Fırat Üniversitesi Müh. Bil. Dergisi
35(2), 517-526, 2023

Araştırma Makalesi
https://doi.org/10.35234/fumbd.1289650

Hastaların Elektronik Sağlık Kayıt (ESK) Sistemleri için Güvenli Blok Zincir Destekli Bulut Sistemi

Hamit MIZRAK[1], Serpil ASLAN[2*]
[1] Enformatik, Lisansüstü Eğitim Enstitüsü, Malatya Turgut Özal Üniversitesi, Malatya, Türkiye
[2] Yazılım Mühendisliği, Mühendislik ve Doğa Bilimleri Fakültesi, Malatya Turgut Özal Üniversitesi, Malatya, Türkiye
[1] hamit.mizrak@ozal.edu.tr, [*2] serpil.aslan@ozal.edu.tr

(Geliş/Received: 29/04/2023; Kabul/Accepted: 31/05/2023)

Öz: Dünyada birçok işlemler artık dijitalleştiğinden dolayı veri güvenliliği, veri paylaşımı, veriye hızlı erişim, verilerin bütünlüğünü korunmak önemli görülmüştür. Her geçen gün, günlük yaşantımızda bilgisayara bağımlılığımız ve bu bağlılığa paralel olarak verilerin oluşması tamamen doğal bütünün bir parçasıdır. Oluşan bu büyük veri topluluğu beraberinde veri güvenliğinin önemini de arttırmıştır. Veri güvenli konusunda son zamanlarda en çok duyulan kelime blok zinciri kelimesidir. Blok zincir, güvenli veri paylaşımını sağlamak ve merkezi olmayan veri işlem bütünlüğünü korumak amacıyla tasarlanmış birçok bilgisayardaki işlemleri kaydeden ve daha sonra hiçbir şekilde geriye dönük olarak değiştirilemeyen halka açık dijital defterlerdir. Son yıllarda bulut tabanlı Elektronik Sağlık Kayıtları (ESK), hasta verilerine uzaktan erişim için birçok araştırmacının ilgi odağı haline gelmiştir. Hasta verilerinin doğruluğu ve gizliliği, sağlık sektöründe önemli bir endişe kaynağıdır. Bu çalışmada, ESK kayıtları için veri erişim kontrolü ve denetimi sağlarken bulut servis sağlayıcıları arasında sağlık verilerinin paylaşılması için blok zincir destekli yeni bir çözüm önerilmiştir. Önerilen yöntemle, hastanın elektronik sağlık kayıtlarının sağlık sektörü tarafından yönetilmesinden ve kontrol edilmesinden, hastaların verilerinin kontrolünde olduğu hasta merkezli bir uygulamaya geçiş hedeflenmektedir.

Anahtar kelimeler: Blok zincir, elektronik sağlık kayıtları, bulut hizmeti sağlayıcısı.

Secure Blockchain-Supported Cloud System for Patients' Electronic Health Record (EHR) Systems

Abstract: Since many transactions worldwide are now digitalized, data security, data sharing, fast access to data, and protecting data integrity have been considered necessary. With each passing day, our dependence on computers in our daily lives and data formation in parallel with this dependence is a part of the natural whole. This large data community has also increased the importance of data security. The word that has been heard most recently about data security is blockchain. Blockchain is a public digital ledger that records transactions across multiple computers, designed to ensure secure data sharing and maintain decentralized data transaction integrity, and cannot be changed retrospectively afterward. In recent years, cloud-based Electronic Health Records (ESK) have become the focus of attention of many researchers for remote access to patient data. The accuracy and confidentiality of patient data is a significant concern in the healthcare industry. This study proposes a new blockchain-supported solution for sharing health data between cloud service providers while providing access control and control for IHC records. The proposed method aims to transition from the management and control of the patient's electronic health records by the health sector to a patient-centered application where the patients' data are in control.

Key words: Blockchain, electronic health record (EHR), cloud service provider.

1. Giriş

Dünyada birçok işlemler artık dijitalleştiğinden veri güvenliliği, veri paylaşımı, veriye hızlı erişim, veri bütünlüğünü korumak son derece önemli görülmüştür. Her geçen gün, günlük yaşantımızda bilgisayara olan bağımlılığımız ve bu bağlılığa paralel olarak yeni verilerin oluşması kaçınılmazdır. Oluşan bu verilerin güvenli bir şekilde paylaşımı her geçen gün önemi artmaktadır. Bu verilerin güvenliliğini korumak, muhafaza etmek son derece değerlidir. Veri güvenliliği konusunda son zamanlarda en çok duyduğumuz kelime olan blok zinciri kelimesidir. Blok zinciri, güvenli veri paylaşımını, veri bütünlüğünü korumakla görevli, merkezi olmayan dijital kayıt defteri olarak tanımlanır. Blok zinciri verileri tek yönlü olarak kaydeden, tersine mühendisliğin imkânsız olan ve paylaşımlarını şeffaflık ilkesine göre veri tabanına verileri gönderir. Blok zincirinde kaydedilen bu verilerin ortak veri paylaşmasına olanak sağlayan teknolojiler toplamıdır.

Elektronik Sağlık Kayıtları (ESK), hastaların geleneksel kâğıt üzerindeki tıbbi kayıtlarına elektronik erişim imkânı sağlayan sağlık kaydı depolama sistemidir [1]. Verilerin kâğıt formda kaydedilmesi ve arşivlenmesi ekstra

[*] Sorumlu yazar: serpil.aslan@ozal.edu.tr. Yazarların ORCID Numarası: [1] 0009-0009-7394-7469, [2] 0000-0001-8009-063X

insan gücüne ihtiyaç duyulmasına sebep olduğu gibi veri giriş hatalarına da sebep olabilir. Bu gibi hatalar tıbbi kararlarda hatalara yol açıp hastaların testlerinin tekrarlanmasına da sebep olacağı için maliyetli olabilir [2,3]. Hastalar tedavi süreçlerinde farklı hastaneleri ziyaret etmek zorunda kalabilirler. Hastalar sağlık kayıtlarını yaşam süreleri boyunca farklı hastanelere dağıtırken önceki sağlık kayıtlarına erişmekte zorlanırlar. Aynı zamanda parçalanmış sağlık veri kayıtlarının kötü yönetilmesine de sebep olabilir. Tüm bu nedenlerden dolayı tıbbi verilerin dijitalleştirilmesi, elektronik olarak depolanması ve profesyoneller tarafından uzaktan erişilebilir olması kaçınılmazdır [4]. Elektronik kayıtlar, hasta ziyaretlerinden sonra hastaneler tarafından oluşturulur ve böylece hastalar elektronik tıbbi kayıtların tek sahibi olur. Hastaların tıbbı bilgilerinin saklanması ve izinsiz kişilerce ele geçmesi hastaya veya hastaneye ciddi zararlar verebilmektedir. ESK hastayla ilgili olarak bütün bilgilerinin tutulduğu ortam olmasından dolayı güvenli bir şekilde saklanması son derece önemlidir. Hasta bilgilerinin doktorlara doğru zamanda ulaşması son derece önemlidir. Günümüzde, sağlık alanı önceki zamanlara göre daha dijitaldir; Örneğin, manyetik rezonans görüntüleme (MRG) ve X-ışınlarından bilgisayarlı tomografiye (BT) ve ultrason taramalarından elektronik tıbbi belgelere kadar büyümektedir.

