çevrimiçi ve çevrimdışı kimlik doğrulama ile sistem entegrasyonu

Bu şekil, yerel olarak veya uzaktan kullanılabilen iki farklı kimlik doğrulama mekanizması türünü açıklamaktadır. Her bir kimlik doğrulama modu (çevrimiçi / çevrimdışı) için zaman alıcının gösterilmesi.

4
SONUÇ VE ANALİZ

4.1 Giriş

Bu bölümde, önerilen modelin sonuçlarını güvenlik özelliği, resmi doğrulama, performans değerlendirmesi, zaman karmaşıklığı, hesaplama karmaşıklığı, mesaj boyutu ve iletişim maliyeti açısından analiz ediyoruz. Mevcut diğer ilgili çalışmalarla karşılaştırıyoruz. Sonuçlar tartışılmış ve hem çevrimdışı hem de çevrimiçi modlarda önerilen şemanın sağlamlığını ve güvenilirliğini göstermek için ayrıntılı olarak analiz edilmiştir.

4.2 Güvenlik Analizi

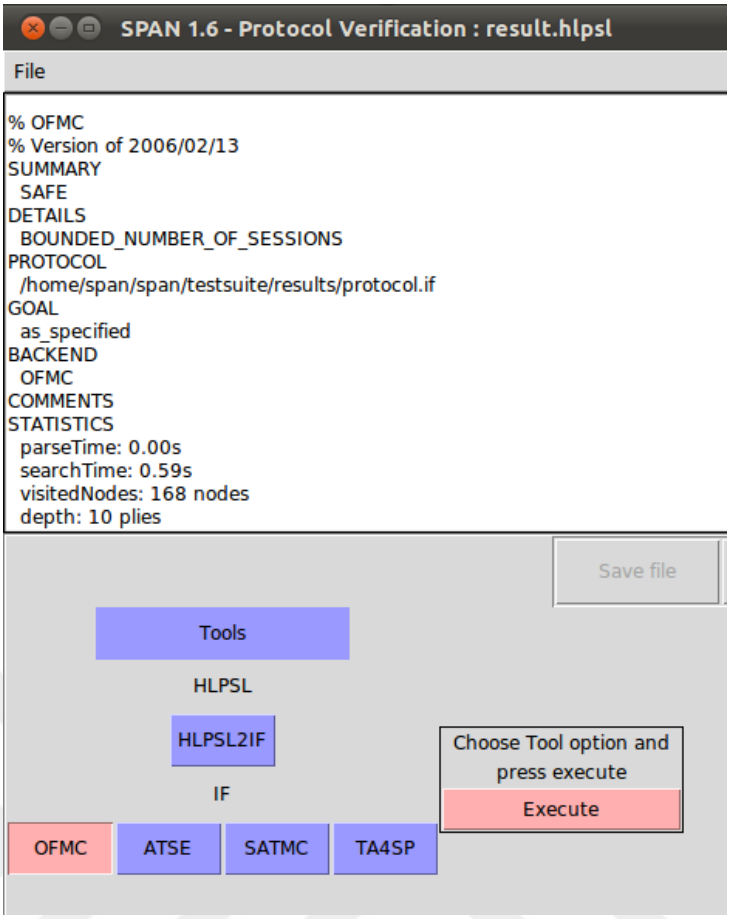
- Güvenli Kanal: Bu çalışmada çevrimdışı modda kullanılan akıllı kartlar ve dinamik QR kod şifrelemesi kullanıldığından, önerilen protokolümüz kayıt için güvenli kanalı tanımlar. Ek olarak, çevrimiçi modda önerilen anahtar değişim mekanizması, grup üyeleri ve ana ağ geçidi arasındaki iletişim için güvenli bir kanal sağlar. Tüm gizli veriler şifrelenir ve iletişim kanalları aracılığıyla güvenli bir şekilde iletilir.
- Ortadaki Adam Saldırılarına Karşı Direnme: Bir saldırgan, görsel Bant Dışı (OOB) kanalı aracılığıyla saldırılar uygulayamaz. İletişim kanalında iletilen şifreli mesajlara ek olarak, oturum anahtarı güvenli bir şekilde değiştirilir, bu nedenle saldırgan anahtarı alamaz.
- Hizmet Reddi (DoS) Saldırılarına Karşı Direnme: Önerilen protokolümüz, bir davetsiz misafir algılama mekanizması kullanarak belirli sayıda başarısız kimlik doğrulama girişiminden sonra saldırgan paketlerini engelleyerek DoS saldırılarına direnebilir. Ayrıca yerel olarak bağlı tarafları yönetmek için uç sunucuyu ana ağ geçidi olarak kullanma. Çevrim içi/Online modda kullanılan Blockchain altyapısı, temel aldığı merkezi olmayan yapıdan dolayı DoS saldırısına karşı yüksek direnç sağlayabilmektedir.
- Yanıt Saldırılarına Karşı Direnme: Bu çalışma, mesaj doğrulama ve saldırganın çevrimdışı modda eski bir mesajı yeniden kullanmasını önlemek için yeni bir oturum anahtarı alışverişi için her kimlik doğrulama girişiminde rastgele

oluşturulmuş gizli numaralara ve farklı nonce'ye (yalnızca bir kez kullanılabilen rastgele sayıya) dayanmaktadır. Grup imzası ile imzalanan her işleme iliştirilen zaman damgası, çevrimiçi modda yeniden oynatma saldırısını önleyebilir.

- Dinleme Saldırılarına Karşı Direnme: Aktarılan tüm veriler, oturum anahtarlarını güvenli bir şekilde değiş tokuş etmek için simetrik veya asimetrik şifreleme kullanılarak şifrelenir. Bu nedenle saldırgan, iletilen mesajlardan herhangi bir yararlı bilgi alamaz.
- Anahtar Günlüğü Saldırılarına Karşı Direnme: Her kimlik doğrulama girişimi için bir giriş cihazı kullanan herhangi bir gizli kimlik doğrulama verisi (parolalar gibi) için giriş yoktur.
- Veri Gizliliği ve Güvenilirliği: Veriler, güvenli bir oturum anahtarı değişimi için şifreli ve imzalı bir biçimde iletilir. kimlik doğrulamadan sonra iletilen tüm veriler, hem çevrimdışı hem de çevrimiçi modda oturum anahtarı kullanılarak doğrulanır ve şifrelenir.
- Gizlilik Değerlendirmesi: Çevrimdışı modda rastgele sayı ve gizli belirtece (token) dayalı olarak her oturum açma kimlik doğrulama girişiminde farklı kullanıcı kimlikleri oluşturma. Çevrimiçi modda üye imzası yerine grup imzasının kullanılması. Kullanıcı kimliğinin izlenemez olduğunu garanti etmek için gizlilik ve anonimlik göz önünde bulundurulur.
- İletim Gizliliği: Her yeni oturum için yeni bir oturum anahtarı oluşturulur. Ve bir sonraki seansta kullanılamaz. Her oturum anahtarı, rastgele oluşturulmuş bir sayıya göre oluşturulur ve güvenli bir şekilde değiştirilir. Bir sonraki oturum anahtarını yeniden hesaplamak veya beklemek için eski oturum anahtarını kullanmanın bir yolu yoktur.

