MEDİKAL VERİLERİN BLOK ZİNCİRİ MİMARİSİYLE GÜVENLİĞİN SAĞLANMASI

Ömer KASIM
Kütahya Dumlupınar Üniversitesi,
Simav Teknoloji Fakültesi Elektrik Elektronik Mühendisliği, Kütahya, Türkiye
Omer.kasim@dpu.edu.tr

ÖZET

Günümüz teknolojik cihazlarının ve sosyal medyanın hayatımıza girmesiyle kişisel verilerde müthiş bir artış olmuştur. Veri miktarındaki bu artış, depolama ve yönetim süreçlerinde bulut ortamını önemli hale getirmektedir. Kişiye ait medikal veriler, hassas verilerdir. Bu verilerinin bulut ortamında saklanması ve korunması kritik öneme sahiptir. Bu problemin çözümünde farklı yaklaşımlar olsa da Blok Zinciri mimarisi, verilerin bloklar halinde saklanmasını sağlayarak bir denetim sürecini etkin kılmaktadır. Çalışmada oluşturulan blok zinciri ile medikal veriler, blok zinciri içerisinde tutularak kayıtların güvenli bir şekilde oluşturulması, erişilmesi ve paylaşılmasını kontrol bloğu ile mümkün hale getirmektedir.

Anahtar Kelimeler— Kişisel Veri, Medikal Veri, Blok Zinciri, Güvenlik, Bulut Ortamı

Securing Medical Data with Blockchain Architecture

ABSTRACT

The current technological devices and social media are integrated to our lives so that there has been a tremendous increase in personal data. This increase in data volume makes the cloud environment important during storage and management processes. The medical records of the personal data are sensitive. The storage and protection of these data in the cloud environment is critical. Though there are different approaches to solve this problem, blockchain architecture makes an audit process effective by storing the data in blocks. The medical data generated in this study are kept within the blockchain, making it possible to securely create, access and share medical records with control block.

Keywords— Personal Data, Medical Data, Blockchain, Security, Cloud Environment

1. GİRİŞ (INTRODUCTION)

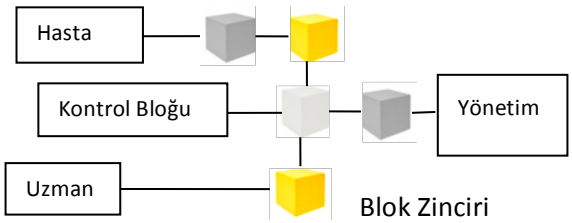
Günümüz teknoloji dünyasındaki üretilen veri miktarındaki müthiş artış hızı, bulut ortamında verilerin saklanmasını gerekli kılmaktadır. Verilerin bulut ortamında saklanması bir bulut veri kaynağı yaratılması ile başlamaktadır. Bu veri kaynağı, bulut ortamında bulunan veri nesnesinde gerçekleştirilen "veri oluşturma" ve işlemlerin geçmişini kaydeden "meta verileri" bileşenlerinden oluşmaktadır [1]. Verilerin bulut ortamında saklanması güvenlik sürecinin etkin kullanımını gerektirmektedir. Kişiye ait hassas verilerin güvenliğinin sağlanması önemli hale gelmektedir.

Bulut ortamında tutulacak hassas verilerden birisi de medikal verilerdir. Medikal verilerin güvenliği açısından bakıldığında kişisel verilere ait gizlilik sorunlarını çözümleyen çeşitli çözüm önerileri literatürde sunulmuştur. Bu çözümlerden birisi veri anonimleştirme olarak isimlendirilmiştir. Veriler anonim hale getirilerek tanımlanabilir bilgilerin korunması sağlanmaktadır [2]. Bu süreçte kişiye ait veriler, hassas verilerden ayrı saklanarak veriye erişim, kontrollü hale getirilmektedir [3]. Hassas verilere erişim kontrolü ise hassas verilerin dağılımını belirleyen "yakınlık derecesi" parametresi ile belirlenmektedir [4]. Bir diğer yaklaşım ise verileri paylaşmadan önce hesaplama işlemine tabi tutarak şifreleme esasına dayanmaktadır. Şifrelenen verinin sahip olduğu örüntüyü bilen kullanıcılar, kullanıcı haklarına göre belirlenen belirli sorguları çalıştırabilmektedir [5].

