Blokzincir Tabanlı Kullanıcı Yönetim Sistemi
Blockchain Based User Management System

Mustafa TEMİZ
Yönetim Bilişim Sistemleri
İktisadi ve İdari Bilimler Fakültesi
Sivas Cumhuriyet Üniversitesi
Sivas, Türkiye
temizmustafa@cumhuriyet.edu.tr

Ahmet SORAN
Elektrik ve Bilgisayar Mühendisliği
Mühendislik Fakültesi
Abdullah Gül Üniversitesi
Kayseri, Türkiye
ahmet.soran@agu.edu.tr

Halil ARSLAN
Bilgisayar Mühendisliği
Mühendislik Fakültesi
Sivas Cumhuriyet Üniversitesi
Sivas, Türkiye
harslan@cumhuriyet.edu.tr

Hilal EREL
Detay Danışmanlık
İstanbul, Türkiye
hilal.aslan@detaysoft.com

***Özetçe*—Blokzinciri, çeşitli kriptografi teknikleri kullanılarak birbirine bağlanmış bloklar içerisinde bulunan verilerin, ağ üzerinde diğer noktalara dağıtılmasıyla oluşturulan güvenilir ve şeffaf bir yapıdır. Mevcut veri tabanı işlemlerinden farkı, yetki ve sorumlukların tek bir merkezi otoritede bulunmaması, bu yetki ve sorumlulukların ağda bulunan diğer düğümlere dağıtılarak görev paylaşımı sağlanmasıdır. Bunu sağlayabilmek için eşler arası ağ altyapısı kullanılmaktadır. Fakat bu aşamada güvenlik anlamında kimlik doğrulama işlemi temel güvenlik mekanizmalarından birini oluşturmaktadır. Bu çalışmada, blokzincirdeki hız sorunlarına çözüm olabileceği düşünülen, daha güvenilir ve güncel teknolojilerle entegre olacak şekilde çalışabilen bir kullanıcı yönetim sistemi önerilmektedir.**

Anahtar Kelimeler — Blokzincir; Keycloak; Kubernetes; Elasticsearch.

***Abstract*— Blockchain is a reliable and transparent structure formed by distributing the data in blocks connected to each other using various cryptography techniques to other points on the network. The difference from the existing database operations is that the authorities and responsibilities do not exist in a single central authority, and that these powers and responsibilities are distributed to the other nodes in the network and the assignment is shared. To provide this, peer to peer network infrastructure is used. However, at this stage, authentication in terms of security is one of the basic security mechanisms. In this study, a user management system which can be integrated with more reliable and current technologies, which is thought to be the solution to speed problems in blockchain, is proposed.**

Keywords — Blokchain; Keycloak; Kubernetes; Elasticsearch.

I. GİRİŞ

Bilgi çağı olarak adlandırılan içerisinde bulunduğumuz çağda en büyük etkiyi teknolojik gelişmeler oluşturmaktadır. Yazılım ve donanım ürünlerindeki gelişmeler teknolojik çağın gelişimine büyük oranda katkı sağlamaktadır. Gelişen teknolojiden payını alan ekonomi çalışma alanı yeni bir sistemin ortaya çıkmasını tetiklemiştir. Bu kapsamda kripto para ve yapay zeka kavramlarının birleşimi ile daha güvenilir bir teknoloji olan blokzincir kavramı ortaya atılmıştır [1]. Teknolojik gelişmeler pek çok güvenlik tehditlerini de beraberinde getirmektedir. Eş tabanlı blokzincir mimarisi kriptografik algoritmalar ve özet fonksiyonlar gibi güvenlik yöntemleri ile bu tehditlere çözümler sunmaktadır. Güvenlik ve mahremiyet konularında blokzincir teknolojisiyle gerçekleştirilen çalışmalar gelecek adına önem arz etmektedir [2].

Veri tabanları karmaşık verilerden oluşan kayıtlar içeren ve bu kayıtlara ait görevleri yerine getirmek için tasarlanmış veri depolama teknolojisidir. Bu depolama teknolojisi verilerin gereksiz tekrarlanmasını, doğruluğunu, güvenliği ve gizliliğini sağlayan, ayrıca özel sorgu dilleri yardımıyla verilere erişilmesine ve güncellenmesine olanak sağlayan bir sistem olarak tanımlanmaktadır. Veri tabanlarının çok sayıda kullanıcı kontrol ve erişimine imkân vermesi ayrıca veri güvenliğini esas alması en önemli özelliklerindendir [3].

