ULUSAL GÜVENLİK İÇİN
BLOKZİNCİRİ TABANLI
SİBER GÜVENLİK MODELİ

Yüksek Lisans Tezi

Enis KONACAKLI

Eskişehir, 2019

ULUSAL GÜVENLİK İÇİN BLOKZİNCİRİ TABANLI SİBER GÜVENLİK MODELİ

Enis KONACAKLI

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Danışman Dr. Öğretim Üyesi Enis KARAARSLAN

Eskişehir

Eskişehir Teknik Üniversitesi

Fen Bilimleri Enstitüsü

Mart, 2019

JÜRİ VE ENSTİTÜ ONAYI

Enis KONACAKLI'nın "Ulusal Güvenlik İçin Blokzinciri Tabanlı Siber Güvenlik Çözümleri" başlıklı tezi 22/03/2019 tarihinde aşağıdaki jüri tarafından değerlendirilerek "Eskişehir Teknik Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği"nin ilgili maddeleri uyarınca, Bilgisayar Mühendisliği Anabilim dalında Yüksek Lisans tezi kabul edilmiştir.

Unvanı-Adı Soyadı		**İmza**
Üye (Tez Danışmanı):	**Dr. Öğr. Üyesi Enis KARAARSLAN**	**……..**
Üye	**:Dr. Öğr. Üyesi Ahmet ARSLAN**	**……...**
Üye	**:Dr. Öğr. Üyesi Esra N. YOLAÇAN**	**…….……..**

Prof.Dr.Ersin YÜCEL
Enstitü Müdürü

ÖZET

ULUSAL GÜVENLİK İÇİN BLOKZİNCİRİ TABANLI SİBER GÜVENLİK ÇÖZÜMLERİ

Enis KONACAKLI
Bilgisayar Mühendisliği Anabilim Dalı
Eskişehir Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Mart, 2019
Danışman: Doktor Öğretim Üyesi Enis KARAARSLAN

Günümüzde İnternete bağlı bilgisayarlar; kolumuzdaki saatten fabrika otomasyon sistemlerine (SCADA) kadar hayatımızın her alanına girmiş durumdadır. İnternetin bu derece genişlemesi, siber saldırıları kişisel ve ulusal güvenliğimizin karşısındaki en büyük tehdit unsuru haline getirmektedir. Devletlerin kritik altyapılarına nüfus edebilecek kadar kabiliyet kazanan siber saldırılar, 2017 yılı içerisinde dünya çapında toplam 600 milyar dolar maddi zarara sebebiyet vermişlerdir. Bulut bilişim ve nesnelerin interneti gibi internet ortamını kullanan teknolojilerdeki gelişmeler, siber ortamdaki riskin yönetimini her geçen gün daha da zorlaştırmaktadır. Son yıllarda suçun tespitinde yaşanan zorluklar ve adli bilişim süreçlerinde öne çıkan diğer bir siber güvenlik unsuru ise inkâr edilemezliğin ve denetlenebilirliğin sağlanmasıdır. Blokzinciri, dağıtık mimarisi ve gerçekleşen işlemlerin tutulduğu silinemez kayıt defteri sayesinde bizlere, tüm bu güvenlik problemlerini giderebilecek yeni nesil bir teknoloji vaat etmektedir. Bu çalışmada blokzinciri sisteminin işleyişi ele alınmış, bu konudaki çalışmaların güvenlik konusunda ortaya koyduğu yeni yaklaşımlar ve bu yaklaşımlarla siber güvenlik için ne tür çözümler geliştirilebileceği incelenmiştir. Blokzincirinin kullanılarak, ulusal kritik altyapılarda bilgi güvenliğinin sağlanmasına örnek teşkil edebilecek bir model oluşturulmuş ve Hyperledger-Fabric'te kodlanarak gerçeklenmiştir. Bu kapsamda blokzincirinin ulusal güvenlik amaçlı kullanımına yönelik çıkarımlarda bulunulmuştur.

Anahtar Sözcükler: Ulusal Güvenlik, Siber Saldırı, Siber Güvenlik, Kritik Altyapılar, Blokzinciri, Radar.

ABSTRACT

BLOCKCHAIN BASED CYBER SECURITY SOLUTIONS FOR NATIONAL SECURITY

Enis KONACAKLI
Department of Computer Engineering
Eskişehir Technical University, Graduate School of Science, March, 2019
Supervisor: Asst. Prof. Dr. Enis KARAARSLAN

With Today, Internet connected computers have entered every fields of our life from the smart watch to the Automation Systems of Factories (SCADA). This expansion of the Internet makes cyber attacks the most dangerous crime that threatens our personal and national security. Cyber attacks, which have gained the ability to directly aim the critical infrastructure of the states, have caused a total of $600 billion global economical collapse in 2017. Developments in technologies that use the internet environment, such as cloud computing and IoT, make the management of the risk in the cyber environment more and more difficult. In recent years, the other cyber security element that stand out in the processes of the challenges of crime detection and forensics are the indisputability and controllability. Blockchain is the new generation of technology that can eliminate all these security problems by means of its blockless, distributed architecture and irrevocable registry which keeps the transactions performed. This technology provides more robust solutions against attacks than the central server architectures with its distributed framework. In this work, the function of the blockchain system is discussed, new approaches of the studies in this subject about security and how these solutions can be developed for the cyber security is examined. By using the blockchain, a model has been formed that can serve as a model for providing information security in national critical infrastructures and is implemented by coding in Hyperledger-Fabric. In this context, deductions were made for areas where the use of blockzincirin would be possible in ensuring national security.

Keywords: National Security, Cyber Attack, Cyber Defence, Crytical Infrastructure, Blockchain, Radar.

22/03/2019

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilemeyen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Eskişehir Teknik Üniversitesi tarafından kullanılan "bilimsel intihal tespit programı"yla tarandığını ve hiçbir şekilde "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara razı olduğumu bildiririm.

.....

Enis KONACAKLI

İÇİNDEKİLER

Sayfa

TABLOLAR DİZİNİ

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

SCADA : Supervisory Control and Data Acquisition System

IoT : Internet of The Things/Nesnelerin İnterneti

MBR : Master Boot Record

AES : Advanced Encryption Standard

RSA : Ron Rivest, Adi Shamir, Leonard Adleman, Cryptography Algorithm

NSA : National Security Agency

USOM : Ulusal Siber Olaylara Müdahale Timi

ITU : Uluslararası Telekomünikasyon Birliği

OSCE : Avrupa Güvenlik ve İşbirliği Teşkilatı

ENISA : Avrupa Ağ ve Bilgi Güvenliği Ajansı

PLC : Programmable Logic Controller

CIA : Confidentiality, Integrity, Availability

1. GİRİŞ

Bilginin en değerli varlık haline geldiği günümüzde iletişim teknolojideki gelişmelerle hayatımızın her alanına girmiş, 20 yıl önce kullandığımız her sistem birer akıllı cihaz veya robotik sistem haline gelmiştir. Yolda yürürken telefonumuz sayesinde arkadaşımızla görüntülü görüşme yapabilmekte, yürüdüğümüz mesafede kaç kalori yaktığımızı internette paylaşabilmekteyiz. Fabrikalar ve enerji üretim tesisleri her geçen gün daha çok gelişen robot teknolojileri ve otonom sistemler sayesinde 10 yıl öncesine göre daha az emekle, daha çok iş üretir hale gelinmiş durumdalar. Tüm bu akıllı sistemler bütünleşmiş çalışabilmek ve birbirleri ile haberleşebilmek için bir yerel alan ağı veya interneti kullanmak zorundalar. Her sistemin bir ağa bağlanma gerekliliği, makineler arası haberleşme trafiği eklenince kullanmakta olduğumuz internet ortamının her geçen gün daha da genişlemesi sonucunu ortaya çıkarmaktadır.

Yaşanan bu gelişmelerin önemli avantajlarının yanında donanım, işletim sistemi ve yazılımlarındaki farklılıklarıyla internete bağlanan teknolojik cihazlar, kötü niyetli siber aktörlere, her geçen gün karmaşıklaşan bir hareket ortamı yaratmaktadır. Bu durum sistemin güvenliğini düşünenleri ise çözülmesi çok zor problemlerle karşı karşıya bırakmaktadır. Son yıllarda meydana gelen siber saldırılarda görüldüğü üzere kötü niyetli siber aktörler ulusal güvenliği tehlikeye sokacak kritik altyapı ve tesisleri doğrudan hedef alınabilecek yeteneğe ulaşmışlardır. Ticari kurumlar, bankalar, her geçen gün yaygınlaşan e-devlet uygulamaları ve enerji ve üretim sektörü, gelişen teknoloji ile güçlenen siber saldırıların doğal hedefi haline gelmişlerdir [1].

Günümüzde gerçekleştirilen siber saldırılarda görüldüğü üzere en kritik altyapılardan sayılabilecek, hiçbir şekilde internet ortamına bağlantısı olmayan bir nükleer reaktörün bilgi sisteminin dahi kontrolü ele geçirilebilmektedir. Bir zararlı yazılım vasıtası ile(Stuxnet) üretim ve enerji sektörü için çok önemli, ağır sanayi için hayati öneme sahip endüstriyel kontrol otomasyon (SCADA, Supervisory Control and Data Acquisition) sistemleri çalışmaz hale getirilebilmektedir [2]. IP kamera sistemlerindeki açıklıklar kullanılarak geniş çaplı DDoS saldırıları (Distributed denial of service, hedef sunucuları veri akışını engelleyerek sistemi servis veremez hale getiren saldırı) gerçekleştirilebilmekte ve merkezi sunuculu mimariler bu ataklara gereken önlemleri almakta yetersiz kalmaktadır. Büyük mali kayıplara sebep olabilen saldırılar aynı anda birden fazla sektörü felce uğratabilmektedir. 2017 Mayıs ayında gerçekleştirilen Wannacry saldırısının dünya genelinde yaklaşık 4 milyar dolar zarara

sebep olduğu tahmin edilmektedir [3]. Haziran 2018'de Şili'de siber güvenlik zafiyetlerini kullanan bilgisayar korsanları 10 milyon dolarlık fonu ele geçirmeyi başarmışlardır. Bu durum Şili hükümetini, saldırılar sırasında yetersiz kaldığını tespit ettiği siber güvenlik mimarisini yeniden yapılandırmaya zorlamıştır [4]. Sistem güvenliğinin sağlanmasında risk sadece siber saldırılarla kısıtlı değildir. Geliştirilen süper bilgisayarların ulaştığı paralel işlem yapma kapasiteleri karşısında, değerli bilgimizi günümüzde kırılamaz kabul ettiğimiz kripto algoritmaları ile koruyabilmemiz, yakın gelecekte mümkün olmayacaktır. Gerçekten güçlü bir siber güvenlik tesis edebilmek için bundan on yıl önce sistemlerimizi koruduğunu öngördüğümüz mimarilerin artık günümüzdeki siber tehdide karşı teknolojik ve yapısal olarak yetersiz kaldığını kabul etmek gerekir [5].

Kriptopara birimleri ile akıllı anlaşmaların ana mimarisini oluşturan ve işlem kayıtlarının güvenliğini sağlama konusunda devrimsel nitelikte çözümler üreten blokzinciri, her geçen gün daha da güçlenen bu siber tehdide karşı kullanılabilecek en önemli güvenlik teknolojisidir. Blokzinciri mimarisi temelde, interneti tam güvensiz ortam olarak kabul ederek taraflar arasındaki güvensizliği kriptografik özet fonksiyonları ve önceden belirlenmiş protokoller vasıtası ile ortadan kaldırmayı amaçlar [6]. Sistemin çalışma prensibi ilk olarak Satoshi Nakamoto mahlası ile yayınlanan bildiride anlatılmış, ilk başarılı uygulaması olan bitcoin ile yıllar içerisinde kendisini kanıtlayarak ve üretilecek yeni uygulamalara öncülük etmiştir [7]. Yapılan araştırmalara göre 27 sektörde kullanım alanı bulacağı öngörülen blokzinciri teknolojisi her geçen gün pek çok araştırma ve çalışmanın yapıldığı önemli bir konu haline gelmiştir [8].

Bu çalışmanın ikinci bölümde Dünyayı ve ülkemizi etkileyebilecek siber tehditler analiz edilmiştir. Üçüncü bölümde blokzincirinin çalışma prensibi, sistemin güvenliği ve sistemin sağladığı güvenlik servisleri anlatılmıştır. Dördüncü bölümde blokzincirinin yeni nesil ulusal siber güvenlik yaklaşımına model oluşturabilecek daha önceden yapılmış akademik çalışmalardan örnekler verilmiştir. Beşinci bölümde ulusal siber güvenliğin sağlanmasında blokzincirinin kullanılabileceği alanlar üzerinde çıkarımlarda bulunulmuştur. Altıncı bölümde bu değerlendirme ve analizler ışığında ulusal güvenlik alanında kullanımına yönelik olarak, NATO'nun müttefik bir ülkede dost milli unsurlarla gerçekleştirdiği harekât ortamı örneklenerek hiçbir şekilde tahrif edilemeyecek veri altyapısı sağlayan bir model oluşturulmuş, bu model Hyperledger-Fabric blokzincir platformu kullanılarak gerçeklenmiştir.

Son bölümde ise bu teknolojinin kullanılmasının önemine değinilmiş ve yapılabilecek sonraki çalışmalar ele alınmıştır.

2. ULUSAL GÜVENLİĞİ HEDEF ALAN SİBER TEHTİDİN ANALİZİ

Türkiye'nin önümüzdeki yıllarda karşı karşıya kalabileceği gerçek siber riski değerlendirdiğimizde, öncelikle ülkemizde teknoloji ve enerji alanlarında yerli girişim ve AR-GE'ye yapılan teşvik, millileşme konusunda yakalanan hız ve nükleer yatırım hamlesi göz önünde bulundurulmalıdır. Bu çerçevede, dünya çapında meydana gelen örnek olaylar değerlendirildiğinde, öncelikli önlem alınması gereken risk grubundaki siber saldırıların, enerji sistem ve altyapılarını, fabrika veri ve altyapılarını, nükleer reaktörleri, katma değeri yüksek dijital verileri (Kamu ve özel sektöre ait mali veriler, AR-GE verileri, kişisel veriler vb.) ele geçirmeyi, kendi çıkarları için kullanmayı veya değiştirmeyi amaçlayacakları beklenmelidir [9]. Bu tip saldırılar arkalarında küresel bazda büyük aktörlerin hatta ülkelerin olduğu güçlü saldırırlardır. Bu saldırılar ancak çok iyi planlanmış kuvvetli altyapı ve siber güvenlik tedbirleri ile bertaraf edilebilirler [10].

