Gazi Üniversitesi
Fen Bilimleri Dergisi
PART C: TASARIM VE TEKNOLOJİ

Gazi University
Journal of Science
PART C: DESIGN AND TECHNOLOGY

GU J Sci, Part C, 12(1): 80-91 (2024)

Blokzincir Teknolojisi ile Nesnelerin İnterneti Tabanlı (IoT) Sistemlerin Veri Güvenliğinin Sağlanması

Gül Fatma TÜRKER[1*] Kubilay TANYERİ[1]

[1]Suleyman Demirel University, Faculty of Engineering, Department of Computer Engineering , Isparta, Turkey

Makale Bilgisi

Research article
Received: 28/10/2022
Revision: 23/05/2023
Accepted: 23/05/2023

Anahtar Kelimeler

Akıllı Ev Sistemi
Blokzincir
Nesnelerin İnterneti (IoT)
Nesnelerin İnterneti Güvenliği
Veri Bütünlüğü

Article Info

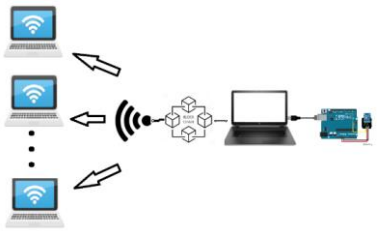
Araştırma makalesi
Başvuru: 28/10/2022
Düzeltme: 23/05/2023
Kabul: 23/05/2023

Keywords

Smart Home System
Blockchain
Internet of Things
Internet of Things Security
Data Integrity

Grafik Özet (Graphical/Tabular Abstract)

Bu çalışmada, bir akıllı ev sistemi örneği sunulmuş, bu sistemde blokzincir teknolojisi ile IoT entegrasyonu gerçekleştirilmiştir. Tasarlanan IoT tabanlı sistemde, veri gizliliği ve bütünlüğü için blokzincir dağıtık veri tabanı kullanılmış ve elde edilen sonuçlar, veri bütünlüğünün korunduğunu ve veri kayıplarının olmadığını göstermiştir. / In this study, an example of a smart home system has been presented, where blockchain technology has been integrated with IoT. In the designed IoT-based system, a distributed blockchain database has been employed for data privacy and integrity, and the obtained results demonstrate the preservation of data integrity and the absence of data losses.



***Şekil A**:IoT sistemlerin güvenliğini sağlayan uygulama tasarımı /**Figure A:** Design of applications ensuring the security of IoT systems.*

Önemli noktalar (Highlights)

- *IoT cihazlarından alınan verilerin güvenliği için kullanılan kimlik doğrulama, kimlik yönetimi, veri bütünlüğü yöntemi, yetkilendirme ve erişim denetimi, birlikte çalışabilirlik ve gizlilik yöntemleri üzerine blokzincir teknolojisi ile çözümler sunulmuştur./ Solutions utilizing blockchain technology have been presented for authentication, identity management, data integrity methods, authorization and access control, interoperability, and privacy methods employed for securing data from IoT devices.*
- *Akıllı bir ev sistemi için tasarlanan IoT ağ sisteminde ortam verilerinin güvenliği blokzincir teknolojisi ile sağlanmıştır./ In the IoT network system designed for a smart home system, the security of environmental data is provided by blockchain technology.*
- *IoT sistemlerde oluşan veri güvenliği problemleri için blokzincir teknolojisi potansiyel çözümler sağlamaktadır./ Blockchain technology provides potential solutions for data security problems arising in IoT systems*

***Amaç (Aim):** IoT cihazlarından alınan verilerin güvenliğini sağlamak için örnek bir uygulama ile akıllı bir ev sistemi olarak tasarlanan IoT ağında ortam verilerinin güvenliği blokzincir teknolojisi ile sağlanmıştır./ The security of environmental data in the IoT network, which is designed as a smart home system with a sample application to ensure the security of data received from IoT devices, is provided by blockchain technology.*

***Özgünlük (Originality):** Çalışma IoT sistemlerde oluşan veri güvenliği problemleri için blokzincir teknolojisinin çözümler sunduğunu gösterdi./ The study demonstrated that blockchain technology provides solutions for data security problems in IoT systems.*

***Bulgular (Results):** Blokzincir teknolojisi ile IoT cihazları arasında güvenli veri aktarımı sağlanması için tasarlanan sistemde verilerin güvenli olarak iletildiği kanıtlanmıştır./ It has been proven that data is transmitted securely in the system designed to ensure secure data transfer between IoT devices with blockchain technology.*

***Sonuç (Conclusion):** IoT tabanlı sistemlere veri gizliliği ve bütünlüğü için blokzincir dağıtık veri tabanı uygulanarak alınan sonuçlardan bir veri bütünlüğü saptandığı ve veri kayıplarının olmadığını göstermektedir./ The results obtained by applying blockchain distributed database to IoT-based systems for data confidentiality and integrity show that data integrity is detected and there is no data loss.*

* Corresponding author, e-mail: gulturker@sdu.edu.tr
DOI: 10.29109/gujsc.1194653

GU J Sci, Part C, 12(1): 80-91 (2024)

Gazi Üniversitesi
Fen Bilimleri Dergisi
PART C: TASARIM VE TEKNOLOJİ

Gazi University
Journal of Science
PART C: DESIGN AND TECHNOLOGY

http://dergipark.gov.tr/gujsc

Blokzincir Teknolojisi ile Nesnelerin İnterneti Tabanlı (IoT) Sistemlerin Veri Güvenliğinin Sağlanması

Gül Fatma TÜRKER[1*] Kubilay TANYERİ[2]

[1]*Suleyman Demirel University, Faculty of Engineering, Department of Computer Engineering , Isparta, Turkey*

Makale Bilgisi

Research article
Received: 28/10/2022
Revision: 23/05/2023
Accepted: 23/05/2023

Anahtar Kelimeler

Akıllı Ev Sistemi
Blokzincir
Nesnelerin İnterneti (IoT)
Nesnelerin İnterneti Güvenliği
Veri Bütünlüğü

Öz

Günümüzde akıllı şehirlerin, akıllı evlerin ve nesnelerin ortaya çıkması ile Nesnelerin İnterneti (Internet of Things - IoT) değeri artan bir teknoloji olarak gelişmektedir. 2025 yılına kadar internete bağlı olan IoT cihaz sayısının 70 milyarı geçmesi beklenmektedir. IoT sistemleri sınırlı kaynaklara ve hesaplama yeteneğine sahip olmaları, merkezi topolojiye sahip olmamaları nedeniyle pek çok gizlilik ve güvenlik sorunlarını oluşturmaktadır. Veri gizliliği ve veri bütünlüğü IoT veri aktarımında oldukça kritik parametrelerdir, bu nedenle IoT çözümlerinde, hizmet potansiyeli ve hassas verileri içermesi açısından topladıkları ve işledikleri verilerin güvenliği ve gizliliği önemlidir. IoT sistemlerde oluşan veri güvenliği problemleri için blokzincir teknolojisi potansiyel çözümler sağlamaktadır. Bu çalışmada, IoT cihazlarından alınan verilerin güvenliğini sağlamak için blokzincir teknolojisi kullanılmıştır. Akıllı bir ev sistemi için tasarlanan IoT ağı uygulaması üzerinde IoT cihazlarındaki güvenlik açıklıklarından kaynaklanan veri mahremiyeti problemi için blokzincir oluşturulmuş ve cihazlar arasındaki veri iletişiminde iletilen verilerin güvenliği oluşturulan hash algoritmaları ile sağlanırken aynı zamanda veri bütünlüğü testleri yapılarak iletilen verilerin doğruluğu kanıtlanmıştır.