Son yıllarda gelişen blokzincir teknolojisinin nesnelerin interneti, eğitim, güvenli depolama, sağlık ve devlet işlerinde kullanımına dair çalışmalar mevcuttur. Kişilere ait sağlık verilerinin tutulduğu veri tabanları, bilgi güvenliğinin önem arz ettiği çalışma alanlarından biridir. Azaria vd., blokzincir teknolojisini kullanarak hasta kayıt sistemi önermişlerdir. MedRec ismini verdikleri bu sistem ile hastalara ait tıbbi bilgilere farklı sağlık kuruluşlarından rahat bir şekilde erişilebilmesi amaçlanmıştır. Bu erişim işleminde kimlik doğrulama, güvenlik, gizlilik ve veri paylaşımı konuları ön planda tutulmaktadır. Ethereum blokzinciri üzerinde akıllı sözleşmeler ile hasta kayıt işlemlerini gerçekleştirmişlerdir. Elektronik tıbbi kayıt sisteminde blokzincir yönteminin kullanılmasıyla büyük ölçekli verilerin kontrol ve yönetiminin başarılı bir şekilde yapılabileceğini göstermişlerdir [4].

Huh vd., blokzincir teknolojisini IoT cihaz kontrol ve yönetiminde kullanarak bir çalışma gerçekleştirmişlerdir. IoT cihazların yönetiminde blokzincir teknolojisi olan Ethereum

978-1-7281-7206-4/20/$31.00 ©2020 IEEE

platformunu kullanmışlardır. Kimlik doğrulama işlemleri için kullanılan ve Etherum platformu üzerinde bulunan açık alt yapı sistemiyle korunmakta olan veri tabanı sistemlerine karşı oluşacak saldırıların engellenmesi amaçlanmıştır. Anahtarların yönetim ve kontrolü için RSA kripto altyapısı kullanılmaktadır [5].

Blokzincir teknolojisinin kamu hizmetleri alanında da kullanımına rastlanılmaktadır. 2018 yılında yayınlanan OECD raporunda 2017 yılında 26 farklı ülkede 117 blokzincir uygulaması hayata geçirilmiş, 2018 yılında ise 45 ülkede 202 farklı uygulama gerçekleştirilmiştir. Bu uygulamaların çözmek istediği temel problemin güvenlik problemi olduğu fark edilmiştir. Estonyada dijital kimlik ve dijital vergilendirme işlemleri gerekli yasal düzenlemelerin ardından blokzincir teknolojisiyle buluşturulmuş ve bu hizmetleri kullanacak farklı kurumların da erişimine olanak sağlayan sistem tasarlanmıştır [6].

Karataş, blokzincir teknolojisi ile öğrenme yönetim sistemi geliştirmiştir. 2018 yılında hazırladığı çalışmasında Uluslararası Enformatik ve Bilgi İşlemsel Düşünme Etkinliği tarafından hazırlanan ve katılımcılara sunulan dijital sertifikalarda Ethereum blokzincir temelli akıllı sözleşmeler kullanarak doğrulama işleminin yapılmasını amaçlamıştır. İlk olarak dijital sertifikalar ile akıllı sözleşme tasarlanmış ardından Ethereum blokzincir teknolojisi ile Moodle öğrenme yönetim sistemindeki sertifikalar güncellenerek blok zincir teknolojisi ile yönetim ve kontrolü sağlanmıştır [7].

Blok zincir teknolojisi kullanıcı yönetimi için her ne kadar güvenli olsa da, veri sayındaki artışa bağlı olarak yavaş çalışması pratikteki kullanımı neredeyse imkansız hale getirmektedir. Bu soruna çözüm olarak bu çalışmada elastic search ve kubbernetes ile entegre, Keycloak kullanıcı doğrulama sitemini kullanan blok zinciri tabanlı bir kullanıcı yönetim sistemi önerilmiştir.

Çalışmanın kalan kısmı şu şekilde özetlenebilir: Bölüm 2'de blokzincir, kubbernetes ve elasticsearch kavramları ele alınmış, Bölüm 3' te uygulamaya yer verilmiş, çalışmadan elde edilen çıkarımlar ise Bölüm 4'te tartışılarak ileride yapılacak çalışmalar için önerilerde bulunulmuştur.

