ISSN: 2618-6055 / 9, (1), 14 – 24, 2025
DOI:10.62301/usmtd.1691033

Uluslararası Sürdürülebilir Mühendislik ve Teknoloji Dergisi
International Journal of Sustainable Engineering and Technology
ISSN: 2618-6055 / Cilt:9, Sayı:1, (2025), 14 – 24
Araştırma Makalesi – Research Article

BLOKZİNCİR DESTEKLİ KİMLİK DOĞRULAMA: MERKEZİ SİSTEMLERE ALTERNATİF BİR YAKLAŞIM

*Didem YANGEÇ[1], Arif KOYUN[1]

[1]Süleyman Demirel Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği Bölümü, Isparta

(Geliş/Received: 05.05.2025, Kabul/Accepted: 31.05.2025, Yayınlanma/Published: 30.06.2025)

ÖZ

Çağımızın dijital dünyasında güvenliğin temel unsurlarından biri olarak kabul edilen kimlik doğrulama, bir kullanıcının, uygulamanın veya cihazın gerçek kimliğini doğrulamak amacıyla uygulanan bir süreçtir. Bu süreç, yalnızca yetkili bireylerin veya hizmetlerin belirli kaynaklara ve verilere erişmesini sağlamak açısından büyük önem taşımaktadır. Kimlik doğrulama; parolalar (yalnızca kullanıcının bildiği bir şifre), biyometrik veriler (yüz tanıma, parmak izi) veya güvenlik belirteçleri gibi çeşitli yöntemler kullanılarak gerçekleştirilebilir ve böylece sistemlerdeki erişim kontrol mekanizmaları etkin bir şekilde yönetilebilmektedir. Günümüzde kimlik doğrulama süreçleri, güvenlik ve gizlilik açısından büyük önem taşımaktadır. Geleneksel merkezi kimlik doğrulama sistemleri, kullanıcı bilgilerini merkezi bir sunucuda saklayarak erişim yetkilendirme süreçlerini yürütmektedir. Ancak, bu sistemler tek bir güvenlik merkezi içerdiğinden, veri ihlalleri ve siber saldırılara karşı risk altında olabilir. Buna karşılık, blokzincir destekli kimlik doğrulama sistemleri, merkezi bir otoriteye bağlı olmadan kimlik doğrulama sürecini yönetmektedir. Bu sistemler, dağıtık bir ağ üzerinde işlem yaparak, her kullanıcı için şeffaf, değiştirilemez ve izlenebilir bir kayıt defteri oluşturmaktadır. Bu sayede verilerin güvenliğini ve gizliliğini koruyarak işlem yapmaktadır. Böylece hem veri ihlalleri hem de siber saldırılar gibi tehditlere karşı daha dayanıklı bir güvenlik yapısı sunmaktadır. Bu çalışmada, geleneksel kimlik doğrulama sistemleri ile blokzincir destekli çözümler mimari yapı, güvenlik, performans açısından karşılaştırılmıştır. Elde edilen bulgular, her iki yöntemin avantajları ve zorluklarını ortaya koyarak, farklı kullanım senaryoları için en uygun kimlik doğrulama modelini belirlemeye yönelik öneriler sunmaktadır.

Anahtar kelimeler: Geleneksel Kimlik Doğrulama, Blokzincir Teknolojisi, Merkeziyetsizlik, Güvenlik, Performans Karşılaştırması.

BLOCKCHAIN-BASED AUTHENTICATION: AN ALTERNATIVE APPROACH TO CENTRALIZED SYSTEMS

ABSTRACT

Authentication, considered one of the fundamental elements of security in the digital world of our age, is a process applied to verify the true identity of a user, application, or device. This process is of great importance in ensuring that only authorized individuals or services have access to certain resources and data. Authentication can be carried out using various methods such as passwords (a secret known only to the user), biometric data (facial recognition, fingerprints), or security tokens, thus allowing effective management of access control mechanisms in systems. Nowadays, authentication processes are of great importance in terms of security and privacy. Traditional centralized authentication systems manage access authorization processes by storing user information on a central server. However, since these systems contain a single security center, they may be at risk of data breaches and

*Sorumlu Yazar/Corresponding Author: yangecdidem@gmail.com

ISSN: 2618-6055 / 9, (1), 14 – 24, 2025
DOI:10.62301/usmtd.1691033

cyber-attacks. In contrast, blockchain-based authentication systems manage the authentication process without relying on a central authority. These systems create a transparent, immutable, and traceable ledger for each user by operating on a distributed network. In this way, it operates while protecting the security and privacy of the data. Thus, it offers a more resilient security structure against threats such as data breaches and cyber-attacks. In this study, traditional authentication systems and blockchain-based solutions are compared in terms of architecture, security and performance. The findings reveal the advantages and challenges of both methods and provide recommendations for determining the most appropriate authentication model for different usage scenarios.

Keywords: Traditional Authentication, Blockchain Technology, Decentralization, Security, Performance Comparison.

1. Giriş (Introduction)

Kimlik doğrulama, bir kullanıcının iddia ettiği kimliğin gerçekten ona ait olup olmadığını doğrulama sürecidir [1]. Günümüzde bankacılık, sağlık hizmetleri gibi birçok çevrimiçi hizmetlerin yaygınlaşmasıyla birlikte kimlik doğrulamanın önemi giderek artmaktadır. Özellikle hassas verilerin korunması ve yetkisiz erişimlerin önlenmesi için güvenilir kimlik doğrulama yöntemleri kritik bir rol oynamaktadır [2].

Kimlik doğrulama yöntemleri, teknolojinin gelişmesiyle birlikte farklılaşmış ve daha güvenli hale gelmiştir. Bu bağlamda, geleneksel kimlik doğrulama ve blokzincir destekli kimlik doğrulama en çok tartışılan yöntemler arasında yer almaktadır.

Geleneksel kimlik doğrulama yöntemleri, genellikle kullanıcı adı ve şifre kombinasyonuna dayanmaktadır. Bunun yanında, iki faktörlü kimlik doğrulama (2FA) ve çok faktörlü kimlik doğrulama (MFA) gibi ek güvenlik katmanlarıyla da desteklenmektedir [3]. Şifre tabanlı doğrulama, kullanıcıların alışık olduğu basit, entegrasyonu kolay ve ekonomik bir yöntemdir. Fakat şifre çalınması, tahmin edilmesi veya yeniden kullanılması gibi riskleri taşımaktadır [4]. Geleneksel kimlik doğrulama yöntemlerinde kimlik bilgilerinin merkezi sunucularda saklanması, veri ihlalleri durumunda bu bilgilerin toplu halde ele geçirilmesine neden olabilecek ciddi güvenlik açıkları doğurmaktadır [5].