2.1. 2017-2018 Genel Siber Risk Değerlendirmesi

Dünya genelinde 2017 yılında gerçekleştirilen saldırılar incelendiğinde ortalama olarak günlük 4,5 milyon civarında siber saldırı meydana geldiği [11], geçtiğimiz senelere göre platformların daha güvenli hale getirilmesi ve alınan önlemler sonucu sistem açıklarını kullanan zararlı yazılım (exploit) saldırılarında ciddi bir azalma olduğu, fakat e-posta yolu ile bulaşan kötü amaçlı yazılım (malware spam/ malspam) atakları ile mobil cihazlar ve IoT üzerinden yapılan saldırılarda artış olduğu gözlemlenmektedir. Özellikle bu sene yaygınlaşan web tabanlı kripto para madenciliği tipi saldırılar ile mobil cihazlar ve IoT üzerinden yapılan botnet tipi atakların (kontrolü saldırgan tarafından ele geçirilmiş bilgisayar veya cihazlar kullanılarak gerçekleştirilen atak) 2018 yılı sonunda en çok öne çıkmış siber trendler olması beklenmektedir [12].

2.2. Türkiye'nin Güncel Siber Risk Haritası

Türkiye son 15 yıl içerisinde siber güvenlik konusunda hukuki altyapısını

tamamlamış, ulusal siber olaylara müdahale timini (USOM) kurmuş [13], ulusal siber güvenli stratejisini oluşturmuş, kendi milli siber savunma tatbikatlarını icra etmeye başlamış ve tüm bu çalışmalarını uluslararası standartlar çerçevesinde şekillendirmiştir [14]. Eğitim, uzmanlaşma ve uluslararası işbirliği konularında ise önümüzdeki yıllarda daha ileri adımlar atması beklenen Türkiye [15]; ITU tarafından yapılan 2017 yılı dünya siber güvenlik derecelendirmesinde 43'üncü sırada yer almaktadır [16]. Özellikle özel sektörde, bankacılık sektöründe ve kamuda son yıllarda alınan önlemler, Türkiye'de konu üzerine artan bir ilgi olduğunu ortaya koymaktadır.

Türkiye'nin saldırı trafiği incelendiğinde, bot trafiğinin toplam saldırıların %20-30'unu oluşturduğu gözlemlenmektedir. 2017 yılında Dünya genelinde toplam 7,5 milyon DDoS saldırılarını gerçekleşirken, Türkiye'de günde 475 DDoS saldırısı gerçekleştiği görülmektedir. DDoS saldırının yaygın olarak mobil cihazlar ve IoT'lerin kullanılması ile gerçekleştirildiği değerlendirilmektedir.

Günümüzde çok boyutlu olarak oldukça geniş bir alana yayılan siber saldırılar, devlet sektöründe ve özel sektörde farklı etkilere hatta yıkıma sebep olabilmektedirler [17]. Bir siber saldırıyı motive eden ana faktörlerden ilki saldırganın bu saldırıdan elde etmeyi beklediği faydanın büyüklüğü(her zaman maddi bir güdüleme olmayabilir), diğeri ise saldırganın saldırıyı yapmak üzere tespit ettiği zafiyetin ona sağladığı imkândır. Türkiye'nin yerli üretime ağırlık vermesi ile hızlanan teknoloji üretimi ve gelişen AR-GE kapasitesi, Türkiye'yi farklılaşan siber saldırıların odağına yerleştirecektir. Bu kapsamada özellikle son yıllarda meydana gelen bazı siber saldırıların ele alınması, siber savunma yöntemlerinin yeniden değerlendirilebilmesi için büyük arz etmektedir.

2.3. Göz Önünde Bulundurulması Gereken Önemli Siber Olaylar

Saldırı amaçları, çalışma şekilleri, bulaşma ve yayılma vektörleri açısından önümüzdeki dönemde ulusal siber güvenliğini doğrudan tehdit edebilecek nitelikteki bazı saldırılar bu bölümde özetlenmiştir.

Titanrain: 2003 yılında bir grup Çinli bilgisayar korsanlarının gerçekleştirdiği ve Çin'in hiçbir zaman arkasında olduğunu kabul etmediği Titan Rain olarak adlandırılan saldırılar gerçekleştirilmiştir [18]. Bu saldırılar bir tarama programının yaptığı zafiyet taraması sonrası, tespit edilen hedeflere birkaç gün sonra

saldırganların tekrar saldırarak değerli buldukları askeri, teknolojik ve lojistik her türlü bilgiyi elde etmeleri ile sonuçlanmıştır. Saldırılardan önemli devlet kurumları, silahlı kuvvetler karargâhları, bilgi işlem merkezleri, özel sektör önemli derecede etkilenirken, saldırılar sırasında iletişiminde kesilmesi sonucu kurumlar tam olarak ne gibi bir sorunla karşı karşıya olduklarını ancak saldırı bittikten sonra anlayabilmiştir. Yapılan saldırılar o anda sahip olunan güvenliğin yeterli olmadığını daha iyi bir güvenlik sağlayabilmek için farklı güvenlik anlayışları benimsenmesi gerektiğini ortaya çıkarmıştır.

Aurora: Çin kaynaklı veri hırsızlığı 2003 saldırısı ile sınırlı kalmamış, 2009 yılında bu sefer tamamen ABD'deki özel sektörü hedef alan ve Operation Aurora olarak adlandırılan saldırılar gerçekleştirilmiştir. Bu saldırılar sonrası büyük miktarda özel sektör ticari verisinin saldırganların eline geçtiği belirlenmiştir.

Stuxnet: Kaynağı ile ilgili pek çok tahmin yürütülse de, Stuxnet saldırısı kapalı ağlara yapılan ve aynı zamanda fiziksel hasar yaratabilen ilk saldırı olması sebebi ile oldukça ilgi çekicidir. Stuxnet'in çalınan Realtek firmasına ait elektronik imzayı kullanarak taşınabilir ortamdan sisteme sızabilmesi, yazılımın PLC (Programmable Logic Controller) yazılımlarını hedef alması, etkili olabilmesi için Siemens donanım ve yazılımında uzman kişilerden destek alınmış olması gerektiği göz önüne bulundurulduğunda bilişim üzerine farklı disiplinlerde bilgiye sahip bir ekip tarafından hazırlandığı tahmin edilmektedir. Stuxnet saldırısından özellikle dış ağlara bağlantısı olmadığı bilinen İran nükleer reaktörlerinin (Buşehr ve Natanz) etkilenmesi bu saldırıyı daha da ilgi çekici hale getirmektedir. Virüsün bir USB veri taşıma cihazı vasıtası ile bu reaktörlerde çalışan mühendis tarafından sisteme bulaştırıldığı değerlendirilmektedir. Endüstriyel casusluk ve endüstriyel sabotaj amaçlı geliştirildiği tahmin edilen Stuxnet virüsü, bulaştığı bilgisayarlar vasıtası ile endüstriyel kontrol otomasyon (SCADA, Supervisory Control and Data Acquisition) sisteminin kontrolünü ele geçirmekte, kodunu kopyalayarak elde etmekte ve bu kodu değiştirerek sensör ve sistem giriş çıkış değerlerini bozmaktır. Virüsün ne kadar etkili olabileceği bir örnekle anlatılmak istenirse; Isıl değeri $18C^{o}$ gördüğünde devreye girmesi gereken bir klimanın sensör eşik değerini $40C^{o}$ olarak değiştirerek soğutma sisteminin devreye girmesini engellemekte böylelikle cihazlara fiziksel zarar verebilmektedir [19].

DeOS (Petya ve WannaCry): Bir diğer ilgi çekici saldırı dalgası ise daha çok 2017 yılına damgasını vuran WannaCry (Mayıs 2017) ve Petya(Haziran 2017) adları ile isimlendirilen fidye yazılımlarıdır (Ransomware) [20]. Bu zararlı yazılımlar, bilgisayar

korsanları tarafından Nisan 2017'de sızdırılan National Security Agency'in (NSA) kullandığı Zero Day açıklarını kullanarak yayılmakta ve bulaştığı sistemdeki dosyaları şifreleyerek kullanılamaz hale getirmektedir. Yazılım akabinde kullanıcıdan şifreyi açarak dosyaların kurtarılmasını sağlamak üzere belirli bir fidye talep etmektedir. Petya zararlı yazılımını diğer fidye yazılımlarından farklı kılan asıl niteliği, ne yazılımın kullandığı Zero Day açıkları, ne dosya ve anahtar şifrelemede kullandığı 128 bit AES ve RSA algoritmaları, ne de sistemin her açılışında (boot edilmesinde) otomatik olarak çalışmak için ana yükleme kaydı (Master Boot Record-MBR) bölümüne yerleşmesidir. Yazılım fidye elde etmeyi hedeflemek ile birlikte, saldırının hemen ardından fidyeyi ödeme sürecinde kullanılan e-posta adresini sağlayan e-postanın sağlayıcısı Posteo e-posta adresini kapattığı için fidyeyi ödeyerek belirli bir şifre elde etmek mümkün değildir. Yani şifreli dosyaların geri getirilmesi imkânsızdır ve yazılım aslında bu yolla bulaştığı sistemi imha etmektedir. CISCO firmasının 2017 ilk altı aylık siber güvenlik raporunda, bu yazılımın daha sonra gelecek fidye yazılımı görünümlü imha tarzı saldırılara örnek teşkil edebileceğini [21], saldırganların sistem ve veri tabanı yedeklerini de hedef alma yeteneğine sahip olduğunu duyurmuş ve kullanıcıları bu konuda uyarmıştır [22].

2.4. Siber Riskleri Gidermek Üzere Alınması Gereken Önlem ve Öneriler

Sistemleri korumak üzere, geniş çaplı güvenlik çözümleri üretebilmek ve sistem zafiyetlerini doğru tespit edebilmek için yakın gelecekte karşı karşıya kalınabilecek tehdidi öngörebilmek gerekmektedir. Meydana gelen önemli saldırılar değerlendirildiğinde, ulusal boyutta etki yaratarak aynı anda birden çok sektörü etkileyerek, büyük hasar ve değerli veri kaybına sebep olabilecek bir siber saldırı, sosyal mühendislik sonucu kişisel verileri elde edilip banka hesap bilgileri ele geçirilen ve bu kanalla hesabından üçüncü şahıslara parası aktarılan Suna hanımın uğradığı zarar kadar veya Facebook profili çalındığı için eski okul arkadaşları ile sosyal ortamda paylaşım yapamayan emekli Veli amcanın uğrayacağı zarar kadar küçük çaplı olmayacaktır. Bu tip bir saldırı Türkiye'nin ilk nükleer santralinin SCADA sistemini etkileyerek bir nükleer sızıntı veya patlamaya sebep olmayı veya ilk üretimi yapılacak milli muharip uçağın yüksek güvenlik altında tutulmakta veya işlenmekte olan kaynak kodlarını ele geçirmeyi, hatta bu saldırılardan politik kazançlar elde etmeyi hedefleyecektir. Son

yıllarda öne çıkan başka bir vektör ise Nesnelerin İnternetinin(Internet of The Things/IoT) ve bulut bilişimin her geçen gün durdurulamaz şekilde artan genişleme eğilimi ve bu alandaki sistem zafiyetlerinin önümüzdeki dönem saldırıları için geniş bir hareket alanı bırakıyor olmasıdır. Özellikle bilgisayarların istenmeyen kişiler tarafından ele geçirilerek kullanıcının rızası dışında kullanımına izin veren Botnet ve DDoS saldırılarına imkân verecek zafiyetleri yazılımsal ve donanımsal niteliğinde barındırıyor olması, IoT güvenliği konusunda çalışmalar yapılması gerekliliğini ortaya çıkarmaktadır. Ulusal güvenliği sağlamak üzere sistem bir bütün olarak değerlendirilmeli ve en zayıf halkanın bütün bir sistemi riske atabileceği unutulmamalıdır. Sistemlerin güvenlik zafiyetlerini giderebilecek güçte ve aynı zamanda birbirleri ile uyum içerisinde çalışabilen mimari yapılar tasarlanmalıdır.

3. BLOKZİNCİRİNİN ÇALIŞMA PRENSİBİ VE SİSTEMİN GÜVENLİĞİ

Blokzinciri en basit tanımı ile üzerinde değiştirilemez kayıtların oluşturulduğu ve bu kayıtların birer kopyalarının P2P mimaride eşler arasında saklandığı bir kayıt defteridir. Bitcoin ve diğer kriptopara birimlerinin kullandığı temel alt yapıdır. İlk piyasaya çıktığında sadece kriptopara transferi için kullanılırken, 2014 yılı itibari ile blokların içerisine işlem yapabilen kodların gömülmeye başlanmasıyla akıllı anlaşmaları da gerçekleyebilir hale gelmiştir.

Blokzincirinin işlem akış şeması ve çalışması Şekil 3.1'de gösterildiği gibidir.

Şekil 3.1 *Blokzinciri Sisteminin Çalışma Prensibi*

Blokzincirinin ana işlem adımları aşağıda belirtildiği şekilde gerçekleşecektir:

İlk olarak babası bilgisayarından, Ela'nın bilgisayarına bir değer aktarma işlemi (transaction)yapar, bu gönderme(işlem) bilgisi Ela'nın bilgisayarı da dâhil P2P ağdaki diğer tüm eşlere yayımlanır. Eşler tarafından henüz doğrulanmayan gönderme, işlem havuzuna düşer. Ağda kullanılmakta olan protokol sonucunda işlem bilgisi, diğer n adet işlemle birlikte yeni bir bloğa yazımı süreci başlar, İşlem doğrulanarak, doğrulama bilgisi ağ içerisindeki tüm düğümlere iletilir. Madenci düğümü; bloğu blokzincirine

ekleme yetkisini almak ve ödülü hak etmek için değeri birkaç sıfır ile başlayan eşik değerini bulmaya çalışır. Bunun için hesaplama gücünü kullanır. Bu değeri bulan madenci, blok içerisindeki ödeme kaydı harçlarını (transaction fee) ve blok ödülünü (block reward) kazanır. Doğrulama bilgisinin tamamlandığı diğer düğümler tarafından teyit edilerek eşler arasında iletilir. Konsensüs protokolü ile seçilen madenci düğüm tarafından blok, bloğu oluşturan diğer işlemlerle birlikte hesaplanan özet değeri ile kapatılır ve son bloğa eklenerek blok zinciri tamamlanır. En son işlem adımında ise yeni blok eşler arasında yayımlanır ve süreç sonuçlanır.