II. KULLANIM

A. Blokzincir

Son yıllarda adını sıkça duyduğumuz blokzincir kavramı, merkezi olmayan, güvenilir, değiştirilemez ve şeffaf işlem yönetim sistemine sahip veri yapısı olarak karşımıza çıkmaktadır [8]. İlk olarak 2008 yılında Nakamoto tarafından tanıtılan bu teknoloji, gerçekleştirilen her işlem bilgisi ve kaydının ilgili ağda bulunan diğer katılımcılar ile paylaşıldığı dağıtılmış bir veri yapısı olarak tanımlanmaktadır [9].

Blokzincir, temelinde bir kayıt defteri gibi veriler üzerinde gerçekleştirilen işlemlerin kayıtlarını bulundurmaktadır. Belirli bir kullanıcı tarafından değiştirilen veriler aynı zamanda diğer kullanıcılar tarafından fark edilmektedir. Blokzincir teknolojisi, verilerin tek bir merkezi sistemde tutulmasından ziyade farklı veri depolama sistemlerinde de bulundurulmasını sağlamaktadır. Veriler ağ üzerinde çok fazla noktaya dağıtılmakta ve kriptolojik bir sıra ile birbirine bağlanarak veri güvenliği sağlanmaktadır [10].

Zhao vd., blokzincirin önemli özellikleri arasında insanlar tarafından manuel olarak yapılan takip ve kontrol sistemlerinin yerini ağa dayalı daha şeffaf ve güvenilir sistemlerin alması olarak ifade etmişlerdir [11].

Blokzincir teknolojisinin sunmuş olduğu avantajların yanı sıra çeşitli dezavantajları da bulunmaktadır [6].

Tablo I. Blokzincir Avantajları ve Dezavantajları

Avantaj	Dezavantaj
• Verilerde meydana gelen değişiklikler tüm kullanıcılar tarafından takip edilebildiği için veri tahribatı önlenmektedir. • Akıllı sözleşmeler yardımı ile bazı işlemler otomatikleştirilerek kullanımı kolaylaştırılmaktadır. • Blokzincirde olan tüm kullanıcılar kendi işlemlerinin durumunu görebildiği gibi diğer katılımcıların işlemlerini de takip edebilmektedir.	• Blokzincir yöntemi çeşitli uzlaşma protokollerinden oluşmaktadır ve bu protokoller içerisinden Proof of Work protokolü çok fazla enerji harcamakta ve maliyeti yüksek bilgisayar sistemleri tarafından desteklenmektedir. • Kullanıcılara ait işlem bilgileri herkes tarafından izlenmesinden dolayı kişisel mahremiyet konusunda sorunlarla karşılaşılmaktadır. • Akıllı sözleşmeler oluşturulduktan sonra tüm katılımcıların erişimine açık halde saklanmaktadır. Kötü amaçlı kişi ve kişiler tarafından saldırılara maruz kalmaktadır.

Blokzincir yapısı içerisinde bulunan verilerin bir yedeği ağda bulunan diğer düğümlerde de saklanmaktadır. Blokzincir üzerindeki veriler güncelleştirildiğinde güvenlik ihlalleri ve uyuşmazlıklardan dolayı tüm düğümler ortak bir uzlaşma protokolü üzerinden haberleşmeli ve tüm düğümlerde ilgili veri güncelleştirme işlemi gerçekleştirilmelidir. İlk olarak Nakamoto tarafından ortaya atılan uzlaşma protokolü İşin İspatı (Proof of Work) protokolüdür. Araştırmacılar tarafından bu protokolün eksikleri fark edilmiş ve zamanla Proof of Stake, Proof of Capacity ve Proof of Elapsed-time protokolleri geliştirilmiştir [6].

B. Keycloak

Keycloak, ilk olarak 2014 yılında JAVA ile yazılmış ayrıca modern uygulama ve servislere yönelik geliştirilen açık kaynak kodlu kimlik doğrulama sunucusudur. Uygulamaları ve servisleri daha güvenilir hale getirmek için kullanılmaktadır. Keycloak, standart protokollere dayanmakta ve SAML, OAuth

2.0 ve OpenID Connect gibi tekli oturum açma protokollerine destek sağlamaktadır [12].