Ensuring Data Security of Internet of Things (IoT) Systems with Blockchain Technology

Article Info

Araştırma makalesi
Başvuru: 28/10/2022
Düzeltme: 23/05/2023
Kabul: 23/05/2023

Keywords

Smart Home System
Blockchain
Internet of Things
Internet of Things Security
Data Integrity

Abstract

Nowadays, with the emergence of smart cities, smart homes and objects, the Internet of Things (IoT) is developing as a technology with increasing value. By 2025, the number of IoT devices connected to the Internet is expected to exceed 70 billion. IoT systems pose many privacy and security problems due to their limited resources, computational capability, and lack of centralized topology. Data privacy and data integrity are critical parameters in IoT data transmission, so in IoT solutions, the security and confidentiality of the data they collect and process is important in terms of service potential and including sensitive data. Blockchain technology provides potential solutions for data security problems in IoT systems. In this study, blockchain technology is used to ensure the security of data received from IoT devices. Blockchain has been created for the data privacy problem caused by security vulnerabilities in IoT devices on the IoT network application designed for a smart home system, and the security of the data transmitted in the data communication between the devices is ensured by the created hash algorithms, while at the same time the data integrity tests have been carried out to prove the accuracy of the transmitted data.

1. GİRİŞ (INTRODUCTION)

Nesnelerin interneti günümüzde oldukça yaygınlaşan bir teknoloji olarak akıllı sistemlerin gelişimine katkı sağlamaktadır. IoT uygulamaları aracılığı ile insanların günlük hayatlarında kullandıkları pek çok elektronik cihaz birbirleriyle haberleşmekte ve ihtiyaç halinde bu cihazlar internete bağlanarak çözümler sunmaktadır [1]. Nesnelerin İnterneti, bir ağa bağlı tüm cihaz/nesnelerin insan müdahalesine ve veri girişine gerek duymadan belirli bir protokol ile kendi aralarında veri iletişimi yapabilen, milyarlarca veri toplayarak bu veriler ile karar verebilen akıllı bir iletişim sistemidir [2-3]. IoT teknolojisi günümüzde akıllı ev, akıllı şehir, enerji ölçüm, inşaat, sağlık, tarım, hayvan takibi, kamu sektörü, lojistik, ulaştırma, denizcilik gibi farklı alanlarda

*Corresponding author, e-mail: gulturker@sdu.edu.tr
DOI: 10.29109/gujsc.1194653

kullanılmaktadır [4]. IoT teknolojisinde meydana gelen hızlı değişimler, düşük maliyetli kablosuz sinyal iletminde ki önemi oluşturmasının yanısıra [1] bu tür cihazların ve kendi aralarında paylaşılan verilerin güvenlik sorunlarını da beraberinde getirmektedir. En önemli sorunlar verileri algılama, depolama ve işleme süreçlerinde karşımıza çıkmaktadır. Genellikle IoT cihazları uzak konumda yer alır ve bu cihazlardan gelen veriler kayıplara uğrayabilir ve değiştirilebilir, bu durum yanlış ve değiştirilmiş bilgilere, gizlilik, güvenlik tehditlerine ve tutarsızlıklara yol açabilir. Farklı IoT cihazlarından alınarak bir araya getirilen veriler kötü amaçlı olabilir ve diğer IoT katmanları tarafından güvenilir olarak bildirilse de güvenilmez hale gelebilir [5]. Güvenli ve güvenilir bilgilerin iletilmesi erişim denetimi, kimlik doğrulama, gizlilik ve bütünlük gibi güven ve gizlilik parametrelerinin korunması için gereklidir.

Blokzincir (Blockchain) teknolojisinin, âdemimerkeziyetçilik, dağıtılmış defterler, veri bütünlüğü konularında etkili olduğu kanıtlanmıştır. Bu teknoloji IoT cihazları açısından düşük karmaşıklık düzeyini sağlayabilir [6]. Hataya dayanıklı veri paylaşımı, hesaplama gücü, enerji, veri depolama vb. gibi özelliklerinden dolayı blokzincir mekanizması IoT ortamında duyulan güvenilirliği ve güvenliği önemli derecede artırabilecek yapıdadır [7]. IoT cihazlarından alınan verilerin, yetkilendirilmesi, kimlik doğrulaması ve denetimi blokzincir teknolojisi ile gerçekleştirilebilir. Blokzincirdeki her blok eşit yetki ve bilgiye sahiptir. Ağ işlemleriyle ilgili tüm bilgileri depolayan evrensel bir defter, tüm bloklar arasında paylaşılarak blokzincir teknolojisini güvenilir ve değişmez hale getirmektedir [8].

Biswas vd. yaptığı çalışmalarında, akıllı şehirler için IoT cihazları arasında güvenli iletişim sağlayan blokzinciri sistemlerine dayalı bir taslak önermişlerdir [9]. Leiding vd. yaptıkları çalışmalarında ise merkezi olmayan, Ethereum Blokzinciri tabanlı, kendi kendini yöneten bir VANET önermişlerdir [10]. Huang vd. çalışmalarında, IoT üzerinde veri erişimi, gizliliği ve transferi gibi konular üzerinde yoğunlaşmışlardır. Bu konularda güvenlik sorunlarına çözüm üretmek için Ethereum kullanılarak blokzinciri tabanlı sistem önermişlerdir [11]. Cha vd. yaptıkları çalışmalarında giyilebilir IoT sistemleri ve kullanıcıların veri gizliliğini sağlayan blokzincir destekli bir ağ sistemi önermişlerdir. Kullanılacak cihazlar şifrelenerek, sadece kullanıcı tarafından ulaşılabilir ve yine kullanıcı tarafından açılabilir şekilde blokzincirde tutulmuştur [12].

IoT cihazların erişim kontrolü için blokzincir sistemine dayalı çözüm yöntemlerinden biri olan 'Control Chain' yöntemi kullanılabilir. Bitcoin blokzinciri ile aynı temel prensipler kullanılarak çoklu blokzincir sistemleri oluşturulabilir [13]. 2012 yılına kadar yapılan çalışmaların özellikle Bitcoin alanına yönelik olduğu görülmektedir. 2013 yılı sonrasında blokzincir teknolojisinin farklı alanlarına yönelik çalışmaların yaygınlaştığı görülmektedir [14].

Akıllı evler için blokzincir tabanlı mimariler ilkesini kullan bir teknik Taylor vd. tarafından öne sürülmüştür. Sunulan çözümlerde haberleşme ve kimlik doğrulama amacıyla genel ve yerel olmak üzere iki tür blokzinciri kullanılmıştır. Sonuçlar, kümeleme ve düğümlerin ağ yükünü ve gecikmeyi azlattığını göstermektedir. Bu yaklaşım IoT tabanlı çözümlerin önemli bir parçası olan enerji ve kullanılabilirlik endişelerini de ortadan kaldırır [15]. Azaria vd. çalışmalarında, MedRec isimli blokzincir tabanlı veri kayıt yönetim sistemi önermişlerdir. Hastaların, geniş çaplı ve değiştirilmesi mümkün olmayan sağlık bilgilerine sahip olması ve bu bilgilere diğer sağlık kuruluşlarından erişim sağlanabilmesi amaçlanmıştır. Madenci bilgisayarları Proof-of Work (PoW) ile sistemin inanılırlığını sağlamıştır [16]. Watanabe vd. çalışmalarında, dijital haklar gibi sözleşmelerin idaresinin daha güvenli olması için yeni bir yöntem sunmuşlarıdır. Oluşturdukları yönteme Proof-of Stake (PoS) yöntemi ekleyerek melez bir blokzinciri sistemi ortaya çıkmıştır [17].

