Türkiye'de Dağıtık Hesap Defteri Teknolojili Nesnelerin İnterneti Ödeme Sistemleri için Sistem Tasarım Önerileri

Literatür Makalesi/Review Article

Ilgın ŞAFAK, Ersin ÜNSAL

Fibabanka Ar-Ge Merkezi, İstanbul
ilgin.safak@fibabanka.com.tr, ersin.unsal@fibabanka.com.tr
(Geliş/Received:07.07.2020; Kabul/Accepted:02.12.2020)
DOI: 10.17671/gazibtd.765841

***Özet*—** Ödeme sistemlerinde gittikçe yaygınlaşan Internet üzerinden (online/mobil) ve temassız ödemeler, ödeme sistemlerinde kullanıcı deneyiminin ve bu sistemlerin kullanıcı dostu olmasının önemini göstermektedir. Akıllı saat gibi giyilebilir nesneler ve nesnelerin internetinin (NesNet) sunabileceği kullanıcı deneyiminin dijital ödemeleri devrimleştirmesi beklenmektedir. Bununla birlikte, NesNet'in güvenlik açıkları olduğu bilinmektedir. Bunun en önemli nedenlerinden biri NesNet'te genelde bulut tabanlı merkezi yapı kullanılmasıdır. NesNet'in merkezi yapıdan dağıtık yapıya geçişini sağlamak için ödeme altyapısı olarak dağıtık hesap defteri teknolojisi (DHT) kullanılabilir. Türkiye'de dijital ödemelerde DHT'nin NesNet ile birlikte kullanımı ile ilgili çalışmalar yeterli değildir ve, bilgimiz dahilinde, halihazırda ülkemiz hukuku ile uyumlu bir NesNet-DHT sistemi bulunmamaktadır. Bu makalede ülkemiz kanunlarına (Kişisel Veri Korunumu Kanunu ve Bilgi ve İletişim Tedbirleri Genelgesi) uygun olarak NesNet ve DHT ile güvenli dijital ödeme sistemleri tasarımında dikkat edilmesi gereken konular ve öneriler sunulmaktadır.

***Anahtar Kelimeler*—** dağıtık hesap defteri teknolojisi, dijital ödemeler, nesnelerin interneti, kişisel veri güvenliği, kişisel veri korunumu kanunu, bilgi ve iletişim tedbirleri genelgesi

System Design Recommendations for IoT Payments Systems in Turkey using Distributed Ledger Technology

***Abstract*—** The trending of internet (online/mobile) and contactless payments emphasizes the importance of consumer experience and user friendliness of digital payment systems. Due to the consumer experience they can provide, it is expected that wearables, such as smart watches, and Internet of Things (IoT) will revolutionize the digital payments landscape. However, IoT devices are known to have security vulnerabilities, one of the most important reasons being that IoT systems typically use centralized cloud-based infrastructures. In order to transform it to a distributed architecture, distributed ledger technology (DLT) can be leveraged as the payment infrastructure. Digital payments in Turkey using IoT and DLT is not a well-studied topic and, to the best of our knowledge, there currently does not exist a system that is fully compliant with local regulations. This paper studies the impact of local laws, including personal data protection law, information and communication precautions circular, on IoT payments via DLT and provides insights and recommendations in the system design of such digital payment systems compliant with local regulations.

***Keywords*—** distributed ledger technology (DLT), digital payments, internet of things (IoT), personal data security, personal data protection law, information and communication precautions circular

1. GİRİŞ (INTRODUCTION)

Nesnelerin İnterneti (NesNet), birbirlerine bağlanmış akıllı nesnelerden (cihazlardan) oluşan bir ağdır. Bu nesnelerin aklı kendi içlerinde veya dış ortamla iletişim kurmak için içerdikleri gömülü bir teknolojiye dayanır. Ucuz işlemciler ve kablosuz ağlar kullanılarak, herhangi bir nesneyi NesNet'in bir parçası haline getirmek mümkündür. Böylece, genelde düşük kapasiteye sahip olan bu cihazlar, bir insanın katılımı olmaksızın, kendi aralarında iletişim kurabilirler [1].