Blokzincir teknolojisi, merkezi olmayan ve değiştirilemez yapısıyla kimlik doğrulamada devrim niteliğindedir. Blokzincir destekli kimlik doğrulama, kimlik bilgilerini dağıtık bir defterde saklayarak güvenliği artırmakta ve veri bütünlüğünü garanti etmektedir. Veriler, merkezi bir sunucuda saklanmadığından tek bir saldırı noktası yoktur. Tüm işlemleri şeffaf ve değiştirilemez şekilde kaydetmektedir. Ancak mevcut sistemlerle entegrasyonunun zor olması ve yüksek maliyet gerektirmesi nedeniyle uygulanması daha karmaşıktır. İşlem doğrulama süresi uzun olması ve ölçeklenebilirlik konusunda iyileştirme gerektirmektedir.

Kimlik doğrulama, bir kullanıcının dijital sistemlere erişimini sağlamak için temel bir güvenlik mekanizmasıdır. Bu alandaki yöntemler, zaman içinde gelişerek çeşitli teknolojik düzeylere evrilmiştir. Geleneksel doğrulama yöntemleri arasında şifreler, akıllı kartlar ve dijital sertifikalar gibi bilgiye dayalı doğrulama teknikleri öne çıkmaktadır. Lal vd. (2016), farklı doğrulama yöntemlerini güvenlik düzeyleri açısından değerlendirmiş ve özellikle şifrelerin yüksek kardinaliteye sahip olması gerektiğini, akıllı kartların ise PIN ile desteklenmesi durumunda daha güvenli hale geldiğini belirtmiştir. Ayrıca, dijital sertifikalar ve çok faktörlü kombinasyonların kullanımıyla güvenlik düzeyinin artırılabileceği vurgulanmıştır [6]. Biyometrik doğrulama ise fiziksel veya davranışsal özelliklere dayalı olarak kullanıcı kimliğini belirlemeyi hedefler. Jain vd. (2004), biyometrik tanımlamanın geleneksel yöntemlere göre daha güvenli bir alternatif sunduğunu ifade etmiştir [7]. Amin vd. (2014) ise mobil cihazlarda kimlik doğrulama konusunu ele alarak geleneksel ve biyometrik yöntemlerin kullanımını değerlendirmiş, davranışsal biyometrinin (yazma ritmi, yürüme tarzı gibi) maliyeti düşürüp kullanılabilirliği artırabileceğini, ancak kişiye özel varyasyonların zorluk oluşturabileceğini belirtmiştir. Bu nedenle çok modlu (multi-modal) sistemlerin geliştirilmesi gerektiği önerilmiştir [8].

Wang vd. (2021), kimlik doğrulama sistemlerine yönelik saldırı türlerini detaylı şekilde inceleyerek, mevcut savunma mekanizmalarının yeterliliğini değerlendirmiştir. Bu çalışmada özellikle parola tabanlı ve biyometrik sistemlerin saldırılara açık olduğu vurgulanmış, savunma mekanizmalarının

*Sorumlu Yazar/Corresponding Author: yangecdidem@gmail.com

ISSN: 2618-6055 / 9, (1), 14 – 24, 2025
DOI:10.62301/usmtd.1691033

geliştirilmesinin gerekliliği ortaya konmuştur. Bu değerlendirme, çalışmamızın ikinci faktör doğrulama bileşenini geliştirirken güvenlik açıklarını dikkate alması açısından önemlidir [9].

Blokzincir teknolojisinin merkeziyetsiz, değiştirilemez ve güvenilir yapısı, kimlik doğrulama alanında yenilikçi çözümler sunmaktadır. Khalid vd. (2020), IoT cihazları için hafif bir blokzincir tabanlı kimlik doğrulama mekanizması önermiş ve mevcut sistemlere göre daha iyi performans sunduğunu göstermiştir [10]. Narayanan vd. (2022) da benzer şekilde IoT ortamında güvenli veri paylaşımı için blokzincir temelli bir model önermiş ve zaman verimliliği, depolama alanı ve işlem hacmi açısından başarılı sonuçlar elde etmiştir [11]. Zhao vd. (2020), dijital eğitim sistemleri bağlamında blokzincir tabanlı iki faktörlü kimlik doğrulama modeli geliştirerek, kimlik verilerinin merkezi olmayan şekilde korunabileceğini göstermiştir [12].

Blokzincirin ikinci faktör doğrulama ile birleştiği diğer bir uygulama alanı da finans ve e-ticaret sistemleridir. Mercan vd. (2021), kredi kartı işlemlerinde SMS doğrulama gibi ikinci faktör yöntemlerinin güvenliğini artırmak için blokzincir temelli bir yapı önermiştir. Bu yapı, hassas doğrulama verilerinin üçüncü taraflarca manipüle edilmesini engellemeyi amaçlamaktadır [13].

Toplumsal katılımın önemli bir alanı olan elektronik oylama sistemlerinde de blokzincir ve çok faktörlü doğrulama kombinasyonları kullanılmaktadır. Abayomi-Zannu vd. (2019), seçmen kimliğinin doğrulanmasında blokzincir destekli çok faktörlü bir sistem önererek, güvenli ve şeffaf mobil oylama çerçevesi sunmuştur [14].

Wanisha vd. (2024), blokzincir temelli çok faktörlü kimlik doğrulama sistemlerinin gizlilik, güvenlik ve kullanılabilirlik açısından avantajlar sağladığını vurgulamıştır. Ancak, bu sistemlerin hala olgunluk aşamasında olduğu ve uygulama karmaşıklığı nedeniyle yaygın kullanım için daha fazla geliştirilmesi gerektiği belirtilmiştir [15].

Literatür incelendiğinde, kimlik doğrulama sistemlerinin güvenliğini artırmak amacıyla çok faktörlü doğrulama yöntemlerinin giderek daha fazla benimsendiği görülmektedir. Aynı zamanda blokzincir teknolojisinin merkeziyetsiz yapı, şeffaflık ve veri bütünlüğü gibi özellikleri sayesinde bu doğrulama süreçlerine entegre edilmeye başlandığı anlaşılmaktadır. Ancak bu çalışmalar genellikle ya sadece merkeziyetsiz yapıyı ele almakta, ya da iki faktörlü doğrulamayı blokzincir dışında ele almaktadır. Bu çerçevede hem geleneksel sistemlerin pratik avantajlarını hem de blokzincir tabanlı yaklaşımların sunduğu güvenlik ve değiştirilemezlik özelliklerini bir araya getiren bütünleşik bir kimlik doğrulama çözümüne duyulan ihtiyaç ortaya çıkmaktadır. Bu çalışmada, merkezi kimlik doğrulama ile blokzincir destekli yapılar birleştirilerek her iki sistemin güçlü yönlerinden faydalanan yenilikçi bir çözüm önerilmektedir. Literatürde bu tür bütünleşik yaklaşımlara az rastlanmakta olup, önerilen sistem bu açıdan özgün bir katkı sunmaktadır.