Kullanıcılar bireysel uygulamalardan ziyade kimlik doğrulama işlemlerini Keycloak ile yapmaktadır. Keycloak uygulamaların giriş formları doldurmadan, sürekli olarak kullanıcı kimlik doğrulama ve kaydedilmesi gibi işlemlere ihtiyaç duymadan giriş yapabilme avantajı sunmaktadır. Keycloak girişi yapıldıktan sonra kullanıcıların farklı bir uygulamaya kimlik bilgileri ile erişmesi için her seferinde kimlik bilgilerini girmesi gerekmemektedir. Kullanıcı çıkışı için de aynı durumlar geçerli olmakla birlikte farklı her bir uygulamadan çıkış yapmasına ihtiyaç yoktur [13].

Bu tanımlamalar ile Keycloak, veri tabanı sistemleri yardımıyla gerçekleştirilen kullanıcı doğrulama işlemlerinde blokzincir teknolojisi ile birlikte kullanımında, her ne kadar dağıtık mimariyi bozsa da, güvenlik ve hız açısından özellikle izne tabi blokzincirler (permissioned blockchain) için önemli katkılar sunma potansiyeline sahiptir.

C. *Elasticsearch*

Elasticsearch, Java programlama dilinde yazılmış açık kaynak kodlu, dağıtık bir mimari ve gerçek zamanlıya yakın olacak şekilde tasarlanmış metin arama motorudur. Metin arama alt yapısı Apache Lucene projesine dayanmaktadır. Her bir elasticsearch indisi shard ismi verilen bir veya daha fazla Lucene indisinden oluşmaktadır. Her bir indisin sahip olduğu şart sayısı sabit bir değerdir ve bu değer indis oluşturmadan önce tanımlanmaktadır. Bir indese belge eklendiğinde, elasticsearch sunucusu bu belgenin depolanmasından ve indislenmesinden sorumlu olan shardı tanımlamaktadır. Bu şekilde elasticsearch, mevcut shardlar arasında yükleri dengelemekte ve tüm shardlar eş zamanlı şekilde kullanıldığından genel performansı artırmaktadır [14].

D. *Kubernetes*

Kubernetes, Google tarafından 2014 yılında GO dilinde geliştirilen açık kaynaklı bir yönetim sistemidir [15]. Uygulamaların kullanılabilirliğini ve otomasyon sistemini kolaylaştırmak ayrıca iş yüklerini ve servislerini yönetmek için kullanılmaktadır. Son yıllarda hızlı bir gelişme kaydetmekte olan Kubernetes, destekleri, servisleri ve araçları yaygın olarak bulunmaktadır [16].

Kubernetes, konteyner içerisindeki uygulamaların daha hızlı ve verimli çalışmasını sağlayan konteyner yönetim sistemidir [17]. Konteyner, sanal makineye benzemektedir fakat işletim sistemini uygulamalar arasında paylaşmak için daha rahat izolasyon özelliklerine sahiptir. Kendi dosya sistemleri, belleği, işlemcisi, işlem alanı ve daha fazla yapı bulunmaktadır. Bulut sistemler ve işletim sistemi dağıtımları arasında taşınabilmektedirler. Konteynerlar uygulamaları bir araya getirip çalıştırmanın iyi bir yoludur.

Bir üretim ortamında uygulamaları çalıştıran konteynerlar yönetilmeli ve aksaklık olmamalıdır. Örneğin bir konteynerda problem olduğunda diğer konteynerın başlaması gerekmektedir. Kubernetes, bu işlemi gerçekleştiren sistem olarak karşımıza çıkmaktadır. Kubernetes dağıtık sistemleri daha rahat ve esnek bir biçimde çalıştırmak için çerçeve sunmaktadır. Gerekli ölçeklendirme ve iş yükü dağılım devretme işlemlerini gerçekleştirmektedir.