Önümüzdeki yıllarda blokzincir tabanlı DNS ve blokzincir tabanlı internet kullanımı yaygınlaşacaktır. DNS Chain; özgür, güvenli ve dağıtık bir DNS çözümü olarak öne sürülmüştür [18]. Secure Chain, log kayıtlarının ve ağda kullanılan cihaz bilgilerinin saklanmasına yönelik bir yaklaşımdır. Barnas çalışmasında, yeni bir siber güvenlik yaklaşımına ihtiyaç duyulduğunu belirtmiş ve ülke ulusal güvenliği için blokzincir kullanımına dair önerilerde bulunmuştur [19]. Sengupta vd. çalışmalarında öncelikle saldırıları, güvenlik açığı nesnelerine göre sınıflandırmış ve endüstriyel IoT uygulamaları üzerine bir vaka çalışması sunmuşlardır [20]. Giannoutakis vd. çalışmalarında akıllı ev kurulumlarının siber güvenlik mekanizmalarını desteklemek için

cihazların değişmezliğine odaklanan bir blokzincir sistemi oluşturmuşlardır. Önerilen metodoloji, akıllı ev ağ geçidi ve IoT cihazlarının bütünlüğünü sağlamak için uygun akıllı sözleşme desteğinin yanı sıra engellenen kötü amaçlı IP'lerin dinamik ve değişmez yönetimini de sağlamaktadır [21].

Blokzinciri IoT'ye entegre etmek için uygulanan teknik yaklaşımlar ve çözümler hakkında yapılan araştırmalarda güvenlik alanında eksikliklerin olduğu tespit edilmiştir [22-23]. Literatür araştırmasında görüldüğü üzere IoT sistemler, yapısı gereği yüksek seviye güvenlik gerektiren ağlardan oluşmaktadır. Özellikle veri güvenliğine yönelik gelişen sorunların kimlik doğrulama ve veri iletim aşamalarında olduğu tespit edilmiştir. Blokzincir teknoljisi ile bu sorunlar üzerine önerilen çözümler verilen literatür araştırmasında sunulmuştur. Özetlenen benzer çalışmalarda Ethereum kullanılarak kimlik doğrulama amaçlı çalışmalar yapılarak güvenli yönetim sistemi kontrolü sağlanmıştır. Bitcoin, Ethereum gibi mevcut teknikler kullanılarak uygulamalar yapıldığı izlenmiştir.

Bu çalışmada, akıllı bir ev sistemi için oluşturulan IoT tabanlı bir uygulamada kişisel verilerin ve mahremiyetin korunmasını sağlamak amacıyla verilerin iletileceği adresler seçilmiş ve sadece belirtilen adreslere verilerin gönderilmesi için blokzincir oluşturulmuştur. Ayrıca blokzincire aktarılan veriler çıkış ve varış noktasında karşılaştırılarak doğruluk testi yapılmıştır. IoT sistemde veri gizliliği, veri bütünlüğü, veri güvenliği geliştirilen yazılımda test edilerek kanıtlanmıştır. Ayrıca blokzincir teknolojisinin işleyişi, IoT mimarisi, blokzincir ve akıllı sözleşmeler ile IoT cihazlarından alınan verilerin güvenliği için kullanılan kimlik doğrulama, kimlik yönetimi, veri bütünlüğü yöntemi, yetkilendirme ve erişim denetimi, birlikte çalışabilirlik ve gizlilik yöntemleri üzerine çözümler incelenmiştir.

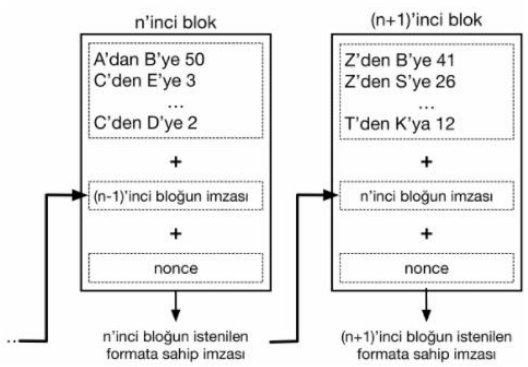
2. BLOKZİNCİR (BLOCKCHAIN)

Veri, teknoloji endüstrisindeki tüm yeniliklerin merkezi olmuştur. Bu durum, çeşitli kuruluşları ve satıcıları, birbirine bağlılığın farklı hizmetlerle iletişim kurmasına izin veren teknolojileri uygulamaya teşvik etmiştir. Bu gelişmeyi destekleyen ana teknolojilerden biri blokzincirdir. Blokzincir, merkezi bir otorite olmadan güvensiz bir ortamda anonimlik ve değişmezliği korurken, farklı müşteriler arasındaki iletişimi ademimerkezileştirmek için kullanılmıştır. Blokzincir geliştiricileri, farklı hizmet türleri ve çözümleri için blokzinciri önermektedir. Blokzincir yeteneklerini benimsemek için önerilen çözümlerden biri IoT paradigmasıdır [24].

2.1. Blokzincir Teknolojisi Yapısı ve Teknikleri
(Blockchain Technology Structure and Techniques)

Blokzincir teknolojisi, sistem kullanıcılarının verilerini ve işlemlerini tutan bloklardan oluşur ve işlemler kriptografi ile güvence altına alınmaktadır. Blokzincir teknolojisinde bulunan düğümler (node) birbirlerine bağlantılıdır ve bu kayıtlar bloklar sayesinde kayıt altına alınmaktadır. Blokzincir kavramı ilk kez 1991 yılında ortaya çıkmış ve Bitcoin adlı elektronik para birimi kullanılarak işlem kayıtlarının bir kamu tarafından tutulduğu ilk blokzincir oluşturulmuştur [6].

Blokzincir temel itibariyle bir veri tabanıdır. Veri tabanında bulunması gereken veriler bloklara sıralı bir şekilde kayıt edilmektedir. Blok büyüklüğü, bloğun veri bilgisi alanları (zaman damgası, başlık, şifre, versiyon numarası, ait olduğu protokol her bir kaydın parmak izi gibi), bilgilerin nasıl kayıt altına alınacağı, hangi veri alanlarını içereceği, bu alanların nasıl ve hangi düzende sıralanacağı, bloklar dolduğunda nasıl davranması gerektiği, bloklarların birbiri ile bağlantı özellikleri, yeni bloğun üretilme koşulları, blokzincirlerin merkezde nasıl dağılacağı, takip ve edileceği gibi konular her bir blokzincirin kendine ait özelliklerini ve kurallarını oluşturmaktadır. Şekil 1'de bir blokzinicir örneği verilmiştir. Her blok bir bloktan oluşur ve bu blokta bir önceki bloğun özet bilgileri yer alır. Blok içinde oluşan ilk zincir bloğu Genesis Blok'tur. Bu başlangıç bloğa kendisinden bir önceki blok olmaması sebebiyle bir önceki blok hash değeri olan değere blok zincir üreticisi tarafından bir değer atanır. Bu değer ise genellikle 256 adet "0" dan oluşur.



Şekil 1. Blokzincir yapısı (Blockchain structure)

Zincire yeni bir blok geldiğinde yeni gelen bloğun girdilerinden bir tanesi önceki bloğun hash değeri olacaktır. Blokları birbirine eklemek için bir önceki bloğun hash değeri kullanıldığından, herhangi bir blokta meydana gelecek değişiklik, o bloğun hash değerini değiştirecektir. Bundan dolayı devamındaki her bloğun hash değeri değişeceği için eklenen bloğun kendisinden gelen tüm blokların hash değerlerinin değişmesine sebep olacaktır. Bu durum ise mevcut zincirin orijinal zincir olmadığını ortaya çıkaracaktır.

Zincirdeki bir bloktan önce gelen bloğa ebeveyn blok (Parent Blok) adı verilmektedir. Her bloğun sadece bir tane ebeveyn bloğu olur. Fakat her ebeveyn bloğun birden fazla yavru (child) bloğu olabilmektedir. Bu durumda blokzincirde çatallanma (forking) olayı meydana gelmiştir.