Kısaca özetlemek gerekirse blokzinciri mimarisinde P2P ağda gerçekleştirilen tüm işlemler öncelikle bir blok oluşturacak şekilde sıraya alınmakta, bloğu tamamlayacak kadar işlem biriktiğinde, konsensüs(uzlaşma) protokolü ile seçilen madenci düğümü kriptografik özet algoritması kullanarak bloğu kapatmaktadır. Bu bloklar birbirlerine ardışık ve bindirmeli kriptografik işlemlerle bağlanarak kırılması imkânsız bir kripto zinciri oluşturmakta, veri bu zincir vasıtasıyla korunmaktadır. Yapılan işlemler merkezi bir otoritenin müdahalesi dışında gerçekleşirken kayıt defteri eşler arasında dağıtık olarak muhafaza edilerek sistemin güvenliği arttırılmaktadır.

3.1. Düğüm Tipleri

Blokzinciri sisteminde, maliyetleri düşürmek ve son kullanıcının makinesi üzerindeki verinin boyutunu en aza indirgemek için işlem bilgileri düğümlerde depolama ve işlem kapasiteleri göz önünde bulundurularak kademeli olarak depolanmaktadır. Düğüm tipleri ve görevleri Tablo 3.1'de örnek kullanım platformları belirtilerek açıklanmıştır.

Düğüm tipleri tüm blokzinciri mimarilerinde aynı özellik ve hiyerarşi ile sıralanmasına rağmen özellikle güvenlik ve mahremiyetin öne çıktığı mimari yapılarda farklı işlevler de kazanabilmektedirler. Bu duruma örnek olarak Hyperledger-Fabric blokzincir platformunda kullanılan Endorser Node yapıları ele alınabilir. Bu yapılarda tüm gönderme işlemi Yönetici düğüme gönderilerek işleme sokulmadan önce konsensüs protokolüne tabi tutularak taklit edilir. Akabinde eğer gönderme ile ilgili bir yetki sorunu veya herhangi bir teknik problem tespit edilmezse işlem başlatılmasına izin verilir. Endorsing işlemi bu yapısı ile Hyperledger-Fabricte ek güvenlik işlemi için kullanılır.

Tablo 3.1 *Farklı Tür Düğümlerin Örnek Kullanım Platformları* **[23]**

Düğüm Tipi	Örnekler	İşlevi
Tam Düğüm (Full Node)	Sunucular, yüksek miktarda depolama ve yüksek işlemci gücüne sahip bilgisayarlar.	Blokzincirinin tam kopyasını oluşturur, Blokları oluşturur, Blokları onaylar, Tüm kayıtları onaylar, Yeni kayıt oluşturur ve yayımlar.
Kısmi Düğüm (Partial/Half Node)	Dizüstü bilgisayarlar.	Blokzincirinin sadece başlık temelli kopyasını oluşturur, Yeni blokları onaylar, Yeni kayıtları onaylar, Eski kayıtları eş desteği olarak onaylar, Yeni kayıt oluşturur ve yayımlar.
Basit Düğüm (Simple/Node)	Tabletler, cep telefonları.	Yeni kayıtları onaylar, Yeni kayıt oluşturur ve yayımlar.

2. Kullanımda Olan Blokzinciri Tipleri ve Konsensüs Modelleri

Dijital değer aktarımı amacı ile ortaya atılarak, durdurulamaz bir ivme ile tüm dünyaya yayılmayı başaran blokzinciri uygulamaları; akıllı anlaşmaların ortaya çıkışı ile birlikte kullanıcılarına her türlü dijital varlığın güvenli bir şekilde paylaşılabildiği bir alt yapı sunmaya başlamıştır. Bu durum ise kullanım amacına uygun olarak farklı blokzinciri tiplerinin ortaya çıkmasına sebep olmuştur. Blokzinciri, kullanıcıların kaynaklara erişim ve değişiklik yapabilme yetkilendirmeleri göz önünde bulundurulduğunda üç başlık altında ele alınabilir. Bunlar sırasıyla:

- **Açık(Public) Blokzinciri:** Etherium ve bitcoini uygulama alanındaki örnekleri olarak tanımlayabileceğimiz, herkesin önceden belirlenen protokoller kapsamında sisteme dâhil olabildiği ve kayıt defterine erişim, değişiklik yapma ve görme yetkilerine sahip olabildiği kamusal sistemlerdir.

- **Özel(Private) Blokzinciri:** Önceden yapılan tanımlamalara göre ağ içerisinde otorite veya herhangi bir üyenin izni olmadan yeni kullanıcıların kayıt defterine

erişimine, değişiklik yapmasına veya görmesine izin verilmediği veya sistemdeki kullanıcılara otorite tarafından gerekli iznin gerekli olduğu kadar verilebildiği, farklı kullanıcılara farklı yetki seviyelerinin atanabildiği sistemlerdir.

- **Melez(Hybrid) Blokzinciri:** Mimaride ihtiyaç duyulacak modele göre, gerekli görüldüğünde, yapılan tanımlamalara göre ağ içerisinde otorite veya herhangi bir üyenin izni olmadan yeni kullanıcıların kayıt defterine erişimine, değişiklik yapmasına veya görmesine izin verilmediği, özel ve açık tip blokzinciri yapılarının her ikisinin de özelliklerini barındıran fakat tam güvenliğin ve tüm mahremiyetin hedeflenmediği sistemlerdir.

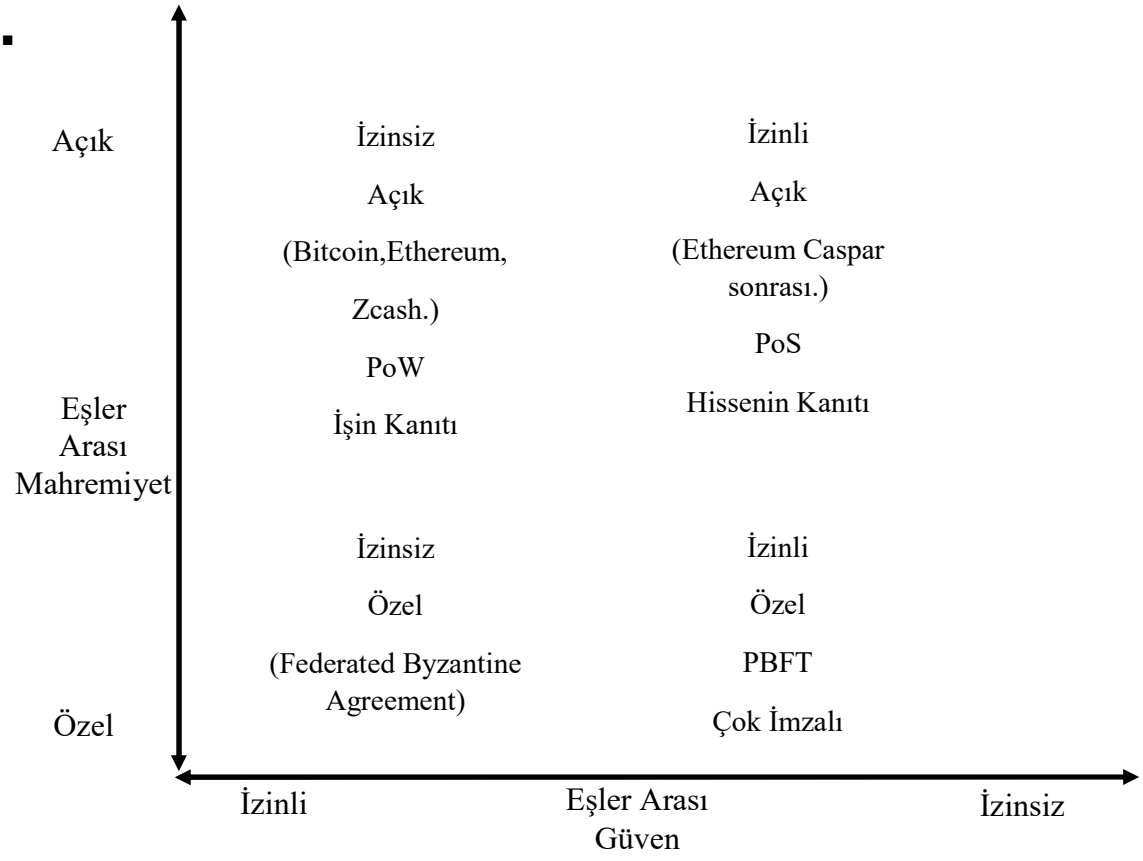
Blokzinciri kullanılarak oluşturulacak bir siber güvenlik modelinde, modeli doğru oluşturabilmek için doğru konsensüs protokolünün ele alınıyor olması önem arz etmektedir. Değişikliklerin hangi düğüm tarafından yapılacağı konsensüs protokolleri tarafından belirlenir. Yaygın olarak kullanılan konsensüs protokollerinden işin kanıtı(PoW) bir düğümün ağdaki işlemi veya işlemleri doğrulayabilmek için matematiksel bir problemi çözerek diğer düğümlere kendilerini kanıtlaması, hissenin kanıtı(PoS) ise bir düğümün ağdaki işlemi veya işlemleri doğrulayabilme hakkını, sahip olduğu hisse ile elde etmesi işlemidir. İşin Kanıtı (PoW) ve Hissenin Kanıtı (PoS) modellerinin yanında, Geçen Zamanın Kanıtı (PoET Proof of Elapsed Time), Uygulamalı Bizans Hata Toleransı (Practical Byzantine Fault Tolerance) protokolü, SIEVE protokolü, Çapraz Hata Toleransı (Cross-Fault Tolerance, XFT), Federe Bizans Anlaşması(Federated Byzantine Agreement) blokzinciri mimarilerinde kullanılmakta olan en popüler konsensus modelleri olarak nitelendirilebilirler. Bu konsensüs protokollerini kısaca aşağıda olduğu gibi açıklamak mümkündür:

- **Geçen Zamanın Kanıtı (PoET, Proof of Elapsed Time):** En kısa bekleme zamanına sahip olan düğümün lider seçilmesi ile gerçeklenen konsensüs protokolüdür. SawtoothLake(Bir açık kaynak blokzinciri platformu) uygulama alanında bu protokole örnek olarak gösterilebilir.

- **Uygulamalı Bizans Hata Toleransı (PFT, Practical Byzantine Fault Tolerance):** En popüler özel(permissioned) blokzincir konsensüs protokolüdür. Hyperledger Fabric tarafından Kullnılmaktadır. Chain-code adı verilen akıllı

anlaşmaları desteklemektedir.

- **SIEVE:** Hyperledger Fabric'de, PBFT ile birlikte kullanılarak hatasız çıktılar elde etmeyi hedefleyen konsensüs protokolüdür.
- **Çapraz Hata Toleransı (Cross-Fault Tolerance, XFT):** Bu protokol Bizans Hata toleransını aktif kullanıma yönelik olarak kabul edilebilir seviyeye indirmeyi amaçlayarak BFT'de tam olarak başarılamayan uygulamaları gerçeklemeyi amaçlar.
- **Federe Bizans Anlaşması(Federated Byzantine Agreement):** Açık-izinsiz (Public-Permission-less) blokzinciri modellerini gerçekleyen bir BFT konsensüs modeli versiyonudur. Ripple ve Stellar bu protokolün hayata geçirildiği kripto para birimleri arasında sayılabilirler. Şekil 3.2'de de görüldüğü üzere blokzinciri modellerinde mahremiyet açık mimari yapıdaki blokzincir modellerinde artarken, eşler arasında duyulan güven de izinli blokzinciri mimarilerinde daha çok artmaktadır.
-



Şekil 3.2 *Blokzinciri Mimarilerinde Mahremiyet Güven İlişkisi*

3.3. Blokzincirinin Güvenliği

Blokzincirinde eşler arasında bir bilgi bloğunun varlığını ve doğruluğunu kanıtlamak için bloğun parmak izi niteliğindeki özet değeri kullanılır. Kriptografik özet fonksiyonları tek yönlüdür. Aldıkları girdinin boyutundan bağımsız olarak sonuçta uzunluğu belirli sabit (fonksiyona göre değer boyutu değişir) bir değer üretirler, fakat ürettikleri değerden girdinin geri elde edilmesi teorik olarak mümkün değildir. Bu sebeple kriptografik özet fonksiyonlarının çıktısı özet değeri, dijital parmak izi, sonuç toplamı veya mesaj özeti olarak adlandırılır. Farklı kripto para birimleri farklı tip özet fonksiyon algoritmaları kullanabilmektedir [24]. Blokzinciri görüldüğü üzere Bitcoin veya diğer herhangi bir kripto para birimi değildir, aksine kriptopara ve akıllı sözleşme(smart contract) gibi uygulamaların üzerinde gerçekleştirildiği bir güvenlik protokolüdür.

Blokzinciri yardımı ile gerçekleştirmeyi planladığımız proje ve uygulamanın birden fazla tarafça kullanılacak olması, verinin taraflar arasında paylaşılıyor olması, tarafların birbirine güven duymuyor olması, denetlenebilir, değiştirilemez ve silinemez kayıtlara ihtiyaç duyuyor olması gerekir. Bunun sonucunda blokzinciri mimarisi ile geliştirilecek proje veya uygulamanın, tam güveni, tüm mahremiyeti, aracı otorite veya kurumun ortadan kaldırılmasını, işlemlerin merkezi olmayan sistem yapısı ile protokoller vasıtası ile eşler arasında(Peer to Peer/P2P) gerçekleştirilmesini sağlaması hedeflenir.