Bulut hizmetlerinin artan popülaritesi ile sağlık kayıtlarının bulut tabanlı platformlara taşınması sağlık ve araştırma kurumları arasında paylaşılmasını daha önce hiç olmadığı kadar kolaylaştırarak daha hızlı ve verimli bir şekilde bilgi alışverişine olanak sağlamıştır [5]. Bulut hizmeti sağlayıcıları, depolarındaki sağlık kayıtlarının kontrolü ve esnek paylaşımı ile yükümlüdür. Etkileşimli işbirliğini kolaylaştıran bulut tabanlı sistemlerin, tedaviler hakkında yeni bilgilerin araştırılması, analiz edilmesi ve nüfus sağlığının daha iyi yönetilmesi gibi avantajları olduğu gibi çeşitli zorlukları da beraberinde getireceği göz ardı edilmemelidir. Örneğin, yüksek boyutlu verilerin depolanması sağlık sektöründe veri yönetimi için büyük bir zorluktur. Sağlık kayıtlarının güvence altına alınması, uzaktan erişim ve doğrulanması sağlık sektöründe ki bir diğer büyük zorluktur [6]. Bu zorlukların üstesinden gelirken sağlık kayıtlarının bütünlüğünü, güvenilirliğini ve gizliliğini sağlamak esastır. Bu nedenle güvenli ve verimli veri yönetimi en önemli gerekliliktir [7] .Veri sahipleri ve emanetçileri için toplanan verilerin kötü amaçlı kullanıcıların elinde savunmasız olma riski vardır. Bu tür risklerden dolayı hizmet sağlayıcılara karşı güvensizlik atmosferi ortaya çıkmaktadır. Tüm engellerin üstesinden gelmek için verimli depolama ve hızlı geri alma, güvenli veri paylaşımı ve ESK kayıtlarının güvenliğini hedef alan yeni kayıt sistemleri oluşturulmuştur [8,9].

Sağlık verilerinin paylaşılması durumunda ortaya çıkacak riskleri ele almak amacıyla çeşitli kriptografik yöntemler önerilmiştir [10,11]. Önerilen yöntemler her ne kadar tüm riskleri ele almaya çalışsa da yetersiz kalmıştır [12]. Tam olarak bu noktada Blok zincir teknolojisi ihtiyaç duyulan tüm hizmetleri sunabilme potansiyeliyle ortaya çıkmıştır. Blok zincir, güvenli veri paylaşımını sağlamak ve merkezi olmayan veri işlem bütünlüğünü korumak amacıyla tasarlanmış birçok bilgisayardaki işlemleri kaydeden ve daha sonra hiçbir şekilde geriye dönük olarak değiştirilemeyen halka açık dijital defterlerdir. Blok zincirler birbirine bağlı zincirlerden oluşur, yeni eklenen zincir bir önceki bloğa bağlanır ve bu şekilde uzun bir zincir meydana gelir. Sonuç olarak, Blok zincir artık kaydın adıdır. Blok zinciri kelimesi bir ağda yapılan işlemlerin blok ve blokların ardı ardına zincirlenmesi ifadesinden dolayı blok zinciri adını almıştır. Blok zincirde veriler üzerinde işlem yapılırken her bir işlem halka açık olarak kaydedilip kontrol edildiğinden dolayı diğer yöntemlere kıyasla yüksek bir hesap verilebilirlik sağlar. Blok zincire girildiğinde hiç kimse önceden eklenen tüm bilgileri değiştiremez. Diğer bir deyişle verilerin gerçek ve değişmemiş olduğunu gösteren yeni bir teknolojidir [13]. Blok zincirde veriler, merkezi bir veri tabanı yerine ağlarda depolanır. Bu sayede, sistemin kararlılığı artar ve saldırıya uğradığı anda göreceği zarar minimize edilir.

Kripto para birimlerinde başarısını kanıtlamış blok zincir teknolojisi bu risklerin üstesinden gelmek amacıyla kullanılabilecek en güçlü teknolojidir. Blok zincirler sağlık hizmetlerinde ciddi veri gizliliği, güvenlik ve bütünlük sorunlarını çözebilecek stratejilere sahiptir. Örneğin, sağlık sektöründe, blok zincir teknolojileri sayesinde hasta kayıtlarının gizliliği kaydedilebilir, aynı zamanda hastaların tıbbı geçmişleri blok zincir teknolojisi kullanılarak saklandığında değiştirilemez. Bu teknoloji sağlık sektörü için büyük bir temel sağlar ve âdemi merkeziyetçilik, değişmezlik yeteneği ve birlikte çalışabilirlik sunar [14]. Bu çalışmada, ESK kayıtları için veri erişim kontrolü ve denetimi sağlarken bulut servis sağlayıcıları arasında sağlık verilerinin paylaşılması için blok zincir destekli yeni bir çözüm önerilmiştir. Önerilen yöntemle, hastanın elektronik sağlık kayıtlarının sağlık sektörü tarafından yönetilmesinden ve kontrol edilmesinden, hastaların verilerinin kontrolünde olduğu hasta merkezli bir uygulamaya geçiş hedeflenmektedir.