NesNet ekosistemi, veri toplamak, işlemek ve göndermek için gömülü işlemcileri, sensörleri ve iletişim donanımları bulunan akıllı cihazlardan oluşur. NesNet cihazları, topladıkları sensör verilerini, analiz edilmek üzere bir NesNet ağ geçidine veya buluta gönderebilir. Bir NesNet cihazı bulut, ağ geçidi üzerinden veya doğrudan başka bir cihazla iletişim kurabilir, veri paylaşabilir ve işlem gerçekleştirebilir. NesNet'e örnek olarak akıllı saat veya adımsayar gibi giyilebilir cihazlar verilebilir [2].

Gün geçtikçe yaygınlaşan NesNet'in, cihazlara kazandırdığı büyük veri analitiği ve bulut bilişim yetenekleri sayesinde, dijital ödemeleri devrimleştirmesi öngörülmektedir [3]. 2018 yılında NesNet nesne sayısı 7 milyar iken, bu sayının 2025'te 22 milyara kadar ulaşması beklenmektedir.

Kullanım kolaylığı NesNet sisteminin tasarımında öncelikli bir yere sahiptir. Örneğin, kullanıcı dostu ara yüze sahip olması, Wi-Fi ağına kolayca bağlanabilmesi ve mobil uygulama ile (giyilebilir cihaz gibi) bir NesNet cihazının yönetilebilmesi bu öncelikler arasında sayılabilir.

Öte yandan, NesNet cihazlarının farklı donanım, işlem gücü, vb. teknik özelliklere sahip olmaları ve tüm NesNet cihazları için ortak bir güvenlik standardının bulunmaması nedeniyle güvenlik seviyesi cihazdan cihaza değişkenlik gösterebilmektedir. Günümüzde, NesNet nesnelerinin %80'inin kullanıcıların gizliliğini ve güvenliğini sağlayabilecek yeteneğe sahip olmadıkları tahmin edilmektedir [4]. Bu nedenle, NesNet'in yaygınlaşması ile bu cihazların maruz kalabilecekleri güvenlik saldırılarının da artması beklenmektedir [5-6]. Geliştirilen hemen hemen her yeni cihazın NesNet yeteneğine sahip olmasına rağmen, yeterli güvenlik önlemlerinin alınmaması nedeniyle, olası siber saldırılar sonucunda kullanıcıların ödeme bilgileri, alışveriş alışkanlıkları, sağlık bilgileri, görüntü/ses kayıtları, ev adresi vb. kişisel veriler kolayca elde edilebilir ve kişinin NesNet sistemine erişimi engellenebilir. Böylece kişilerin hak ve özgürlükleri kısıtlanabilir ve maddi ve manevi zarara uğratılabilir. Bu nedenle, NesNet ağının tasarımında, cihazların kullanım kolaylıklarının yanı sıra, sistemin güvenlik mimari tasarımı da büyük önem arz etmektedir.

NesNet'teki güvenlik sorununun en önemlisi sistemin merkezi mimarisinden kaynaklanmaktadır. Bu sistemde, tüm cihazlar *merkezi* bir bulut sunucu tarafından kimlik doğrulaması yapılarak yetkilendirilmekte ve ağa bağlanmaktadır. *Dağıtık* mimariye geçilmesi ile tek arıza noktasının önlenmesi (birden fazla sunucu ile merkezi sunucuya bağlı kalmama) sonucunda, cihazların bağlanabileceği daha esnek ve güvenli bir mimari yapıya sahip olunacaktır [7]. Bu bağlamda Dağıtık Hesap Defteri Teknolojisi (DHT)'nin kullanılması büyük yarar sağlayacaktır [8-9].

DHT, dağıtık olarak sürekli büyüyen veri kayıtlarının yönetildiği bir veri tabanı veya hesap defteri olarak düşünülebilir. DHT hesap defterinin değişmez yapısı ve DHT ağındaki tüm katılımcıların gerçekleşen işlemleri dağıtık bir şekilde doğrulamaları nedeniyle hesap defterinin manipüle edilmesi önlenebilmektedir [10]. DHT NesNet ile yapılan dijital ödemeler, veri bütünlüğünü koruması nedeniyle, önemli güvenlik üstünlüğü sağlamaktadır [11].

Bu çalışmada, yukarıda sıralanan görüşlerin ışığında, Türkiye'de NesNet ile güvenli ödemelerin yapılabilmesi ve kişisel verilerin korunabilmesi için sistem tasarımında göz önüne alınması gereken konulara değinilmiş ve ülkemiz hukukuna uygun sistem tasarım önerileri sunulmuştur.