Tablo 1. Blok yapısı (Block structure)

Alan Adı	Boyut	Açıklama
Sihirli Sayı	4 Byte	"Aşağıdaki bir bloktur " anlamında
Blok Boyutu	4 Byte	Blok büyüklüğünü gösterir
Blok başlığı	80 Byte	Farklı alanlardan oluşmaktadır
Kayıt sayacı	1-9 Byte	Kayıt (işlem) adedini gösterir
İşlem Kayıtlar	Değişken	Kayıt altına alınan işlemler ya da veriler

Blokzincirde bir bloğun genelde 5 alanı vardır. Tablo 1'de blokzinciri oluşturan bir bloğun alanları verilmiştir. Sihirli sayı herzaman 0xD9B4BEF9'dur. Bu alan blokzinicir veri tabanında bir veri okunurken devamında gelecek olan bilgilerin de bir blok olduğunu belirler. Blok boyutu ise blok sonuna kadar ne kadar alan olduğunu ifade eder. Yani bu alan bloğun sonunu ifade eder.

Blok Versiyonu; doğrulama kurallarından hangilerinin uygulanacağını belirler. Bir blok oluşturulurken uyulması gereken kurallar; bloğun yapısı, uzunluğu, kayıtların şekli, alanlarının sırası (syntax, standart) önemlidir. Belirlenen bu kurallar zaman içerisinde değiştirilebilir.

Merkle Ağaç Kökü Özeti; blok içerisine kayıt edilen işlemler ikişerli olarak gruplanır ve hash değerleri alınır. Bu şekilde hesaplamalar ikişerli olarak hesaplanıp en sonunda iki hash değeri kalır, onlar da hash yapılarak merkle ağacı kökü hesaplanmış olur. En son ulaşılan hash değeri merkle ağacı kökünü verir. Merkle ağaç kökü bloktaki tüm işlem kayıtlarının özeti olarak değerlendirilebilir. Bloklar hakkında bir diğer önemli kısım ise, blok yüksekliğidir. Blokzincirin oluşturulduğu tarihten günümüze kadar blokzincire eklenmiş olan blokların sayısını belirler.

3. NESNELERİN İNTERNETİ (IoT) (INTERNET OF THINGS (IoT))

IoT sistemler kuruldukları ortamlardaki verileri alır, birbirleriyle ağ üzerinden iletişime geçer ve kullanım amaçlarına göre bilgi servisi oluştururlar. Toplanan tüm bilgilerin güvenliği ve mahremiyeti dijital alanda önemli bir problem olarak karşımıza çıkmaktadır. Sensörler ve aktüatörler gibi teknoloji entegrasyonunun daha az güvenli bileşenleri istismar edilmeye açıktır ve temel güvenlik parametrelerini sızdırabilmektedir. Bu nedenle saldırgan üst düzey düğümlere ulaşabilir ve bütün ağı ele geçirebilir. Kaynak kısıtlı uç cihazlar ve yüksek performanslı üst düzey düğümler için kriptografik yöntemler oluşturmak IoT için büyük önem arz etmektedir. IoT kullanıcıları, IoT uygulamasının maliyet optimizasyonunun ve fiziksel dağıtımının değişen özelliklere sahip bileşenlere bağlı olduğunu bilmelidir [26].

IoT ve geleneksel ağlar arasındaki en önemli farklardan bir tanesi, cihazlarda bulunan kaynak seviyeleridir. Sensor ve RFID düğümlerine sahip olan IoT cihazları kısıtlı kaynağa sahip gömülü cihazları barındırmaktadır. Sınırlı pil ömrü, düşük işlemci gücü ve düşük bellek yapısı IoT cihazlarının en belirgin özelliklerindendir. Geleneksel ağlar bunun tersine akıllı telefonlar, güçlü bellek ve işlemci gücüne sahip sunucular ve bilgisayarları kapsamaktadır. Bundan dolayı geleneksel ağlar, çok yüksek karmaşık ve güvenlik protokolleri ile güvence altına alınabilirken, IoT cihazlarının oluşturmuş olduğu ağların güvenliğinin artırılması için bellek, işlemci gücü, pil ömrü vb. gibi etkenler göz önünde bulundurulmalıdır [27-28].

4. IoT GÜVENLİĞİ İÇİN BLOKZİNCİR ÇÖZÜMLERİ (BLOCKCHAIN SOLUTIONS FOR IoT SECURITY)

Blokzincirin güçlü alt yapısı kullanılarak IoT'nin gizlilik ve bütünlük sorunları çözülebilir. Örneğin, heterojen IoT cihazları arasında veri güvenilirliğinin garantisi ve güvenli veri paylaşımının zorluğu, verilerin değişmezliğini garanti eden ortak blokzincir platformu ile sağlanabilir. Blokzincirin IoT güvenliğinde kullanılabilecek alanları:

Kimlik Doğrulama Yönetimi: IoT sistemleri farklı türlerde kısıtlı kaynakların birlikte çalıştığı karmaşık bir ağ sistemi olduğu için, IoT senaryolarında çok faktörlü kimlik doğrulama ve hafif kimlik doğrulama protokolleri çok elzem olmaktadır. Pek çok kimlik doğrulama yöntemlerinin mevcut olmasına rağmen çeşitli protokoller ve IoT cihazlarının sınırlı kaynakları kimlik doğrulamasını oldukça zorlaştırmaktadır. X.509 sertifikaları, Donanım Güvenlik Modülü (HSM), Güvenilir Platform Modülü (TPM) ve Simetrik Anahtarlar gibi bazı yaygın kimlik doğrulama yöntemleri kullanılabilir. Bunların yanı sıra her yöntemin kendi içerisinde avantajları mevcuttur ve doğru türde kimlik doğrulama mekanizmasını seçmek IoT cihazları arasında güvenilir iletişimin sürdürülmesi açısından oldukça önemlidir. Akıllı sözleşmeler (smart contracts), IoT cihazlarına merkezi olmayan kimlik doğrulama yetenekleri elde etmesini sağlar. Ayrıca akıllı sözleşmeler, geleneksel yetkilendirme protokelleriyle karşılaştırıldığında, sisteme bağlı olan IoT cihazlarına daha etkili bir yetkilendirme erişim kuralı sağlayabilir. Akıllı sözleşmeler kullanılarak, grup, makine ve kişilerin verilere erişim süresi, durumu ve koşulu belirlenerek verilerin gizliliği sağlanabilir [29-30].

Kimlik Yönetimi: Dijital ortamlardaki kimlik, normal geleneksel yöntemler üzerine işleyen kimlik yönetimleri ile benzer şekilde çalışmaktadır. Geleneksel yöntemler olarak, birleştirilmiş, merkezileştirilmiş ve yalıtılmış sistemler kimlik yönetimi olarak bilinmekte ve dijital kimlik yönetimi olarak kullanılmaktadır. Dijital kimlik, süreçleri olduğundan hızlı hale getirip aktörlerin sayısını azaltsa bile çoğu kimlik yönetim sistemleri kimlik verilerini merkezi bir sunucuda depolayarak bu sistemi birçok güvenlik saldırısına karşı savunmasız hale getirmektedir. Blokzincir güvenlik özellikleri, güvenli ve güvenilir bir kimlik yönetim sistemi oluşturulması için kullanışlıdır. Blokzincir geleneksel kimlik yönetim sistemlerinden gelen birçok sınırlamaları ortadan kaldırabilmektedir [31]. Blokzinciri tabanlı kimlik yönetim sistemleri, dijital kimliklerin doğrulanması için Merkezi olmayan tanımlayıcılar veya DID (Decentralized ID) adı verilen benzersiz bir tanımlayıcı kullanır. Bir DID çözülebilir, kriptografik olarak doğrulanabilir, merkezi olmayan, yeniden atanamaz bağımsız sağlayıcılar olmalıdır. Blokzincir yapılı sistemlerde, kimliği veren kişi, kimlik bilgilerine DID ekler ve bu DID blokzincirde saklanır. Blokzincir gerçek veri erişim kısıtlamaları olan herkese aynı bilgiyi sağlayarak kimlik doğrulayıcı görevi üstlenir. Bundan dolayı blokzincir tabanlı sistemlerde kimlik bilgilerinin doğrulanması, kimlik doğrulayıcının kimliği verenin güvenilirliğine ilişkin değerlendirmesine bağlıdır. Bazı popüler kimlik yönetim sistemleri Sovrin, ShoCard ve Uport kimlik yönetim sistemleridir. Bu protokeller otomatik bir şekilde çalışır ve açık kaynak kodludur [32].