2. İlgili Çalışmalar

Ying ve ark. [15] çalışmalarında, ESK için kriptografik teknikleri kullanan şifreli metin politikası özniteliğine dayalı şifreleme CP-ABE şifreleme tekniği önerdiler. Yazarlar önerilen yöntemin gelir gider maliyetine karşı büyük oranda ESK kayıtlarını koruduğunu iddia etmektedir. Azarm ve ark. [16] çalışmalarında işbirliğini arttırmak

amacıyla ESK sistemlerinde paylaşılan verileri denetlemek için bulut tabanlı bir uygulama ve web hizmeti API önerdiler. Önerilen çerçeve, topluluk bakımından alınan karşılaştırmalı bir kullanım senaryosu kullanılarak test edilmiştir. Sistem, hastaneyi veya sağlık merkezlerini ESK sistemi ile yönetmek için Sağlık Bakanlığı tarafından kontrol edilmektedir. Yue ve ark. [17] çalışmalarında, sağlık veri paylaşım sistemleri için erişim kontrolü yönetimi için tek merkezli erişim kontrol modeli önerdiler. Çalışmada veri kullanıcıları, (1) ham verileri okumaya çalışan kullanıcılar ve (2) verileri okumaya ve sonuçlarını almaya çalışan kullanıcılar olmak üzere iki türe ayrıştırılmıştır. Önerilen modelde her bir veri talebi için, bir işlem amaçlarına bağlı olarak belirli bir kategorideki verilere sınırlı bir süre tanımlanır. Samarin ve ark. [18] çalışmalarında bulutta özel olarak depolanan ve yalnızca hasta tarafından erişime açık olan sağlık kayıtlarını ele almıştır. Çalışma, sağlık verilerinin sağlık hizmeti sağlayıcıları gibi birden fazla kuruluşla paylaşma ihtiyacını göz artı etmektedir.

Xia ve ark. [19] çalışmalarında blok zincirin değişmezliği özelliğini kullanarak bulutta depolanan ESK verilerinin erişim kontrolü zorluklarını ele alan blok zincir tabanlı bir veri paylaşım modeli önerdiler. Önerilen modelde güvenli şifreleme teknikleri kullanılarak izin verilen bir blok zincir ile veri havuzlarına verimli erişim kontrolü sağlanması ve paylaşılması hedeflenmiştir. Wang ve ark. [20] çalışmalarında, ESK sistemleri için öznitelik tabanlı kriptografi ve blok zincir teknolojisini birlikte kullanarak güvenli bir BBDS ismini verdikleri yeni bir şema önerdiler. Önerilen model hibrit bir modeldir. Önerilen modelde, tıbbi verileri şifrelemek amacıyla nitelik tabanlı şifreleme kullanılırken dijital imzaları uygulamak içinde birleşik öznitelik tabanlı/kimlik tabanlı şifreleme ve imza (C-AB/IB-ES) adı verilen yeni bir kriptografik yöntem sunulmuştur. Ayrıca çalışmada tıbbi verilerin bütünlüğünü ve erişilebilirliğini sağlamak amacıyla da blok zincir teknikleri kullanılmıştır. Ferdous ve ark. [21] çalışmalarında, tıbbi verilerin bütünlüğünü, güvenilirliğini ve paylaşımını sağlamak için DRAMs olarak adlandırdıkları blok zincir tabanlı yeni bir sistem önerdiler. Önerilen yöntem temelinde iyi tanımlanmış bir tehdit modeli varsayımına dayandırılarak dağıtık erişim kontrolüne olanak sağlayan merkezi olmayan bir mimaridir. Ramani ve ark. [22] çalışmalarında, ESK sistemleri için blok zincir tabanlı işbirliği şaması önerdiler. Önerilen model, bir sağlık hizmeti ortamında doktor-hasta blok zincirine dayanan güvenli ve etkili bilgi erişim modelidir. Yazarlar önerilen modeli deneysel sonuçlarla desteklemişlerdir. Deneysel sonuçlar önerilen modelin bütünlüğü koruduğunu ve literatürde bilinen saldırılara karşı direnebildiğini kanıtlamaktadır. Azaria ve ark. [23], büyük ölçekli ESK sistemleri için yeni bir merkezi olmayan MedRec modeli önerdiler. Çalışmada, tıbbi verilerin gizliliği, kimlik doğrulaması ve denetimler blok zincir tekniği kullanan MedRec modeli kullanılarak kapsamlı bir günlük aracılığıyla tutulmuştur.

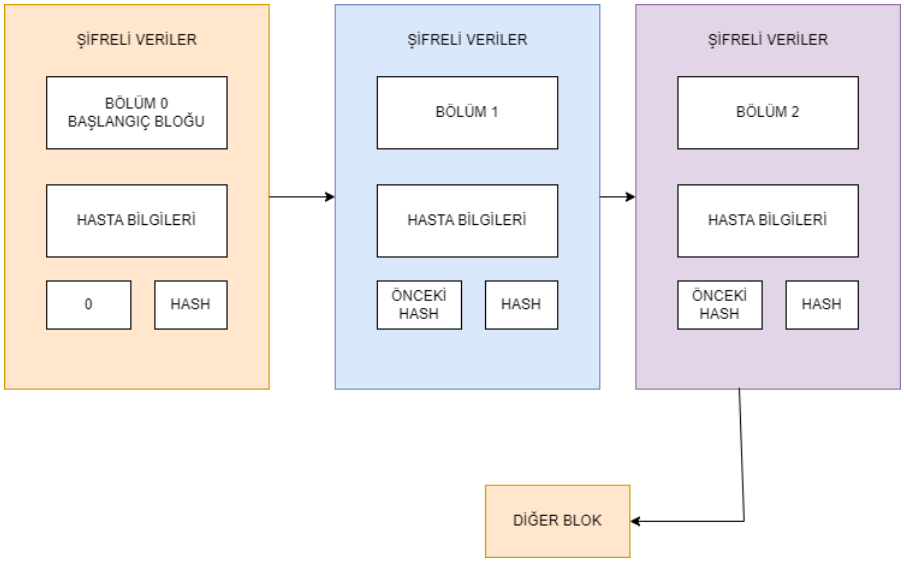
3. Materyal ve Yöntem

3.1. Blok zincir

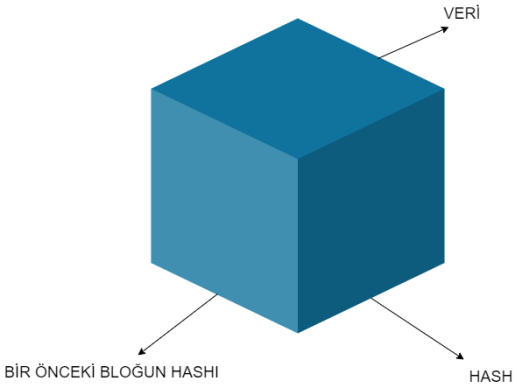
Blok zinciri merkezi sistemi olmayan uçtan uca bağımlı kullanıcılar arasında dinamikleşerek veri paylaşımını sağlayan dağıtık mimari teknolojisidir [13]. Blok zinciri kelimesi, bir ağda yapılan işlemlerin blok ve blokların arka arkaya zincirlenerek bağlanması olayına dayanmaktadır. Blok zinciri için veri güvenliği birinci önceliktir. Ağda doğrulanmış yöntemlerin listesi bir zincirin sonuna yeni bir veri bloğu eklenmesiyle devam ederek blok zincirini oluşturur. Şekil 1, hasta verilerinin bloklar halinde zincirlenerek ve şifrelenerek art arta bloklar halinde sıralanmasını temsil etmektedir.