Bu bağlamda, çalışma kimlik doğrulama sistemlerinin gelişen teknolojiyle birlikte karşılaştığı güvenlik, performans ve kaynak kullanımı gibi kritik konuları ele almakta; geleneksel ve blokzincir tabanlı yaklaşımları bu yönleriyle karşılaştırmalı olarak değerlendirmeyi amaçlamaktadır. Araştırma kapsamında, blokzincir teknolojisinin kimlik doğrulama süreçlerine sağladığı katkılar ile bu sistemlerin performans ve uygulanabilirlik açısından ortaya koyduğu sınırlılıklar detaylı bir biçimde incelenmektedir. Ayrıca, farklı kullanım senaryolarına göre hangi yaklaşımın daha uygun olduğuna dair çıkarımlarda bulunulmaktadır.

2. Materyal ve Metot (Material and Method)

Çalışmanın bu bölümünde, Duende IdentityServer ile geleneksel kimlik doğrulama ve Hyperledger Fabric ile blokzincir destekli kimlik doğrulama için kullanılan bileşenler ve doğrulama süreçlerine ait detaylı bilgiler aşağıdaki alt başlıklarda verilmiştir. Çalışma, iki farklı kimlik doğrulama yönteminin performans karşılaştırması ve analizine dayanmaktadır. Performans ölçümleri için yaygın olarak kullanılan açık kaynaklı bir test aracı olan Apache JMeter kullanılmıştır. JMeter, özellikle web uygulamaları ve hizmetlerinin yük (load) ve stres (stress) testlerini gerçekleştirmek amacıyla kullanılan bir performans test aracıdır. Bu çalışma kapsamında, kimlik doğrulama süreçlerinin farklı kullanıcı yükleri altındaki tepki süreleri ve işlem süreleri JMeter ile senaryolaştırılarak analiz edilmiştir.

*Sorumlu Yazar/Corresponding Author: yangecdidem@gmail.com

ISSN: 2618-6055 / 9, (1), 14 – 24, 2025
DOI:10.62301/usmtd.1691033

2.1. Duende kimlik sunucusu (Duende identityserver)

Çalışmada, geleneksel kimlik doğrulama için Visual Studio platformunda .NET Core 8 kullanılarak geliştirilen Duende IdentityServer ile bir kimlik doğrulama sistemi geliştirilmiştir. Duende IdentityServer, OpenID Connect ve OAuth 2.0 protokollerini destekleyen açık kaynaklı bir kimlik doğrulama ve yetkilendirme sunucusudur. Bu yapı, modern web uygulamaları ve API'ler için merkezi kimlik doğrulama ve yetkilendirme sağlamaktadır [16]. Bu sayede, sistemler arası güvenli kimlik paylaşımı sağlanabilmekte ve kullanıcıların erişim yetkileri merkezi bir yapı üzerinden yönetilebilmektedir. Duende IdentityServer aynı zamanda, yüksek düzeyde esneklik ve özelleştirilebilirlik sunarak farklı güvenlik ihtiyaçlarına uyarlanabilmektedir. Bu esneklik, çalışmada önerilen sistemin hem geleneksel doğrulama mekanizmaları hem de blokzincir tabanlı süreçlerle entegre bir şekilde çalışmasına olanak tanımıştır. Geniş geliştirici topluluğu ve kapsamlı dokümantasyonu sayesinde, geliştirme süreci hızlı ve sorunsuz ilerlemiş, sistemin kurulum ve yönetimi kolaylaştırılmıştır. Ayrıca, erişim denetimi, token yönetimi ve istemci doğrulama gibi güvenlik açısından kritik işlevleri sağlaması nedeniyle, kurumsal düzeyde güvenli bir kimlik doğrulama altyapısı sunma kapasitesi de önemli bir tercih sebebi olmuştur. Duende IdentityServer'ın hem teknik özellikleri hem de .NET Core mimarisiyle olan doğal uyumu sayesinde, çalışmada ihtiyaç duyulan güvenli, esnek ve sürdürülebilir kimlik doğrulama yapısı başarıyla geliştirilmiştir.

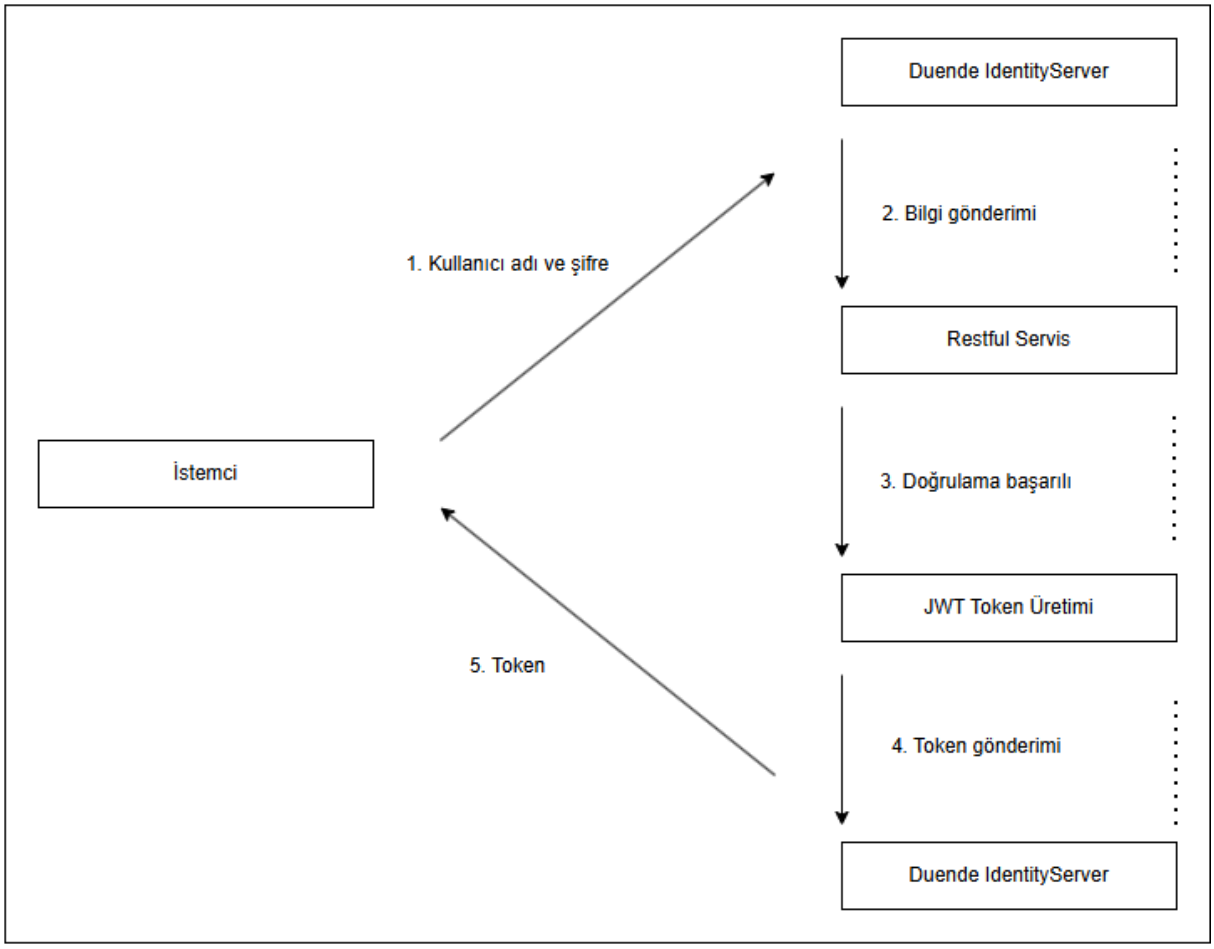
2.1.1. Kimlik doğrulama süreci (Authentication process)