Veri Bütünlüğü Yönetimi: Blokzincir tabanlı bir IoT sistemde işlem bloğunun farklı alanlarının birleştirilmesi ile oluşan şifreleme işlemi veri bütünlüğünü korumanın uygun bir yoludur [33]. Blokzincir ağına bağlı IoT cihazlarından alınan veriler tekil bir anahtara sahiptir ve bu veriler ağ aracılığı ile doğrulanmaktadır. Bu sayede iletilen verilerin bütünlüğü ve doğrulanması gerçekleştirilir. Bununla birlikte IoT cihazlarından aktarılan veriler dağıtılmış sisteme sahip olan blokzincirler tarafından kayıt altına alınır ve verilerin bütünlük ve güvenliği takip edilir.

Yetkilendirme ve Erişim Denetimi: Blokzincir, tüm sistem merkezi olmadığı ve ağdaki her düğüm veya üye başkaları tarafından doğrulandığı için varsayılan olarak kimlik doğrulama sağlar [34]. Yetkilendirme süreci, IoT ağında bulunan servis hizmetlerine erişimleri denetler. Cihazlar arasında güveni devam ettirmek oldukça gereklidir, bununla birlikte belirli hizmetleri belirli cihazlara atamak

oldukça zordur. IoT ağında geleneksel veri erişiminden farklı olarak veri iletişimi gerçek zamanlı olarak yürütülür. Sorguların yürütülme işi ve veri akışı IoT ağında gerçek zamanlı olarak gerçekleşir, bundan dolayı oldukça güçlü bir erişim mekanizması kullanılması gerekmektedir. Blokzincirin âdemimerkeziyetçi yapısı ve değişmez altyapısı kullanıcı ile Authorization Server arasında güvenilir bir veri iletişimi sağlar ve IoT cihazlarına merkezi olmayan kimlik doğrulama yeteneği kazandırır. Bununla birlikte erişim kontrol mekanizmaları politikalarını şeffaf ve değişmez bir hale gelir.

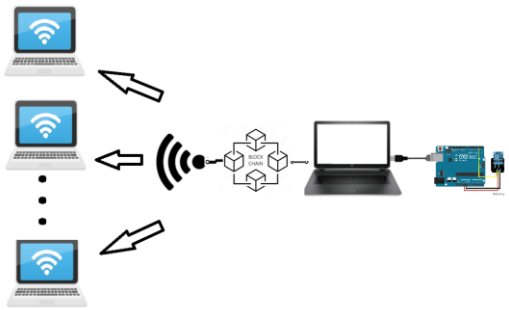
Birlikte Çalışabilirlik Yöntemi: Mevcut birlikte çalışabilirlik, ağ geçitleri ve ağ cihazlarına dayanmaktadır. Fakat bu ağ cihazlarının ve ağ geçitlerinin stabil şekilde çalışabilmeleri için sınırlı yetenekleri mevcuttur. Birlikte çalışabilirlik için henüz belirlenmiş bir standart yoktur ancak bu standartların oluşabilmesi için hizmet sağlayıcıların ve geliştiricilerin ortak çalışmaları bir zorunluluktur. Bir diğer sorun IoT cihazlarının üzerinde kullanılan güvenlik çözümlerinden kaynaklanmaktadır. Birlikte çalışabilirlik için blokzincir mekanizması etkin bir çözüm oluşturabilmektedir. Blokzincir mekanizması dağıtılmış ve otomatik bir şekilde çalışır. S2GHOST, Work (Co-PoW) ve Tornado otoritelerce tanımlanmış iç model olarak bilinmektedir.

Gizlilik Yöntemi: Veri gizliliği, dijital platformlardaki en önemli sorunlardan birisidir. Gizlilik sorunu için, iletişim sisteminde çeşitli simetrik (AES, IDEA) ve asimetrik (ECC, RSA) anahtar şifreleme sistemleri ve tokenizasyon yaygın olarak kullanılmaktadır [35]. IoT cihazlarının kullanım alanlarından olan, akıllı araç sistemleri, akıllı sağlık sistemleri, akıllı evler vb. gibi sistemler üzerinden akan bilgilerin gizliliğinin korunması gerekmektedir. IoT cihazlarının mimari yapısı gizlilik risklerini artırmaktadır. Son zamanlarda yapılan araştırmalarda IoT cihazları için kriptografi kullanan bazı protokoller önerilmiştir ancak gizliliği korumada bazı sınırlamaları ve zorlukları mevcuttur. Blokzincir verilerin şifrelenmesini kullanarak IoT sistemlere potansiyel çözüm sunmaktadır. Tüm kullanıcılara açık olan blokzincir herkesin sistemde bulunan verilere erişmesine izin verirken, özel blokzincir, blokzincir ağ kullanıcılarını sınırlamak için ideal bir çözüm olarak düşünülebilir.

5. BLOKZİNCİR TEKNOLOJİSİ İLE IoT GÜVENLİĞİNİ SAĞLAYAN UYGULAMA (APPLICATION PROVIDING IoT SECURITY WITH BLOCKCHAIN)

Kişisel ve hassas veriler çeşitli casus yazılımlar veya servisler gibi yasal olmayan yöntemler ile ele geçirilmektedir. Nesnelerin İnterneti teknolojisinde ağın büyüklüğü, verilerin fazlalığı, IoT cihazlarının güvenilirlik düzeyinin düşük olması sebebi ile mevcut IoT sistemi iyileştirmek için farklı teknikler ve algoritmalar kullanılmaktadır [36]. IoT ağlar üzerinde verilerin güvenliğinin sağlanması için blokzincir teknoljisinin etkili çözümler sunduğu bilinmektedir.

Bu çalışmada akıllı ev sistemleri için bir IoT ağı tasarlanmıştır. IoT cihazlar üzerinden alınan ortamdaki veriler blokzincir kullanılarak ağda ki diğer cihazlara güvenli şekilde iletilmesini sağlayan bir uygulama gerçekleştirilmiştir. Sunucu bilgisayarın bulunduğu ortamdan DHT11 sensörü ile alınan nem ve sıcaklık verileri, oluşturulan blokzincir sistemine aktarılmıştır. Dağıtık bir yapıda olan blokzincir verileri (nem, sıcaklık) sunucu (server) bilgisayara bağlanan istemci (client) bilgisayarlara güvenli bir şekilde iletilmiştir. Blokzincir ile IoT cihazlarının güvenliğini sağlamak için geliştirilen bu çalışmada sunucu ile istemci arasında 8890 portu üzerinden iletişim kanalı oluşturulmuştur. İstemci bilgisayarlar bağlanma isteğini bu port üzerinden blokzincirin üretildiği sunucu bilgisayara gönderir ve sunucuya bağlanma istekleri, sunucu bilgisayarın istemci isteklerine izin vermesi koşulu ile gerçekleşir.



Şekil 2. IoT sistemlerin güvenliğini sağlayan uygulama tasarımı (Application design that ensures the security of IoT systems)

Şekil 2'de IoT sistemde veri güvenliğini sağlayan örnek tasarım verilmiştir. Blokzincir ile IoT cihazlarının güvenliğini sağlayan uygulama C# programlama dili ile gerçekleştirilmiştir. Tasarlanan IoT sistemde ardunio cihazı ve DHT11 nem ve sıcaklık sensörü kulanılmıştır. Nem ve sıcaklığı algılayacak şekilde programlanan ardunio (IoT düğümü) ile veriler elde edilmiştir. Sunucu bilgisayara bağlanan ardunio ortamın nem ve sıcaklık değerlerini alabilmektedir. Kullanılacak sistemlerin ihtiyaçlarına göre ağa dahil edilen cihazlar bluetooth ya da Wi-Fi teknolojileri ile desteklenebilir.