4.3 AVISPA kullanarak Resmi Doğrulama

Protokolleri kontrol etmek ve doğrulamak için farklı tipte protokol doğrulama araçları kullanılır; resmi doğrulama için en iyi bilinenlerden biri (AVISPA)'dır. Bu araç (HLPSI) üst düzey protokol belirtim dilini destekler. Bu çalışmada, önerilen protokolümüzün güvenlik saldırılarından etkilenip etkilenmediğini doğrulamak için AVISPA aracını kullanarak protokolümüzü kontrol ettik. Sonuç, Şekil 4.1'de gösterildiği gibi belirtilen hedeflere göre güvenlidir.



Şekil 4.1 AVISPA SPAN protokolü kontrol sonucu

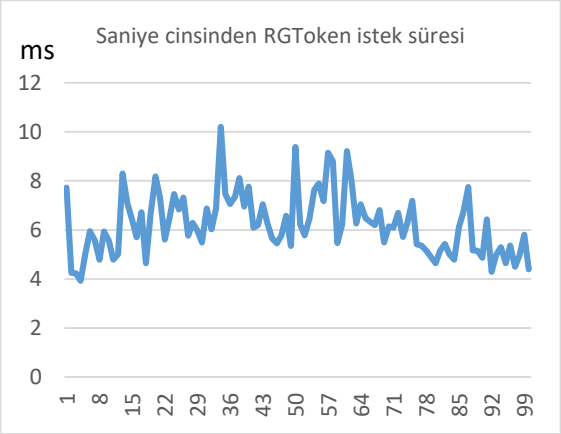
4.4 Deneysel Sonuçlar

4.4.1 Harcanan Zaman

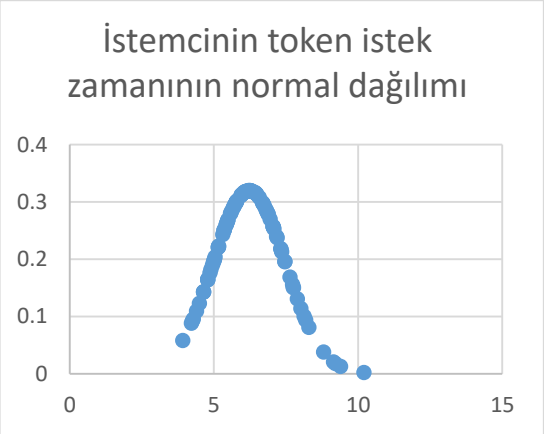
Deneysel sonuca göre harcanan zaman tartışılmıştır.

- Jeton/belirteç (token) İsteği

100 yinelemeden sonra deneysel sonuca göre belirteç (token) talep süresi Şekil 4.2A'da gösterilmektedir. İsteklerin zaman alıcı normal dağılımını gösteren şekil 4.2B'ye göre, çoğu istek, belirteç/jeton (token) isteğini tamamlamak ve yanıt almak için 6 ms civarındadır.



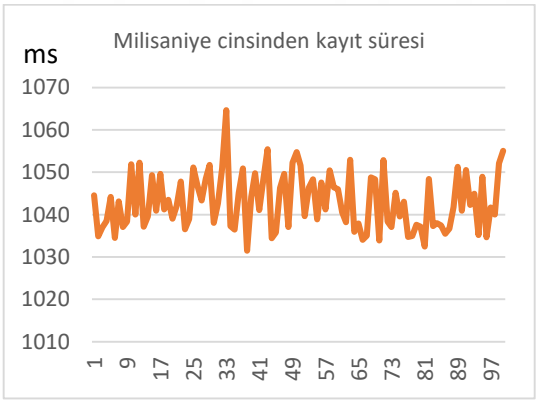
Şekil 4.2A Saniye cinsinden RGToken istek süresi



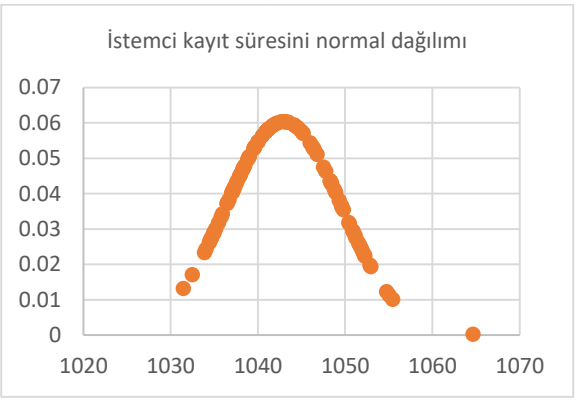
Şekil 4.2B İstemci token istek süresinin normal dağılımı

• Kayıt

100 yinelemeden sonra deneysel sonuca göre kayıt süresi şekil 4.3A'da gösterilmiştir. Bu işlem, zaman alıcı olan blok oluşturmaya ihtiyaç duyar. Bu işlemin ilgili her cihaz için bir kez uygulanması gerekir. Şekil 4.3B, kayıt süresinin normal dağılımını göstermektedir. Kayıt işlemini tamamlamak ve onay almak için ortalama süre yaklaşık 1045 ms'dir.



Şekil 4.3A Milisaniye cinsinden kayıt süresi

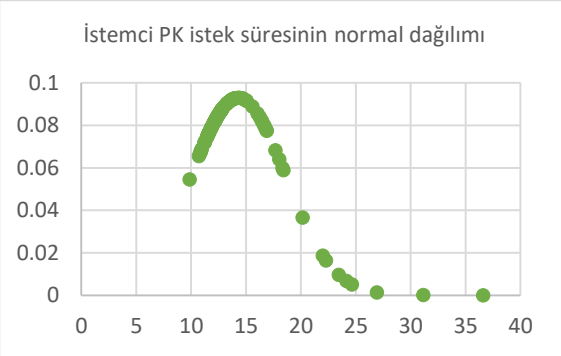


Şekil 4.3B Müşteri kayıt süresinin normal dağılımı

• PK talebi

Deney sonucuna göre PK talep süresi şekil 4.4A ve şekil 4.4B'de gösterilmiştir, PK talebini tamamlamak ve yanıtı almak için ortalama süre yaklaşık 14 ms'dir.

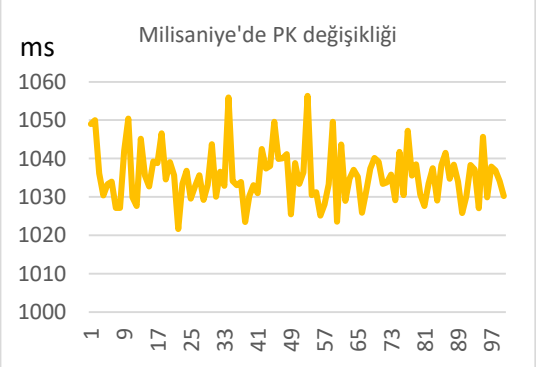
Şekil 4.4A PK gereksinimi milisaniye olarak



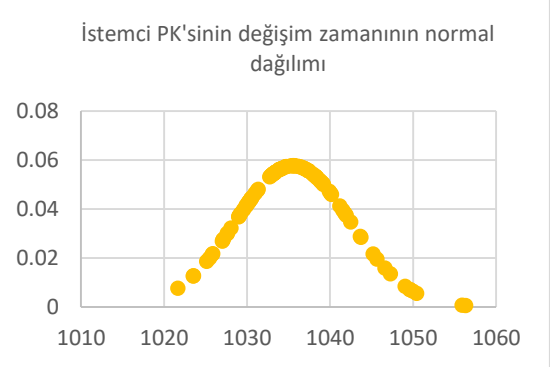
Şekil 4.4B İstemci PK talep süresinin normal dağılımı

- PK güncellemesi

Deney sonucuna göre PK güncelleme süresi şekil 4.5A ve şekil 4.5B'de gösterilmiştir, Pk güncellemesini tamamlamak ve onay almak için ortalama süre yaklaşık 1035 ms'dir.