Bu çalışmada, kullanıcı kimlik doğrulaması kullanıcı adı (email) ve şifre bilgileri kullanılarak yapılmıştır. Duende IdentityServer, kullanıcının girdiği bilgileri doğrulamak için bir RESTful servis ile iletişime geçer. Bu doğrulama süreci şu adımlardan oluşmaktadır:
Kullanıcı Girişi ve Bilgi Toplama: Kullanıcı, giriş sayfasında email ve şifre bilgilerini girer. Bu bilgiler, istemci (Client) tarafından Duende IdentityServer'a iletilir.

- RESTful Servis ile Doğrulama: Duende IdentityServer, kullanıcının girdiği bilgileri doğrulamak için bir RESTful servis ile iletişim kurmaktadır. Bu doğrulama işlemi için serviceToken, projectName, email ve password parametrelerini kullanmaktadır. ServiceToken, kimlik doğrulama işleminin güvenliğini sağlamak için kullanılan bir güvenlik anahtarıdır. ProjectName hangi proje için doğrulama yapıldığını belirtmektedir. Email, kullanıcının kimliğini doğrulamak için kullanılmaktadır. Password, kullanıcının kimliğini doğrulamak için gerekli olan şifre bilgisidir.
- Kimlik Doğrulama ve JWT Üretimi: RESTful servis, gönderilen parametreleri kontrol eder ve bilgilerin doğruluğunu teyit eder. Doğrulama başarılı olursa, Duende IdentityServer tarafından JWT (JSON Web Token) üretilmektedir. Bu token, kullanıcının kimliğini doğrulamak ve yetkilendirilmiş kaynaklara erişimini sağlamak için kullanılmaktadır. JWT içerisinde, kullanıcının kimlik bilgileri, yetki düzeyleri ve token süresi gibi bilgiler yer almaktadır.
- Token İletimi ve Yetkilendirme: Üretilen JWT (JSON Web Tokens), istemciye geri gönderilir. İstemci, bu token'ı her istek yaptığında HTTP Header içerisinde ileterek yetkilendirme işlemini gerçekleştirir. Duende IdentityServer, token'ı doğrulayarak kullanıcının kimliğini ve yetkisini teyit eder. Bu sayede, kullanıcı yalnızca yetkili olduğu kaynaklara erişebilir.
  Geleneksel kimlik doğrulama süreci Şekil 1'de gösterilmiştir.

*Sorumlu Yazar/Corresponding Author: yangecdidem@gmail.com

ISSN: 2618-6055 / 9, (1), 14 – 24, 2025
DOI:10.62301/usmtd.1691033



Şekil 1. Geleneksel kimlik doğrulama süreci (Traditional authentication process)

2.2. Blokzincir kimlik doğrulama süreci (Blockchain authentication process)

Blokzincir destekli kimlik doğrulama sistemi, merkezi olmayan ve güvenli bir yapı sunarak, kullanıcıların kimliklerini doğrulama sürecini daha güvenilir hale getirmektedir. Bu yapı, her işlemi dağıtık bir ağda kayıt altına alarak, verilerin değiştirilmesini veya sahtecilik yapılmasını imkânsız hale getirir [17]. Blokzincirinin sunduğu şeffaflık ve güvenlik özellikleri sayesinde, kimlik doğrulama işlemleri daha güvenli ve izlenebilir hale gelir [18].

Bu çalışmada, blokzincir destekli kimlik doğrulama sistemi, Hyperledger Fabric kullanılarak geliştirilmiştir. Bunun için sanal makine kurularak Linux tabanlı bir ortamda çalıştırılmıştır. Çünkü, Hyperledger Fabric, Linux Foundation tarafından geliştirilmiştir ve en güncel destek ile dokümantasyonun bu platformda bulunmasını sağlamaktadır [19].

Hyperledger Fabric, akıllı sözleşme (chaincode) geliştirme sürecinde Go, Java ve JavaScript gibi çeşitli programlama dillerini destekleyerek geliştiricilere esneklik sunmaktadır. Ancak, Hyperledger Fabric'in varsayılan programlama dili Go olduğu için, bu çalışmada kimlik doğrulama sistemi Go dilinde geliştirilmiştir. Bu sayede, sistemin güvenliği ve işleyişi Go'nun verimli ve güçlü yapısından faydalanarak sağlanmıştır.

Bunun yanı sıra, Hyperledger Fabric'in tercih edilme sebeplerinden biri de izinli (permissioned) bir blokzincir olmasıdır. Geleneksel açık blokzincir sistemlerinden farklı olarak, Hyperledger Fabric'de yalnızca yetkilendirilmiş kullanıcılar ağa katılabilir ve işlem gerçekleştirebilir. Bu özellik, sistemin güvenliğini artırarak yalnızca doğrulanmış kullanıcıların erişimine izin verir. Ayrıca, Fabric madencilik (mining) gerektirmediği için işlem onay süreleri çok daha hızlıdır. Geleneksel blokzincirlerde

*Sorumlu Yazar/Corresponding Author: yangecdidem@gmail.com

ISSN: 2618-6055 / 9, (1), 14 – 24, 2025
DOI:10.62301/usmtd.1691033

madencilik işlemi büyük hesaplama gücü gerektirirken, Hyperledger Fabric'in farklı konsensüs mekanizmaları sayesinde işlemler düşük gecikme süresiyle tamamlanır. Bu durum, özellikle kimlik doğrulama gibi anlık ve güvenilir işlem gerektiren sistemler için büyük bir avantaj sağlamaktadır.