2. TÜRKİYE'DE DHT İLE NESNET ÖDEMELER (IOT PAYMENTS USING DLT IN TURKEY)

Veri güvenliği, kişilerin özel hayatının gizliliği ile temel hak ve özgürlüklerinin korunması açısından önemlidir. Kişisel Verilerin Korunumu Kurumu, 2016 yılında Resmi gazetede yayınlanan 6698 sayılı Kişisel Verilerin Korunması (KVK) Kanunu [12] kapsamında, kişisel verilerin korunmasını sağlamaya yönelik çalışmaktadır [13]. Bu bağlamda alınması gereken idari ve teknik tedbirlere ilişkin rehber yayınlamıştır [14].

Kişisel verilere ek olarak, ödeme bilgisi gibi diğer kritik verilerin güvenliğinin sağlanması, ülke güvenliğinin yanı sıra kişi ve kurumlar için de büyük önem arz etmektedir. Cumhurbaşkanlığı tarafından yayınlanan Bilgi ve İletişimi Tedbirleri Genelgesi (BITG) [15], kamu kurum/kuruluşları ve bankalar gibi kritik altyapı sağlayıcıları için geçerli olan bilgi ve iletişim güvenliği kurallarını içermektedir.

Ülkemizde, kişisel ve kritik verilerin güvenliğinin sağlanabildiği, KVKK ve BITG ile uyumlu, NesNet nesneleri ile DHT üzerinden dijital ödemelerin yapılabildiği herhangi bir platform bilgimiz dâhilinde bulunmamaktadır. Türkiye'de DHT ile ödemeler konusunda çalışan kurumlar, mevcut platformlar ve yapılan çalışmalar aşağıda özetlenmiştir.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TUBITAK)'in Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (TÜBİTAK BİLGEM)'inde blokzincir teknolojisi üzerine çalışmalar yürütülmektedir. Blokzincir Araştırma Laboratuvarı (BZLab) kamu/özel kurumlar ve akademi ile ortak

çalışmalar gerçekleştirmektedir. Böylece Ulusal Blokzincir Araştırma Ağı ekosistemi aracılığı ile Türkiye'de bu alanda çalışan araştırmacıların iş ve güç birliği yapmaları sağlanmaktadır. Bu kapsamda, finansal hareketler, tedarik zincirleri, NesNet, risk yönetimi ve sağlık hizmetleri de dâhil olmak üzere farklı elektronik işlemlerle ilgili ağların kurulması üzerine çalışmalar yürütülmektedir [16].

Türkiye Bilişim Vakfı (TBV) liderliğinde yürütülen Blokzincir Türkiye Platformu, Türkiye'de sürdürülebilir blokzincir ekosisteminin oluşturulmasını hedeflemektedir. Bu kapsamda yaygınlaştırma çalışmaları, konsorsiyum ve çalışma gruplarının oluşturulmasına ve prototip geliştirilmesine destek olmak gibi çalışmalar mevcuttur. Kişisel Veri Korunumu Hukuku ve Blokzincir Teknolojisi [17] raporunda blokzincir teknolojisinin KVKK [12] ve General Data Protection Regulation (GDPR) [18] açısından uygulama alanı ve bölgesel kapsamı bakımından değerlendirilmesine yer verilmiştir. Raporda özellikle açık ve izin gerektirmeyen blokzincir ağlarının, dünyanın herhangi bir yerinde olabileceğinden, hangi ülkenin mevzuatının bölgesel alanı içerisinde olduklarının tespit etmenin zorluğundan bahsedilmekte, olası hukuki sorunlara ve teknik çözümlere yer verilmektedir.

Takas İstanbul tarafından yürütülen ve Türkiye'nin finansal alandaki ilk blokzincir ağı olan Bir Gram Altın (BİGA) projesinde, fiziki karşılığı altın ile bloke altına alınmış olarak blokzincir teknolojisi ile transfer işlemlerinin yapılabileceği bir altyapı geliştirilmiştir [19]. Mevcut blokzincir çerçeve altyapıları kullanılarak geliştirilmiş olan BİGA altyapısı, izinli blokzincir mimarisi sayesinde mahremiyet ve regülasyonlara uyum sorunlarına çözüm sağlamaktadır. Uygulamaya alınmış ve yaygınlaştırma çalışmaları planlanmış BİGA platformundan hizmet sağlayacak olan katılımcı bankaların, kendi sistemlerinde yapacakları geliştirmelerle, altın bakiyelerinin katılımcı bankalar arasında 7/24 transferi mümkün olabilecektir.