Alınan bu önlemler güvenlik noktasında denetim mekanizması sağlasa da medikal verileri içeren

meta verilerdeki hassas bilgilerin korunması gerekmektedir. Bulut ortamında oluşturulacak veriler, sahteciliğine karşı savunmasız olduğu ilgili çalışmada tespit edilmiştir [6]. Bu durum veri güvenilirliğini önemli hale getirmektedir. Bu verilerin güvenliğinin sağlanarak bulut ortamında saklanabilmesi günümüzde blok zinciri mimarisiyle mümkün olabilmektedir [7].

Blok zinciri, finans sektöründe kullanılan eşler arası dağıtılmış blok teknolojisi üzerine inşa edilmiştir. Bir kullanıcının kimliğinin bir ağ içinde nasıl tanımlandığına bağlı olarak izin verilen ve izinsiz blok zinciri olarak iki farklı türde tasarlanabilmektedir. İzinsiz bir sistem tasarımında katılımcıların kimliğinin sahte veya anonim olması önem arz etmemektedir. Bu tasarımda her kullanıcı blok zinciri mimarisine yeni bir blok ekleyebilmektedir [8]. Diğer taraftan izin verilen bir blok zincir tasarımında ise bir kullanıcının kimliği, bir kimlik sağlayıcı tarafından kontrol edilmektedir. Bu tasarımda kimlik sağlayıcısının rolü kritik öneme sahiptir. Bu sağlayıcı, ağ içinde erişim kontrolünü ve kullanıcının uzlaşmaya katılma haklarını koruma görevini üstlenmektedir. Ayrıca yeni bir bloğu onaylamak için güvenilir olması zorunluluğu bulunmaktadır [9].



Şekil 1. Blok Zinciri Algoritmanın Akış Diyagramı

Blok zinciri teknolojisini kullanarak oluşturulacak bir bulut ortamı, veri kaynağı ile verilerin gizliliğini ve kullanılabilirliğini güvenli hale getirilebilmektedir [10]. Bu süreç ile proaktif siber güvenliğe katkı sağlanmaktadır [11].

Çalışmada medikal verileri içeren bir blok zinciri mimarisi geliştirilmiştir. Geliştirilen yapı Şekil 1'de verilmiş olup, blok zincirinde her bir hastaya ait veriler bir blok içerisinde tutulmaktadır. Verilerin eklenmesi ya da güncellenmesi durumunda blokların "hash" içerikleri değişmektedir. Bu durum içeriği değişen bloktan sonraki zincir içerisindeki blokların "hash" bilgilerinin güncellenmesi ile son bulması gerekmektedir. Blok zinciri mimarisinde Madencilik süreci olarak isimlendirilen işlem ile zincirdeki bloklar taranmakta ve "hash" bilgileri SHA algoritması ile onaltılık kodlara dönüştürülerek güncellenmektedir. Bu süreç ile blok zinciri doğrulanması yapılmaktadır. Doğrulama süreci ve madencilik işlemi orta noktadaki kontrol bloğu ile sağlanmaktadır. Bu blok üzerinden birbirine bağlı olan blokların hash kodları eşlenerek zincir oluşmaktadır. Kontrol bloğu ile aynı zamanda veri eklenmesi ve güncellenmesi yapılmaktadır. Ayrıca kontrol bloğu sayesinde doğrulama işlemi ile araya eklenebilecek ya da saldırı amaçlı içeriği güncellenecek blokların doğrulaması yapılmayacak olduğundan bulut ortamındaki verilerin korunması noktasında siber güvenliğe destek olunmaktadır. Ayrıca kontrol bloğu ile blok içerisindeki verilerin okunması hasta, uzman ya da yönetim rollerine göre erişim hakkı sağlanmaktadır. Blok zincirine özel bir başlangıç noktası olduğundan bu bilgiyi bilmeyen bir kullanıcı, zincire müdahale edememektedir. Ayrıca bloğa ait zaman damgası bilgisi ile "hash" içeriği güncellendiğinden verilerin oluşma zamanına göre de bir güvenlik süreci geliştirilen yöntem ile sağlanmaktadır.