Blokzincir destekli kimlik doğrulama süreci, merkezi bir otoriteye ihtiyaç duymadan kullanıcıların güvenli bir şekilde kimliklerini doğrulamalarını sağlamaktadır. Bu süreçte kullanılan en önemli güvenlik özelliklerinden biri, zaman tabanlı tek kullanımlık şifreler (TOTP-Time-Based One-Time Password) kullanımıdır. TOTP, özellikle iki faktörlü kimlik doğrulama (2FA) mekanizmalarında yaygın olarak kullanılan bir güvenlik aracıdır. TOTP, her kullanıcı için belirli bir zaman diliminde geçerli olan ve yalnızca bir kez kullanılabilen dinamik şifreler üretir. Bu dinamik şifreler, kimlik doğrulama sürecine ekstra güvenlik katmanı ekler ve şifrelerin sadece belirli bir süre için geçerli olmasını sağlar, bu da saldırganların şifreyi ele geçirme olasılığını azaltır. Blokzincir destekli kimlik doğrulama süreci şu adımlarla gerçekleştirilir:

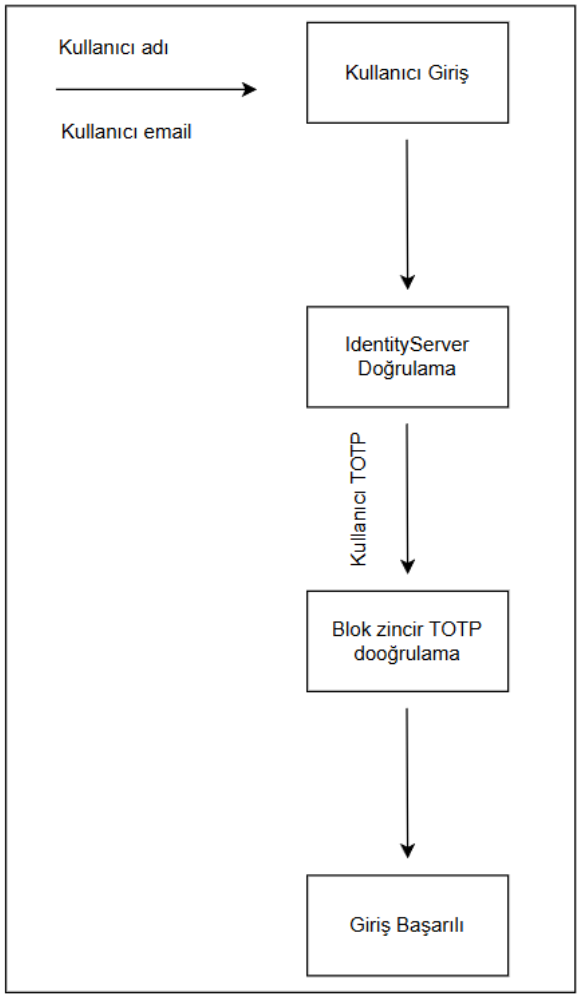
• Kullanıcı kayıt işlemi: Kullanıcı kayıt işlemi sırasında, kullanıcıya ait email adresi ile benzersiz bir TOTP gizli anahtarı (secret key) oluşturulur. Bu bilgiler, Hyperledger Fabric üzerinde çalışan bir chaincode (akıllı sözleşme) aracılığıyla blokzincirine kaydedilir. Kullanıcı bilgileri, anahtar-değer (key-value) formatında depolanarak hem verimlilik hem de güvenlik sağlanır. TOTP gizli anahtarı, her kullanıcı için özel olarak oluşturulur ve böylece kimlik doğrulama süreci her kullanıcı için benzersiz hale gelir.

• Kullanıcı doğrulama: Kullanıcının kimlik bilgileri (email ve şifre) IdentityServer üzerinden doğrulandıktan sonra, kullanıcıdan Google Authenticator gibi bir uygulama aracılığıyla oluşturulmuş olan 6 haneli TOTP kodunu sisteme girmesi istenir. Sistem, blokzincirinde kayıtlı olan kullanıcının TOTP gizli anahtarını kullanarak aynı kodu hesaplar. Hesaplanan TOTP kodu ile kullanıcının girdiği kod eşleşirse, kimlik doğrulama başarılı olur. Eşleşme durumunda, kullanıcı sisteme giriş yapabilir. Eğer kodlar eşleşmezse, giriş işlemi reddedilir.

Blokzincir destekli kimlik doğrulama süreci Şekil 2'de gösterilmiştir.

*Sorumlu Yazar/Corresponding Author: yangecdidem@gmail.com

ISSN: 2618-6055 / 9, (1), 14 – 24, 2025
DOI:10.62301/usmtd.1691033



Şekil 2. Blokzincir destekli kimlik doğrulama süreci (Blockchain-based authentication process)

Bu süreç, blokzinciri teknolojisinin sağladığı dağıtık yapı sayesinde merkezi bir otoriteye ihtiyaç duymadan güvenli ve bağımsız bir kimlik doğrulama mekanizması sunar.

3. Araştırma Bulguları (Research Findings)

Geleneksel kimlik doğrulama sistemi ile blokzincir destekli kimlik doğrulama sisteminin performansları, farklı kullanıcı yükleri altında karşılaştırmalı olarak değerlendirilmiştir. Karşılaştırma, farklı kullanıcı yükleri altında sistemlerin yanıt süresi, CPU ve bellek (RAM) kullanımı gibi metrikler üzerinden gerçekleştirilmiştir. Performans testleri, 1, 10 ve 100 kullanıcı senaryoları için uygulanmıştır. Geliştirilen test uygulamaları, Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz, 16 GB RAM, 64-bit işletim sistemi ve x64 tabanlı 4 çekirdekli bir donanım üzerinde çalıştırılmıştır. Geleneksel kimlik doğrulama sistemi, Duende IdentityServer altyapısı kullanılarak test edilmiştir. Testlerde performans ölçümleri için Apache JMeter kullanılmıştır. Geleneksel kimlik doğrulama sistemi ile blokzincir destekli doğrulama sistemine ait test senaryoları üç aşamada yapılandırılmıştır. Senaryolarda kullanılan temel parametreler şu şekildedir:

- **Kullanıcı sayısı (Threads)**: Aynı anda sisteme erişim sağlayacak kullanıcıların sayısını (clients) ifade etmektedir. Bu çalışma kapsamında sırasıyla 1, 10 ve 100 kullanıcı senaryoları uygulanmıştır.
- **Ramp-Up süresi**: Belirtilen sayıdaki kullanıcının sisteme ne kadar süre içinde dahil olacağını tanımlamaktadır. Tüm senaryolarda bu süre 10 saniye olarak belirlenmiştir. Bu sayede, kullanıcılar aynı anda değil, kısa aralıklarla sisteme giriş yaparak daha gerçekçi bir yük simülasyonu sağlanmıştır.
- **Döngü sayısı (Loop Count)**: Her bir kullanıcının aynı işlemi kaç kez tekrar edeceğini göstermektedir. Bu sayı, kullanıcı başına gönderilecek istek sayısını belirlemektedir.

*Sorumlu Yazar/Corresponding Author: yangecdidem@gmail.com

ISSN: 2618-6055 / 9, (1), 14 – 24, 2025
DOI:10.62301/usmtd.1691033

Uygulanan senaryolar şu şekilde özetlenebilir:

- İlk senaryoda, 1 kullanıcı 10 saniyelik ramp-up süresiyle teste başlamakta ve 100 kez işlem tekrarlayarak toplam 100 istek üretilmiştir.
- İkinci senaryoda, 10 kullanıcı aynı ramp-up süresi içinde sisteme dahil olmakta ve her biri 100 kez işlem yaparak toplamda 1000 istek gerçekleştirmiştir.
- Üçüncü ve en yoğun senaryoda ise 100 kullanıcı, yine 10 saniyelik ramp-up süresiyle sisteme giriş yapmakta ve her biri 50 kez işlem yaparak toplam 5000 istek üretmiştir.