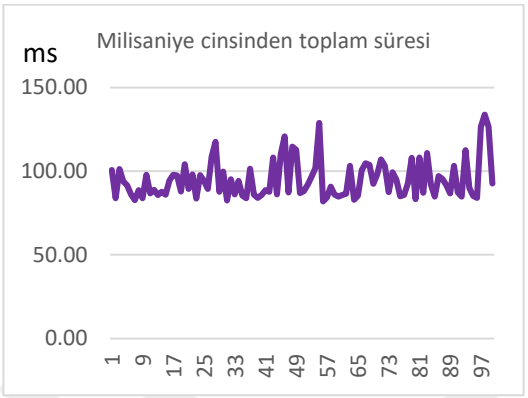
Şekil 4.5A pk değişimi milisaniye cinsinden



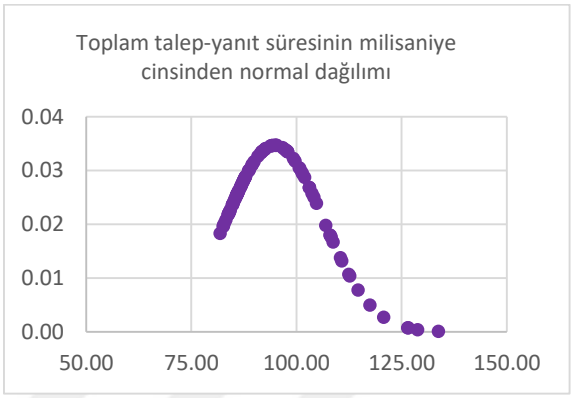
Şekil 4.5B İstemci PK'sinin normal dağılımı değişim zamanı

- Toplam talep/yanıt (Req-Resp) süresi

Deney sonucuna göre Toplam talep/yanıt (Req-Resp) süresi şekil 4.6A ve şekil 4.6B'de gösterilmektedir, herhangi bir kontrol sırasının tam Req-Resp'ini tamamlamak için ortalama süre yaklaşık 90ms'dir.



Şekil 4.6A Milisaniye cinsinden toplam talep/yanıt (Req-Resp) süresi

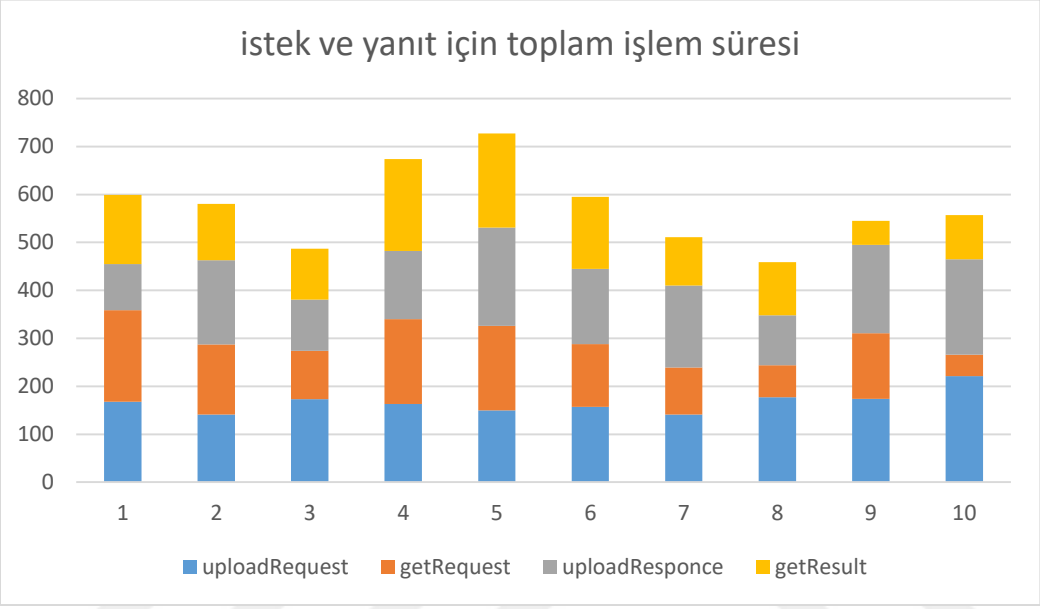


Şekil 4.6B Toplam talep/yanıt (Req-Resp) normal dağılımı

4.4.2 Performans karşılaştırması

Şekil 4.7'deki HomeChain deneysel sonucu, kullanıcı ile ev ağ geçidi arasındaki herhangi bir kontrol siparişinin talep ve yanıt için ortalama süreyi gösterir ve bu süre yaklaşık 500ms'dir. Kullanıcı cihazı ile ev ağ geçidi arasındaki anahtar alışverişi için ortalama 90 ms ve akıllı cihaz ile ev ağ geçidi arasındaki anahtar alışverişi için ortalama 100 ms süren modelimize kıyaslayınız. Önerilen modelin toplam anahtar değişim süresi ortalama 190 ms civarındadır. Buna göre modelimiz HomeChain modelinden daha hızlıdır. Bunun nedeni, HomeChain modelinin her işlem için yeni bir blok oluşturması gereken asenkron iletişim yaklaşımını kullanması, HomeChain yaklaşımında istek ve yanıtlı herhangi bir kontrol emrinin 4 işleme ihtiyaç duymasıdır. Bu süreç zaman alıcıdır ve hedeflenen tarafa herhangi bir yeni işlem için anında bildirim sağlamaz. Bu, herhangi bir tarafın yeni işlem için akıllı sözleşme aracılığıyla Blockchain'i sık sık kontrol etmesini sağlar. Önerilen yaklaşımımızda, oturum anahtarı ile şifreli güvenli kanal oluşturarak asenkron iletişimi senkronize iletişimle değiştirdik. Anahtar değişim mekanizması, bir oturum anahtarı oluşturmak için Blockchain ve

DHKE'ye dayanmaktadır. Önerilen anahtar değişim mekanizması, yeni blok oluşturmaya ihtiyaç duymaz, çünkü özel anahtara ve iletilen her bir tarafın ortak anahtarını içeren Blockchain'de depolanan kayıt verilerine dayanır. Blok oluşturma sayısının en aza indirilmesi ve kimlik doğrulama aşaması yerine kayıt aşaması ile sınırlandırılması, kimlik doğrulama ve anahtar değişim sürecini hızlandırır.