2. MEDİKAL VERİ İŞLEMLERİ (MEDICAL DATA PROCESSING)

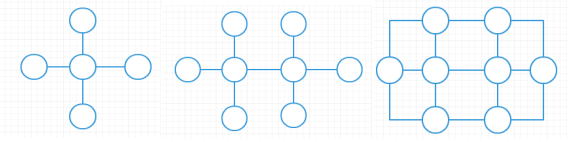
Uzun süreli tedavi ve hastanın ömür boyu izlemesini gerektiren ciddi bir tıbbi rahatsızlık içeren hastalıklar ve bu hastalılara ait tedavi süreçleri hassas bilgileri içermektedir. Bu nedenle, hastanın tıbbi geçmişini muhafaza etmesi, tedavi ve tedavi sonrası izleme sırasında tıbbi verilerine erişebilmesi veya araştırma amaçlı paylaşılması önem arz etmektedir. Bir hastanın hareketliliği nedeniyle, her hastanın ziyareti sırasında üretilen verilerin yönetimi, özellikle sağlık verilerinin hassas doğası göz önüne alındığında zor bir süreci içermektedir. Blok zinciri mimarisi olmadan yapılacak bir tasarımda hassas verilerden herhangi birinin Hastane 1'den Hastane 2'ye aktarılması gerekiyorsa belirli bir protokol takip edilmektedir. Bu protokolün işlemesi sürecinde hasta veya onun resmi temsilcisi bir rıza anlaşması imzalamak zorundadır. Bu anlaşmanın içeriğinde aktarılacak verileri belirten ve verilerin alıcısıyla ilgili bilgileri bulunmaktadır. Bu anlaşma sonrasında hastaya ait veriler bir başka sağlık kuruluşuna aktarılabilmektedir. Her bir aktarımda hasta ile ilgili olan tahlil ve tedavi süreçlerini içeren

verilerin güvenliğinden dolayı tekrar tanımlama yapılması gerekmektedir. Tahlillerin tekrar yapılması hastaya ait klinik işlemlerin tekrarlanması gibi sonuçları olan bu süreçte zaman kaybı yaşanmaktadır. Ayrıca bu yaklaşımla, hastanın verilerinin herhangi bir erişim kontrolünü sürdürmesi ve verileri tam olarak görebilmesi oldukça zor bir süreçtir.

3. BLOK ZİNCİR MİMARİSİ (BLOCKCHAIN ARCHITECTURE)

Blok zincir mimarisi, tek nokta üzerinden merkezi olarak oluşturulmuş güven sistemi yerine verilerin bloklar ile ifade edilmesi sürecine dayanmaktadır. Bu durum sistemin şifreli kayıt defteri biçiminde oluşarak daha verimli çalışmasını sağlamaktadır.

Üç farklı biçimde blok zinciri oluşturulabilmektedir. Üç türe ait sistem yapısı Şekil 2'de gösterilmiştir. Şekil 2a'da görüldüğü üzere merkezi esas alan bir blok zinciri tasarımı görülmektedir. Bu tasarımda merkez düğümdeki blok üzerinden tüm süreç idare edilmektedir. Sorumluluğun paylaşılması ile farklı düğümdeki bloklardaki giriş seviyeleri ile bloklar arası iletişim süreci sağlanmaktadır. Bu durum Şekil 2b'de ifade edilmiştir. Herkesin eşit sorumluluğa ve haklara sahip olduğu dağıtık yapıda ise şekil 2c'de görüldüğü üzere bloklar arası iletişim ile herkes her bloğa ulaşabilmekte ve müdahale edebilmektedir. Her bir tasarım sürecinde izinli ya da izinsiz bir süreç üzerinden yapılan bilgi güncelleme ve veri ekleme işlemleri ile hash bilgileri güncellenmektedir. Madencilik işleminin ardından blok zinciri doğrulaması yapılarak bulut ortamında veriler saklanmaktadır.