3.4. Blokzincirinin Sağladığı Güvenlik Servisleri:

Blokzinciri temelde tam güvensizlik ortamı içerisinde, eşler arası ağda teşkil edilen bir protokol hiyerarşisi sayesinde birbirine güvenen eşler yaratmak üzere yapılandırılmıştır. Sistem güvenlik ihtiyaçları çok bilinen “CIA“, gizlilik (Confidentiality), bütünlük (Integrity) ve erişilebilirlik (Availability) maddeleri üzerinden, alt maddelerle genişleterek ele alındığında ve bu mimaride güvenlik servislerini sağlanma durumu değerlendirildiğinde sonuçlar, Tablo 3.2’de olduğu gibidir.

Blokzinciri mimarisinde kayıtlar değiştirilemez, eşler arası yapıda kayıt defterinin bir örneğinin kısmen veya tamamen her bir eşin yerel hafızalarında da tutuluyor olmasından dolayı sistem çökmeye karşı yüksek korumalıdır. Kriptografik şifreleme ile

güvenlik sağlanırken, dağıtık mimari yapısı ile taraflar arasında tam güven tesis edilir. Bu yapıda eşlerin izni olmadan yetki dışı işlem gerçekleştirilemez [25].

Tablo 3.2 *Blokzincirinin Güvenlik Servislerini Karşılanma Durumu*

Güvenlik Servisleri	**Blokzinciri Mimarisinde Karşılanma Durumu**
Gizlilik	Bilgiye sadece yetkili kişilerin erişimine izin verilmesidir, bu unsur uygulamaya göre değişiklik göstermekle birlikte blokzincirinde simetrik kriptolama ile sağlanmaktadır.
Bütünlük	Yetkilendirilmemiş veri değişimlerine izin verilmemesidir. Blokzincirinde özet fonksiyonları (Hash) kullanılarak bütünlük sağlanır.
Erişilebilirlik	Bilginin sürekli ulaşılabilir ve kullanılabilir olmasıdır. Dağıtık ve eşler arası mimaride verinin kısmi veya tam kopyası her bir düğümde tarafından tutulabilir. Böylece bir veya birden fazla düğümün bağlantısı kesilse bile bilgi akışı diğer eşler üzerinden devam edecektir.
Kimlik Denetimi	Dağıtık kayıt defteri ve blokzincirinde kullanılan anahtarlar vasıtası ile gerçekleştirilir.
Kullanıcı Kontrolü ve Ağdaki Bilginin Doğruluğunun Teyidi	İşlem yapmak isteyen kullanıcının gerçekten iddia edilen kullanıcı olduğunun ve işlemin doğruluğunun teyididir. Özet fonksiyonları ve dağıtık kayıt defteri ile sağlanır.
Denetlenebilirlik	Kayıtların değiştirilemezliği sayesinde gerçekleştirilen işlemler sonradan denetlenebilir.
İnkâr Edilemezlik	Kayıtların değiştirilemezliği sayesinde yapılan işlemler sonradan inkâr edilemez.

4. İLGİLİ ÇALIŞMALAR

Blokzinciri ve siber güvenlik üzerine yapılan çalışmalar incelendiğinde, bu çalışmalardan bazılarının ulusal siber güvenliği teşkil edebilecek modelleri destekleyebilecek nitelikte olduğu tespit edilmektedir. Çalışmalar genel olarak son yıllarda ortaya çıkan siber güvenlik gereksinimlerine paralel olarak, nesnelerin interneti ve bulut bilişim teknolojilerine yoğunlaşmaktadır [26]. Özellikle blokzinciri teknolojisi ile ağ üzerinde defteri kebir/kayıt defteri mantığı ile tutulan değiştirilemez kayıtlar sayesinde, her türlü dosya ve dokümana erişim yetkisinin tanımlanması, erişimin kontrolünün sağlanması ve bu erişimlerin silinmesi mümkün olmayan kayıtlarının oluşturulması hedeflenmiştir. Sınır güvenliği temelli mimariler yerine kullanılabilecek güvenli, dağınık mimari yapıları oluşturma ve internet isim sunucularının(DNS) dolayısı ile internetin bu mimaride yeniden değerlendirilmesini amaçlayan çalışmalarda doğrudan ulusal siber güvenlik mimarileri oluşturabilecek nitelikte konulara değinilmiştir.

4.1. Blokzinciri İle Genel Siber Güvenliğin Sağlanması

Özellikle blokzincirinin siber güvenlik üzerine getireceği çözümlere odaklanılan çalışmalar incelenerek, iki başlık altında kategorize edilmiş ve elde edilmek istenen modele yol haritası çizilmeye çalışılmıştır. Blokzinciri kullanılarak gerçekleştirilmesi hedeflenen, belirlenmiş problem sahaları bazında siber güvenlik çözümleri üretilmesine yönelik çalışmalar Tablo 4.1'de, uygulama alanı bazında siber güvenlik çözümleri üretilmesine yönelik çalışmalarda ise Tablo 4.2'de özetlenmiştir. Bu çalışmalar arasında; özellikle Copos ve arkadaşları ile Gaetani ve arkadaşlarının bulut teknolojisinde blokzinciri kullanımı üzerine gerçekleştirdikleri çalışmalar, Jamsrandorj ve arkadaşlarının dağıtık veri tabanında blokzinciri temelli veri erişim modeli ile ilgili yaptıkları çalışma Ramachandran ve Kantarcioglu'nun akıllı kaynak yönetimi ile ilgili yaptığı çalışma, Li ve arkadaşlarının büyük verinin kontrol ve güvenliğini blokzinciri kullanarak sağlamayı hedefledikleri çalışma ve Karaarslan ve Adıgüzel ile Dickson'un blokzinciri mimarisi kullanarak tasarladıkları güvenli DNS modelini içeren çalışmaları, ulusal anlamda siber güvenliği destekleyebilecek başlıca çalışmalar olabileceği değerlendirilmektedir. Bu çalışmalar blokzinciri ve siber güvenlik konularında gelecekte yapılacak çalışmalarda referans olabilecek niteliktedirler.

Tablo 4.1 *Veri Dosya Yönetimi ve Diğer Çözümlere Yönelik Çalışmalar*

Uygulama Alanı	Referans Numarası	Çalışmanın Konusu
IoT	[8]	Blokzinciri mimarisini nesnelerin interneti güvenlik ihtiyaçlarına göre yeniden yapılandırılarak "Light Weight Scalable BC" adı altında tekrar tasarlamış, karmaşık konsensüs algoritması daha basit hale getirilerek işlem adımlarının hızlandırılması hedeflenmiştir.
	[27]	Blokzinciri mimarilerinin nesnelerin interneti üzerinde kullanılması durumunda yaşanabilecek sorunlar göz önünde bulundurularak bir melez blokzinciri topolojisi önerilmiştir.
	[28]	Akıllı evler için tasarlanmış bir ağ geçidi olan GHOST araştırma projesinin tanıtımı yapılmış, GHOST projesinde savunma mimarisi olarak blokzinciri ve akıllı anlaşmalar kullanılmakta bununla, sertifikasyon, güvenlik, eşler arası güven, kimlik doğrulama ve mahremiyet ile sorunlara çözüm üretilmektedir.
	[29]	Blokzincirinin nesnelerin internetinin hangi zafiyetlerine çözüm üretebileceği analiz edilmiş, klasik bulut teknolojisi ile Blokzinciri arasındaki farkların, avantaj ve dezavantajların değerlendirmesi yapılmıştır.
	[30]	Yakın gelecekte edge computing, yapay zekâ ve nesnelerin interneti teknolojilerindeki gelişmelerin siber güvenlik ihtiyaçlarına yön vereceğine değinilmiş, blokzinciri ise bu zafiyetleri giderebilecek mimari yapı olarak ele alınmıştır.
	[31]	Makineler arası haberleşmeyi sağlamak üzere blokzinciri mimarisi kullanan projelere yönelik genel bir inceleme yapılmıştır.
	[32]	IoT cihazlarında mahremiyet merkezli güvenlik problemi ele alınmış, bu soruna çözüm üretmek için yazılım tabanlı ağ (SDN) üzerinde bir geniş alan ağı tasarlanmış ve güvenliği sağlamak üzere blokzinciri mimarisinin kullanılması planlanmıştır.
Veri-Dosya Yönetimi	[33]	Bir dijital veri kaynak sistemi modelleyerek blokzinciri tabanlı bir veri yönetim ve takip oluşturulmuş, veri üzerinde yapılan her değişikliğin kullanıcı bazında kayıt altına alarak denetlenebilirliğinin sağlanması hedeflenmiştir.
	[34]	Blokzinciri tabanlı bir dağıtık veri erişim sistemi tasarlanarak veri üzerinde beraber iş birliği içerisinde çalışmak zorunda olan taraflar arasında güvenin sağlanması hedeflenmiştir.
Bulut Bilişim	[35]	Bir Avrupa Birliği projesi olan SUNFISH bulut bilişim veri tabanında, veri bütünlüğünün blokzinciri ile sağlandığı bir model üzerinde durulmuştur.
	[36]	Bulut ortamında şifrelenen bilgiler üzerinde arama işleminin eşit yetkiler ile yapılabilmesi ve bilgilerin adil erişiminin sağlanması için blokzinciri tabanlı bir model üzerinde durulmuştur.
Büyük Veri	[37]	Büyük verinin kontrol ve güvenliğini blokzinciri kullanarak sağlamak üzerine bir çalışma yapmışlar ve değerlendirmelerde bulunmuşlardır.
Makineler Arası Haberleşme	[38]	Blokzinciri, siber fiziksel sistemler ve makineler arası haberleşmede güvenliğin sağlanabilmesi için kullanılabilecek mimari yapı olarak ele alınmıştır.
	[39]	Siber fiziksel sistemlerin zafiyetlerin den bahsedilmiş, blokzinciri ile çok kuvvetli sistem mimarileri tasarlanabileceğine, herhangi bir ağa bağlı olmayan sistemlerde dahi yeterli seviyede güvenliğin sağlanabileceğine değinilmiştir.

Tablo 4.2 *Uygulama Alanı Bazında Üretilen Siber Güvenlik Çalışmaları*

Uygulama Alanı	Referans Numarası	Çalışmanın Konusu
Ulusal Siber Güvenlik	[23]	Blokzincirinin siber güvenlikte kullanımı üzerinde durulmuş, IoT, DNS sunucuları, akıllı şehirler, kişisel verilerin korunmasında nasıl kullanılabileceğine değinilmiştir.
	[40]	Blokzinciri kullanılarak ulusal güvenlik için kullanım alanlarının araştırılması gerektiğine değinilmiş, bu kapsamda blokzinciri düğüm yapısını hava kuvvetleri harekât merkezleri, hava savunma unsurları, uçan platformlar ve son kullanıcı cihazları üzerinde örneklenmiştir.
	[41]	Blokzincirinin ağ üzerinde sağlayacağı güvenlik hava kuvvetleri silah sistemleri ve komuta kontrol sistemleri üzerinde ele alınarak, gelecekte üretilecek teknolojilere blokzincirinin hangi konularda uygulanabileceği konusunda değerlendirmelerde bulunulmuştur.
	[42]	Ulusal güvenlik modelinin gerçeklenebilmesi için blokzinciri tabanlı güvenlik mimarisi ile desteklenen kimlik ve giriş yönetimi modeli üzerinde durulmuştur.
Siber Güvenliğin Sağlanması Üzerine Genel Konular	[43]	Blokzincirinin sağladığı faydalar ve güvenlikteki uygulama alanları listelenmiş, finansal servisler, akıllı varlıklar, IoT, akıllı sağlık yönetimi, akıllı devlet uygulamaları başlıkları altında detaylandırılmıştır.
	[44]	Blokzincirinin güvenlik servislerine değinilmiş, gizlilik dereceli evrakın ifşasını önleme amaçlı kullanımı, e-oylama, sayısal kimlik, IoT güvenliği ve sistem güvenliği üzerine değerlendirmelerde bulunulmuştur.
DDoS Saldırılarının Engellenmesi	[45]	Guardtime şirketinin blokzinciri alanındaki güvenlikle ilgili çalışmalarına değinilmiş, blokzinciri DDoS saldırıları ve internet üzerindeki çeşitli güvenlik açıklarına karşı gelecek vaat eden bir model olarak nitelendirilmiştir.
	[46]	2016'da meydana gelen DDoS saldırıları örneklenerek kişisel güvenliğin sağlanması için mevcut yöntemlerin dışında blokzinciri teknolojisinin kullanılabilirliğine değinilmiştir.
E-Devlet Uygulamaları	[47]	Blokzincirinin e-devlet işlemlerinde kullanılabilirliğine değinilmiş, bu alanda hedef kullanım alanlarını tespit edilerek, blokzincirinin bu kullanım alanlarında sağlayacağı fayda ve güvenlik çözümleri listelenmiştir.
	[48]	Blokzincirinin e-devlet uygulamalarındaki kullanım alanları değerlendirilerek, farklı veri tabanı modellerinde elde edilecek kullanım kolaylıkları karşılaştırılmıştır.
DNS Güvenliği	[49]	DNS mimarisinin zafiyetlerine değinilmiş, blokzinciri tabanlı özgür, dağıtık ve güven temelli bir internet mimarisinin sağlanabilirliği üzerinde durulmuştur.
	[50]	Akıllı anlaşma kullanan DNS projesi Nebulis blokzinciri tabanlı bir DNS çözümü olarak örneklendirilmiştir.
Güvenli Mesajlaşma	[51]	DARPA'nın blokzinciri tabanlı değiştirilemez ve güvenlik bir mesajlaşma sistemi çalışmaları üzerinde durulmuştur.
Veri Kaynak Yönetimi	[52]	Ethereum tabanlı akıllı anlaşmalar vasıtası ile bir veri kaynağı yönetim sistemi (Smart Data Provenence System) modellemiştir.