Şekil 4.7 İstek ve yanıt için toplam işlem süresi

Bu şekil, istek ve yanıt içeren herhangi bir kontrol siparişi için toplam işlem süresini gösterir. Her sipariş dört işlemden oluşur (uploadRequest, getRequest, uploadResponce, getResult). Bu işlemlerin ortalama toplam süresi yaklaşık 500 ms sürer.

4.5 Performans Değerlendirmesi

Bu bölümde, benzer çalışmalarla verimlilik değerlendirmesi ve sıkıştırma tartışılmaktadır.

4.5.1 Algoritma Zaman Karmaşıklığı

Bu tezin 4. bölümünde önerdiğimiz algoritmalarda algoritmayı Big O notasyonu açısından analiz ediyoruz. Algoritmaları, bu algoritmalarda kullandığımız fonksiyonların hesaplama karmaşıklığına göre bölüyoruz. O(n2) ile Şifreleme ve Şifre Çözme, tek seferlik karma işlevi, Rastgele sayı oluşturma ve O(n) ile bit düzeyinde işlem ve O(1) ile

bazı küçük sabit hesaplama işlemleri kullandık. Algoritmamızda çok Yüksek O notasyonu ile kullanılan karmaşık bir işlem ve aşırı yuvalanmış döngüler yoktur. Tüm hesaplamalar ve süreç işlemleri hafiftir ve kaynakları kısıtlı cihazlar için uygundur.

4.5.2 Hesaplama Karmaşıklığı

Çalışma, önerilen protokolümüz ve ilgili mevcut protokoller arasındaki hesaplama karmaşıklığını ve maliyetini karşılaştırdı. [54] [63] [55] Tex, Tmp, Tmu, Tbio, Th, Tx ve Ted, ECC noktasının Modüler üslü, çift doğrusal eşleme, ECC noktasının skaler çarpımı, biyo karma süresi, tek yönlü karma işlevi, XoR işlemi ve simetrik şifreleme/şifre çözmenin yürütme süresini belirtir. Tablo 4.1, hesaplama karmaşıklığı karşılaştırmasının sonucunu içerir.

Tablo 4.1 Hesaplama karmaşıklığı

Protokol	Hesaplama karmaşıklığı	Zaman maliyeti
Wang ve diğerleri **[54]**	8Tmu+11Th+1Tx	209ms
Kumar ve diğerleri **[63]**	10Ted+4Tbio+7Th	202ms
Wu ve diğerleri **[55]**	2Tex+4Tmu+1Tmp+10Th+2Tx	164ms
Chao Lin ve diğerleri **[14]**	3Tmp+7Tmu+4Th+4Ted+ 4BCm	500ms
Önerilen model	12Tmu+15Th+2Tx+4Ted	190ms

Hesaplama karmaşıklığı maliyetini ve işlem hızını hesapladıktan sonra, Çalışma, Wang ve arkadaşlarının en yüksek hesaplama maliyetini aldığını buldu. [54] Wu ve diğerleri ayrıca daha fazla hesaplama süresine ihtiyaç duyarlar çünkü onlar zaman alıcı işlem ve daha yüksek hesaplama karmaşıklığı olan Modüler üstel ve çift doğrusal haritalamayı kullanmışlardır. [55] Kumar ve diğerleri, güvenlik seviyesi pahasına en düşük zaman tüketimini gösteren basit bir matematiksel işleme dayanmaktadır. [63] Kabul edilebilir hesaplama maliyetine sahip önerilen protokolümüz gereklidir. Çünkü şemamız verimli fonksiyonlar, en yüksek güvenlik seviyesi ve düşük karmaşıklıktaki matematiksel işlem kullanmıştır.

4.5.3 Güvenlik özelliği

Çalışma, Tablo 4.2.'de gösterilen güvenlik özelliğini sunmuştur. Önerilen protokolümüz ve ilgili mevcut protokoller arasında, [54] [63] [55] Bu protokollerin aksine bizim protokolümüz daha fazla güvenlik özelliğine sahiptir ve daha fazla güvenlik saldırısını önler.

Tablo 4.2 Güvenlik özelliği

Güvenlik özelliği	Wang ve diğerleri	Kumar ve diğerleri	Wu ve diğerleri	Chao Lin ve diğerleri	Önerilen Şema
Ortadaki Adam	Evet	Evet	Evet	Evet	Evet
Yanıt Saldırıları	Evet	Evet	Evet	Evet	Evet
Hizmet Reddi (DoS)	Hayır	Evet	Hayır	Evet	Evet
Gizlice Dinleme	Hayır	Evet	Evet	Evet	Evet
Veri Gizliliği ve	Hayır	Evet	Hayır	Evet	Evet
Gizlilikle İlgili Hususlar	Hayır	Hayır	Hayır	Evet	Evet
Anonimlik	Hayır	Evet	Hayır	Evet	Evet
Karşılıklı Kimlik	Evet	Evet	Evet	Evet	Evet
İletim Gizliliği	Hayır	Evet	Hayır	Evet	Evet
Çalınan cihaz	Hayır	Hayır	Evet	Hayır	Evet
Cihaz sahibi doğrulama	Hayır	Hayır	Hayır	Hayır	Evet
GDPR Uyumluluğu	Hayır	Hayır	Hayır	Hayır	Evet
Tek hata noktası	Hayır	Hayır	Hayır	Evet	Evet

Tablo 4.2'ye göre, çalışma Wang ve diğerlerinin protokolünün farklı güvenlik tehditlerine karşı güvensiz olduğunu, Wu ve diğerlerinin daha güvenli olduğunu ancak yine de bazı güvenlik tehditlerine maruz kaldığını bulmuştur. [54] [55] Kumar ve diğerleri de birçok saldırı türüne karşı güvensizdir ve bazıları dikkate alınmaz. [63] Chao Lin ve diğerleri, Blockchain ve grup imza teknolojisine dayandığı için yüksek güvenlik özellikleri gösterir, ancak yine de bunlarda bazı güvenlik özellikleri eksiktir. [14]Önerdiğimiz protokol, farklı güvenlik tehditlerine karşı daha güvenlidir.

4.5.4 Kimlik Doğrulama Mesaj boyutu ve iletişim maliyeti

Çalışma, protokollerimiz ve ilgili mevcut protokoller [36], [45], [37] ve [5] arasındaki iletişim maliyetini Tablo 4.3'deki mesaj boyutuna göre [54] [63] [55] [14] karşılaştırmıştır. Kimlik doğrulama ve oturum anahtarı değişiminin mesaj numarası ve mesaj boyutu terimlerinde iletişim maliyeti sonucunu gösterir.