Blok zincir yöntemlerinde bilinmesi gereken önemli kavramlar bulunmaktadır:

- Veri (Data): İşlenmemiş, ham bilgilere denir.
- Jeton (Token): Jeton bir platformun tüm yetkilerinden faydalanılmasına olanak sağlayan yapıdır.
- Doğrulama (Hash): Her bir blok ve bütün bloklar kendi içinde benzersizdir. Bu bloklar parmak izi gibi eşsiz ve benzersizdir. Herhangi bir blokta en küçük bir değişiklik meydana gelirse tekrardan hesaplanır ve sistemin çalışmamasını sağlar. “Hash Of Previous” anlamı önceki bloğun karması anlamına gelmektedir: Her blok önceki bloğun karmasını içerir ve her bloğun bir önceki bloğa işaret etmesine yardımcı olması için bir blok zinciri oluşturulur. İlk blok, blok zincirindeki ilk blok olduğu için bir önceki bloğa işaret edemez ve ilk bloğa "Genesis Block" adı verilir. Buradaki blokta herhangi bir değişiklik meydana geldiğinde bütün karma da değişmektedir. Bir sonraki blok değişmesi zincirleme olarak diğer bütün blokları etkiler ve artık eşleşmeyen bloklara dönüşür ve tüm blokların hash kodu değişmiş olur. Şekil 2, bir blok zincirinin öz niteliklerini temsil etmektedir.



Şekil 1. Blok zincir ile şifrelenmiş hasta verileri.

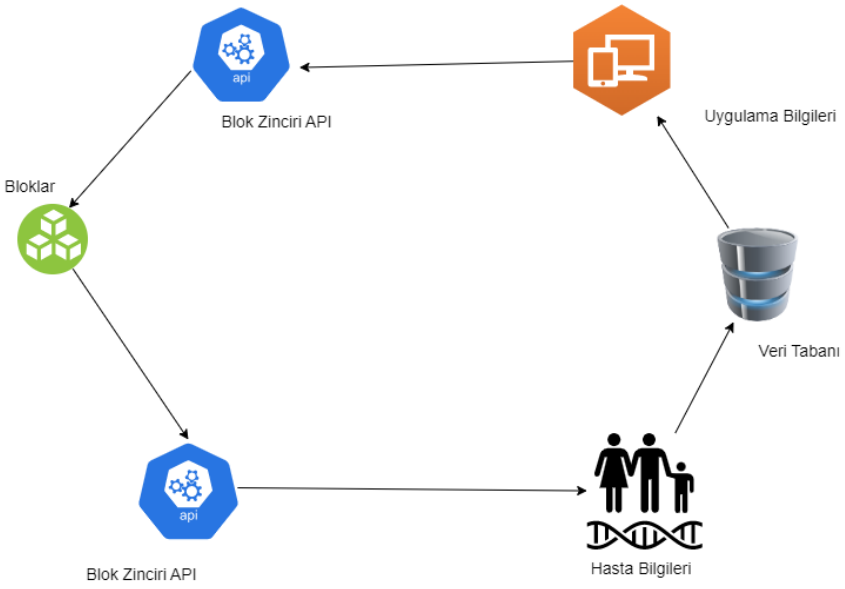


Şekil 2. Blok zincirindeki her bir blok.

3.2. Blok zincir türleri

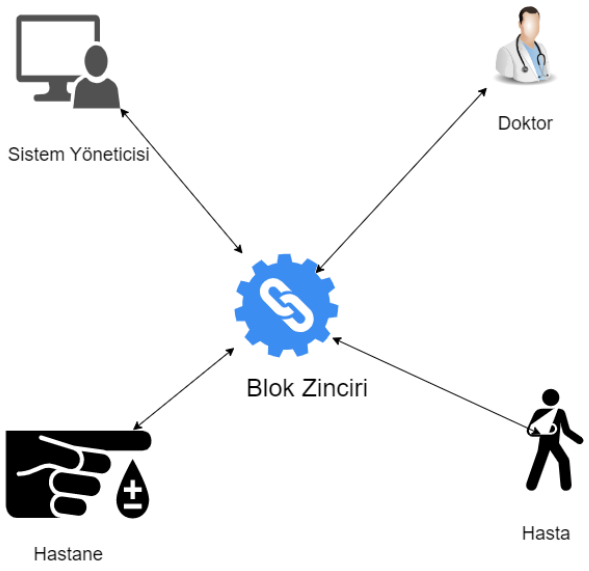
Blok zinciri mimarisi izinli blok zinciri ve izinsiz blok zinciri olmak üzere ikiye ayrılır. İzinsiz blok zinciri mimarisinde; kullanıcının kimliği kontrol edilmeden yani gerçek kişinin kimliği olup olmamasına bakılmadan alınmasına denir. İzinli blok zinciri kullanıcının kimlik kontrolü incelenerek gerçek kişi olmasına dikkat edilerek işleme alınmasına denir.

İzinsiz blok zinciri mimarisi Şekil 3'te gösterildiği gibidir. Mimaride, blok zincir uygulama sağlayıcı hizmeti ile hasta kullanıcı veri tabanı hizmeti birbirine bağlıdır. Üretilen her bir veri, sağlayıcı uygulaması üzerinden bir API aracılığıyla blok zincire eklenmektedir. Eklenen bu blok yine API üzerinden hasta kullanıcı uygulamasına veri sağlayarak döngüyü oluşturmaktadır.



Şekil 3. İzinsiz blok zinciri mimarisi.

İzinli blok zinciri mimarisi Şekil 4'te gösterildiği gibidir. İzinli blok zinciri mimarisinde tüm blok yapısı merkezi bir noktada dağıtık olarak tutulmaktadır.



Şekil 4. İzinli blok zinciri mimarisi.

3.3. Genel anahtar ve özel anahtar

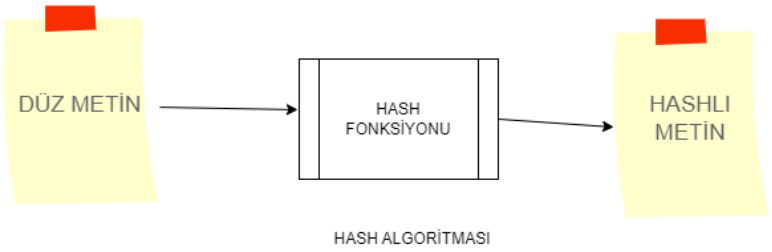
Genel ve özel olmak üzere iki anahtar türü vardır. Genel anahtar türü herkes tarafından bilinmektedir ancak özel anahtar türü sadece belirli kişide bulunur. Genel anahtar posta adresi olarak düşünülebilir. Herkes onu arayabilir ve bu adrese herhangi bir şey gönderebilir. Özel anahtar ise işlemleri doğrulamak ve bir blok zincir adresinin sahipliğini kanıtlamak için kullanılır. Özel anahtar iyi saklanmalıdır.