5. ULUSAL GÜVENLİK İÇİN BLOZİNCİRİ

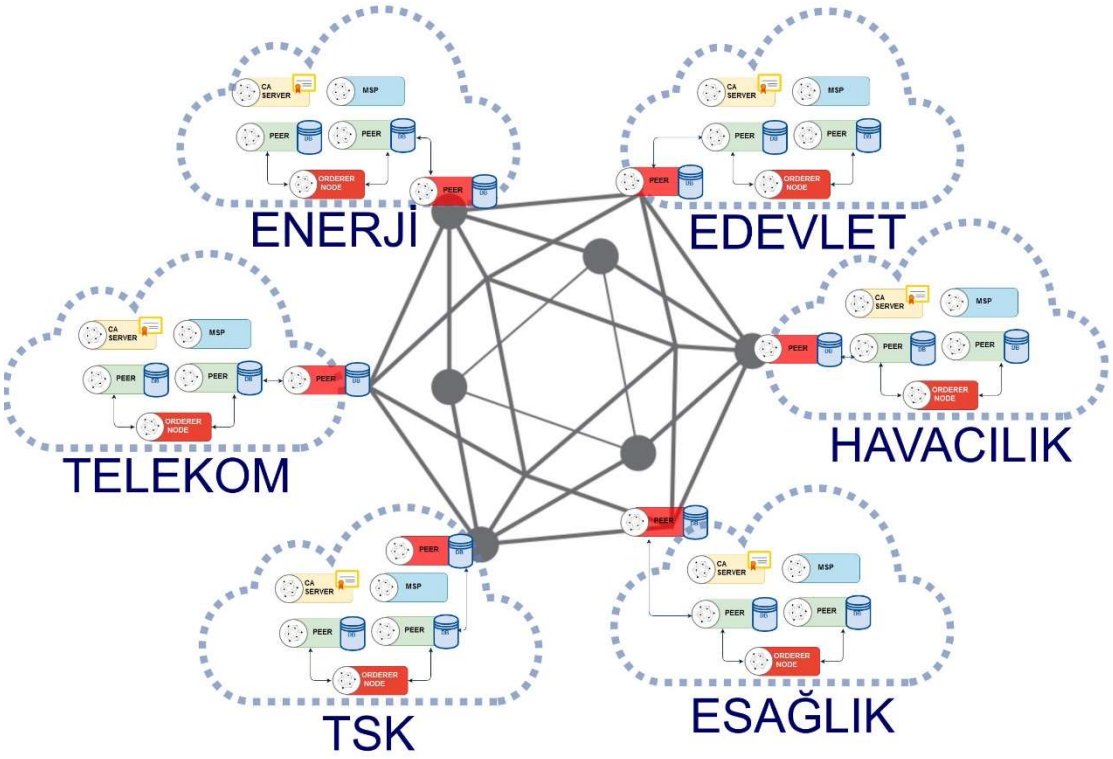
Ulusal siber güvenlik, ulusal ağı oluşturan yazılımsal ve donanımsal teknolojiler ile bu teknolojiler vasıtasıyla sağlanan hizmetlerin güvenliğine verilen isimdir. Özellikle son yıllarda siber güvenlik, ülkelerin kendi bilgi hazinelerini koruyabilmeleri ve riskleri en aza indirebilmeleri için en çok önem verdikleri ulusal güvenlik sorunu haline gelmiştir. Siber güvenlik, Uluslararası Telekomünikasyon Birliği (ITU), Avrupa Güvenlik ve İşbirliği Teşkilatı (OSCE), Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) gibi büyük kuruluşların da en önemli gündem maddesidir. Bu teşkilatlar tarafından yapılan çalışmalarda katılımcı ülkeler, siber risklerin azaltılmasını sağlamak üzere yönlendirilmekte, uluslararası platformlarda siber farkında lığın arttırılması hedeflenmektedir.

Son yıllarda siber güvenlik üzerine yürütülen çalışmalar, özellikle iki önemli konu üzerinde yoğunlaşmaktadır. Bunlardan birincisi, kritik altyapılar olarak adlandırılan, ülkelerin kritik tesislerinin haberleşme ve bilgi sistemleri ihtiyaçlarını karşılayan, yüksek öneme haiz bilgi ve iletişim altyapılarıdır. Bu altyapılar, gizliliği bütünlüğü ve ulaşılabilirliği ihlal edildiğinde; can kaybı, büyük ölçekli ekonomik buhranlar, güvenlik sorunları ve kamu düzeninin bozulmasına yol açabilecek nitelikteki altyapılardan. Diğer önemli konu ise, ağ üzerinde işlenen, ele geçirildiği takdirde değer kazandırılabilecek veya saldırgana amacı doğrultusunda hizmet edebilecek her türlü sayısal verilerinin güvenliğinin sağlanmasıdır. Üzerinde bu nitelikte yüksek miktarda bilginin işlendiği İnternet de, 2011 yılında Avrupa Birliği tarafından kritik altyapı statüsüne alınmıştır.

Blokzinciri kullanılarak çok çeşitli kritik bilginin güvenliğini tesis edebilmek mümkündür. Bu çalışmada bu kapsamda üretilecek alt modellere örnek teşkil edecek bir model hazırlanmış, bu model çerçevesinde bir alt model oluşturularak uygulaması yapılmış ve örneklendirilmiştir. Bu örneklendirme ve modelin gerçeklemesini sağlamak üzere Hyperledger-Fabric tercih edilmiş, yazılan kod yine bir Hyperledger alt programı olan Hyperledger Composer Playground'da denenerek simule edilmiştir. Diğer uygulamalara model olarak tasarlanan örnek model Şekil 5.1'de gösterildiği gibidir.

5.1. Blokzinciri İle Güvenliği Arttırılabilecek Ulusal Altyapılar

Blokzinciri teknolojisinin ulusal güvenlik alanında nasıl kullanılabileceği değerlendirildiğinde; öncelikle temel nitelikleri olan akıllı anlaşmaların, değiştirilemez kayıt



Şekil 5.1 Tasarlanan Blokzinciri Siber Güvenlik Modeli

defterinin ve dağıtık mimari yapısının ulusal güvenliğin sağlanmasına getireceği faydalar ele alınmalıdır. Bu kapsamda blokzincirinin ulusal güvenliği desteklemek üzere kullanılabileceği ulusal kritik altyapılar Tablo 5.1'de sunulmuştur.

Oluşturulacak değiştirilemez dosya ve klasör yetkilendirmeleri; bulut ortamında, sunucular üzerinde, web tabanlı uygulamalarda ve işletim sistemini oluşturulan dosya kütüklerinde tam kontrolü elde etmemizi sağlayacaktır. Bu sayede işletim sistemindeki yazılım ve dosya dizinleri ile kayıt dizinindeki(registry) değişiklikler, özet değerleri karşılaştırılarak tespit edilebilecektir. Böylece herhangi bir zararlı yazılımının dosya yapısını değiştirerek sistemi etkilemesi de engellenebilecektir. Sistem üzerinde yaratılan gizlilik dereceli dosyanın kimin tarafından yaratıldığı, değişikliklerin kimin tarafından yapıldığı bilgisi silinmesi mümkün olmayan şekilde kayıt altına alınabilecektir. Bu durum özellikle güvenliği sağlarken bir yandan da inkâr edilemez ve denetlenebilir veri yapıları oluşturabilmemize imkân sağlayacaktır. Dağıtık mimari üzerinde bu yapının oluşturulabiliyor olması ise tek bir sunucudan hizmet alan mimarilerin aksine, devamlı erişilebilirliği mümkün kılacaktır. Blokzincirinin bu güvenlik yeteneklerini e-devlet uygulamalarında, IoT, ağ anahtarlama cihazlarında, bilgi sistem yan donanımlarında, bankacılıkta, bulut iletişim üzerinde uygulamak mümkündür.

P2P uygulamalarında dosya sunucularının yerine konsensüs protokolleri kullanarak kontrol ve güvenlik mekanizmasını tesis edebilen P2P sunucu mimarileri oluşturulabilir. Böylece siber saldırı veya doğal afet vb. durumunda sunuculardaoluşan erişilebilirlik problemlerine çözüm üretilebilir. İletişim altyapısına saldırı yapıldığında dahi iletişimin devamını sağlayabilen sunucu sistemleri ve altyapılar tesis edilebilir.

Büyük çaplı bir siber saldırıda, saldırıya uğrayanlardan elde edilecek ilk veri, saldırının doğru tespiti ve bertaraf edilebilmesini sağlayacak en önemli kaynaktır. Oysa ki saldırıya uğrayanlar saldırı sonucunda kayba uğradıklarını paylaşmayabilir, veya gerçekten saldırıya uğradığını fark etmeyebilir. Blokzinciri kullanılarak birbiri ile siber saldırı verilerini açıkça paylaşabilen eşler yaratılabilir, böylece işbirlikçi saldırı destek sistemleri tesis edilebilir.

Blokzinciri, ağ trafik izlerinin denetlenebilir şekilde güvenle saklanması sorununa da etkili bir çözüm yöntemi olarak düşünülebilir. Kritik Altyapılara hizmet veren Dağıtık ve kompleks yapısı ile yüksek risk grubunda olduğu değerlendirilen SCADA sistemleri blokzinciri mimarisi ile daha güvenli hale getirilebilir [53], sistem üzerinde yetkilendirme ve kayıt mekanizmaları tesis edilebilir, kritik kontrol elemanlarına değiştirilemez eşik değerleri tanımlanarak sistemlerin daha güvenli çalışması sağlanabilir.

Blokzinciri ile kullanılmakta olan merkezi sunucu sistemleri ile yapılandırılmış DNS mimarisi yerine, dağıtık yapıda blokzinciri tabanlı DNS mimarisine geçilmesi mümkündür. Bu sayede DNS bilgisinin daha güvenli dağıtımı sağlanırken, DNS zehirlenmesi tipi ataklara, sunucuların herhangi bir afet durumunda veya siber atak (DDoS, DeOS vb.) karşısında servisten düşmesi problemine çözüm üretilebilir.

5.2. Blokzincirinin Kullanılabileceği Askeri Silah ve Haberleşme Sistemleri

Siber güvenliğin ulusal güvenliği sağlamak üzere tesis edilmek zorunda olduğu diğer bir alan ise askeri silah sistemleri ve bu sistemlerin haberleşme altyapısını sağlayan taktik data link [54] ve taktik haberleşme sistemleridir. Blokzincirinin kullanılabileceği askeri silah sistemleri, taktik haberleşme ve link sistemleri Tablo 5.2'de sunulmuştur.

Savaş sistemleri teknolojik gelişmelere paralel olarak her geçen gün yeni yetenekler kazanmakta, otonom sistemler haline dönüşmektedir. Günümüzde savaş sahasında yerini çoktan almış olan insansız araçlar ve akıllı silah sistemleri için en büyük risk, silah sisteminin düşman tarafından ele geçirilmesidir.

Tablo 5.1 *Blokzincirinin Kullanılabileceği Ulusal Kritik Altyapılar*

Altyapılar	Hedef
Ulusal İnternet	Merkezi DNS sunucuları yerine blokzincir tabanlı DNS mimarileri teşkil edilerek DNS'in ve Ulusal İnternet'in güvenliğinin sağlaması, E-devlet uygulamalarının çalıştığı bulut ve web tabanlı sistemler ile sunucularının yetkilendirme kontrolü ve güvenliğinin sağlanması, Bankacılık ve finans sektöründe sunucular ve web tabanlı uygulamalarda yetkilendirme kontrolü ve işlenen değerli verilerinin güvenliğinin sağlanması,
Ulusal Kritik Altyapılar	Ağ trafik izlerinin sonradan denetlenebilirliğinin ve inkar edilemezliğinin sağlanması, IoT, ağ anahtarlama cihazları, ve bilgi sistem yan donanımlarının güvenliği, Blokzincir tabanlı işbirlikçi saldırı tespit sistemi mimarileri, Blokzincir tabanlı elektronik imza ve IP kripto sistemi anahtar dağıtım sistemi uygulaması, Blokzincir tabanlı SCADA Sistemi yetkilendirme kontrol yönetimi ve güvenliğinin sağlanmasına yönelik uygulamalar, Merkezi mimaride konuşlandırılmış dosya sunucuları yerine blokzincir tabanlı güvenliği arttırılmış P2P dosya sunucu mimarileri.

Blokzinciri teknolojisi bu alanda da gelecek vaat eden mimari çözümler sunmaya adaydır. İnsansız hava araçlarına gönderilen komutlar blokzinciri yapısında tutulabilir, bu yapıda tesis edilen link sistemi sayesinde kimlik denetleme (authentication) yer istasyonu ve diğer insansız araçlar arasında güvenli bir haberleşme sistemi tesis edilebilir. İnsansız araçların ve sürü sistemlerin komuta ve kontrolü [55], blokzinciri ile güvenliği sağlanmış merkezi yer istasyonu üzerinden veya dağıtık yapıda çalışan, yapay zekâ destekli otonom sistemler ile sağlanabilir. Görev emirlerindeki değişiklikler uçuş esnasında pilotlara blokzinciri tabanlı sistemlerle daha güvenli yayımlanabilir. Atılan akıllı mühimmatın hedef ve vuruş noktası değişikliği, mühimmat hedefe varmadan önce, atıldıktan sonra dahi güvenli bir şekilde, anlık olarak pilot veya yer kontrol istasyonu tarafından yapılabilir. Uçakların tüm bakım ve lojistik süreçlerinin silinemez kayıtları oluşturulabilir, silah sistemlerinde kullanılan ve uçaklara yüklenen mühimmatların tüm süreçlerinin takibi, daha sonradan kanıtlanabilir ve denetlenebilir

Tablo 5.2 *Blokzincirinin Kullanılabileceği Silah Ve Taktik Haberleşme Sistemleri*

Altyapılar	Hedef
Askeri Link Sistemleri ve Taktik Haberleşme	Askeri link sistemlerine erişimde yaşanabilecek problemlere eşler arasında çözüm üretilmesi ve güvenliğinin sağlanması, Görev emirlerindeki değişikliklerin uçuş esnasında pilotlara daha güvenli yayımlanması, Radar iz bilgilerinin harekat merkezleri ve diğer radarlara aktarımlarının güvenliği,
İnsansız hava araçları	İnsansız hava araçlarına gönderilen komutların değiştirilmesinin engellenmesi, Sürü sistemlerin kontrolünde dağıtık ve/veya merkezi otonom kontrol mekanizmalarının tesisinde kusursuz ve güvenli altyapıların kurulması, İnsansız hava aracının merkez ile bağlantısı kesilse dahi en yakın aktif cihazdan güncel verileri alarak harekata devam edebilmesi,
Silah Lojistik Takip Süreci	Uçaklara yüklenen mühimmatların tüm süreçlerinin takibinde, kayıtların silinemeyecek, kanıtlanabilir ve kontrol edilebilir nitelikte olması,

nitelikte süreçlerinin takibi, daha sonradan kanıtlanabilir ve denetlenebilir nitelikte blokzincirinde saklanabilir. Blokzinciri tabanlı bir model ile tüm bu uygulamaları güvenli bir şekilde tesis etmek mümkün olacaktır.