Tablo 4.3 Kimlik doğrulama için mesaj boyutu ve iletişim maliyeti

Protokol	Toplam Mesaj	Mesaj sayısı
Wang ve diğerleri	1568 bit	3
Kumar ve diğerleri	959 bit	5
Wu ve diğerleri	1404 bit	3
Chao Lin ve	3296 bit	6
Önerilen model	1664 bit	5

5
SONUÇ VE ÖNERİLER

IoT ve uygulamaları hızla günlük hayatımızın bir parçası haline gelmektedir. Gerçekten de kullanımı artmakta ve ve bu da birçok IoT cihazı ve hizmetinin ortaya çıkmasına neden olmaktadır. Her cihaz erişilebilir olmalı ve bulunduğu yerden bağımsız olarak herhangi bir yetkili kullanıcı tarafından alınabilecek içerik üretmelidir. Çoğu durumda, bu cihazlara erişim ve iletişim alışverişleri güvenli olmalıdır. IoT'de, işler insan müdahalesi olmadan verileri işler ve değiştirir. Bu nedenle, bu tam özerklik nedeniyle, bu varlıkların birbirlerini tanımaları ve kimliklerini doğrulamaları ve ayrıca değiş tokuş edilen verilerinin bütünlüğünü sağlamaları gerekir. Aksi takdirde kötü niyetli kullanıcıların ve kötü niyetli kullanımların hedefi olurlar. Şu anda tüm dünyada Nesnelerin İnterneti (IoT) günlük hayatımızın hemen hemen tüm alanlarında yer almaktadır. Artan bağlı cihaz sayısına göre Gerçekten de vatandaşlar yavaş yavaş evlerini akıllı TV'ler, internet kutuları, ısıtma sistemleri, evin uzaktan kumandası, aydınlatma sistemleri vb. IoT cihazlarıyla donatmaktadır. Fabrikalarda ve endüstriyel ortamlarda robotların ve diğer akıllı araçların işbirliği, otomasyon sistemlerinin verimliliğini artırmakta ve daha iyi üretimlere olanak tanımaktadır. IoT katılımı bu kullanım durumlarıyla sınırlı kalmamış, ancak sağlık, askeriye, tarım ve akıllı şehirler gibi diğer birçok alanda yaygın olarak benimsenmiştir. IoT'nin ve farklı uygulamalarının arkasındaki fikir, çok çeşitli hizmetler sağlamak için birbirleriyle etkileşime girebilecekleri ve işbirliği yapabilecekleri çeşitli şeylerin her yerde bulunmasıdır. Böylece, çok sayıda cihaz dahil edilecektir. Her fiziksel veya sanal cihaz erişilebilir olmalı ve konumlarından bağımsız olarak kullanıcılar tarafından alınabilecek içerik üretmelidir. Ancak, sistemi yalnızca kimliği doğrulanmış ve yetkili kullanıcıların kullanması çok önemlidir. Aksi takdirde bilgi hırsızlığı, veri değişikliği ve kimlik gaspı gibi çok sayıda güvenlik riskine açık olacaktır. Gerçekten de güvenlik sorunları, çeşitli nedenlerle saldırılara karşı oldukça savunmasız olduğu için, IoT'nin büyük ölçekli olarak benimsenmesi ve dağıtılmasının önündeki en büyük engel olmaya devam etmektedir. İlk olarak, iletişimlerin çoğu kablosuzdur ve bu da sistemi kimlik sahtekarlığı, mesajların gizlice dinlenmesi,

mesajların kurcalanması ve diğer güvenlik sorunları gibi sayısız saldırılara karşı daha savunmasız hale getirmektedir ve ikincisi, birden fazla cihaz türünün enerji, bellek ve işleme kapasitesi açısından sınırlı kaynakları vardır ve bu da gelişmiş güvenlik çözümlerini uygulamalarını engeller. IoT'nin boyutu ve diğer özellikleri nedeniyle verimli bir merkezi kimlik doğrulama sistemi oluşturmak neredeyse imkansızdır. Bu, cihazların sağlam bir şekilde tanımlanmasını ve kimlik doğrulamasını sağlar. Ayrıca, veri bütünlüğü kullanılabilirliğini korur ve tek bir arıza noktasına direnir. Merkezi sistem sorununun üstesinden gelmek için Blockchain tabanlı merkezi olmayan sistemler kullanılmıştır. Blok Zinciri, işlem verilerinin kalıcı ve kurcalanmaya dayanıklı kaydını tutan dağıtılmış bir veritabanı (defter) olarak tanımlanır. Bir Blockchain, eşler arası bir ağa güvenerek tamamen merkezi değildir. Daha doğrusu, ağın her düğümü, tek bir arıza noktasını önlemek için defterin bir kopyasını tutar. Tüm kopyalar aynı anda güncellenir ve doğrulanır. Blockchain defteri birden fazla bloktan oluşur, her blok iki bölümden oluşur. Birincisi, parasal işlemler, sağlık verileri, sistem günlükleri, trafik bilgileri vb. gibi herhangi bir türden olabilen işlemleri veya gerçekleri (veritabanının saklaması gereken) temsil eder. İkincisi başlık olarak adlandırılır ve bloğu hakkında bilgi içerir örn. zaman damgası, işlemin hash'i vb. ve önceki bloğun hash'i. Böylece, mevcut blokların kümesi, bağlantılı ve sıralı bloklardan oluşan bir zincir oluşturur. Zincir ne kadar uzun olursa, onu tahrif etmek/bozmak o kadar zor olur. Gerçekten de, kötü niyetli bir kullanıcı bir bloktaki bir işlemi değiştirmek veya takas etmek isterse, ilk olarak, hash'leri ile bağlantılı olduklarından, aşağıdaki tüm blokları değiştirmesi gerekir. Ardından, katılan her düğümün depoladığı blok zincirinin sürümünü değiştirmelidir. Blockchain izinli (özel) veya izinsiz (genel) olabilir. İlk kategori, fikir birliğine katkıda bulunanlara kısıtlamalar getirir. Yalnızca seçilen güvenilir aktörlerin işlemleri doğrulama hakları vardır. Bir fikir birliğine varmak için çok fazla hesaplama gerektirmez, bu nedenle fazla zaman ve enerji tüketmez. Son olarak, yalnızca yetkili katılımcılar bunlara erişebildiğinden, işlemlerin gizliliğini sağlar. İkinci tür (genel Blockchain), sınırsız sayıda anonim düğüm kullanır. Kriptografiye dayalı olarak, her aktör güvenli bir şekilde iletişim kurabilir. Her düğüm, bir çift özel/genel anahtarla temsil edilir. Herhangi bir aktör Blockchain'deki işlemleri okuyabilir, yazabilir ve doğrulayabilir. Blok zinciri