(a) (b) (c)

(a) Merkezi Blok Zinciri,
(b) Sorumluluğun Dağıtıldığı Blok Zinciri,
(c) Dağıtık Blok Zinciri

Şekil 2. Blok Zinciri Mimarisi Tasarımı

4. GELİŞTİRİLEN YÖNTEM (DEVELOPED METHOD)

Blok zinciri yapısı, birbirine bağlı bloklardan oluşan bir mimariye sahiptir. Zincirde yer alan her bir blok kendine ait sayısal bir imzaya sahiptir. Bu imza kendisinden önceki bloğun sahip olduğu imza ve blok içerisindeki veriye göre belirlenmektedir. İmzanın blok zinciri sürecindeki ismi "hash" olarak isimlendirilmektedir. Hash sadece kendisinden önceki bloğun verisine sahip değildir. Önceki bloğun "hash" içeriği, blok içerisindeki veri, zaman damgası ve işlenen zincir sayısı bilgileri kullanılarak bloğun kendine ait "hash" içeriği hesaplanmaktadır. Bir bloktaki verinin değişmesi "hash" içeriğinin değişmesine de neden olacaktır. Bu durum "hash" içeriği değişen bloktan sonraki bloklara yansıtılması gerekmektedir. Dolayısıyla değişiklik yapılan bloktan sonraki blokların "hash" içeriklerinin güncellenmesi gerekmektedir. Hash içerikleri hesaplanarak bir bloğun geçerli ya da geçersiz olduğu kararı madencilik işlemi ile verilmektedir.

Geliştirilen sistem Şekil 2a'da ifade edilen merkezi blok zinciri mimarisine sahiptir. Bu mimaride ortada yer alan blok kontrol bloğu olarak tasarlanmıştır. Veri girişi, güncellemesi ve madencilik işlemleri bu blok üzerinden yapılmaktadır. Bu süreç JAVA platformunda geliştirilmiştir. Oluşturulan veri blokları ise dizi listesi biçiminde olduğu için hastane içerisindeki yerel bir bulut üzerine aktarılmaktadır.

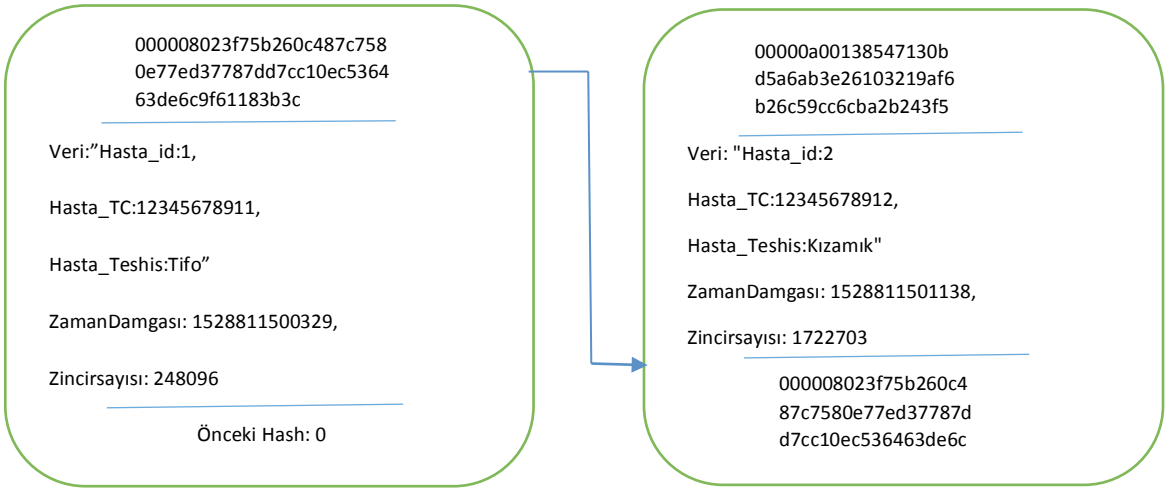
Kontrol bloğunda üç farklı kullanıcı tipi bulunmaktadır. Her bir kullanıcı sisteme bağlanırken kullanıcı rolünü seçmektedir. Seçilen rol doğrultusunda blok üzerinde görebileceği bilgiler süzülmektedir. Bilgiler metin dosyasında saklandığından veri okuma işlemi JAVA dilinin metin dosyası satır numarası okuma işlemi ile gerçekleştirilmektedir. Hasta kullanıcı adıyla sadece birinci ve ikinci satırda yer alan "hastatc" ve "hastaid" alanları görülebilmektedir. Uzman kullanıcı yetkisiyle hasta yetkisine istinaden ek olarak teşhis bilgisi görülebilmektedir. Yönetim yetkisi ile giriş yapıldığında ise zaman damgası ve işlenen zincir sayısı satırları görülebilmektedir.