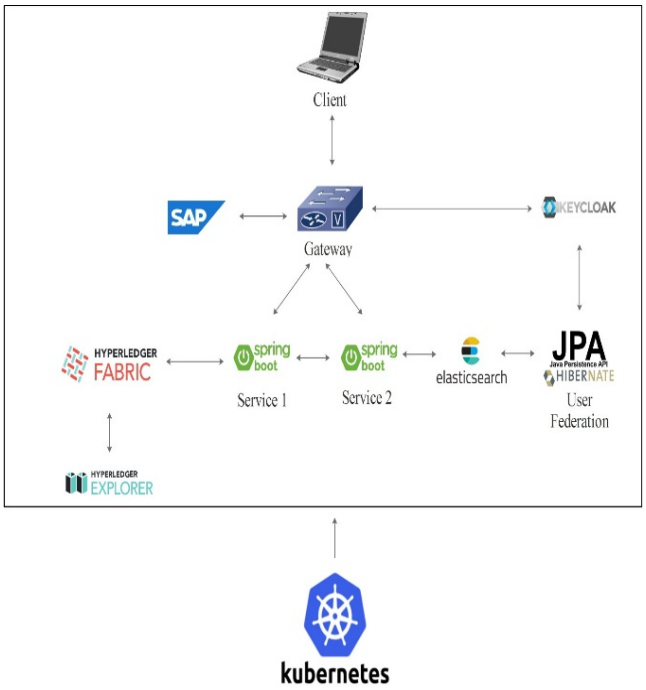
Kubernetes, servis keşfetme ve yük dengeleme, depolama yönetimi, otomatik rollout ve rollback, konteynerları hataya düştüğünde kendini onarma, gizlilik ve konfigürasyon yönetimi gibi hizmetler sağlamaktadır [16].

III. ÖNERİLEN YÖNTEM

Çoklu veri tabanlarına erişim ve yönetim noktasında tekli oturum açma protokolü ile kimlik doğrulaması yapan, veri tabanlarına erişim için merkezi olmayan dağıtık bir yapı olan blokzincir üzerinde biletler(token) kullanılarak giriş yapılan bir sistem önerilmektedir.

Bu çalışmada geliştirilen mimari Şekil 1'de gösterilmektedir. Bu mimaride ilgili adımlar aşağıda ayrıntılı şekilde ifade edilmektedir.

Şekil I. Sistem Mimarisi



1) *Kimlik doğrulama*: Veri tabanlarına erişim gerçekleşmesi için kullanıcı kimliklerinin Keycloak ile doğrulanması ve biletlerin oluşturulması.

2) *İlgili veri tabanına bağlanma*: Kimlik doğrulama için çoklu veri tabanları içerisinden etkileşime geçilecek veri tabanın belirlenmesi. Burada Java geliştiriciler için tasarlanmış nesne/ilişkisel eşleme (ORM) aracı olan Hibernate teknolojisi kullanılmaktadır.

3) *İndisleme(indexleme)*: Blokzincir teknolojisinin kısıtları arasında yavaşlık kavramından giriş kısmında bahsetmiştik. Bu adımda blokzincir üzerinde işlemlerin daha hızlı yapılması için ilgili veriler Elasticsearch teknolojisi ile indislenmektedir.

4) *Uygulama geliştirme ve blokzincir*: Spring tabanlı bir uygulama geliştirme ara yüzü olarak springboot web servisleri

kullanılmaktadır. Web servis yardımı ile bilgiler blokzincir teknolojisi olan Hyperledger ile birleştirilmektedir.

5) *İş yükü dengeleme*: Son aşama olarak kubernetes teknolojisi ile çoklu programlarda oluşan iş yükünden dolayı bu iş yükü dengelenerek sistemin daha verimli ve etkili hale getirildiği aşamadır.

IV. SONUÇ

Blokzincir teknolojisi daha güvenilir, şeffaf ve dağıtık yapısı sayesinde günümüz teknoloji çağına yeni bir bakış açısı kazandırmış ve farklı çalışma alanlarında pek çok uygulama geliştirilmiştir. Kullanıcı kimlik doğrulama ve yönetim işlemlerinde karşılaşılan önemli sorunlardan biri güvenlik problemidir. Blokzincir teknolojisinde bu güvenlik probleminin önüne geçmek için çeşitli teknik ve algoritmalar bulunmaktadır.

Bu çalışmada blokzincir tekniklerine dayalı yeni bir veri tabanı erişim ve kullanıcı kimlik doğrulama sistemi önerilmektedir. Bu sistem kimlik doğrulama işlemleri için Keycloak, kullanıcı ve veri tabanı ile etkileşim için Hibernate, indexleme işlemleri için elasticsearch, blokzincir teknolojisi olarak Hyperledger ve iş yükü dengelemek için ise kubernetes tekniklerinden faydalanılacaktır. Bu sayede önerilen yöntemin daha güvenilir ve hızlı olacağı öngörülmektedir.

Blokzincir teknolojisi ile daha güvenilir bir yapı haline gelen bu kontrol sisteminin standart veri tabanı işlemleri ile kullanıcı kimlik doğrulama işlemlerinin yerini alacağına inanıyoruz. Bu çalışmada sistem önerisi sunulmuş sonraki çalışmalarda geliştirmekte olduğumuz bu sistemin uygulaması yapılacaktır.