Blokzincir oluşturulma aşamasında her bir blok oluşumu için kullanılacak blok sınıfı tanımlanır. Bloklarda her bir bloğun index numarası, oluşturulma zamanı, nem ve sıcaklık değerlerinin aktarılacağı veri alanı, bir önceki bloğun hash değeri ve kendi hash değeri tutulmaktadır. Her bir bloğun oluşturulacak hash değeri, SHA256 şifreleme algoritması sayesinde CalculateHash() fonksiyonu aracılığı ile TimpeStamp, PreviousHash ve Data alanları kullanılarak oluşturulmaktadır. Böylece çözülmesi ve oluşturulması neredeyse imkânsız olan bloğa ait bir biricik hash değeri üretilmektedir.

Blokların birbirleriyle ilişikli ve sıralı bir şekilde tutulacağı blokzincir ise, Blokzincir MainBlockchain = new Blockchain(); ile MainBlockchain olarak tanımlanmıştır. Blokzincir sınıfının içerisinde üretilen blokların ekleneceği kod parçası Şekil 3'te tanımlanmıştır.

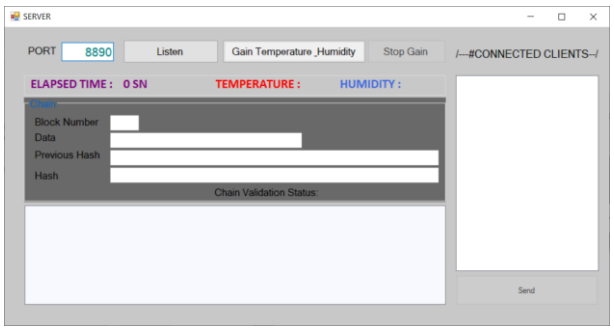
```
1  public void AddBlok(Blok blok)
2  {
3      Blok latestBlok = GetLatestBlok();
4      blok.Index = latestBlok.Index + 1;
5      blok.PreviousHash = latestBlok.Hash;
6      blok.Hash = blok.CalculateHash();
7      Chain.Add(blok);
8  }
```

Şekil 3. Blokları zincire ekleyen kod parçası (Piece of code that adds blocks to the chain)

AddBlok(Blok blok) fonksiyonu her 3 saniyede bir IoT cihazı tarafından okunan ortamın nem ve sıcaklık değerlerinin bir blok olarak oluşturulmasından sonra MainBlockchain olarak tanımlanan blokzincire eklemekle görevlidir. Blok ekleme ve blokzincir doğrulamasının yapılacağı IsValid() fonksiyonu "Public Class Blokzincir" sınıfı içerisinde tanımlanmıştır.

Arduino cihazından alınan verilerin sisteme aktarılması readtime_Tick(object sender, EventArgs e) fonksiyonu aracılığı ile gerçekleştirilir. Bu sayede ardunio cihazı her 3 saniyede bir ortamın nem ve sıcaklık değerini okur. Bu değer create_Blok() fonksiyonuna gönderilerek blok oluşturulur. Oluşan her bir bloğun hash değeri bir sonraki bloğun previousHash değeri olacak şekilde blokzincir sistemine kayıt edilir.

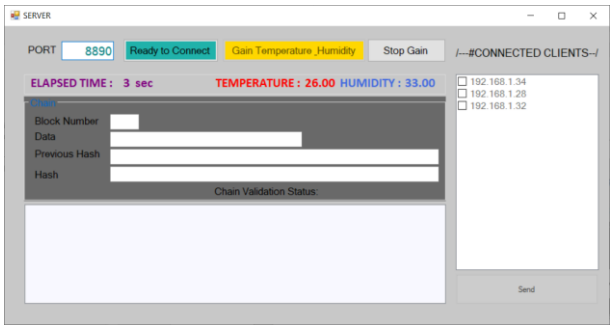
Şekil 4'te sunucu bilgisayar için tasarlanan arayüz verilmiştir. Arayüz üzerindeki Listen butonu aktif edildiğinde istemci bilgisayarlar sunucu bilgisayara bağlanabilir hale gelir. Bu durumda IoT düğüm üzerindeki nem ve sıcaklık verileri blokzincire aktarılmaya hazırdır.



Şekil 4. Sunucu bilgisayarda kullanıcı arayüzü (User interface on server computer)

'Gain Temperature_Humidity' butonu aktif duruma getirildiğinde verileri alıp blokzincire aktarmaya başlayacaktır. 'Connected Clients' alanı sisteme bağlanıp ardunio cihazından alınan verilerin

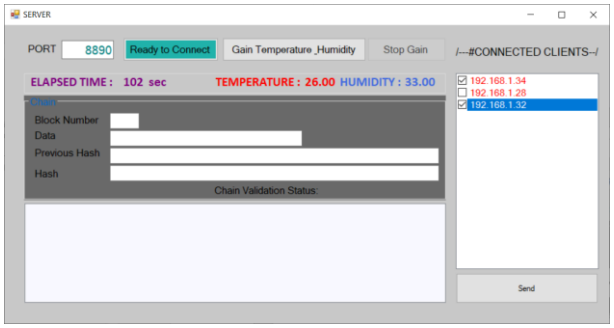
aktarılacağı istemci bilgisayarların IP (internet protocol) adreslerini göstermektedir. Sunucu'nun IP numarası 192.168.1.27 olarak tespit edilmiştir. Şekil 5'te IP adresleri 192.168.1.28, 192.168.1.32, 128.168.1.34 olan 3 istemcinin sunucuya bağlanmış olduğu görülmektedir. 'Gain Temperature_Humidity' butonu aktif edilmiş ve sistemin bulunduğu ortamın nem ve sıcaklık değerleri her 3 saniyede bir okunarak blokzincire aktarılması başlamıştır.



Şekil 5. Sunucu bilgisayarda program başlatılması (Starting a program on the server computer)

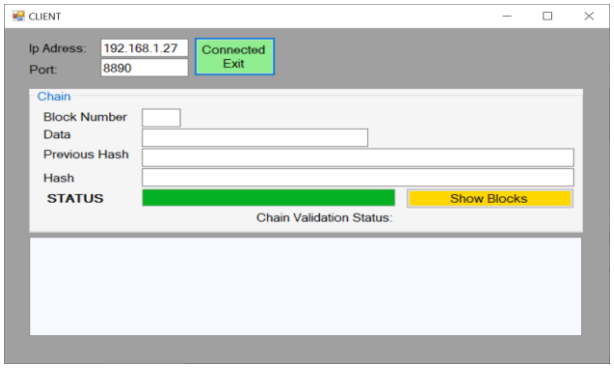
'Gain Temperature_Humidity' butonu aktif hale getirilmesi ile nem ve sıcaklık değeri alma işlemi başlatılmakta ve ortamın nem ve sıcaklık değeri her 3 saniyede bir ekranda gösterilmektedir. Bu değerler aynı zamanda blokzincirde veri alanlarına aktarılan değerlerdir. Kullanıcının isteğine bağlı olarak 'Stop Gain' butonu ile ortamın nem ve sıcaklık değerlerini blokzincire aktarma işlemi durdurulabilir. Bu süreç içerisinde her 3 saniyede bir nem ve sıcaklık değerlerinden oluşan veriler blokzincir oluşumunda kullanılmaktadır.

Şekil 6'da sistemde 102 saniye geçmiş ve 'Stop Gain' butonu ile 34 adet bloktan oluşan blokzincir oluşumu tamamlanmıştır. Bu aşamada sunucu'ya bağlanan istemcilere ait IP numaralarının renk durumu kırmızıya dönmesi ile sunucudan hangi istemciye blokzincir verilerinin aktarılacağı belirlenecektir. Şekil 6'da sunucu'ya bağlanan 192.168.1.32 ve 192.168.1.34 IP adresli istemcilere verilerin gönderileceği sunucu kullanıcısı tarafından seçilmiştir.