Dijital imza, blok zinciri üzerinde tutulan verilerin güvenliğini ve bütünlüğünü sağlamanın temel yöntemlerinden biridir. Dijital imzalar asimetrik kriptografiyi kullanır ve şifrelenen bilgi herkese açık bir anahtar kullanılarak paylaşılabilir. Blok zincirinde her kullanıcının bir genel bir de özel anahtarı bulunmaktadır. Gizli tutulan özel anahtar işlemleri imzalamak için kullanılmaktadır. Dijital olarak imzalanan işlemler tüm blok zinciri ağında yayınlanır. Bir dijital imza, imzalama ve doğrulama olmak üzere iki aşamadan oluşmaktadır. Örneğin A

kullanıcısı B kullanıcısına dijital imzalı bir mesaj göndermek istemektedir. İmzalama aşamasında, A kullanıcısı verilerini özel anahtarı ile şifreler ve B kullanıcısına şifrelenmiş mesajı ve orijinal verileri gönderir. Doğrulama aşamasında B kullanıcısı, eline geçen mesajı A kullanıcısının genel anahtarı ile doğrular. Böylelikle, B kullanıcısı verilerin tahrif edilip edilmediğini kolayca kontrol edebilir.

3.4. Hash fonksiyonları

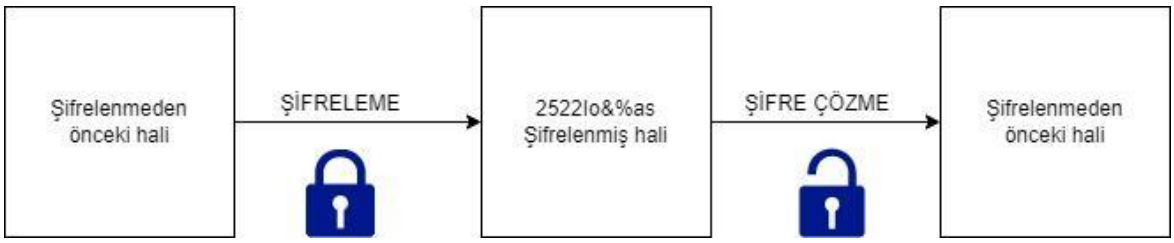
Farklı boyuttaki verilerden sabit boyutta çıktı oluşturan matematiksel süreçlere denir. Hash fonksiyonları kriptografi kullanımında önemli bir yere sahiptir. Hash fonksiyonları sayesinde blok zinciri, dağıtık sistemlerde veri bütünlüğü ve güvenliği elde etmiştir. Hash fonksiyonları deterministik fonksiyonlardır. Diğer bir deyişle hash fonksiyonları farklı büyüklükte bitlere sahiptir ve her bir algoritmada her zaman aynı girdi için aynı çıktı alınmaktadır. Veri güvenliğini sağlamak adına hashing fonksiyonları özellikle kripto paralarda tek yönlü fonksiyonlar olarak kullanılır ki tersine çalışma olmasın ve güvenlik sağlanmış olsun. Hashing kaba kuvvet saldırılarına karşı dayanıklıdır. Şekil 5'te, hash algoritmalarının çalışma şemasını temsil eder. Şifreleme algoritmaları çift yönlü olarak kullanılmaktadır.



Şekil 5. Hash algoritmalarının şeması.

Hash algoritmalarına örnek olarak MD5, SHA, RIPED-D algoritmaları verilebilir. MD5 algoritmasının güvensizlik problemi nedeniyle SHA çok daha kullanılışlıdır. MD5 128 bit uzunluğunda çıktı oluşturmaktadır. MD6 256 bit uzunluğundadır. SHA(Secure Hash Algoritm) Türkçesi "güvenli hash algoritması anlamına" gelir. NSA(National Security Agency) tarafından geliştirilmiştir. Örneğin: SHA-1 her zaman 160 bit özet oluştururken, SHA-256 algoritması 256 bit özet meydana getirir. SHA-2 ve SHA-3 daha güvenlidir. SHA-0 ve SHA-1 farklı girdiler ile aynı hash'in üretilmesi durumunda çakışma meydana gelir. SHA-0 ve SHA-1 çakışmalar meydana geldiğinde güvenli değildir.

Hash fonksiyonları kriptografik hash fonksiyonlarında dijital parmak izi, bilgi güvenliği, mesaj doğrulama, DNA dizilerinde benzer dizilimleri bulmak, veri güvenliği uygulamalarında, veri tabanlarında veri aramayı hızlandırmak, e-ticaret uygulamalarında, güvenli giriş uygulamalarında kullanılır. Şekil 6'da Hash algoritma şeması görülmektedir.



Şekil 6. Hash algoritmalarının şeması.

3.5. Blok zincir uzlaşma (konsensüs) algoritmaları

Uzlaşma algoritmaları, var olan grup içindeki bireylerin geri kalanlar arasında en iyisi olduğuna karar veren fikir birliği algoritmalarıdır. Dağıtık sistemlerde güvenliği sağlayan yapıdır. Ağ güvenliğini sağlar ve etkili iletişim için gerekli alt yapıyı sunar. Merkezi bir sistem özelliğine sahiptir. Ağ üzerinde bütün veriye erişim yetkisi vardır. Böylelikle bütün verilere erişim vardır. Blok zincirinde eşitlik ve başarıyı sağlamak için kullanılır. Uzlaşma

algoritmalarında herhangi bir en küçük hata toleransında düğümler anlaşmazlığa gider. Ağ içindeki düğümlerin birbirine olan güveni söz konusu değildir önemli olan toplu bir karar vermektir. Merkezi yapıyla ilgili problemler olduğu durumlarda kolaylıkla bilgi sahibi olunabilir. Merkezi olmayan teknolojilerde art arda birbirine bağlanarak blok zincirini meydana getirmektedir ve merkezi olmayan veya dağıtık defter yapı sistemlerinde uzlaşma algoritmasına ihtiyaç duyulmaktadır. Uzlaşma algoritmalarının birden fazla çeşidi bulunmaktadır. En önemli iki algoritma:

- İş Kanıtı (Proof of Work (PoW)): Bitcoin kurucusu Satoshi Nakamoto [24] tarafından blok zincir ağında işlemleri onaylamak ve zincirde yeni bloklar oluşturmak için önerilmiş uzlaşma algoritmasıdır. PoW, bir kripto para biriminin blok zincirine yeni işlem blokları eklemenin bir şeklidir. Bu durumda iş, mevcut blok için hedef karma ile eşleşen bir karma (uzun bir karakter dizisi) üretir. Bunu yapan kripto madencisi, o bloğu blok zincirine ekleyerek ödül alma hakkını kazanır. PoW, Bitcoin için SHA-256, Litecoin Scrypt, Ethereum ise Equihash kullanmaktadır.
- Hisse Kanıtı (Proof of Stake (PoS)): Bir blok zincirin güvenliğini ve sürdürülebilirliğini sağlamak amacıyla oluşturulmuş bir uzlaşma mekanizmasıdır. Karmaşık çözümler yerine var olanla yetinmeye çalışır. PoS algoritmasında her bir bloğun doğrulu doğrulayıcılar tarafından yapılmaktadır. PoW mekanizmasına alternatif olarak geliştirilen PoS, hesaplama gücünü değil sermaye gücünü ön plana çıkarmaktadır.