6. UYGULANAN BLOKZİNCİRİ MODELİ

Ulusal güvenliğe yönelik yaşanmakta olan problem sahaları ve blokzinciri ile çözüm üretilmesi hedeflenen sahalar göz önünde bulundurulduğunda mimarisi oluşturulacak blokzincirinin:

- Tam kontrol edilebilir bir yapıya sahip olması,

- Değiştirilemez olması,
- Belli uygulama alanlarında şeffaflığa izin verilebilirken özellikli bilginin işlendiği alanlarda gizlilikten taviz vermemesi,
- Gizliliğin sağlanması,
- Veri bütünlüğünün sağlanabiliyor olması,
- Siber saldırılara karşı dayanıklı bir mimariye sahip olması,
- İç ağdan ve sistemden gelebilecek saldırı ve hatalara karşıda sistemi koruyabiliyor olması,
- Tek merkezli sunucu mimarilerinin aksine doğal afetlere afetlerde ve fiziksel yazılımsal çökme durumlarında sürdürülebilir niteliğe sahip olması,
- Diğer blokzincir yapıları ile karşılaştırıldığında işletme maliyetlerinin ve enerji sarfiyatlarının düşük ve kabul edilebilir seviyelerde olması,
- Verimliliğinin yüksek olması,
- Denetlenebilir ve inkâr edilemez olması,
- Bilgiye erişimin hılı ve güvenli bir şekilde gerçeklenebilmesi,
- İnsan hatalarını azaltması gerekmektedir.

Bu kapsamda tespit edilen modelin dağıtık ve yönetilebilir yapıda bir blokzinciri mimarisine sahip olması öngörülmüştür. Akıllı anlaşmalar yolu ile bu tarz uygulamaların farklı blokzincir platformlarında gerçekleştirilmesi mümkündür. Linux Faundation tarafından desteklenerek, yönetilebilir dağıtık mimari modelleri ve uygulamalara kullanım alanı sunan, HyperLedger belirtilen niteliklere en uygun platform olarak değerlendirilmiş ve bu çalışmada örnek uygulama ortamı olarak seçilmiştir.

6.1. Blokzinciri Tabanlı Siber Güvenlik Modeli

Komuta ve kontrol (C2) sistemleri, harekat esnasında hava üstünlüğünü sağlamak ve devam ettirebilmek için gerekli olan en önemli unsurdur. Komuta kontrol

sistemlerinin en önemli elemanı ise, komutan ve harp karargâhına gerçek zamanlı durumsal farkındalığı oluşturabilecek yekpare ve doğru hava resmidir (RAP). Hava resminin manipülasyonu, hava harekâtını tamamen başarısızlığa sürükleyebilecek bir olaylar zincirini tetikleyebilir. Bu zafiyeti önlemek üzere blokzinciri teknolojisinin kullanılması mümkündür. Bu teknoloji, merkezi sunuculu mimarilerde yaşanan zafiyetleri, dağıtık ve değiştirilemez yapısı ile ortadan kaldırma potansiyeline sahiptir. Siber ortamda dost hava komuta kontrol C2 (Command & Control) yeteneklerinin güvenliğini sağlamak için kilit unsur olarak kullanılabilir.

Bu çalışmada tasarlanan modeldeki alt elemanlar örnek bir NATO harekât ortamı üzerinden seçilmiş, gerçek ülke isimleri kullanılmamıştır. Gizliliğe her parametrede dikkat edilmiş ve gerçek veri bilgisine yer verilmemiştir. Model gerçek veriler yerleştirildiğinde de aynı şekilde çalışabilecek yapıda tasarlanmıştır. Prototip modelin ana elemanları NATO ve NATO olmayan müttefikik unsurlardan oluşmaktadır. Hyperledger-Fabric platformunda geliştirilen bir NATO Hava Operasyonu simüle edilmiştir. Bu kapsamda blokzinciri kullanılarak tasarlanan örnek model Şekil 6.1'de, gösterildiği gibidir. Sistemin ana elemanları Şekil 6.2'de ve Tablo 6.1'de belirtildiği gibidir.

Hyperledger platformunun seçilmesindeki nedenler olarak aşağıda verildiği gibidir:

- Diğer blokzinciri platformlarının aksine, Hyperledger Fabric ortamındaki blokzinciri sistemlerinde ihtiyaca yönelik geliştirmeler yapılabilmektedir.
- Modüler yapısı sayesinde, organizasyonun yapısına göre değişik çözüm önerileri sunabilmesi,
- Hyperledger Fabric'in, izinli kamusal ve izinli özel blokzinciri uygulamaları geliştirmeye uygun bir platform olması,
- Hyperledger Fabric içerisinde bulunan açık anahtar yapısı ile kriptografik sertifikaların etkin bir şekilde oluşturulabilmesi,
- Özel konsensüs protokolleri geliştirmeye uygun yapısı ve konsensüs açısından daha az işlemci gücüne ihtiyaç duyması ve daha kısıtlı işlemcili cihazlarda bile çalıştırılabilmesi,
- Bir kripto paraya ve madenciliğe ihtiyaç duymaması. Bu nedenle daha ekonomik ve daha az çevreye zarar veren (daha az enerji ve daha az ısı üretmesinden

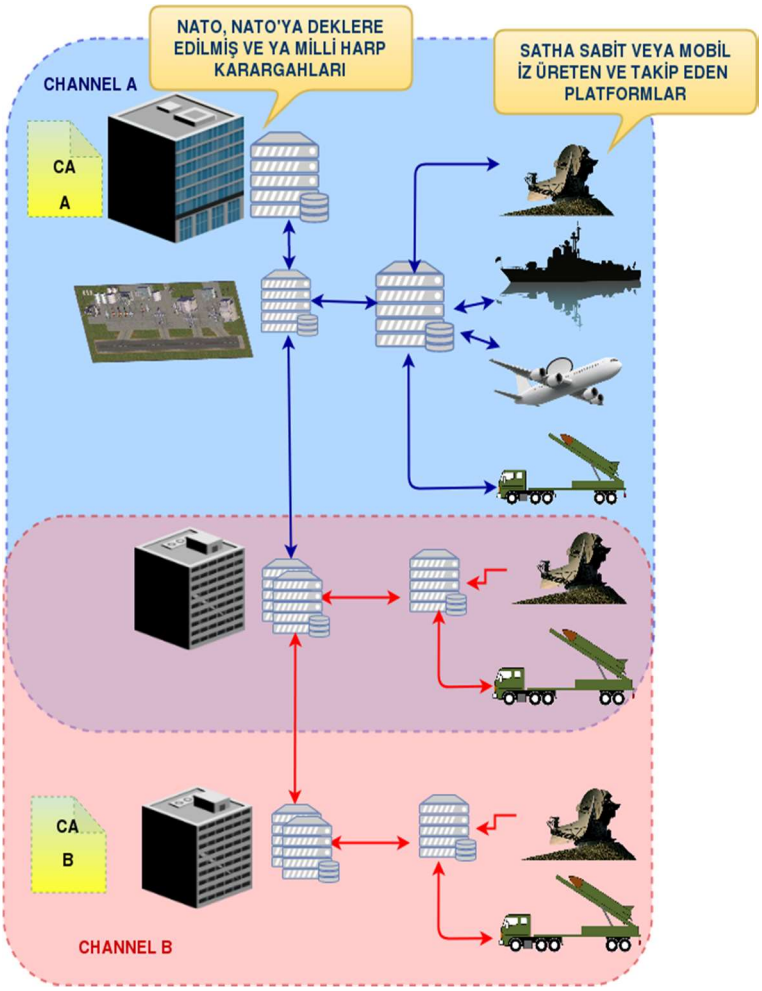
dolayı ekolojiye etkisi daha az) çözümlerin söz konusu olabilmesi,

- Akıllı sözleşmelerin çalışması veya sisteme dahil edilmesi için ek bir giderin (token veya kripto para gibi) olmaması,
- Açık kaynak projesi ve lisanslardan dolayı geliştirme konusunda özgür ortam sağlaması (Ref:Gür Ö., Öksüzer Ş., Karaarslan E., 2019. "Blockchain Based Metering and Billing System Proposal with Privacy Protection for the Electric Network", ISCG 2019'da sunulmak üzere kabul edildi.).

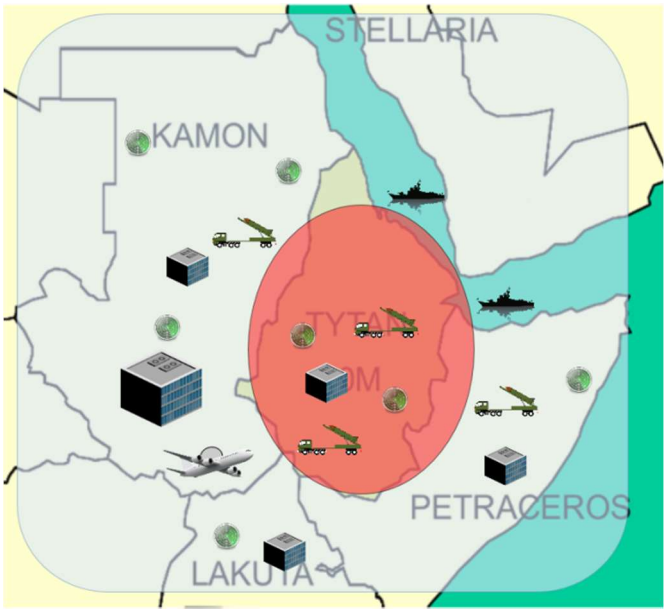
Uygulama ortamı, Hyperledger Fabric 1.3'ün sıradan bir bilgisayar üzerine kurulması ile tesis edilmiştir. Test ortamı olarak Hyperledger Composer Playground kullanılmıştır. Tüm işlemler 8 GB RAM, 500 GB sabit disk ve i5 Intel 2.6 GHz CPU'ya sahip bir bilgisayarda gerçekleştirilmiştir. Kullanılan uygulama teknolojileri Şekil 6.3'te gösterildiği gibidir. Hyperledger Fabric, Virtualbox üzerinde sanal bir makinede çalıştırılmış, sanal makineye erişmek için Vagrant kullanılmıştır. Eşler, Hyperledger Fabric Docker sanal makineleri kullanılarak oluşturulan Docker Containerlerde teşkil edilmiştir. İşlem günlüklerini ve varlıkların mevcut durumunu korumak için her eş için bir ayrı veritabanı tanımlanmıştır. Rapor oluşturma sırasında kullanılacak karmaşık sorgulamalara izin verdiği için veritabanı olarak CouchDB seçilmiştir. Her kanal için ayrı sertifika yetkilisi tespit edilmiş, sertifikaları teyidi ve kullanıcı kimlik doğrulaması Üyelik Hizmet Sağlayıcısı (MSP) tarafından sağlanmıştır.

Tablo 6.1 *Sistemin Ana Elemanları*

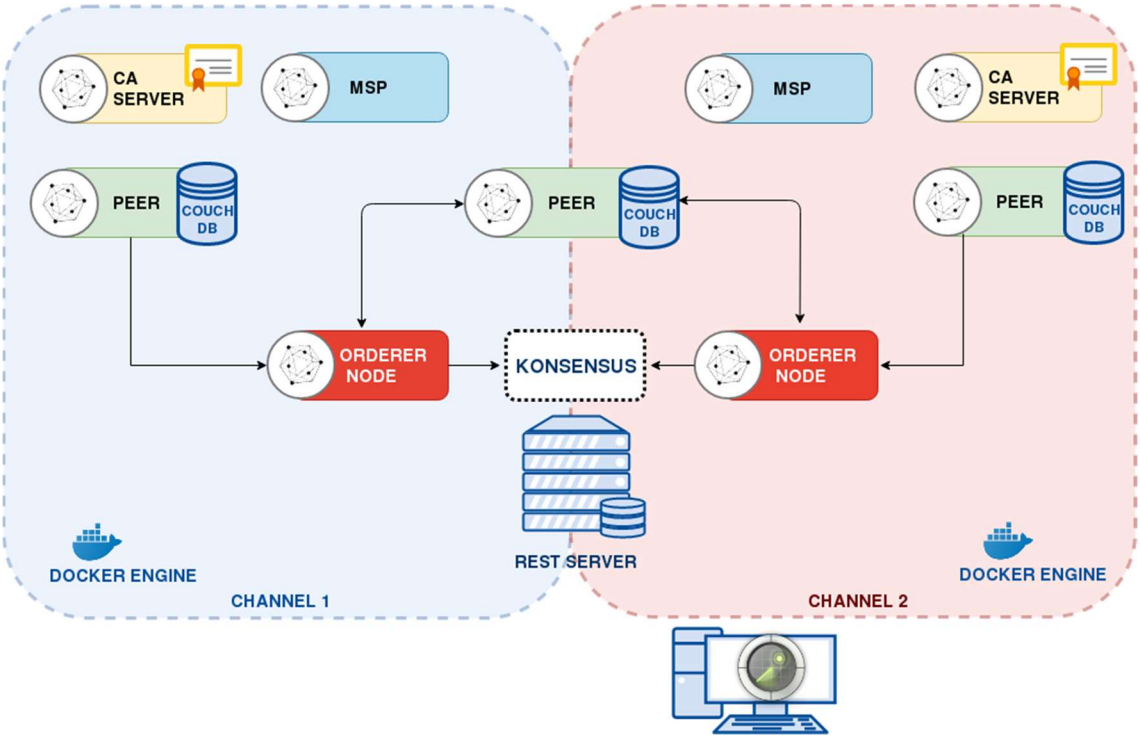
NATO PARTICIPANT		**NATIONAL PARTICIPANT**	
Natotrack**&**Natoradar		Nationaltrack**&**Nationalradar	
AWACS	TRACK NATO ONLY	AIR RADAR	TRACK NATIONAL
AIR RADAR		AIR DEFENCE RADAR	
AIR DEFENCE RADAR		HQ	
NAVY RADAR		-	
HQ			



Şekil 6.1 *Blokzinciri Kullanılarak Tasarlanan Örnek Model*



Şekil 6.2 *Sistemin Ana Elemanları*



Şekil 6.3 *Tasarımda Kullanılan Teknolojiler*

Kodlama ve test platformu olarak Hyperledger Composer Tool ve basit zincir kodlamaları için JavaScript kullanılmıştır. Oluşturulan kural tablosu ile NATO kullanıcılarının tüm iz bilgilerine ulaşırken, müttefik ülke kullanıcılarının sadece izin verilen izlere ulaşabilmesi sağlanmıştır. Dağıtmada, test için SOLO konsensüs protokolü seçilmiştir. Önemli kod blokları bu bölümün devamında sunulmuştur.