Bu yapılandırma sayesinde, sistemin farklı seviyelerdeki eşzamanlı kullanıcı yüklerine verdiği yanıt süreleri ölçülmüş ve performans analizleri yapılmıştır.

Her test senaryosu yanıt süreleri milisaniye (ms) cinsinden kaydedilmiştir. Elde edilen sonuçlar kullanıcı sayısı, kullanıcı başına istek sayısı, toplam istek sayısı, ortalama yanıt süresi ve standart sapmalar ile birlikte değerlendirilmiştir. Tablo 1 ve Tablo 2'de yer alan performans ölçüm sonuçları, geleneksel kimlik doğrulama sistemi ile blokzincir destekli kimlik doğrulama sisteminin farklı kullanıcı yükleri altındaki tepkilerini ortaya koymaktadır. Her iki sistem için 1, 10 ve 100 kullanıcı senaryolarında ölçülen yanıt süreleri, sistemlerin ölçeklenebilirlik düzeylerini ve kaynak kullanımına verdikleri tepkileri değerlendirmek açısından önemli veriler sunmaktadır.

Duende IdentityServer altyapısı kullanılarak gerçekleştirilen geleneksel kimlik doğrulama testlerinde, tek kullanıcı ve 100 istek senaryosu altında ortalama yanıt süresi 7 ms olarak ölçülmüştür. 10 kullanıcı ve her biri için 100 istek olmak üzere toplam 1000 istek içeren senaryoda ortalama yanıt süresi hafif artış göstererek 9 ms'ye ulaşmıştır. 100 kullanıcı ve kullanıcı başına 50 istek olmak üzere toplam 5000 isteğin gerçekleştirildiği en yoğun senaryoda ise ortalama yanıt süresi 139 ms'ye yükselmiştir. Sistemin yanıt süresinde görülen bu artış, eşzamanlı kullanıcı sayısı ve toplam istek sayısının artışına bağlı olarak beklenen bir performans yavaşlamasıdır. Ancak, bu artışa rağmen 100 kullanıcı ve 5000 toplam istek altında dahi sistemin performansının hala kabul edilebilir seviyelerde olduğu söylenebilir. Standart sapma değerlerinin düşük ve nispeten sabit kalması (1.76 ms'den 134.39 ms'ye) ise, sistem yanıt sürelerinin tutarlı ve öngörülebilir olduğunu göstermektedir.

Hyperledger Fabric tabanlı blokzincir destekli kimlik doğrulama sisteminde ölçülen yanıt süreleri geleneksel sisteme kıyasla daha yüksektir. Tek kullanıcı ve kullanıcı başına 100 istek olmak üzere toplam 100 istek yapılan senaryoda ortalama yanıt süresi 8 ms ile başlamıştır. 10 kullanıcı ve kullanıcı başına 100 istek ile toplam 1000 isteğin gerçekleştirildiği senaryoda ortalama yanıt süresi 11 ms'ye yükselmiştir. En yoğun senaryo olan 100 kullanıcı ve kullanıcı başına 50 istek olmak üzere toplam 5000 istekte ise ortalama yanıt süresi 334 ms'ye çıkmıştır. Standart sapma değerlerinin geleneksel sisteme göre oldukça yüksek olması (7.02 ms'den 267.38 ms'ye) blokzincir sisteminde yanıt sürelerinde daha fazla dalgalanma yaşandığını göstermektedir. Bu durum, blokzincir mimarisinde bulunan işlem doğrulama, konsensüs mekanizmaları ve blok yazma süreçlerinin doğal bir sonucu olarak değerlendirilebilir. Blokzincir sisteminin yüksek eşzamanlılık altında yanıt sürelerinde daha fazla değişkenlik göstermesi, ölçeklenebilirlik ve performans açısından önemli bir sınırlama oluşturmaktadır. Geleneksel kimlik doğrulama sistemi, merkezi mimarisi sayesinde hem düşük gecikme süreleri hem de tutarlı performans göstermektedir. Kullanıcı sayısı ve istek yükü arttıkça yanıt süresi artsa da sistem 100 kullanıcı ve 5000 toplam istek altında ortalama 139 ms yanıt süresi ile kabul edilebilir bir performans sergilemektedir. Standart sapmanın nispeten düşük olması, sistem yanıt sürelerinin öngörülebilir ve stabil olduğunu göstermektedir. Buna karşın, blokzincir destekli kimlik doğrulama sistemi, güvenlik ve veri bütünlüğü avantajları sunmasına rağmen, işlem doğrulama ve konsensüs süreçlerinden dolayı daha yüksek ve dalgalı yanıt sürelerine sahiptir. 100 kullanıcı ve 5000 toplam istek senaryosunda ortalama yanıt süresi 334 ms'ye yükselirken, standart sapma değeri 267 ms gibi yüksek bir seviyede seyretmektedir. Bu yüksek standart sapma ve yanıt süresi dalgalanmaları, blokzincir altyapısının yoğun kullanıcı yüklerinde performans açısından daha değişken ve öngörülemez olduğuna işaret etmektedir. Özetle, geleneksel kimlik doğrulama sistemi, performans ve kararlılık açısından yüksek kullanıcı yüklerinde daha uygun bir çözüm sunarken, blokzincir destekli sistem daha güçlü güvenlik özellikleri sağlamasına rağmen performans açısından belirgin sınırlamalara sahiptir.

*Sorumlu Yazar/Corresponding Author: yangecdidem@gmail.com

ISSN: 2618-6055 / 9, (1), 14 – 24, 2025
DOI:10.62301/usmtd.1691033

Tablo 1. Geleneksel kimlik doğrulama performans ölçüm sonuçları (Traditional authentication performance measurement results)

Kullanıcı Sayısı	Kullanıcı Başına İstek Sayısı	Toplam İstek Sayısı	Ortalama Yanıt Süresi (ms)	Standart Sapma
1	100	100	7	1.76
10	100	1000	9	3.23
100	50	5000	139	134.39

Tablo 2. Blokzincir destekli kimlik doğrulama performans ölçüm sonuçları (Blockchain-based authentication performance measurement results)

Kullanıcı Sayısı	Kullanıcı Başına İstek Sayısı	Toplam İstek Sayısı	Ortalama Yanıt Süresi (ms)	Standart Sapma
1	100	100	8	7.02
10	100	1000	11	9.28
100	50	5000	334	267.38

Tablo 3. Geleneksel kimlik doğrulama ile blokzincir tabanlı kimlik doğrulaması karşılaştırılma kriterleri (Comparison criteria between traditional authentication and blockchain-based authentication)