Şekil 3'te oluşturulan blok zinciri yapısı içerisindeki "hash" içerikleri SHA256 algoritması ile şifrelenmektedir. Zincirdeki ilk bloğun "hash" bilgisi "0" olarak çalışmada belirlenmiştir. Bu değer ile zincire giriş yapılması mümkün olacaktır. Bu sayı üzerinden "hash" içerikleri oluşturulmaktadır. Bu değeri sadece zincire veri ekleyecek kullanıcıların bilmesi güvenlik açısından önemlidir. Hash içeriği oluşturulurken

önceki blok, "hash" içeriğinin yanı sıra zaman damgası ve çözülen zincir sayısı bilgisi de sürece dâhil edilmektedir. Madencilik sürecinde eğer farklı bir içeriğe sahip blok sisteme eklenmiş ise blok geçersiz olacaktır.

Geliştirilen programda her bir blok dizi listeleri üzerinde saklanmaktadır. Oluşturulan dizi listelerinde blok ve blok bağlantıları içerik olarak saklanmaktadır. Medikal verilerin olduğu her bir blok içerisinde barındırdığı verilerin yanı sıra kendi "hash" bilgisine de sahip olmaktadır. Zaman damgası ve çözülen zincir sayısı bilgileri ile birlikte önceki "hash" kodlarıyla eşleştirilerek blok zinciri oluşmaktadır. Çalışmada elde edilen 5 bloğa ait sürece ait bilgiler Şekil 4'te ifade edilmiştir. Her bir blokta "hash" bilgisi, önceki hash bilgisi, medikal veri, zaman damgası ve çözülen zincir sayısı bilgileri bulunmaktadır. Bloktaki hash bilgisi bloğun kendi imzasını belirlemektedir. Geliştirilen ilk bloğun hash bilgisi 64HEX olarak kodlanmış karaktere sahip olan *"000008023f75b260c487c7580e77ed37787 dd7cc10ec536463de6c9f61183b3c"* bilgisini içermektedir. Bu bilgi SHA256 şifreleme algoritması ile elde edilmektedir. Birbirine bağlı 5 blok hem kendi "hash" bilgisini hem de kendinden önceki bloğun "hash" bilgisini tutmaktadır. Bu süreç sonucu blok zinciri yapısına benzer bir mimariyi oluşturmamıza olanak sağlamaktadır. Blok içerisinde yer alan ilk değer 0 (sıfır) olarak belirlenmiştir. Bu değere zaman damgası yani verinin oluşturulma zamanı bilgisi eklenmektedir. Verinin oluşturulma zamanı bilgisi verinin güvenliğinin sağlanması için gerekmektedir. Kendi içerisinde yer alan veri, verinin oluşturulma ya da güncellenme zamanı bilgisi ve çözülen zincir sayısı bilgilerini de içerin bir kod olan "hash" kod ile verinin güvenliği sağlanmaktadır. Hash kod üretme süreci Şekil 5'te ifade edilmiştir. Şekil 5'deki "A" bilgisi çözülen zincir sayısını, "T" bilgisi zaman damgası bilgisini, "D" bloktaki hastalıkla ilgili olan veriyi ve "H" 'de bloktaki güncellemeden önceki "hash" bilgisini ifade etmektedir. Dizi listesi içerisindeki "hash" içerikleri karşılaştırılarak geçerli ya da geçersiz blok kararı, zincir içerisinde denetim sonucu verilmektedir. Çalışmada elde edilen doğrulama süreci, Şekil 6'da ifade edilmiştir. Bloklar arası eşleşme "hash" kodları ile sağlanmaktadır. Her bir bloğa yeni veri eklenmesi ya da yeni bir blok eklenmesi ile "hash" kodları güncellenmektedir. Bu güncelleme sonucu eşleşen bloklar, blok zincirini oluşturmaktadır. Bu mimari dışında bir blok sürece dahil edilse bile doğrulama adımından geçilemediği için veriler güvende kalmaktadır [12].