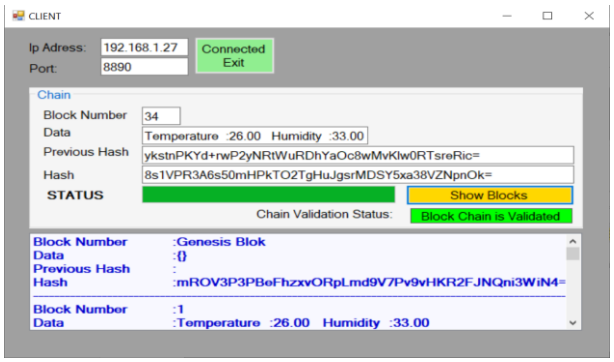
Şekil 6. Sunucu bilgisayarda veri okunmasının durdurulması (Stopping data reading on the server computer)

Sunucu bilgisayardan 192.168.1.28 IP adresli istemciye blokzincir verilerinin gönderilmeyeceği görülmektedir. 'Send' butonu ile 34 adet bloktan oluşan blokzincir verileri IP numaraları seçili istemcilere gönderilmiştir.



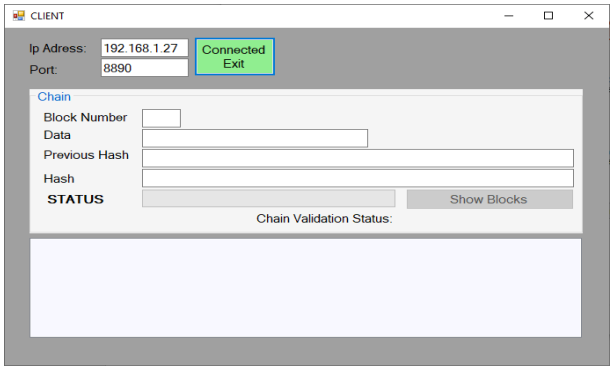
Şekil 7. İşlemci bilgisayarda veri alınmasının tamamlanması (Completing data retrieval on the processor computer)

Şekil 7'de sunucu'dan istemcilere verilerin gönderilme durumu 'STATUS' bardan anlık olarak takip edilebilmektedir. 'STATUS' barın tamamı yeşile döndüğü durumda artık blokzincirde bulunan nem ve sıcaklık verileri içeren blokların istemcilere gönderilme işlemi tamamlanmıştır. Şekil 8'de istemci bilgisayarda yer alan arayüz verilmiştir, programda bulunan 'Show Bloks' butonu ile blokzincirdeki bloklara ait veriler ekranda görülmektedir. Ayrıca tüm bloklar alt kısımda yer alan bilgi ekranından da takip edilebilir durumdadır. Blokzincirdeki blokların ekranda gösterilmesi ile blokzincirin doğrulanması yapılabilmektedir. Tüm blokların, bir önceki ve bir sonraki bloklarının hash değerleri kontrol edilerek bloklar arasında herhangi bir kopma, veri kaybı veya kötü niyetli saldırganlar tarafından herhangi bir blok eklenip eklenmediği kontrol edilir. Eğer blokzincirde bir veri kaybı söz konusu değilse veya blok ya da bloklar eklenmesi durumu yok ise verilerin güvenli ve doğru bir şekilde aktarıldığı anlaşılır. Bu durumda sistem 'Blokcahin is Validated' bilgisini vermektedir. Bu aşamada IsValid() fonksiyonu kullanılmıştır. Bloklardaki verilerde ve zincirde bir bozulma olması durumunda sistem, istemci tarafında 'Blockchain is not Validated' uyarısı vermektedir.



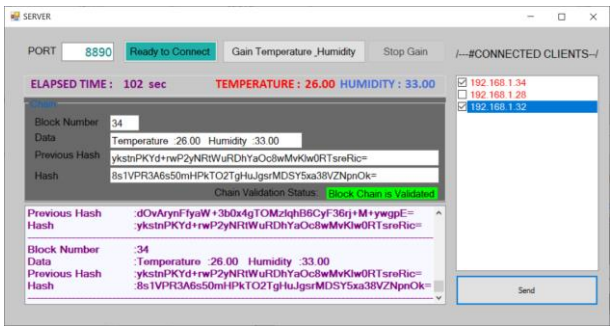
Şekil 8. İşlemci bilgisayarda blokların doğrulama durumu (Validation status of blocks on the processor computer)

İstemci bilgisayar ekranında blok numaraları, data, previous hash ve bloğun kendi hash değerleri görülmektedir. Sunucu bilgisayar ile ağ bağlantı sonlandırılması 'Connected Exit' butonu ile yapılır. Şekil 9'da 192.168.1.28 IP numaralı istemci 192.168.1.27 IP numaralı sunucu tarafından seçilmediği için blokzincir verilerinin bu istemciye iletilmediği görülmektedir.



Şekil 9. İşlemci bilgisayarda veri alma durumu (Data retrieval status on the processor computer)

Şekil 10'da sunucu'da verilerin IP numaraları seçili istemci bilgisayarlara iletilmesi bilgisi verilmiştir. Gönderilen blokzincir blokları ve doğrulama durumu 'Chain Validation Status' alanında görülmektedir.



Şekil 10. İşlemci bilgisayarda blokzincir verilerinin gösterimi (Display of blockchain data on the processor computer)

Şekil 10'da sunucu bilgisayar tarafından blokzincir ile iletilen veriler Şekil 8'de verilen istemci bilgisayar arayüzünde veri kayıpsız olarak iletildiği görülmektedir.

Tasarlanan IoT sistemi üzerinde veri kayıplarını engellemek için blokzincir teknolojisi kullanılmıştır. Cihazlar arasında gönderilen veriler blokzincire aktarılarak değiştirilemez bir yapı oluşturulmuş ve veri güvenliği sağlanmıştır. Tasarlanan uygulamada iletilen verilerin alınan veriler ile testleri yapılarak veri bütünlüğü sağlandığı kanıtlanmıştır.

5. SONUÇ VE ÖNERİLER (CONCLUSION AND SUGGESTIONS)

IoT sistemleri siber saldırı gibi güvenlik ve gizlilik sorunları ile karşılaşmaktadır. Bunun gibi güvenliği tehdit eden durumları engellemek amacıyla blokzincir teknolojisinin kritik bir önem taşıdığı görülmektedir. Bu çalışmada blokzincir teknolojisi ile IoT entegrasyonu yapılan bir akıllı ev sistemi örneği oluşturulmuştur. Tasarlanan IoT tabanlı sisteme veri gizliliği ve bütünlüğü için blokzincir dağıtık veri tabanı uygulanmış ve alınan sonuçlardan bir veri bütünlüğü saptandığı ve veri kayıplarının olmadığı gösterilmiştir. IoT veri haberleşmesinde kimlik doğrulama ve denetimi ve veri paylaşımı aşamalarında saldırılara karşı ortaya çıkabilecek olası veri kayıplarının önlenmesi için blokzincir teknolojisi ile bilgilerin depolandığı evrensel bir defter oluşturularak güvenilir ve değişmez bir yapı oluşturulmuştur. Örnek uygulamada ortam nem ve sıcaklık değerleri her 3 saniyede bir alınarak blokzincirdeki bloklar oluşturulmuş ve veri alanlarına aktarılmıştır.