Metrik	Geleneksel Kimlik Doğrulama (Duende IdentityServer)	Blokzincir Destekli Kimlik Doğrulama (Hyperledger Fabric)
Merkezileşme	Tek bir otorite yönetir.	Dağıtık yapı, merkezi otorite yok
Güvenlik	Orta	Yüksek
Erişim Kontrolü	Yetkilendirme merkezi sunucuya bağlı	Kullanıcılar kendi verilerini yönetebilir
Gizlilik	Merkezi otorite tüm verileri görebilir.	Kullanıcılar verileri üzerinde tam kontrole sahiptir.
Ölçeklenebilirlik	Yüksek	Orta
Erişilebilirlik	Sunucu çökmesi durumunda kesinti olur	Tüm düğümler çalıştığı sürece kesintisiz

Tablo 3'te sunulan karşılaştırma, geleneksel kimlik doğrulama sistemi ile blokzincir tabanlı kimlik doğrulama sisteminin yapısal ve işlevsel farklılıklarını ortaya koymaktadır. Geleneksel kimlik doğrulama sistemleri, merkezi bir otorite tarafından yönetilir ve tüm kimlik doğrulama süreçleri bu otorite üzerinden yürütülür. Bu yapı, hızlı yanıt süreleri ve yüksek ölçeklenebilirlik gibi avantajlar sunsa da güvenlik ve gizlilik açısından bazı sınırlamalar barındırmaktadır. Özellikle merkezi sunucunun çökmesi durumunda sistemin tamamen devre dışı kalması erişilebilirlik açısından zafiyet oluşturabilir. Ayrıca, kullanıcı verilerinin merkezi bir noktada toplanması, gizlilik ve veri ihlali risklerini artırmaktadır.

Öte yandan, blokzincir destekli kimlik doğrulama, verilerin merkezi bir otoriteye bağlı olmadan, dağıtık bir yapı üzerinde saklanması sayesinde yüksek güvenlik ve gizlilik sunmaktadır [20]. Bu sistemlerde güvenlik, temel olarak blokzincirin değiştirilemezlik (immutability), kriptografik imzalar ve işlem geçmişinin şeffaflığına dayanmaktadır. Örneğin, her kimlik doğrulama işlemi kriptografik olarak imzalanır ve blokzincire kaydedildiğinde sonradan değiştirilmesi mümkün değildir. Bu sayede kimlik sahteciliği, veri manipülasyonu ve yetkisiz erişim gibi tehditlere karşı direnç sağlamaktadır. Ayrıca, her kullanıcı verisinin yalnızca gerekli olduğunda ve kullanıcı izniyle paylaşılması, veri gizliliğini arttırmaktadır. Sistem, Sybil saldırılarına karşı düğüm doğrulama mekanizmaları (örneğin Proof-of-Authority veya Proof-of-Stake) ile korunabilir. Buna ek olarak, veri bütünlüğü ve erişim kontrolü gibi güvenlik kriterleri, merkezi sistemlere göre daha güçlü şekilde uygulanabilmektedir. Örneğin, blokzincire entegre edilen akıllı sözleşmeler aracılığıyla sadece yetkili tarafların belirli verilere erişmesine izin verilebilir. Bu tür güvenlik özelliklerinin değerlendirilmesi, sistemin dışarıdan saldırılara karşı direnci, veri sızıntısı ihtimali ve işlem geçmişinin şeffaflığı gibi kriterler göz önünde bulundurularak yapılmıştır. Bu yönleriyle, blokzincir destekli kimlik doğrulama sistemleri, geleneksel sistemlere kıyasla daha yüksek düzeyde güvenlik sağlamaktadır. Ancak, bu yüksek güvenlik düzeyinin

*Sorumlu Yazar/Corresponding Author: yangecdidem@gmail.com

ISSN: 2618-6055 / 9, (1), 14 – 24, 2025
DOI:10.62301/usmtd.1691033

bir maliyeti vardır. Dağıtık yapının doğası gereği, her işlem ağda çok sayıda düğüm tarafından doğrulanmak zorunda olduğu için, işlem yükü artmakta ve yanıt süreleri uzamaktadır. Gerçekleştirilen testlerde, blokzincir destekli sistemlerin geleneksel sistemlere kıyasla daha fazla CPU ve RAM kaynağı tükettiği, dolayısıyla daha yüksek donanımsal gereksinimlere ihtiyaç duyduğu gözlemlenmiştir. Bu nedenle, blokzincir tabanlı kimlik doğrulama sistemleri güvenlik açısından avantajlı olmakla birlikte, performans ve kaynak kullanımı açısından bazı sınırlamalar barındırmaktadır.

4. Tartışma ve Sonuç (Results and Discussion)

Bu çalışmada, geleneksel kimlik doğrulama ile blokzincir destekli kimlik doğrulamanın performans ve güvenlik açısından karşılaştırılması amaçlanmıştır. Yapılan performans testleri, her iki yöntem arasındaki farkları net bir şekilde ortaya koymuştur. Geleneksel kimlik doğrulama, merkezi sunucu yapısı sayesinde daha hızlı yanıt süreleri ve yüksek ölçeklenebilirlik sunmaktadır. Bu, verilerin merkezi bir noktada saklanması ve işlemlerin daha verimli bir şekilde gerçekleştirilmesinden kaynaklanmaktadır. Ancak, merkezi yapının getirdiği güvenlik riskleri, kullanıcı verilerinin gizliliğini tehdit edebilir ve merkezi otoritenin güvenilirliğine bağımlılığı artırabilir. Özellikle sunucu çökmesi veya saldırılar durumunda, sistemin tamamının erişilemez hale gelmesi ciddi bir sorun teşkil etmektedir

Diğer taraftan, blokzincir destekli kimlik doğrulama, dağıtık yapısı sayesinde daha yüksek güvenlik ve gizlilik sağlar. Kullanıcılar, verileri üzerinde tam kontrol sahibidir ve veriler yalnızca ihtiyaç duyulduğunda paylaşılmaktadır. Bu yapı, merkezi otoriteye dayalı sistemlerden bağımsızlık sunar. Ancak, bu avantajların maliyeti, daha uzun yanıt süreleri ve yüksek işlem yükü olarak karşımıza çıkmaktadır. Blokzincir destekli sistemler, ağda her kullanıcı işlemi için doğrulama gerçekleştirdiğinden, ölçeklenebilirlik açısından geleneksel yöntemlere göre sınırlamalar göstermektedir. Ayrıca, daha fazla CPU ve RAM kaynağı gerektiren bu sistemler, performans açısından daha fazla işlem gücü ve zaman tüketmektedir. Sonuç olarak, her iki kimlik doğrulama yönteminin kendine özgü güçlü ve zayıf yönleri vardır. Geleneksel kimlik doğrulama, hızlı ve ölçeklenebilir yapısıyla yüksek performans sunarken, güvenlik ve gizlilik açısından zayıf kalmaktadır. Blokzincir destekli kimlik doğrulama ise daha güvenli ve gizlilik odaklı bir çözüm sunmakta, ancak yüksek işlem gücü ve performans gereksinimleri nedeniyle daha fazla kaynak kullanmaktadır. Bu çalışmanın bulguları, geleneksel kimlik doğrulamanın hız ve ölçeklenebilirlik gerektiren senaryolarda, blokzincir destekli kimlik doğrulamanın ise güvenlik ve gizlilik öncelikli uygulamalarda daha uygun olduğunu göstermektedir.