BİLGİLENDİRME

Bu çalışma, Detaysoft Ar-Ge Merkezi bünyesinde yürütülen çalışmaların bir sonucudur. Desteklerinden ötürü teşekkür ederiz.

KAYNAKLAR

[1] T. Murathan ve F. Murathan, "Spor Sektöründe Blok Zinciri Uygulamaları", *Gaziantep Üniversitesi Spor Bilimleri Dergisi*, ss. 64-74, Mar. 2019, doi: 10.31680/gaunjss.484614.

[2] H. Halpin ve M. Piekarska, "Introduction to Security and Privacy on the Blockchain", içinde *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Paris, 2017, ss. 1-3, doi: 10.1109/EuroSPW.2017.43.

[3] İ. R. Karaş, İ. Baz, ve A. Geymen, "Farklı Formattaki Konumsal ve Özniteliksel Verilerin Otomatik Olarak Bir Coğrafi Veri Tabanına Dönüştürülmesi, 4", *Coğrafya Bilgi Sistemleri Bilişim Günleri, Fatih Üniversitesi, İstanbul-Türkiye13-16 Eylül*, 2006.

[4] A. Azaria, A. Ekblaw, T. Vieira, ve A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management", içinde *2016 2nd International Conference on Open and Big Data (OBD)*, 2016, ss. 25-30, doi: 10.1109/OBD.2016.11.

[5] S. Huh, S. Cho, ve S. Kim, "Managing IoT devices using blockchain platform", içinde *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017, ss. 464-467, doi: 10.23919/ICACT.2017.7890132.

[6] M. Tanriverdi, M. Uysal, ve M. T. Üstündağ, "Blokzinciri Teknolojisi Nedir ? Ne Değildir ?: Alanyazın İncelemesi", *Bilişim Teknolojileri Dergisi*, ss. 203-217, Tem. 2019, doi: 10.17671/gazibtd.547122.

[7] E. Karataş, "Moodle Öğrenme Yönetim Sistemi için Ethereum Blok Zinciri Tabanlı Belge Doğrulama Akıllı Sözleşmesinin Geliştirilmesi", *Bilişim Teknolojileri Dergisi*, c. 11, sy 4, ss. 399-406, Eki. 2018, doi: 10.17671/gazibtd.452686.

[8] A. Reyna, C. Martín, J. Chen, E. Soler, ve M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities", *Future Generation Computer Systems*, c. 88, ss. 173-190, Kas. 2018, doi: 10.1016/j.future.2018.05.046.

[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", s. 9.

[10] A. Tüfekci ve Ç. Karahan, "BLOKZINCIR TEKNOLOJISI VE KAMU KURUMLARINCA VERILEN HIZMETLERDE BLOKZINCIRIN KULLANIM DURUMU", s. 37.

[11] J. L. Zhao, S. Fan, ve J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue", *Financial Innovation*, c. 2, sy 1, s. 28, Ara. 2016, doi: 10.1186/s40854-016-0049-2.

[12] D. P. D. Paiva, "Authentication modules for Keycloak authentication server", 2018.

[13] H. Short, P. Tedesco, ve M. E. H. Hussein, "Reproducible Examples for Integration with Keycloak", s. 14.

[14] O. Kononenko, O. Baysal, R. Holmes, ve M. W. Godfrey, "Mining modern repositories with elasticsearch", içinde *Proceedings of the 11th Working Conference on Mining Software Repositories - MSR 2014*, Hyderabad, India, 2014, ss. 328-331, doi: 10.1145/2597073.2597091.

[15] D. Bernstein, "Containers and Cloud: From LXC to Docker to Kubernetes", *IEEE Cloud Computing*, c. 1, sy 3, ss. 81-84, Eyl. 2014, doi: 10.1109/MCC.2014.51.

[16] "Production-Grade Container Orchestration". [Çevrimiçi]. Erişim adresi: https://kubernetes.io/. [Erişim: 17-Ara-2019].

[17] H. V. Netto, L. C. Lung, M. Correia, A. F. Luiz, ve L. M. Sá de Souza, "State machine replication in containers managed by Kubernetes", *Journal of Systems Architecture*, c. 73, ss. 53-59, Şub. 2017, doi: 10.1016/j.sysarc.2016.12.007.