Bu algoritma türleri dışında Proof of Burn, Proof-of-Activity, Proof-of-Capacity, Proof of Elapsed Time, Delegated, Proof of Stake, Proof of Authority, Hibrit Pow/PoS türleri de mevcuttur.

3.6. JavaEE ve spring boot teknolojileri

Java yüksek seviyeli bir programlama dilidir. Java üç kısımdan oluşmaktadır. Birinci kısım JavaSE (Java Standart Edition) JAVA'nın temel bileşenlerini oluşturmaktadır. İkinci kısım JavaME (Java Micro Edition) JAVA'nın gömülü sistem kodlamaları için kullanılır. Üçüncü kısım ise JavaEE (Java Enterprise Editon) kurumsal projelerde kullanılan teknolojinin adıdır. Bu makalede JavaEE kullanımında son teknoloji olan Spring Boot teknolojisi kullanılmıştır. Spring Boot teknolojisi, Spring Framework üzerine kurulmuş konfigürasyon teknolojisi olup, Spring Framework'un aksine kodlama kolaylıkları sağlamaktadır. Makalede önerilen yöntemde, veri yapıları sistemleri için JavaSE kullanılmıştır. Farklı cihazlarda veri paylaşımı için Spring Boot API (Application Programming Interface) sisteminden yararlanılmıştır. API kısa uygulama ara yüzüdür. Farklı cihazlarda veri alış verişini sağlayan teknolojinin genel adıdır. Hasta bilgilerinin kaydedilmesinde veri tabanı olarak gömülü veri tabanı olan H2DB kullanılmıştır. H2DB sistem üzerinde çalışabilen gömülü bir veri tabanı sistemidir. Java'da veri güvenliği içinde Spring Security kullanılmıştır. Sisteme kötü niyetli istekler geldiğinde filtreden geçiren ve sistem içinde olmayan kullanıcıları engellemek için kullanılır.

3.7. Önerilen yöntem

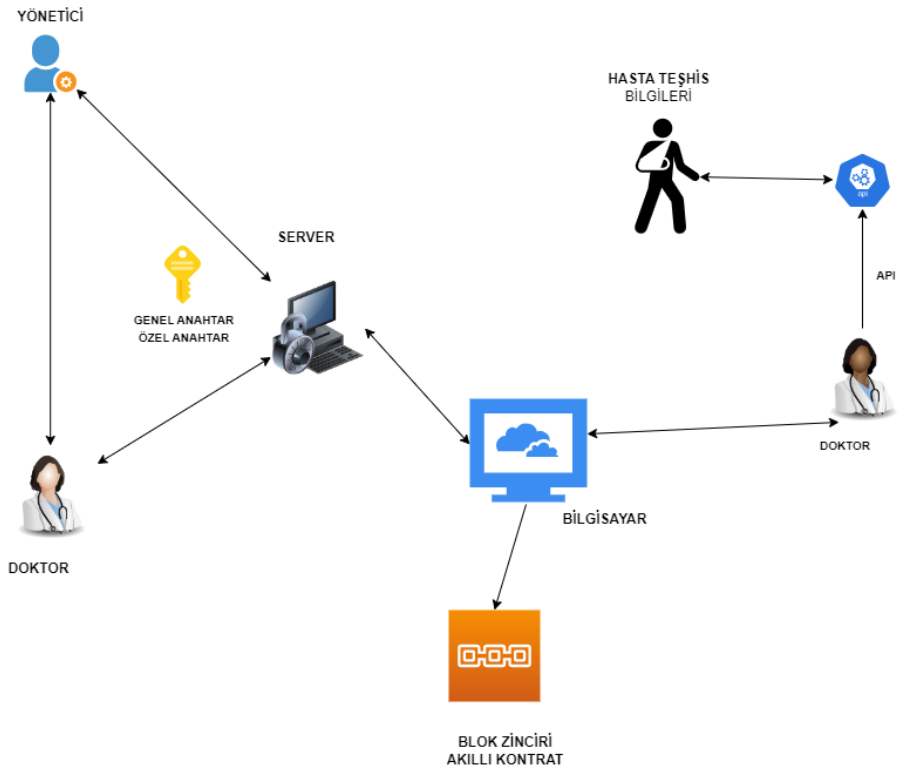
Önerilen yöntemle sağlık alanında veri taşınma hızı, veri güvenliği, veri şeffaflığı ve klasik veri tabanı saklama, sistem kullanıcı girişinin veri tabanı, oturum (session) yöntemi yerine dağıtık veri tabanı olan blok zincir teknolojisi kullanılmıştır. Blok zincirini kullanarak bulut servis sağlayıcıları arasında bir veri paylaşım modeline ek olarak sisteme güvenli giriş sağlamak ve akıllı sözleşmelerin erişim kontrol mekanizmalarının kullanılması daha yüksek düzeyde veri denetimi sağlayacaktır. Katmanlı mimari yapısıyla tasarlanan sistemde bulut hizmeti sağlayıcıları arasında veri paylaşımına yönelik mevcut son teknolojiler kullanılmıştır. Bulut hizmet sağlayıcılarının daha hızlı bilgi alış verişi sağlayabilecek bir model oluşturduk. Veri gizliliği konusunda bilinen klasik yöntemlere kıyasla daha risksizdir. Ayrıca, sistemde ki yetkilendirme ile hasta bilgi mahremiyetine önem verilmiştir.

Bu çalışmada ESK için blok zincir ve bulut bilişim kullanılarak önerilen sistemin genel çerçevesi Şekil 7'de gösterildiği gibidir. Önerilen yöntem ile sistem merkezsizleştirilerek tek bir başarısızlık noktası önlenir ve hastalara kendi verilerine sahip olma ve bunlara erişim hakkı verilir. Önerilen sistem ile tüm sağlık hizmeti verilerine erişmek her zamankinden daha kolay olacaktır. Ayrıca veriler güvence altına alınır ve dağıtılır. Blok zincir verilerinde yapılan herhangi bir yasadışı değişiklik kolayca tespit edilebilir ve tanımlanabilir. Önerilen sistemde, hangi blok zincir madencilerine ne tür bilgilerin görüneceğine dikkat eden onay gerçekleştirilir.