güvenlidir ve ağ konsensüsüne ulaşılırken, düğümlerin %51'i dürüsttür. Genellikle izinsiz Blockchain, sistemin güvenliğini güçlendirmek için bir hesaplama miktarı içerdiğinden enerji ve zaman alıcıdır. Akıllı ev sistemlerinde birbirine bağlı birçok akıllı ev cihazı bulunur, kullanıcılar bu cihazlara erişerek onları kontrol edebilir. Bazı durumların akıllı cihazları evin içinden veya başka bir durumda evin dışından uzaktan kontrol etmesi gerekir. Bu tezde hibrit bir kimlik doğrulama sistemi öneriyoruz. Bu, kimlik doğrulama sistemlerinin hem merkezi hem de merkezi olmayan mimarilerinden yararlanır. Merkezi kimlik doğrulama, yerel uç sunucusuna dayalı olarak her akıllı evde yerel olarak (çevrimdışı) kullanılır. Önerilen güvenli tekniği kullanarak cihazları ev sistemine güvenli bir şekilde kaydetmek için akıllı kart ve dinamik QR kodu gibi en son teknolojileri kullandık. Bu, yerel olarak tüm kullanıcılar ve akıllı cihazlar için hızlı bağlantı ve kimlik doğrulama sağlayabilir. Kimlik doğrulama için sözde rastgele kimlik kullanarak yüksek güvenlik ve gizlilik değerlendirmesine ek olarak. Ancak sorun, tüm akıllı evler, uzaktaki kullanıcıların akıllı evlerine erişmesine izin veren merkezi bir sunucuya bağlandığında ortaya çıkar. Tek bir arıza noktası, DDoS gibi diğer güvenlik sorunlarına ek olarak sistemi tehdit edebilir. Bu nedenle akıllı evleri uzaktaki kullanıcıları ile güvenli bir şekilde bağlamak için merkezi olmayan sistemler kullanılmaktadır. Blockchain tabanlı kimlik doğrulama sistemi, uzak kullanıcılar ile akıllı evin yerel uç (edge) sunucusu arasında uzaktan (çevrimiçi) kimlik doğrulaması sağlamak için kullanılır. Blockchain zaman ve enerji tüketse bile, kimlik doğrulama sistemlerinin merkezi mimarisinin sorunlarının üstesinden gelebilir. İki farklı kimlik doğrulama yaklaşımını (çevrimdışı/çevrimiçi) tek bir entegre sistemde birleştirerek. Bu, yüksek güvenilirlik, yüksek güvenlik ve gizliliğe önem vererek en iyi performansı sağlayabilir. Önerilen model üzerindeki deneysel sonuca göre, karşılaştırma, güvenlik, güvenilirlik, performans ve gizlilik açısından diğer ilgili çalışmalarla karşılaştırıldığında önemli sonuçlar göstermektedir.

Gelecekteki çalışmalar için ilk olarak, IoT cihazı ile uzak kullanıcılar arasındaki toplam kimlik doğrulama süresini en aza indirmek için akıllı IoT cihazının çevrimdışı kimlik doğrulama süresini iyileştirmeyi ; ikincisi, güvenliği ihlal edilmiş cihazlar için bir izleme ve iptal mekanizması uygulamayı; üçüncüsü, tanımlanmış bir sistemdeki madenci sayısının optimizasyonunu ve seçilen madencilerin nasıl

yerleştirilebileceğini hedefleyen bir protokolü incelemeyi ve tasarlamayı planlıyoruz. Ayrıca, diğer protokollerle paralel olarak çalışırken güvenliği garanti etmek için evrensel birleştirilebilirlik ayarında güvenli protokol tasarımını ele alacağız. Ayrıca, gerçek dünyada daha yüksek fayda sağlamak için genişletilmiş sistemin bir prototipini uygulamak ve değerlendirmek niyetindeyiz.

KAYNAKÇA

[1] Okai, Ebenezer, Xiaohua Feng, and Paul Sant, «Smart cities survey,» %1 içinde *IEEE 20th international conference on high performance computing and communications; IEEE 16th international conference on smart city; IEEE 4th international conference on data science and systems (HPCC/SmartCity/DSS). IEEE*, 2018 .

[2] Al-Azzam, Majed Kamel, and Malik Bader Alazzam, «Smart city and smart-health framework, challenges and opportunities,» *International Journal of Advanced Computer Science and Applications,* cilt 10, no. 2, 2019.

[3] S. Smys, «A survey on internet of things (IoT) based smart systems,» *Journal of ISMAC,* cilt 2, no. 4, pp. 181-189, 2020.

[4] Chand, H. Varun, and J. Karthikeyan, «Survey on the role of IoT in intelligent transportation system,» *Indonesian Journal of Electrical Engineering and Computer Science,* cilt 11, no. 3, pp. 936-941, 2018.

[5] Miglani, Arzoo, Neeraj Kumar, Vinay Chamola, and Sherali Zeadally., «Blockchain for Internet of Energy management: Review, solutions, and challenges,» *Computer Communications,* cilt 151 , pp. 395-418, 2020.

[6] G. Dileep, «A survey on smart grid technologies and applications,» *Renewable energy,* cilt 146 , pp. 2589-2625, 2020.

[7] Friha, Othmane, Mohamed Amine Ferrag, Lei Shu, Leandros Maglaras, and Xiaochan Wang, «Internet of things for the future of smart agriculture: A comprehensive survey of emerging technologies,» *IEEE/CAA Journal of Automatica Sinica,* cilt 8, no. 4, pp. 718-752, 2021.

[8] Esmaeilian, Behzad, Ben Wang, Kemper Lewis, Fabio Duarte, Carlo Ratti, and Sara Behdad, «The future of waste management in smart and sustainable cities: A review and concept paper,» *Waste management ,* cilt 81, pp. 177-195, 2018.

[9] Dwivedi, Ashutosh Dhar, Rajani Singh, Uttam Ghosh, Raghava Rao Mukkamala, Amr Tolba, and Omar Said, «Privacy preserving authentication system based on non-interactive zero knowledge proof

suitable for Internet of Things,» *ournal of Ambient Intelligence and Humanized Computing,* cilt 13, no. 10, pp. 4639-4649, 2022.

[10] M. El-hajj, A. Fadlallah, M. Chamoun and A. Serhrouchni, «A survey of internet of things (iot) authentication schemes,» *Sensors,* cilt 19, no. 5, p. 1141, 2019.

[11] L. Atzori, A. Iera and G. Morabito, «The internet of things: a survey,» *Computer networks,* cilt 54, no. 15, pp. 2787-2805, 2010.

[12] Ammar, Mahmoud, Giovanni Russello, and Bruno Crispo, «Internet of Things: A survey on the security of IoT frameworks,» *Journal of Information Security and Applications,* cilt 38 , pp. 8-27, 2018.

[13] A. K. Singh, M. Alshehri, S. Bhushan, M. Kumar, O. Alfarraj et al., «Secure and energy efficient data transmission model for WSN,» *Intelligent Automation & Soft Computing,* cilt 25, no. 3, pp. 761-769, 2021.

[14] Chao Lin, Debiao He, Neeraj Kumar, Xinyi Huang, Pandi Vijaykumar and Kim-Kwang Raymond Choo, «HomeChain: A blockchain-based secure mutual authentication system for smart homes,» *IEEE Internet of Things Journal,* cilt 7.2, pp. 818-829, 2019.

[15] C.-S. Tsai, C.-C. Lee, and M.-S. Hwang, «Password authentication schemes: Current status and key issues,» *Int. J. Netw. Security,* cilt 3, no. 2, p. 101–115, 2006.

[16] Kurniawan, Dwi Ely, Mohd Iqbal, John Friadi, Fendi Hidayat, and Ririt Dwiputri Permatasari., «Login Security Using One Time Password (OTP) Application with Encryption Algorithm Performance,» *Journal of Physics: Conference Series,* cilt 1783, no. 1, p. p. 012041, 2021.

[17] vJ.-Y. Liu, A.-M. Zhou, and M.-X. Gao, «A new mutual authentication scheme based on nonce and smart cards,» *Computer Communication,* cilt 31, no. 10, p. 2205–2209, 2008.