Geliştirilen sistemde verilerin kayıpsız olarak iletilmesi veri bütünlüğü testleri ile yapılmaktadır. Bu aşamada verilerin ilk olarak algılandığı IoT sensör verileri ile gönderilmek istenen noktada ki veri karşılaştırması yapılarak sistemin doğruluğu kanıtlanmıştır. İletilecek veri şifrelenerek, sadece yetkilendirilmiş kullanıcı tarafından ulaşılabilir ve yine kullanıcı tarafından açılabilir şekilde blokzincirde tutulmuştur. Özellikle yetkili kullanıcı seçilmesi sayesinde düğümlerin ağ yükü hafifletilmiştir. Veri iletişimindeki güvenliğin yanı sıra bir diğer önemli husus olan veri gizliliği verilerin blokzincirde kullanılan hash yöntemiyle saldırganların kaynakları ele geçirmesinin önüne geçilmiştir. Veri iletim aşamasında hem saldırılara karşı veriler korunmuş hem de verilerin iletildiği noktada testleri yapılarak veri bütünlüğü sağlanmıştır. Blokzincir teknolojisinin IoT sistemler için güvenli bir hizmet oluşturduğu kanıtlanmıştır. Sonuçlar dikkate alınarak yeni algoritmalar geliştirilebilir ve gelecekte blokzincir teknolojisi kullanılarak hızla büyüyen bir ağ olan IoT tabanlı cihazlar arasında güvenli veri aktarımı sağlanabilir.

ETİK STANDARTLARIN BEYANI (DECLARATION OF ETHICAL STANDARDS)

Bu makalenin yazarları çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler.

The author of this article declares that the materials and methods they use in their work do not require ethical committee approval and/or legal-specific permission.

YAZARLARIN KATKILARI (AUTHORS' CONTRIBUTIONS)

***Gül Fatma TÜRKER*:** Deneyleri yapmış, sonuçlarını analiz etmiş ve maklenin yazım işlemini gerçekleştirmiştir.

***Kubilay TANYERİ*:** He conducted the experiments, analyzed the results and performed the writing process.

She/He conducted the experiments, analyzed the results and performed the writing process.

ÇIKAR ÇATIŞMASI (CONFLICT OF INTEREST)

Bu çalışmada herhangi bir çıkar çatışması yoktur.

There is no conflict of interest in this study.

KAYNAKLAR (REFERENCES)

[1] Erkan, E., Fidan, Ş., & Oğraş, H. (t.y.). LoRa Modülasyon Tabanlı Saha Aydınlatma Sistemi Uygulaması. Gazi University Journal of Science Part C: Design and Technology, 203-216.

[2] Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008

[3] Ashton, K. (2009). That 'internet of things' thing. RFID journal, 22(7), 4986,2009.

[4] Gündüz, Muhammed Zekeriya, D. A. Ş. Resul. (2018). Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları, Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 24, 327-335.

[5] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164. https://doi.org/10.1016/j.comnet.2014.11.008

[6] Kumar, R., & Sharma, R. (2021). Leveraging blockchain for ensuring trust in IoT: A survey. Journal of King Saud University - Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2021.09.004

[7] Christidis, K. & Devetsikiotis. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303.

[8] Pilkington, M. (2016). Blockchain Technology: Principles and Applications.

[9] Biswas, K., & Muthukkumarasamy, V. (2016). Securing Smart Cities Using Blockchain Technology. 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 1392-1393.

[10] Leiding, B., Memarmoshrefi, P., & Hogrefe, D. (2016). Self-managed and blockchain-based vehicular ad-hoc networks (s. 140). https://doi.org/10.1145/2968219.2971409

[11] Huang, Z., Su, X., Zhang, Y., Shi, C., Zhang, H., & Luyang, X. (2017). A decentralized solution for IoT data trusted exchange based-on blockchain (s. 1184). https://doi.org/10.1109/CompComm.2017.8322729

[12] Cha, S.-C., Chen, J.-F., Su, C., & Yeh, K.-H. (2018). A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things. IEEE Access, 6, 24639-24649.

[13] Pinno, O. J. A., Gregio, A. R. A., & De Bona, L. C. E. (2017). ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT. GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 1-6. https://doi.org/10.1109/GLOCOM.2017.8254521

[14] Mendi, A. F. (2021). Blokzincir Uygulamaları ve Gelecek Öngörüleri. GSI Journals Serie C: Advancements in Information Sciences and Technologies, 4(1), 76-88.

[15] Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2020). A systematic literature review of blockchain cyber security. Digital Communications and Networks, 6(2), 147-156.

[16] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. 2016 2nd International Conference on Open and Big Data (OBD), 25-30.

[17] Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. J. (2016). Blockchain contract: Securing a blockchain applied to smart contracts. 2016 IEEE International Conference on Consumer Electronics (ICCE), 467-468.

[18] Singh, S., & Singh, N. (2016). Blockchain: Future of financial and cyber security. 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), 463-46717.

[19] Barnas, N. B. (2016). Blockchains in national defense: Trustworthy systems in a trustless world. Blue Horizons Fellowship, Air University, Maxwell Air Force Base, Alabama.

[20] Sengupta, J., Ruj, S., & Bit, S. D. (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, 102481. https://doi.org/10.1016/j.jnca.2019.10248191

[21] Giannoutakis, K. M., Spathoulas, G., Filelis-Papadopoulos, C. K., Collen, A., Anagnostopoulos, M., Votis, K., & Nijdam, N. A. (2020). A Blockchain Solution for Enhancing Cybersecurity Defence of IoT. 2020 IEEE International Conference on Blockchain (Blockchain), 490-495.

https://doi.org/10.1109/Blockchain50366.2020.00071

[22] Lo, S. K., Liu, Y., Chia, S. Y., Xu, X., Lu, Q., Zhu, L., & Ning, H. (2019). Analysis of blockchain solutions for IEEE Access, 7, 58822-58835.

[23] [23] Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. Sensors, 22(4), 1304.

[24] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., Teo, J., & Zakarya, M. (2022). An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. Sensors, 22(2), 572.

[25] D. Lee Kuo Chuen, Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data, Elsevier, 2015. (t.y.).

[26] Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex & Intelligent Systems, 1-33.

[27] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. Wireless Networks, 20(8), 2481-2501. https://doi.org/10.1007/s11276-014-0761-7

[28] Beechamresearch. (son). (2016). "IoT Sector Map". http://www.beechamresearch.com/article.aspx?id=4

[29] Abdelmaboud, A., Ahmed, A. I. A., Abaker, M., Eisa, T. A. E., Albasheer, H., Ghorashi, S. A., & Karim, F. K. (2022). Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. Electronics, 11(4), 630.

[30] İrfan Kösesoy. (2019). Nesnelerin İnterneti Güvenliğinde Blok Zinciri Uygulamaları. Yıl 2019, Cilt 2, Sayı 1.

[31] Rathee, T., & Singh, P. (2021). Secure data sharing using Merkle hash digest based blockchain identity management. Peer-to-Peer Networking and Applications, 14(6), 3851-3864. https://doi.org/10.1007/s12083-021-01212-4

[32] Haddouti, & El, S. (2020). 3rd International Conference on Advanced Communication Technologies and Networking, CommNet 2020. 3rd Int. Conf. Adv. Commun. Technol. Networking, CommNet 2020 1–7.

[33] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Lsb: A lightweight scalable blockchain for iot security and privacy," arXiv preprint arXiv:1712.02969, 2017.

[34] Roy, S., Ashaduzzaman, M., Hassan, M., & Chowdhury, A. R. (2018). Blockchain for IoT security and management: Current prospects, challenges and future directions. 2018 5th International Conference on Networking, Systems and Security (NSysS), 1-9.

[35] S. Roy, A. R. Shovon, and M. Whaiduzzaman, "Combined approach of tokenization and mining to secure and optimize big data in cloud storage," in Humanitarian Technology Conference (R10-HTC), 2017 IEEE Region 10. IEEE, 2017, pp. 83–88.

[36] Pattewar, G., Mahamuni, N., Nikam, H., Loka, O., & Patil, R. (2022). Management of IoT Devices Security Using Blockchain—A Review. Sentimental Analysis and Deep Learning, 735-743.