Önerilen sistemde, blok zinciri otomasyon sistemine giriş yapılmadan öncesinde kullanıcı eğer kayıt olmamışsa öncelikle kayıt olmalı ve daha sonra sisteme giriş yapabilmektedir. Doktor veya hastanın sisteme giriş yapabilmesi için öncelikle sisteme kayıt olmaları gerekmektedir. Sisteme kayıt olduktan sonra hastane veya yönetici admin tarafından onay verildikten sonra sisteme giriş yapabilirler. Sisteme giriş yapmış bir doktor hasta

bilgilerini sisteme ekleyebilmektedir. Blok zincirine gönderilmeden öncesinde değişiklik yapabilmektedir ancak blok zincirine gönderildikten sonra artık hasta bilgilerini değiştirmesi mümkün değildir. Hasta bilgileri bloklar halinde hash fonksiyonu ile bit dizisine dönüştürülerek blok zincirine eklenmektedir. Her bir hasta için ayrı bir blok zinciri vardır. Eğer bu hasta bilgilerinden bir tanesi bile değişirse blok zincirinin kimliği tamamen değişecektir. Hasta giriş yaptıktan sonra bilgileri şifrelenmiş bir şekilde saklanmakta ve kendisiyle alakalı teşhis bilgilerini görebilmekte ancak bilgileri değiştirememektedir. Admin günlük olarak eklenen hasta bilgilerini görmekte ve hasta bilgilerini değiştirildiğinde veri tabanı üzerinde veya log dosyasında takip edebilmektedir. Doktor hastasının teşhis bilgilerini ekledikten sonra blok zincirine gönderebilmektedir.

Hastaların tıbbi kayıt bilgilerin çalınması, değiştirilmesi hastaların mahremiyeti için çeşitli riskler doğurmaktadır. Bu bilgilerin kötü amaçlı kişilerin vereceği zarar hem hastaya hem de finanse eden kuruma ciddi zararlar vermektedir. Bundan dolayı bulut tabanlı Elektronik Sağlık Kayıtları (ESK), hasta verilerine uzaktan erişim birçok araştırmacının ilgi odağı haline gelmiştir. Hasta verilerinin saklanması, veri doğruluğu, veri gizliliği, veriyi bulut sisteminde hızlı iletilmesi sağlamak sağlık sektöründe önemli bir endişe kaynağıdır. Bu makalede, ESK kayıtları için veri erişim kontrolü ve denetimi sağlarken, bulut servis sağlayıcıları yardımıyla sağlık verilerinin paylaşılması için blok zincire ek olarak katmanlı mimari yapısı, API (Uygulama Ara Yüzü) ile hasta bilgilerini özet fonksiyonu (Hashing) uygulamak destekleyici yeni ek çözümler önerilmiştir. Önerilen bu yöntemlerle, hastanın elektronik sağlık kayıtlarının sağlık sektörü tarafından yönetilmesinden ve kontrol edilmesinde kullanılacaktır. Bu nedenle blok zinciri platformunda kullanılan bu teknolojilerle önerilen yöntem daha güvenli yeni modeller geliştirilmesine imkân sağlayacaktır.



Şekil 7. Önerilen blok zincirli ESK sistemi.

- Yönetici Modülü (Super Admin Modülü): Bu modülde güvenli giriş sistemi spring güvenlik modülü ile yapılmaktadır. Admin bütün modüllere erişim sağlayabilmektedir. Hastanede çalışan doktorların güncellenmesi, sistem bakım işlemlerinde sorumlu ve sistemde meydana gelebilecek sorunları izlemek ve çözümlemekte sorumlu modüldür. Sisteme izinsiz giriş yapmaya çalışan kişilerin listesi loglama yöntemiyle tespit edilir. Sistem kullanıcılarında doktor, hastane veya hasta kullanıcı girişindeki sisteme şüpheli girişler tespit edilirse bu kullanıcılar kilitlenir. Bu kilitlenmeyi yönetici modülü sağlamaktadır. Veri tabanı verilerine erişim sağlayabilmesi için uygulama özelliklerine eklediği kullanıcı adı ve şifre ile

erişim sağlayabilmektedir. Sistemin yedeğini almakla sorumludur. Sistemin olası saldırılarına karşı serveri kapatma yetkisi bulunmaktadır.

- Hastane Modülü (Admin): Bu modülde kendisine daha önceden verilmiş kullanıcı adı ve şifre ile spring güvenlik aracılığıyla sisteme giriş yapar. Hastanede çalışan sağlık çalışanların sisteme eklendiği ve hasta bilgilerinin yönetildiği modüldür. Doktor veya hastanın şüpheli giriş işlemlerinde ilgili kullanıcıların sisteme girişini kilitleyebilir. Kilitlenen kullanıcı modülü sadece yönetici modülü tekrardan aktifleştirebilir. Doktor ve hastanın bilgilerine erişim sağlayabilmekte ve çıktısını alabilmektedir. Hastanesinde ayrılacak sağlık çalışanın bilgisini sisteme eklemekle sorumludur. Sağlık çalışanların sisteme eklediği bilgileri ve hastaya konulan teşhisi görebilmektedir. Şüpheli doktor veya hasta için kullanıcı bilgilerini askıya alabilen modüldür.
- Doktor Modülü: Bu modülde kendisine daha önceden verilmiş kullanıcı adı ve şifre ile sisteme spring güvenlik aracılığıyla giriş yapar. Hasta bilgilerini, teşhisini sisteme kayıt etmekle sorumlu modüldür. Hastanedeki hasta bilgisine erişim sağlayabilmektedir. Blok zincirine göndermeden önce değişiklikler yapabilmektedir. Blok zincirine kayıt edildiğinde herhangi bir değişiklik yapamamaktadır. Doktorlar hastaların bilgilerine hızlı ve güvenli erişimi hasta teşhisinde önemli bir rol oynamaktadır.
- Hasta Modülü: Bu modülde kendisine daha önceden verilmiş kullanıcı adı ve şifre ile sisteme spring güvenlik aracılığıyla sisteme giriş yapar. Bu modülde doktor tarafından sorulan bilgileri cevaplayacak modüldür. Hasta kendi bilgilerini okuyabileceği ancak değiştiremeyeceği bu modülde bütün bilgileri saklanacaktır.