[18] Sharma, Geeta, and Sheetal Kalra, «A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications,» *Journal of information security and applications,* cilt 42 , pp. 95-106, 2018.

[19] B. Vaidya, J. H. Park, S. Yeo, and J. J. P. C. Rodrigues, «Robust onetime password authentication scheme using smart card for home network environment,» *Computer Communication,* cilt 34, no. 3, p. 326–336, 2011.

[20] Das, Ashok Kumar, Basudeb Bera, Mohammad Wazid, Sajjad Shaukat Jamal, and Youngho Park, «On the security of a secure and lightweight authentication scheme for next generation IoT infrastructure,» *IEEE Access,* cilt 9, pp. 71856-71867, 2021.

[21] Trnka, Michal, Tomas Cerny, and Nathaniel Stickney, «Survey of Authentication and Authorization for the Internet of Things,» *Security and Communication Networks,* 2018.

[22] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, «Blockchain technologies for the Internet of Things: Research issues and challenges,» *IEEE Internet Things J.,* cilt 6, no. 2, p. 2188–2204, 2019.

[23] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, «A decentralized lightweight blockchain-based authentication mechanism for IoT systems,» *Cluster Comput,* pp. 1-21, 2020.

[24] Ruth Andea, Bamidele Adebisi, Mohammad Hammoudeh, and Jibran Saleem, «Internet of Things: Evolution and technologies from a security perspective,» *Sustainable Cities and Society,* cilt 54, p. 101728, 2020.

[25] Sinanović, Hamdija, and Sasa Mrdovic, «Analysis of Mirai malicious software,» %1 içinde *In 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2017.

[26] A. C. Dwyer, «The NHS cyber-attack: A look at the complex environmental conditions of WannaCry,» *RAD Magazine,* cilt 44 , 2018.

[27] O. Rajaee, «IoT, Resource Constrained Devices, Security,» %1 içinde *RSA 2017*, San Francisco, CA, 2017.

[28] Abeer Assiri, and Haya Almagwashi, «IoT security and privacy issues,» %1 içinde *2018 1st International Conference on Computer Applications & Information Security (ICCAIS). IEEE*, Riyadh, Saudi Arabia, 2018.

[29] Meng, Yan, Wei Zhang, Haojin Zhu, and Xuemin Sherman Shen, «Securing consumer IoT in the smart home: Architecture, challenges, and

countermeasures,» *IEEE Wireless Communications ,* cilt 25, no. 6, pp. 53-59, 2018.

[30] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati and M. Rossi, «Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples,» %1 içinde *2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, San Francisco, CA, USA, 2012.

[31] Siham Al Hinai, Ajay Vikram Singh, «Internet of things: Architecture, security challenges and solutions,» %1 içinde *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)*, Dubai, United Arab Emirates, 2017.

[32] «QR Code. com,» [Çevrimiçi]. Available: http: // www. denso-wave.com/ qrcode/ index-e.html. [Erişildi: 16 Sept 2009].

[33] Sha Liu, and Shuhua Zhu, «A Novel QR Code and mobile phone based Authentication protocol via Bluetooth,» %1 içinde *International Conference on Materials Engineering and Information Technology Applications (MEITA)*, Guilin, China., August 2015.

[34] Wahsheh, Heider AM, and Flaminia L. Luccio. , «Security and privacy of QR code applications: a comprehensive study, general guidelines and solutions,» *Information ,* cilt 11, no. 4, p. P.217, 2020.

[35] Fong, Sim Liew, David Wui Yung Chin, Rabab Alyaham Abbas, Arshad Jamal, and Falah YH Ahmed, «Smart city bus application with QR code: a review,» %1 içinde *In 2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, 2019.

[36] Prof. Dülger , and Cansu Ceren Kahraman. , «GDPR ve KVKK Ekseninde Bağlayıcı Şirket Kuralları (Binding Corporate Rules within GDPR and KVKK).,» *Hukuk ve Daha Fazlası,* 31 07 2021.

[37] Zaeem, Razieh Nokhbeh, and K. Suzanne Barber, «The effect of the GDPR on privacy policies: Recent progress and future promise.,» *ACM Transactions on Management Information Systems (TMIS) ,* cilt 12, no. 1, pp. 1-20, 2020.

[38] P. Regulation, «General data protection regulation,» *INTOUCH,* 2018.

[39] Tikkinen-Piri, Christina and Rohunen, Anna and Markkula, Jouni, «EU General Data Protection Regulation: Changes and implications for personal data collecting companies,» *Computer Law \ Security Review, Elsevier,* cilt 34, no. 1, pp. 134-153, 2018.

[40] Finck, Michèle, and Frank Pallas, «They who must not be identified—distinguishing personal from non-personal data under the GDPR,» *International Data Privacy Law ,* cilt 10, no. 1, pp. 11-36, 2020.

[41] Truong, Nguyen Binh, Kai Sun, Gyu Myoung Lee, and Yike Guo. , «Gdpr-compliant personal data management: A blockchain-based solution,» *IEEE Transactions on Information Forensics and Security,* cilt 15, pp. 1746-1761, 2019.

[42] helpIT systems ltd, «HelpIT,» helpIT systems ltd, 28 June 2017. [Çevrimiçi]. Available: https://think.360science.com/gdpr-key-definitions/. [Erişildi: 12 5 2022].

[43] «i-scoop,» [Çevrimiçi]. Available: https://www.i-scoop.eu/gdpr/gdpr-personal-data-identifiers-pseudonymous-information/. [Erişildi: 10 10 2022].

[44] Mustafa Kara, Şevki Gani Şanlıöz, Hisham R. J. Merzeh, Muhammed Ali Aydın, and Hasan Hüseyin Balık, «Blockchain Based Mutual Authentication for VoIP Applications with Biometric Signatures,» %1 içinde *2021 6th International Conference on Computer Science and Engineering (UBMK). IEEE*, 2021.

[45] A. K. Das,, «A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor,» *Int. J. Commun. Syst.,* cilt 30, no. 1, p. e2933, Jan. 2017.

[46] J. Gowthami and N. Shanthi, «Secure Fuzzy Extractor based remote user validation scheme for Wearable devices,» *Accessed: May 31, 2021. [Online]. Available: www.ijert.org.*

[47] T. Ho, L. Yen, and C. Tseng, «Simple-yet-efficient construction and revocation of group signatures,» *Int. J. Found. Comput. Sci.,* cilt 26, no. 5, p. 611–624, 2015.

[48] N. Z. Aitzhan and D. Svetinovic, «Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous

messaging streams,» *IEEE Trans. Depend. Secure Comput.,* cilt 15, no. 5, p. 840–852, 2018.

[49] El-hajj, Mohammed and Fadlallah, Ahmad and Chamoun, Maroun and Serhrouchni, Ahmed, «A Survey of Internet of Things (IoT) Authentication Schemes,» *Sensors, Multidisciplinary Digital Publishing Institute,* cilt 19, no. 5, p. 1141, 2019.