Modelin içinde değişkenlerin ilk tanımlamaları mode.cto dosyası içerisinde yapılmıştır. Şekil 6.4'te NATO ve milli iz bilgisinin değişken tanımlamaları gösterilmektedir. Şekil 6.5'te abstract bir sınıf olarak AIROPSparticipernt adında bir üye oluşturulmuş, bu üyeden NATO iz bilgisini ürettiği ve okuduğu kabul edilen Natoradar üyesi ve milli iz bilgisini okuduğu ve ürettiği kabul edilen Nationalradar kullanıcısı üretilmiştir. Ayrıca bu bölümde daha sonra logic.js dosyasında kodu belirtilecek olan gönderme fonksiyon ununda ana değişken tanımlamaları yapılmış bunlar ise Şekil 6.6'da belirtilmiştir. logic.js dosyası içerisinde gönderi içeriklerinin oluşturulduğu fonksiyonları içeren bölüm ise Şekil 6.7'de sunulmuştur. Şekil 6.8'de kullanıcı iz yaratma yetkileri, Şekil 6.9'da ise kullanıcı bazında tanımlanan iz okuma yetkileri gösterilmiştir.

```
45  asset Natotrack identified by NatotrackId{
46    o String    NatotrackId
47    o iff       iffType optional
48    o Long      trackNumber
49    o DateTime  trckTime  optional
50    o String    pilotName optional
51    o Route     route
52  }
53
54  asset Nationaltrack identified by NationaltrackId{
55    o String    NationaltrackId
56    o iff       iffType optional
57    o Long      trackNumber
58    o DateTime  trckTime  optional
59    o String    pilotName optional
60    o Route     route
```

Şekil 6.4 *NATO Ve Milli İz Bilgisinin Değişken Tanımlamaları*

```
63  abstract participant AIROPSparticipant identified by participantId{
64    o String participantId
65  }
66  participant Natoradar     extends AIROPSparticipant {
67  }
68  participant Nationalradar extends AIROPSparticipant {
69  }
70  participant NetworkAdmin  extends AIROPSparticipant {
71  }
```

Şekil 6.5 *Modele Ait Üye Tanımlamaları*

```
82  transaction createnatoTrack {
83    o Long      trackNumber
84    o String    origin
85    o String    destination
86    o Long      latilong
87    o Long      speed
88    o Long      height
89    o DateTime  trckTime
90  }
91
92  transaction createnationalTrack {
93    o Long      trackNumber
94    o String    origin
95    o String    destination
96    o Long      latilong
97    o Long      speed
98    o Long      height
99    o DateTime  trckTime
100 }
```

Şekil 6.6 *Gönderme Fonksiyonu Ana Değişken Tanımlamaları*

```
15          // Get the asset registry
16          return getAssetRegistry('nato.airops.participant.Natotrack')
17              .then(function (flightRegistry) {
18
19                  // Get resource factory
20                  var factory = getFactory();
21                  var NS = 'nato.airops.participant';
23                  // Create the Resource instance
24                  var  trackId = generateFlightId(flightData.trackNumb
25                  var  flight = factory.newResource(NS,'Track',trackId
26                  flight.trackNumber = flightData.trackNumber;
27
28                  // Create a new concept using the factory & set the
29                  var route = factory.newConcept(NS,"Route");
30
31                  // Set the data in the concept 'route'
32                  route.origin = flightData.origin;
33                  route.destination = flightData.destination;
34                  route.latilong = flightData.latilong;
35                  route.speed = flightData.speed;
36                  route.height = flightData.height;
37                  route.trckTime = flightData.trckTime;
38
39                  //  Set the route attribute on the asset
40                  flight.route = route;
41
42
43
44                  // Add to registry
45                  return flightRegistry.addAll([flight]);
46              });
```

Şekil 6.7 *Fonksiyonları İçeren Logic.js Dosyası*

```
40  //    Needed for Creating the "CreateTrack" transaction
41  //    NATOradar can execute NATOTRACK transaction
42  rule NATOradarCREATEPermission {
43    description: "NATORADAR can create a NATOTRACK"
44    participant: "nato.airops.participant.Natoradar"
45    operation: CREATE
46    resource: "nato.airops.participant.Natotrack"
47    transaction: "nato.airops.participant.createnatoTrack"
48    action: ALLOW
49  }
50  //    Nationalradar can execute NationalTRACK transaction
51  rule NationalradarCREATEPermission {
52    description: "NationalRADAR can create a NationalTRACK"
53    participant: "nato.airops.participant.Nationalradar"
54    operation: CREATE
55    resource: "nato.airops.participant.Nationaltrack"
56    transaction: "nato.airops.participant.createnationalTrack"
57    action: ALLOW
58  }
```

Şekil 6.8 *NATO ve Milli Kullanıcı İz Yaratma Yetkisi*

```
rule NatoRADARCanReadEverything {
    description: "Allow Nato participants read access to all
    resources"
    participant: "nato.airops.participant.Natoradar"
    operation: READ
    resource: "**"
    action: ALLOW
}
rule NationalRADARCanReadNationaltrack {
    description: "Allow Nato participants read access to all
    resources"
    participant: "nato.airops.participant.Nationalradar"
    operation: READ
    resource: "nato.airops.participant.Nationaltrack"
    action: ALLOW
}
/**
 * NATO vs. National access control submit.
 */
rule NatoradarCanSubmitEveryTransaction {
    description: "Allow Natoradar participants to submit every
    transaction"
    participant: "nato.airops.participant.Natoradar"
    operation: CREATE
    resource: "**"
    action: ALLOW
}
rule NationalradarCanSubmitNationalTransactions {
    description: "Allow all participants to submit transactions"
    participant: "nato.airops.participant.Nationalradar"
    operation: CREATE
    resource: "nato.airops.participant.createnationalTrack"
    action: ALLOW
```

Şekil 6.10 *Kullanıcı İz Okuma Yetkileri*

7. SONUÇ VE YORUMLAR

Modelin Uygulamasında modüler, yüksek güvenliğe sahip, çoklu ortamlarda çalışabilen, kripto para üretim süreçlerinden bağımsız, endüstriyel çaplı güvenlik uygulamaları için geliştirilmiş Hyperledger kullanılmış, yapılan uygulamasında hali hazırda uygulanmakta olan yöntemlerden farklı olarak:

- Veri tabanı dağıtık bir mimari yapıya geçirilerek, doğal afet ve siber sadırılara kinetik saldıra karşı daha yüksek güvenlik sağlanmış,
- Herhangi bir hukuki süreç dahilinde, kanıtların silinmesi veya tahrif edilmesine karşı daha sağlam bir güvenlik, inkar edilemez ve denetlene bilirlik sağlanmış,

- Verinin bütünlüğü ve güvenliği en üst seviyede sağlanırken, aynı zamanda bilmesi gereken prensibi dâhilinde bilgi gerekli kullanıcılarla paylaştırılmış,
- İnsan faktörü en aza indirilerek insan kaynaklı hatalar minimize edilmiş,
- Diğer blokzincir yapıları ile karşılaştırıldığında işletme maliyetlerinin ve enerji sarfiyatlarının düşük ve kabul edilebilir seviyelerde tutularak, verimliliği yüksek bir yapı elde edilmiştir.

Siber saldırılar, günümüzde sistemlerin ve bilginin güvenliğini tehdit etmekte, bilginin istenmeyen ellere geçmesine, yok edilmesine, bilgi sistemlerinin tahrip edilmesine sebep olabilmektedir. Bu durum özellikle; askeri tesisler, enerji hatları, fabrikalar, petrol rafineri gibi kritik altyapıların korunması konusunda kuvvetli önlemler alınmasını kaçınılmaz hale getirmektedir. On yıl önceki güvenlik ve sistem analizlerine göre yapılandırılmış günümüz siber güvenlik teknolojileri ile yakın gelecekte karşılaşılması muhtemel siber saldırı tiplerine karşı önlem alınabilmesi mümkün değildir. Sağlam bir siber güvenlik altyapısı ancak iletişim ağının tam güvensiz olduğu baştan kabul edilerek ve tüm mimari yapı bu çerçevede geliştirilerek sağlanabilir. Sınır güvenliği temelli siber güvenlik teknolojilerinde varsayılanın aksine, tehdidin içeriden de gelebileceği kabul edilmelidir. Aracı otorite, iç ağdaki sistemler ve kullanıcıların oluşturabileceği risk göz ardı edilmemelidir. Saldırının doğru analizini yapabilmek ve tersine mühendislik ile zararlı yazılım analizinde doğru sonuçlara ulaşabilmek için kanıtların koruna bilirliğinin sağlanması büyük önem arz etmektedir. Sistemlerde denetlene bilirliğin ve inkâr edilemezliğin sağlanması da, suçun ve suçlunun tespitini kolaylaştırabilmesi sebebi ile son dönmede üzerinde çalışılan konulardan biri haline gelmiştir.

Blokzinciri teknolojisi, tüm bu problem sahalarını tek başına giderebilecek bir güvenlik teknolojisi vaat etmektedir. Blokzincirinin en güçlü özelliği, üzerinde silinmesi mümkün olmayan kayıtların tutulabildiği kayıt defteridir. Makalede bu konudaki güncel çalışmalar incelenmiş ve sınıflandırılmıştır. İncelenen çalışmalar arasında özellikle internetin güvenliğini sağlamak üzere blokzinciri tabanlı dağıtık internet ve DNS altyapıları ile dosya sistemi, yazılım ve değerli dokümanların güvenliğinin ve denetiminin silinemez kayıt defteri sayesinde sağlandığı çalışmaların ulusal altyapıların siber güvenliğinin sağlanmasında doğrudan kullanılabilecek nitelikte önemli çalışmalar olduğu değerlendirilmektedir.

Silinemeyen kayıt defteri sayesinde dağıtık DNS yapıları teşkil edilerek ulusal internet ağının DNS güvenliğini sağlamak mümkündür. Ulusal internet ağı üzerinde sanal ağlarla ayrıştırılmış olsalar da E-devlet ve sağlık bilgi sistemi gibi değerli verinin tutulduğu bulut ve ağ ortamları blokzinciri mimarisi ile kontrol edilebilir ve güvenli hale getirilebilir. Blokzinciri mimarisinin sahip olduğu dağıtık kayıt defteri teknolojisinin tapu kayıtlarının tutulduğu sistemlerden nüfus bilgilerinin tutulduğu sunucu ortamlarına kadar e-devlet işlemlerinin yürütüldüğü tüm sistemlerde siber güvenliği sağlamak üzere uygulama alanı bulması mümkündür. Önemli devlet verisinin denetim ve takibi blokzinciri mimarisinde sağlanırken, dağıtık mimari yapısı sayesinde bir veya birden çok sunucu devre dışı kalsa bile sistem faaliyetini sürdürmeye devam edecektir. Dosya ve klasörlere giriş çıkış kayıt bilgisinin blokzincirinde muhafazasıyla bulut sistemlerinin takibi daha kolay hale getirilebilir, siber saldırılardan etkilenmeyecek daha kuvvetli bulut mimarileri teşkil edilebilir. Blokzinciri sayesinde mevcut açıklıkları sebebi ile son dönemde siber saldırılarda sıkça kullanılan nesnelerin interneti, ağı yöneten anahtarlama cihazları, yazıcı, kamera gibi ağa bağlı tüm cihazların yazılım ve yapılandırma değişikliklerini denetleyebilecek ve güvenliklerini arttırabilecek mimariler oluşturulabilir. Blokzincirinin kullanımı ile aygıt yazılımlarının takip edilmesi sağlanabilir.

Muharebe sahasında sağladığı fayda sonucunda kullanım alanları artan ve genişleyen insansız hava araçlarının güvenliğini sağlamak üzere blokzinciri teknolojisinin kullanımı, gelecekte araştırılması gereken bir konu olarak değerlendirilmelidir. Sürü sistemleri olarak bir grup cihazın birlikte çalıştığı, merkez ile iletişim bağlantısı kesildiğinde dahi yan insansız araçlarla iletişime geçerek son komutu almaya devam eden ve görevini başarılı bir şekilde ile ifa edebilen blokzinciri tabanlı insansız hava, kara, deniz araçları tasarlanabilir. Blokzinciri teknolojisi milli askeri link sistemlerinde kullanılabilir. Yapay zekâ teknolojisinin de kullanımıyla geliştirilecek otonom sistemlerin iletişim altyapılarında kullanılabilir.

Kapalı kaynak kodlu işletim sistemlerinin yerine açık kaynak kodlu milli işletim sistemlerinin devlet kurumlarında uygulamaya geçirilmesi ve blokzinciri teknolojisinin bu sistemler üzerindeki kullanım alanlarının tespit edilmesi de milli siber güvenliği sağlamak üzere araştırılması gereken önemli konulardan biridir. Blokzinciri mimarisi kullanılarak yüksek güvenliğe sahip, denetlenebilir nitelikte evrak dağıtım sistemi,

mesajlaşma ve elektronik posta sistemleri teşkil edilebilir. Sunucu ve istemcilerdeki tüm dosya kütüklerine erişim yetkilendirmeleri blokzinciri kayıt defteri teknolojisi ile yapılandırılabilir, tüm dosya ve gizlilik dereceli evrak üzerinde yapılan değişiklikler yaşam döngüsü boyunca kayıt altına alınabilir ve sonradan denetlenebilir. Dosya ve evrak yönetim sistemi ve dosya paylaşım ortamları blokzinciri tabanlı P2P uygulamalarla gerçekleştirilebilir.