Gelecekte, blokzincir destekli sistemlerin performansını artırmak ve ölçeklenebilirlik sorunlarını çözmek adına çeşitli iyileştirme çalışmaları yapılabilir. Örneğin, işlem yükünü azaltan ve doğrulama süresini kısaltan Layer-2 çözümleri kimlik doğrulama süreçlerine entegre edilebilir. Ayrıca, akıllı sözleşmelerin daha verimli ve güvenli çalışabilmesi için, statik analiz araçları kullanılarak potansiyel güvenlik açıklarının erken tespiti sağlanabilir. Bunun yanında, hibrit kimlik doğrulama modelleri geliştirerek, kullanıcıların ihtiyaçlarına göre geleneksel ve blokzincir tabanlı sistemler arasında dinamik geçiş yapılmasına olanak tanıyan adaptif mimariler araştırılabilir. Bu tür hibrit sistemlerde, örneğin kritik olmayan işlemlerde geleneksel doğrulama tercih edilirken, hassas veri erişimlerinde blokzincir teknolojisi devreye alınabilir. Son olarak, kullanıcı deneyimini iyileştirmek amacıyla, mobil cihazlara özel optimize edilmiş blokzincir çözümleri geliştirilebilir. Bu doğrultuda, blokzincir destekli kimlik doğrulamanın geleceği yalnızca güvenlik değil, aynı zamanda erişilebilirlik ve kullanıcı dostu çözümlerle de şekillenebilir.

5. Kaynaklar (References)

[1] L. Shinder, M. Cross, Chapter 11. Passwords, vulnerabilities, and exploits, In book: Scene of the Cybercrime (Second Edition) (2008) 467-503 doi.org/10.1016/B978-1-59749-276-8.00011-X.

[2] P. P. Piyush, A. S. Rajawat, S.B. Goyal, P. Bedi, C. Verma, M. S. Raboaca, F. M. Enescu, Authentication and authorization in modern web apps for data security using nodejs and role of dark web, Procedia Computer Science. (2022) 781-790 doi.org/10.1016/j.procs.2022.12.080.

[3] A. Henricks, H. Kettani, On data protection using multi-factor authentication, The International Conference on Information System and System Management, (2019) 1-4. doi.org/10.1145/3394788.339478

*Sorumlu Yazar/Corresponding Author: yangecdidem@gmail.com

ISSN: 2618-6055 / 9, (1), 14 – 24, 2025
DOI:10.62301/usmtd.1691033

[4] A. Ezugwu, E. Ukwandu, M. Ezema, C. Olebara, J. Ndunagu, L. Ofusori, U. Ome, Password-based authentication and the experiences of end users, Scientific Africa, (2023) e01743. doi.org/10.1016/j.sciaf.2023.e01743.

[5] C. Mole, E. Chalstrey, P. Foster, T. Hobson, Digital identity architectures: comparing goals and vulnerabilities, (2023). doi.org/10.48550/arXiv.2302.09988.

[6] N. A. Lal, S. Prasad, M. Farik, A Review of authentication methods, International Journal of Scientific & Technology Research, (2016) 246-249.

[7] A. K. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition, IEEE Transactions on Circuits and Systems for Video Technology, 14(1) (2004) 4-20. doi.org/10.1109/TCSVT.2003.818349.

[8] R. Amin, T. Gaber, G. Eltaweel, A. E. Hassanien, Biometric and traditional mobile authentication techniques: Overviews and open issues, Chapter in Intelligent Systems Reference Library, (2014) 423-446. doi.org/10.1007/978-3-662-43616-5_16.

[9] X. Wang, Z. Yan, R. Zhang, P. Zhang, Attacks and defenses in user authentication systems: A survey, Journal of Network and Computer Applications, (2021).

[10] U. Khalid, M. Asim, T. Baker, P.C. Hung, M.A. Tariq, L. Rafferty, A decentralized lightweight blockchain-based authentication mechanism for IoT systems, Cluster Comput (2020) 2067-2087. doi.org/10.1007/s10586-020-03058-6.

[11] U. Narayanan, V. Paul, S. Joseph, Decentralized blockchain based authentication for secure data sharing in cloud-IoT, J. Ambient Intell. Humaniz. Comput, (2022) 769-787. doi.org/10.1007/s12652-021-02929-z.

[12] G. Zhao, B. Di, H. He, Design and implementation of the digital education transaction subject two-factor identity authentication system based on blockchain, 22nd International Conference on Advanced Communication Technology, ICACT, IEEE (2020). doi.org/10.23919/ICACT48636.2020.9061393.

[13] S. Mercan, M. Cebe, K. Akkaya, J. Zuluaga, Blockchain-based two-factor authentication for credit card validation, Data Privacy Management, Cryptocurrencies and Blockchain Technology, Springer International Publishing (2021). doi.org/10.1007/978-3-030-93944-1_22.

[14] T.P. Abayomi-Zannu, I.A. Odun-Ayo, T. Barka, A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication, Journal of Physics: Conference Series, IOP Publishing (2019). doi.org/10.1088/1742-6596/1378/3/032104.

[15] I. Wanisha, J. B. James, J. S. Witeno, L. H. M. Bakery, Multi-Factor authentication using blockchain: Enhancing privacy, security and usability (2024). doi.org/10.62951/ijcts.v1i3.24.

[16] Duende Software. https://duendesoftware.com/docs/ (erişim tarihi: 10.02.2025).

[17] S. Saranya, K. Monika, Manikandan, J. Nagaraju, S. Nagendiran, Geetha B. T., Blockchain-based identity management: Enhancing privacy and security in digital identity system, International Conference on Contemporary Computing and Informatics (IC3I) (2024). doi.org/10.1109/IC3I61595.2024.10829044.

[18] G. Zyskind, O. Nathan, A. S. Pentland, Decentralizing privacy: Using blockchain to protect personal data, IEEE Security and Privacy Workshops (2015). doi.org/10.1109/SPW.2015.27.

[19] A Blockchain Platform for the Enterprise (BPE). https://hyperledger-fabric.readthedocs.io/en/release-2.5/index.html (erişim tarihi: 20.02.2025).

[20] A. Torongo, M. Toorani, Blockchain-based decentralized identity management for healthcare systems. Cryptography and Security, (2023) 20s. doi.org/10.48550/arXiv.2307.16239.

*Sorumlu Yazar/Corresponding Author: yangecdidem@gmail.com