4. Sonuç

Blok zinciri, birden fazla blokların ortaklaşa birbirine bağlanarak verilerin güvenli bir şekilde saklanması olayıdır. Blok zincir, bulut bilişimde veri depolama ve paylaşımının diğer merkezi güvenlik çözümlerinin tüm zorluklarına bir cevaptır. İnternetteki veri belgelerinin yeni bir paradigmasıdır. Bu teknoloji kullanarak hasta bilgilerinin gizliliğini sağlamak ve uzaktaki bir hastanedeki hastanın bilgisine güvenli bir şekilde erişimin yolları araştırılmış ve blok zincirinin mantığı çerçevesinde uygulama yapılmıştır. Sağlıkta veri transferi, veri güveliği, verinin dağıtık bir sistemde yönetilme süreci önemli olduğundan bu problemin blok zinciriyle yapılması son derece önemlidir. Blok zincirin birçok uygulama alanında başarıyla kullanılması sağlık alanında da veri paylaşımının ve güvenlik sorunlarını çözebilecek nitelikte olduğunu kanıtlar. Blok zincirin sağlık alanında bulut teknolojisiyle birlikte kullanılmasının veriyi doğru işleme, veri paylaşımını sağlama, verilerde oynama yapılmasını engelleme ve kötü niyetli kimselerin eline geçmeden paylaşılma gibi birçok avantaj sağladığı gözlemlenmiştir. Blok zincirinde önemli olan veri şifrelemede hashing algoritmaları kullanarak veri paylaşımını güvenli olacak şekilde işlenmesidir. Verileri bloklar halinde şifreleyerek bir sonraki düğüme bağlanarak düğümleri oluşturmaktadır. Bu blok süreci ve etkileşim ile tüm veriler entegre hale gelmekte ve verileri bütünlük ilkesini gereği değişen en ufak bir bilginin bozulmasıyla silsile grubunda diğer düğümleri etkiyeceğinden dolayı diğer düğümlerin çalışmamasına bağlı olacaktır. Bu çalışmada JavaEE Spring Boot teknolojisinden yararlanılarak veri kaydetme, veri paylaşımının API üzerinden sağlanmasını sağlamak için Spring rest, veri güvenliğini sağlamak için Spring Security kullanılmıştır. Blok zincirinin en önemli özelliği güvenilmeyen taraflar arasında güven köprüsünü kurmaktır.

Blok zinciri yeni olduğu için gelecek vaat ediyor ve şimdiden birçok alanda kullanımı söz konusudur. Özellikle sağlık ve dijital alanda yerini almıştır. Blok zinciri birçok teknolojiyle eşzamanlı olarak çalışmaktadır. Bu teknolojilerden hashing ve uzlaşma algoritmaları yardımıyla güvenli veri paylaşımı sağlanmaktadır.

Teşekkür

Bu çalışma, H.M.'nin Malatya Turgut Özal Üniversitesi, Enformatik Anabilim Dalı bünyesinde ki "Blok Zinciri ve Sağlık Uygulamaları" başlıklı yüksek lisans tezinin bir parçasıdır. H.M. fikir sahibi ve uygulamayı gerçekleştirdi. S.A. yöntemi yorumladı, yol gösterdi ve düzeltmeleri gerçekleştirdi. H.M. makaleyi yazdı.

Kaynaklar

[1] Sun, Y., & Zhang, D. (2019). Diagnosis and analysis of diabetic retinopathy based on electronic health records. Ieee Access, 7, 86115-86120.

[2] Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. Health information science and systems, 2, 1-10.

[3] Krumholz, H. M., & Waldstreicher, J. (2016). The Yale Open Data Access (YODA) project--a mechanism for data sharing. The New England journal of medicine, 375(5), 403-405.

[4] Taichman, D. B., Backus, J., Baethge, C., Bauchner, H., De Leeuw, P. W., Drazen, J. M., ... & Wu, S. (2016). Sharing clinical trial data: a proposal from the International Committee of Medical Journal Editors. Annals of internal medicine, 164(7), 505-506.

[5] Longo, D. L., & Drazen, J. M. (2016). Data sharing. New England Journal of Medicine, 374(3), 276-277.

[6] Fernandes, L. M., O'Connor, M., & Weaver, V. (2012). Big data, bigger outcomes. Journal of AHIMA, 83(10), 38-43.

[7] Grozev, N., & Buyya, R. (2014). Inter-Cloud architectures and application brokering: taxonomy and survey. Software: Practice and Experience, 44(3), 369-390.

[8] UNC (2013) Healthcare relies on "Analytics to better manage medical data and improve patient care" IBM.

[9] Burghard, C. (2012). Big data and analytics key to accountable care success. *IDC health insights*, *1*, 1-9.

[10] Thilakanathan, D., Chen, S., Nepal, S., Calvo, R. A., Liu, D., & Zic, J. (2014, June). Secure multiparty data sharing in the cloud using hardware-based TPM devices. In 2014 IEEE 7th International Conference on Cloud Computing (pp. 224-231). IEEE.

[11] Yang, J. J., Li, J. Q., & Niu, Y. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Generation computer systems, 43, 74-86.

[12] Dong, X., Yu, J., Luo, Y., Chen, Y., Xue, G., & Li, M. (2014). Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. Computers & security, 42, 151-164.

[13] Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied sciences, 9(9), 1736.

[14] Begoyan, A. (2007). An overview of interoperability standards for electronic health records. USA: society for design and process science.

[15] Ying, Z., Wei, L., Li, Q., Liu, X., & Cui, J. (2018). A lightweight policy preserving EHR sharing scheme in the cloud. IEEE Access, 6, 53698-53708.

[16] Azarm, M., Backman, C., Kuziemsky, C., & Peyton, L. (2017). Breaking the healthcare interoperability barrier by empowering and engaging actors in the healthcare system. Procedia computer science, 113, 326-333.

[17] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40, 1-8.

[18] Fatokun, T., Nag, A., & Sharma, S. (2021). Towards a blockchain assisted patient owned system for electronic health records. *Electronics*, *10*(5), 580.

[19] Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, *8*(2), 44.

[20] Wang, H., & Song, Y. (2018). Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. Journal of medical systems, 42(8), 152.

[21] Ferdous, M. S., Margheri, A., Paci, F., Yang, M., & Sassone, V. (2017, June). Decentralised runtime monitoring for access control systems in cloud federations. In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) (pp. 2632-2633). IEEE.

[22] Ramani, V., Kumar, T., Bracken, A., Liyanage, M., & Ylianttila, M. (2018, December). Secure and efficient data accessibility in blockchain based healthcare systems. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 206-212). IEEE.

[23] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In *2016 2nd international conference on open and big data (OBD)* (pp. 25-30). IEEE.

[24] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, 21260.