Bu çalışmada blokzinciri modelleme platformu olarak Hyperledger Fabric seçilerek tasarlanan model üzerinde hava harekâtı için yüksek öneme sahip iz verisinin güvenliğinin sağlanabileceği bir uygulama geliştirilmiştir. Bu model ve uygulama ile daha sonra konu üzerinde bu temelde yapılabilecek çalışmalara örnek teşkil edilmesi hedeflenmiştir. Halihazırda saniyede binlerce gönderi üretebilen blokzincir platformları ile bu model daha kompleks mimarilerde ve çok daha geniş kullanım alanlarında başarı ile uygulanabilir. Blokzinciri mimarisine sahip açık kaynak kodlu milli iletim sistemi ve yazılımlarla donatılmış ağ yapılarının Türkiye'nin bilgi hazinelerini korumada çok önemli görevler üstlenebileceği değerlendirilmektedir. Bu teknoloji, doğru kullanıldığı takdirde Türkiye'nin ulusal siber güvenliğini sağlamak üzere önünde duran en önemli fırsatlardan biri olmaya adaydır.

KAYNAKÇA

[1] ITU İnternet Sitesi. Global Cybersecurity Index 2017. https://www.itu.int (Erişim tarihi: 13.08.2018).

[2] Arbornetworks İnternet Sitesi. Siber Bilgilendirme Raporu. https://www.arbornetworks.com (Erişim tarihi: 06.04.2018).

[3] Berr (2017).CBS News. https://www.cbsnews.com (Erişim tarihi: 13.08.2018).

[4] Hürriyet Gazetesi İnternet Sitesi. Meydana Gelen Siber Dolandırıcılık İle İlgili Haber. http://www.hurriyet. com.tr (Erişim tarihi: 13.08.2018).

[5] Wilner, A. (2017). CyberDeterrence And Critical-Infrastructure Protection: Expectation, Application, And Limitation. Comparative Strategy Journal, 36, 309-318, s.313.

[6] Durğay, Z. ve Karaarslan, E.(2018). Blokzinciri Teknolojisinin E-Devlet Uygulamalarında Kullanımı: Ön İnceleme. Akademik Bilişim'de sunulan bildiri. 31 Ocak-02 Şubat 2018. Karabük Üniverstesi.

[7] Nakamoto, S.(2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[8] Dorri, A., Kanhere, S.S., Jurdak, R., ve Gauravaram, P. LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy. IEEE Internet of Things Journal. 04 Ekim 2018. 2018.

[9] Check Point Software Technologies İnternet Sitesi. Softwaredefined Protection. https://www.checkpoint.com (Erişim tarihi: 14.05.2018).

[10] Check Point Software Technologies İnternet Sitesi. 5th Generation Cyber Attacks Are Here And MostBusinesses Are Behind- A New Model For Assessing and PlanningSecurity. http://www.infosecurityeurope.com (Erişim tarihi: 14.05.2018).

[11] Check Point Software Technologies İnternet Sitesi. Checkpoint Online Cyber Attack Map. https://threatmap. checkpoint.com (Erişim tarihi: 13.05.2018).

[12] Check Point Software Technologies İnternet Sitesi. Global Cyber Attack Trends Report. https://www.Check point.com (Erişim tarihi: 13.05.2018).

[13] Çelikpala, M., Bıçakcı S. ve Ergun, F.D. The Cyber Security Scene In Turkey. EDAM. edam.org.tr (Erişim Tarihi:17.10.2018).

[14] Şeker, E. (2017). Siber Savunma Tatbikatları: Planlama, Uygulama Ve

Değerlendirme. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi. 3(2), 33-41, s.33.

[15] T.C. Ulaştırma ve Altyapı Bakanlığı İnternet Sitesi. Türkiye 2016-2019 Ulusal Siber Güvenlik Stratejisi. http://www.udhb.gov.tr (Erişim tarihi: 10.04.2018).

[16] ITU İnternet Sitesi. Cyberwellness Profile Turkey. https://www.itu.int/en/ITU-D/ Cybersecurity/Pages/ Country_Profiles.aspx. (Erişim tarihi: 06.04.2018).

[17] Check Point Software Technologies İnternet Sitesi. Stepping Up to Gen V (5th Generation) of Cyber Security. www.checkpoint.com/gen-v-cyber-security/. (Erişim tarihi: 06.03.2018).

[18] Emmett, J.(2017).Wired For War: An Analysis of Wired For War: An Analysis of United States CyberSecurity Against a Rising China Lisans Tezi. Graduate School of International Studies Seoul National University Seoul, Seul, Republic of Korea. s.37.

[19] Trautman, L.J. ve Ormerod, P.C. Industrial Cyber Vulnerabilities: Lessons From Stuxnet And The Internet Of Things. University of Miami Law Review. 72, 761-826, s.787.

[20] Siberest İnternet Sitesi. WanaCrypt0r Fidye Yazılımı: WannaCry Hakkında Bilmeniz Gerekenler. http:// siberest.com.tr (Erişim tarihi: 10.04.2018).

[21] Infosecurty Magazine İnternet Sitesi. CISCO Warns of Comming Destruction. https://www.infosecurity-magazine.com (Erişim tarihi: 10.04.2018).

[22] CISCO İnternet Sitesi. CISCO 2017 Midyear Cybersecurity Report. https://www.cisco.com (Erişim tarihi: 10.05.2018).

[23] Barnas, N.B. Blockchain Technology. http://www.airuniversity.af.mil (Erişim tarihi: 31.05.2018).

[24] Karaarslan, E. ve Akbas, M.F.(2017).Blokzinciri Tabanlı Siber Güvenlik Sistemleri. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi. 3, 16-21, s.16.

[25] Poonam, N.R., Mahamure, S. ve Mahalle,P.N. Application Security using Blockchain in Cyber Physical System. CIS Communications Knowledge Digest for IT Community. Aralık 2017, 25-28, s.25.

[26] Check Point Software Technologies İnternet Sitesi. Cybersecurity Executive. https://www.checkpoint.com (Erişim tarihi: 31.05.2018).

[27] Jitendra, M.(2017). Using innovation from blockchain technology to address privacy and security problems of Internet of Things, Yüksek Lisans Tezi. KTH Industrial Engineering and Management, Stockholm,s.1.

[28] Collen,A..GHOST - Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control. International ISCIS Security Workshop, 26-27 Şubat 2018, Euro-CYBERSEC 2018. Security in Computer and Information Sciences Yayını. Londra, İngiltere, s.6.

[29] Kshetri,N. Can Blockchain Strengthen the Internet of Things?. IEEE IT Professional IEEE Computer Society Eylül-Ekim, 2017, 68-72, s.68.

[30] Pan J. ve Yang Z. Cybersecurity Challenges and Opportunities in the New Edge Computing + IoT World. The 8th ACM Conference on Data and Application Security and Privacy. 19-21 Mart 2018, Tempe, Amerika Birleşik Devletleri, s. 29.

[31] Jan, J.K. ve Guillaume B. (2017). Connecting Multiple Devices With Blockchain In The Internet Of Things, Research paper for Seminar on Blockchain Technology (MTAT.03.323). Tallinn Unıversity Of Technology, Tallinn.

[32] Copos,B., Levitt,K., Rowe,J., Kianmajd, P., Chuah C. ve Kesidis,G. Security and Privacy for Emerging Smart Community Infrastructures. Open Access Publishments From The University Of California UCDAVIS, escholarship.org(Erişim Tarihi:17.10.2018).

[33] Ramachandran, A. ve Kantarcioglu,M. Using Blockchain and smart contracts for secure data provenance management. Cornel Universty Library. https://arxiv.org(Erişim Tarihi:17.10.2018).(arXiv:1709.10000v1).

[34] Uurtsaikh,J. (2017) Decentralized Access Control Using Blockchain. Yüksek Lisans Tezi, University of Saskatchewan, Saskatoon, s.1.

[35] Li, Y.,HUANG,J., QIN,S. ve WANG,R. Big Data Model of Security Sharing Based on Blockchain. 3rd International Conference on Big Data Computing and Communications. 10-11 Ağustos 2017. Sichuin, China, s.117.

[36] Gaetani, E., Aniello, L., Baldoni,R., Lombardi,F., Margheri,A. ve Sassone,V. Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments. First Italian Conference on Cybersecurity (ITASEC17). 17-20 Ocak 2017. Venedik, İtalya.

[37] Hu,S.,Cai,C. Wang,Q. Wang,C., Luo,X. ve Ren,K..Searching an Encrypted Cloud Meets Blockchain: A Decentralized, Reliable and Fair Realization. IEEE International Conference on Computer Communications. 15-19 Nisan 2018. Honolulu, Amerika Birleşik Devletleri.

[38] Yin,S.,Bao,J., Zhang,Y. ve Huang,X. M2M Security Technology of CPS Based on Blockchains. Journal Symmetry. Eylül 2017, Cilt: 9, 193-201, s.198.

[39] Ivezic,M. When Hackers Threaten your Introduction to Cyber-Kinetic and Security of Cyber-Physical Systems. http://ivezic.com (Erişim tarihi: 10.04.2018).

[40] Neil,B.B. (2016). Blockchains in National Defense: Trustworthy Systems in a Trustless World. Yüksek Lisans Tezi, Air University, Alabama, s.12.

[41] Alcazar,V. (2017). Data You Can Trust, Blockchain Technology. Air&Space Power Journal. 2017, Cilt: 31, 91-101, s.91.

[42] Patterson,T., Liebig,E., Sapp,R., Searcy,B., Desai,D., Blask,C., Bone, J.ve Spiker,S. Enhancing National Cybersecurity: The Current and Future States of Cybersecurity in the Digital Economy. Amerika Birleşik Devletleri Resmi Gazetesi, 2017.

[43] Puthal,D., Malik,N., Mohanty,S.P.,Kougianos,E. ve Yang,C. The Blockchain as a Decentralized Security Framework. IEEE Consumer Electronics Magazine. Mart 2018, 18-22, s.18.

[44] Magrassi,C. The Role Of Blockchain In Revolutionizing And ReOrganizing Security. Evidence And Policy Recommendations. Yüksek Lisans Tezi, 2017, s.1.

[45] Dickson,B.Blockchain's brilliant approach to cybersecurity. https://venturebeat.com (Erişim tarihi: 06.03.2018).

[46] Datta,S.P.A. Cybersecurity – Personal Security Agents as Modular Models representing People, Process, Atoms and Bits. Journal of Innovation Management. 2017, Cilt: 5, 4-13, s.7.

[47] Durğay,Z. ve Karaarslan,E. Blokzinciri Teknolojisinin E-Devlet Uygulamalarında Kullanımı: Ön İnceleme. Akademik Bilişim Konferansı, 2018.

[48] Chibuye,M. ve Phiri,J. (2017). Blockchain – It's Practical Use For National Data Centres. Zambia Informatıon Communıcatıon Technology Journal. 2017, 57-62, s.58.

[49] Karaarslan,E. ve Adıgüzel,E. Blockchain Based DNS and PKI Solutions", IEEE Communications Standards Magazine, Eylül 2018 "Standards for Major Internet Disruptors özel sayısında yayınlanmak üzere kabul aldı.

[50] Shackelford,S. ve Myers,S. (2017)Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace. Yale Journal of Law and Technology. 2017, Cilt19, 336-383, s.355.

[51] Ramachandran,A. ve Kantarcioglu,M. (2018). Smart Provenance: A Distributed, Blockchain Based Data Provenance System" , The 8th ACM Conference on Data and Application Security and Privacy. 19-21 Mart 2018, Tempe, Amerika Birleşik Devletleri, s. 35.

[52] Alexopoulos,N., Vasilomanolakis,E., Ivanko,N.R., ve Muhlhauser,M. (2017). Towards Blockchain-Based Collaborative Intrusion Detection Systems. CRITIS 2017, 8-13 Ekim 2017, Lucca, İtalya .

[53] Weed,S.A. US Policy Responce To Cyber Attack On SCADA Systems Supporting Critical National Infrostructure. Air Universty Press. Air Force Research Institude. Alabama, Temmuz 2017.

[54] Bulucu,M. ve Çıblak,E. Muharebe Sahasının Dijitalleşmesi Stratejik Sektörel Değerlendirme Raporu. STM, 2016.

[55] Ferrer,E.C. The Blockchain: A New Framework For Robotic Swarm Systems", Cornel Universty Library. https://arxiv.org(Erişim Tarihi:17.10.2018).(arXiv:1608.00695).

[56] Poonam,N.R., Mahamure,S. ve Mahalle,P.N. Application Security using Blockchain in Cyber Physical System. CIS Communications Knowledge Digest for IT Community. Aralık 2017, 25-28, s.25.

ÖZGEÇMİŞ

Adı-Soyadı : Enis KONACAKLI

Yabancı Dil : İngilizce

Doğum Yeri ve Yılı: Konak/21.03.1978

E-Posta : enisk@eskisehir.edu.tr

Eğitim ve Mesleki Geçmişi:

- Hava ve Uzay Teknolojileri Enstitüsü, Elektronik Mühendisliği Bölümü, Hava Harp Okulu, İstanbul, Türkiye, Ağustos 2001.
- Muhabere Elektronik ve Bilgi Sistemleri Tabur Komutanı, 1'inci Ana Jet Üs MEBS Tabur K.lığı, Eskişehir, 2016.
- NATO NRF/TurJFAC CIS INFOSEC/ Cyber SO, TurJFAC, Eskişehir, 2016.
- NATO Saraybosna Karargahı Muhabere Elektronik ve Bilgi Sistemleri Teknik Danışmanı, BosnaHersek Savunma Bakanlığı, Saraybosna/BosnaHersek, 2016.
- Bilişim Sistemleri Bölük Komutanı, 1'inci Ana Jet Üs MEBS Tabur K.lığı, Eskişehir, 2014.
- Muhabere Elektronik ve Bilgi Sistemleri Bölük Komutanı, Işıklar Askeri Hava Lisesi Komutanlığı, 2008.
- TAFICS Bölük Komutanı, Merzifon/AMASYA, 2005.
- Muhabere Elektronik ve Bilgi Sistemleri Bölük Komutanı, Merzifon Hava Radar Mevzi K.lığı, Merzifon/AMASYA, 2003.