[50] Zhao, Min and Yao, Xuanxia and Liu, Hong and Ning, Huansheng, «Physical Unclonable Function Based Authentication Protocol for Unit IoT and Ubiquitous IoT,» *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI),IEEE,* pp. 179-184, 2016.

[51] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot , and Ahmed Serhrouchni, «Bubbles of Trust: A decentralized blockchain-based authentication system for IoT,» *Computers & Security,* cilt 78, pp. 126-142, 2018.

[52] S. Kalra and S. K. Sood, «Secure authentication scheme for iot and cloud servers,» *Pervasive and Mobile Computing,* cilt 24, pp. 210-223, 2015.

[53] C. Chang, H. Wu and C. Sun, «Notes on “secure authentication scheme for iot and cloud servers”,» *Pervasive and Mobile Computing,* cilt 38, pp. 275-278, 2017.

[54] K. Wang, C. Chen, W. Fang and T. Wu, «A secure authentication scheme for internet of things,» *Pervasive and Mobile Computing,* cilt 42, pp. 15-26, 2017.

[55] H. Wu, C. Chang and L. Chen, «Secure and anonymous authentication scheme for the internet of things with pairing,» *Pervasive and Mobile Computing,* cilt 67, p. 101177, 2020.

[56] M. Shuai, N. Yu, H. Wang and L. Xiong, «Anonymous authentication scheme for smart home environment with provable security,» *Computer & security,* cilt 86, pp. 132-146, 2019.

[57] B. Yu and H. Li, «Anonymous authentication key agreement scheme with pairing-based cryptography for home-based multi-sensor Internet of Things,» *International Journal of Distributed Sensor Networks,* cilt 15, no. 9, p. 1550147719879379, 2019.

[58] S. Naoui, M. h. Elhdhili and L. A. Saidane, «Novel smart home authentication protocol lrp-shap,» %1 içinde *IEEE Wireless Communications and Networking Conference (WCNC).*, 2019.

[59] M. Hussain and U. Jain., «Simple and secure device authentication mechanism for smart environments using Internet of things devices,» *International Jornal of Communication System,* cilt 33, no. 16, p. e4570, 2020.

[60] Q. Lyu, N. Zheng, H. Liu, C. Gao, S. Chen et al., «Remotely access "my" smart home in private: An anti-tracking authentication and key agreement scheme,» *IEEE Access,* cilt 7, pp. 41835-41851, 2019.

[61] U. Coruh and O. Bayat, «Hybrid secure authentication and key exchange scheme for m2m home networks,» *Security and Communication Networks,* cilt 2018, 2018.

[62] X. Sun, S. Men, C. Zhao and Z. Zhou, «A security authentication scheme in machine-to-machine home network service,» *Security and Communication Networks,* cilt 8, no. 16, pp. 2678-2686, 2015.

[63] P. Kumar and L. Chouhan, «A secure authentication scheme for iot application in smart home,» *Peer-to-Peer Networking and Applications,* cilt 14, p. 420–438, 2020.

[64] Cui, Zhihua, et al, «A hybrid blockchain-based identity authentication scheme for multi-WSN,» *IEEE Transactions on Services Computing,* cilt 13.2, pp. 241-251, 2020.

[65] Ma Zhaofeng, Meng Jialin, Wang Jihui, and Shan Zhiguang, «Blockchain-Based Decentralized Authentication Modeling Scheme in Edge and IoT Environment,» *IEEE Internet of Things Journal,* cilt 8.4, pp. 2116-2123, 2020.

[66] Patwary, Abdullah Al-Noman, et al. , «FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain,» *Computer Communications,* cilt 162 , pp. 212-224, 2020.

[67] Shijie Zhang and Jong-Hyouk Lee, «A Group Signature and Authentication Scheme for Blockchain-Based Mobile-Edge Computing,» *IEEE INTERNET OF THINGS JOURNAL,* cilt 7, no. 5, 2020.

[68] Jiang Yanji, Shaocheng Ge, and Xueli Shen., «AAAS: An Anonymous Authentication Scheme Based on Group Signature in VANETs,» *IEEE Access,* cilt 8, pp. 98986-98998, 2020.

[69] C ZHANG, X XUE,L FENG, X ZENG,and J MA, «Group-Signature and Group Session Key Combined Safety Message Authentication Protocol for VANETs,» *IEEE Access,* cilt 7, pp. 178310-178320, 2019.

[70] Biljana L. Risteska Stojkoska, and Kire V. Trivodaliev, «A review of Internet of Things for smart home: Challenges and solutions,» *Journal of Cleaner Production,* cilt 140, no. 3, pp. 1454-1464, 2017.

[71] S. Putz, T. Wiemann and J. Hertzberg, «The mesh tools package – introducing annotated 3d triangle maps in ros,» *Robotics and Autonomous Systems,* cilt 138, p. 103688, 2021.

[72] Cryptosys, «CryptoSys,» D.I. Management Services Pty Limited, 30 June 2020. [Çevrimiçi]. Available: https://www.cryptosys.net/pki/uuid-rfc4122.html.

[73] N. H. Kumar and G. Deepak, «Mutual authentication and data security in iot using hybrid mac id and elliptical curve cryptography,» *Turkish Journal of Computer and Mathematics Education (TURCOMAT),* cilt 12, no. 11, pp. 501-507, 2021.

[74] Microsoft, «Microsoft Docs,» Microsoft Corporation, 2021. [Çevrimiçi]. Available:https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.eccurve.namedcurves.brainpoolp256r1?view=net-5.0.

[75] D. Hankerson, S. Vanstone, and A. Menezes, «Guide to elliptic curve cryptography,» *Comput. Rev,* cilt 46, no. 1, p. 13, 2005.

[76] Gruschka, Nils, Vasileios Mavroeidis, Kamer Vishi, and Meiko Jensen., «Privacy issues and data protection in big data: a case study analysis under GDPR,» %1 içinde *In 2018 IEEE International Conference on Big Data (Big Data)*, 2018.

TEZDEN ÜRETİLMİŞ YAYINLAR

Konferans Bildirileri

1. Kara, M., Şanlıöz, Ş. G., Merzeh, H. R., Aydın, M. A., & Balık, H. H. (2021, September). Blockchain Based Mutual Authentication for VoIP Applications with Biometric Signatures. In 2021 6th International Conference on Computer Science and Engineering (UBMK) (pp. 133-138). IEEE.
2. Merzeh, H. R., Kara, M., Aydın, M. A., & Balık, H. H. (2022, May) “Secure Mutual Authentication Scheme for IoT Smart Home Environment using Biometric and Group Signature Verification Methods”, 4th International Conference on Artificial Intelligence and Applied Mathematics in Engineering (ICAIAME 2022) Baku, Azerbaijan.

Makaleler

1. Merzeh, H. R., Kara, M., Aydın, M. A., & Balık, H. H. "GDPR compliance IoT authentication model for smart home environment" Intelligent Automation and Soft Computing (2022), https://doi.org/10.32604/iasc.2022.021297

2. Kara, M., Merzeh, H. R., Aydın, M. A., & Balık, H. H. “VoIPChain: A decentralized identity authentication in Voice over IP using Blockchain”, Computer Communications, 2022, https://doi.org/10.1016/j.comcom.2022.11.019