Bir kullanıcı, blok zinciri mimarisi içerisindeki bloklardan daha fazlasını ekleyebilirse blok zincirine sahip olma olasılığı bulunmaktadır [13]. Bu süreci engellemek amacıyla çalışmada yerel sistem üzerinde üretilen veriler, metin dosyaları ile zincire aktarılmaktadır. Bu metin dosyası belirli bir örüntü içerisinde oluşturulmaktadır. Bu örüntüye sahip olan dosyalar zincire eklenmeden önce denetlenmektedir. Bu doğrulama adımı sağlanmaz ise zincire erişim engellenmektedir. Aynı zamanda güncelleme yapılacağı zaman aynı süreç geçerlidir. Programdaki metot ile zincire eklenecek veriler, metin dosyalarından çekilerek denetim mekanizmasının ardından zincire blok olarak eklenmektedir.



Şekil 3. Medikal Verinin Blok Zinciri Mimarisindeki Tasarımı

Blok 1
Hash: "000008023f75b260c487c7580e77ed37787dd7cc10ec536463de6c9f61183b3c",
oncekiHash: "0",
Veri: "Hasta_id:1,Hasta TC:12345678911 Hastalığı:Tifo",
Zaman Damgası: 1528811500329,
Çözülen Zincir Sayısı: 248096
Blok 2
Hash: "00000a00138547130bd5a6ab3e26103219af6b26c59cc6cba2b243f58400d5e9",
oncekiHash: "000008023f75b260c487c7580e77ed37787dd7cc10ec536463de6c9f61183b3c",
Veri: "Hasta_id:2,Hasta TC:12345678912 Hastalığı:Kızamık",
Zaman Damgası: 1528811501138,
Çözülen Zincir Sayısı: 1722703
Blok 3
Hash: "00000a8f1e4daa6b472bc414ec3d800f3c4e4f11fb93606d2465af218b60e3ec",
oncekiHash: "00000a00138547130bd5a6ab3e26103219af6b26c59cc6cba2b243f58400d5e9",
Veri: "Hasta_id:3,Hasta TC:12345678913 Hastalığı:HIV",
Zaman Damgası: 1528811506083,
Çözülen Zincir Sayısı: 3050138
Blok 4
Hash: "00000a04d97fcebb1ddfae25d2a1917c3052c01d06ce577767f8cf82465804fd",
oncekiHash: "00000a8f1e4daa6b472bc414ec3d800f3c4e4f11fb93606d2465af218b60e3ec",
Veri: "Hasta_id:4,Hasta TC:12345678914 Hastalığı:Sağlıklı",
Zaman Damgası: 1528811514665,
Çözülen Zincir Sayısı: 260346
Blok 5
Hash: "000005a84cc4a5cf00cb8df5214f911fbcadf84218ba781fe79a47658f4178c3",
oncekiHash: "00000a04d97fcebb1ddfae25d2a1917c3052c01d06ce577767f8cf82465804fd",
Veri: "Hasta_id:5,Hasta TC:12345678915 Hastalığı:Sağlıklı",
Zaman Damgası: 1528811515417,
Çözülen Zincir Sayısı: 170066

Şekil 4. Medikal Verinin Blok Zinciri Mimarisindeki Tasarımı

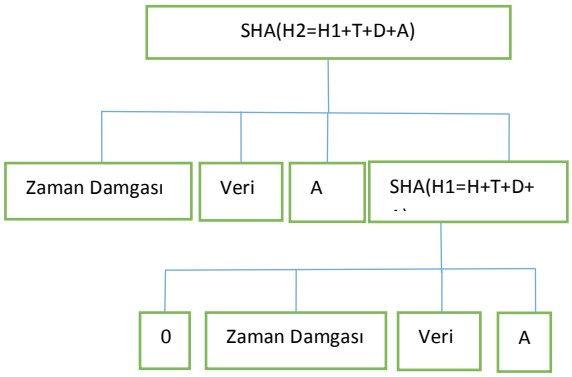
5. SONUÇLAR (RESULTS)

Medikal verilerin gizliliği ve güvenliğinin sağlanması amacıyla bu çalışmada, kullanıcı korunabildiği sağlayan blok zinciri mimarisine sahip bir bulut veri kaynağı süreci tasarlanmıştır. Blok zinciri süreci içerisinden yer alan ve değiştirilemeyen zaman damgasıyla hastaya ait verilerin blok zincirine kayıt süreci gerçekleştirilmiştir.

Sistemin tasarımında yer alan kontrol bloğu ile zincire eklenecek veri bloğu hastane ortamında güvenilir bir kaynak üzerinden beslenmesi veri güvenliği açısından önemlidir. Bu kaynak dışında bir veri eklemesi yapılırsa Madencilik süreci sonunda doğrulama yapılamayacağı için bulut ortamına eklenen veri bloğunun farklı bir kaynaktan eklendiği tespit edilecektir. Bu süreç kişiye ait hassas verilerin korunmasını sağlamaktadır. Veri ekleme süreci metin dosyası ile yapılmakta olup belirli bir ekleme stiline sahiptir. Eklenecek veriler bu stile uygun olarak zincire blok olarak eklenmektedir. Farklı bir stilde eklenecek veriler yine Madencilik sürecinden geçemeyecektir. Bu sistem yapısında çözülen blok zinciri sayısı bilgisi ve "hash" içeriği oluşturulmaktadır. Bir blok içerisinde saklanan bu veriler ile oluşturulan blok zinciri ile hastaya ait verilerin doğrulanması Madencilik süreci ile gerçekleştirilmektedir. Doğrulama işleminin ardından siber saldırı ile blok zinciri içerisine sızılsa bile blok doğrulamadan geçilmediği için verilerin güvenliği sağlanmaktadır. Aynı zamanda veri okuma işlemi de kontrol bloğu üzerinden sağlanmaktadır. Hasta, yönetim ya da uzman rolünde belirlenen kullanıcılar kontrol bloğunda tespit edilerek veri bloklarına okuma amacıyla erişebileceklerdir. Bu süreç her bir kullanıcıya ait parola yardımıyla yapılmaktadır. Çalışmada geliştirilen bu yaklaşımla, hastaya ait verilerin bulut ortamına blok zinciri mimarisinde alınması sağlanmaktadır.

Bulut ortamına saf veri olarak alınması durumunda veri eklemesi, güncellemesi ve kişiye ait verilerin manipüle edilmesi söz konusudur. Bu problem blok zinciri mimarisi ile mümkün olmamaktadır. Ayrıca veriyi okuyacak kullanıcılar rollerine göre hasta, uzman ya da yönetim olarak bağlanıp sadece kendi ilgi alanlarındaki blok satırlarına ulaşabilmektedir. Bu süreç kontrol bloğu ile hastane merkezinde yer alan bir sunucu ile sağlanmaktadır. Bu sunucu sistemi Madencilik sürecini yine yerel bulut ortamına bağlanarak yapmakta ve bulut veri bloklarını doğrulamanın ardından güncellemektedir.

Hastanın farklı sağlık kuruluşlarından hizmet alması ya da bilgilerinin aktarılması gerektiğinde hastaya ait verilerinin kurumların arasında geçişi önlenmiş olacaktır. Bu süreç kontrol bloğuna erişim izni yönetim ya da uzman olarak verildiğinde gerçekleştirilmektedir. Yapılan tahlil ve tedavi bilgileri de kolay ve güvenli bir şekilde kurumlar arasında taşınmış olacaktır. Bu süreç ile özellikle hastanın bütün yaşamı boyunca sahip olduğu medikal verilerin tek bir blokta saklanması sağlanmış olmaktadır.



Şekil 5. Hash Kodunun Oluşum Evreleri

İşlenen Blok 1

Yeni Hash: 000008023f75b260c487c7580e77ed37787dd7cc10ec536463de6c9f61183b3c

İşlenen Blok 2

Yeni Hash: 00000a00138547130bd5a6ab3e26103219af6b26c59cc6cba2b243f58400d5e9

İşlenen Blok 3

Yeni Hash: 00000a8f1e4daa6b472bc414ec3d800f3c4e4f11fb93606d2465af218b60e3ec

İşlenen Blok 4

Yeni Hash: 00000a04d97fcebb1ddfae25d2a1917c3052c01d06ce577767f8cf82465804fd

İşlenen Blok 5

Yeni Hash: 000005a84cc4a5cf00cb8df5214f911fbcadf84218ba781fe79a47658f4178c3

Blok zinciri geçerliği: ***Doğrulandı***.

Şekil 6. Medikal Verilerin Blok Zinciri Mimarisindeki Hash Kodlarının Üretilmesi Süreci

KAYNAKLAR (REFERENCES)

[1] Y. L. Simmhan, B. Plale, D. Gannon, "A survey of data provenance in e-science," ACM Sigmod Record, vol. 34, no. 3, 2005:pp. 31–36.

[2] L. Sweeney, "k-anonymity: A model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems vol:10, no:05 2002: pp. 557-570.

[3] A. Machanavajjhala, D. Kifer, Johannes Gehrke, Muthuramakrishnan Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," ACM Transactions on Knowledge Discovery from Data (TKDD), vol:1, no:1, 2007:pp.1-52.

[4] N. Li, T. Li, S. Venkatasubramanian. "t-closeness: Privacy beyond k-anonymity and l-diversity," IEEE 23rd International Conference onData Engineering, 2007:pp.106–115.

[5] C. Gentry, "Fully homomorphic encryption using ideal lattices," Proceedings of the 41st annual ACM symposium on Symposium on theory of computing-STOC'09. Vol. 9, 2009:pp. 169–178.

[6] B. Lee, A. Awad, M. Awad, "Towards secure provenance in the cloud: A survey," in 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC), 2015:pp. 577–582.

[7] Lin, Iuon-Chang, Tzu-Chun Liao, "A Survey of Blockchain Security Issues and Challenges," International Network Security Vol:19, No:5, 2017:pp:653-659.

[8] Junqueira, Flavio P., Benjamin C. Reed, Marco Serafini, "Zab: High-performance broadcast for primary-backup systems," IEEE/IFIP 41st International Conference on Dependable Systems and Networks (DSN), 2011:pp. 245-256.

[9] T. Swanson, "Consensus-as-a-service: a Brief Report on the Emergence of Permissioned," Distributed Ledger Systems2015:pp:1-66.

[10] D. Tosh, S. Sengupta, C. A. Kamhoua, and K. A. Kwiat, "Establishing evolutionary game models for cyber security information exchange (cybex)," Journal of Computer and System Sciences, vol:98, 2016:pp.27-52.

[11] D. K. Tosh, S. Sengupta, S. Mukhopadhyay, C. Kamhoua, and K. Kwiat, "Game theoretic modeling to enforce security information sharing among firms," in IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud),2015:pp. 7–12.

[12] I. Eyal, E.G. Sirer, "Majority is not enough: Bitcoin Mining is vulnerable, in: Financial Cryptography and Data Security", 18th International Conference, in: Lecture Notes in Computer Science, vol:8437, 2014:pp. 436–454.

[13] Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q., "A survey on the security of blockchain systems." Future Generation Computer Systems, 2017:http://dx.doi.org/10.1016/j.future.2017.08.020.