2017 yılında Ripple işbirliği ile blokzincir kullanarak uluslararası para transferi çalışmalarına başlayan Akbank, yayınlanan son güncelleme ile Santander UK'ye Ripple üzerinden blokzincir altyapısı kullanılarak GBP para transferlerine başlamıştır [20].

Bankalararası Kart Merkezi (BKM), T2 Yazılım A.Ş. firması ile birlikte Türkiye'nin ilk blokzincir uygulaması olan Bay Bay Nakit'i (BBN) geliştirmiştir. BBN mobil uygulaması aracılığı ile BKM; dijital kimlik oluşturma, blokzincire kaydetme, puan kazanma, puanları diğer kullanıcılara transfer etme ve uygulamalar içerisindeki mağazalarda listelenen ürünleri puanları ile satın alma olanağı sağlanmaktadır. BBN'de sadakat puanları ise "keklik" isimli kripto para üzerine kurgulanmıştır. Hyperledger Fabric platformu üzerinde gerçekleştirilen ve izin gerektiren özel blokzincir yapısına sahip olan BBN'nin ilk faz raporuna göre, blokzincirin henüz büyük çaplı sistemlerde kullanılabilecek kadar olgunlaşmadığı sonucuna varılmıştır [21].

'Blockchain as-a-service' olarak bulut üzerinden kurumlara blokzincir altyapısı sunan T2 Yazılım A.Ş. firması, BKM ile ortak çalışmalar yürütmektedir. Blokzincir ile aynı teknolojik altyapıyı paylaşan, mobil cihazlarda çevrimdışı olarak da çalışabilen P2P bir ödeme sistemi geliştirmektedir [22].

Banka ve hava yolu şirketlerinden bağımsız bir mil programı sunan Global Miles, Ethereum blokzincir altyapısıyla ile milleri dijital bir varlık olarak güvenli bir şekilde işlem ve transfer yapılmasına olanak sağlamaktadır [23].

NETAŞ, H2020 Avrupa Birliği Programı kapsamında yer aldığı "Critical-Chains" projesinde, AB'nin yeni nesil finans dünyasında siber güvenlik, kara para aklama ve sahtecilik gibi tehditlerin önlenmesi konusunda çalışmalar yapmaktadır [24].

Proofstack, nitelikli otorite ve blokzincir protokollerini (Bitcoin, Ethereum, Litecoin, EOSIO, NEO) tek platformda toplayan, küresel ve yerel yasal deliller oluşturulmasına aracılık edebilen dünyadaki ilk ve tek şirkettir [25].

Türkiye Cumhuriyeti Merkez Bankası (TCMB) tarafından geliştirilen blokzincir tabanlı dijital paranın uygulamaya konulduğu Fonların Anlık Sürekli Transferi (FAST) isimli anlık ödeme sisteminin tamamlandığı ve 18 Aralık 2020'de kullanıma açılacağı duyurulmuştur [15]. TCMB, Hazine ve Maliye Bakanlığı ve BDDK tarafından yürütülecek tedbirler kapsamında, FAST ödeme sisteminin Payment Services Directive 2 (PSD2) ile mevzuat uyumu sağlanacağı belirtilmektedir.

3. TÜRKİYE'DE DHT İLE NESNET ÖDEMELERİN HUKUKA UYGUNLUĞU (COMPLIANCE WITH LOCAL REGULATIONS OF IOT PAYMENTS USING DLT IN TURKEY)

Türkiye'de NesNet nesneleri ile DHT üzerinden dijital ödemelerin yapılabilmesi için ilgili sistemin KVKK ve 2019/12 Sayılı Bilgi Güvenliği Tedbirleri Cumhurbaşkanlığı Genelgesi ile uyumlu geliştirilmesi gerekmektedir.

Ülkemiz hukukuna uygun bir güvenli NesNet – DHT sistemi geliştirmek için, bu çalışmada sunulan sistem tasarım önerileri, yazılım geliştirme süreçlerinin tamamını (analiz, tasarım, geliştirme, test ve entegrasyon, vb.) etkileyebilir; bu durum ek efor, süre ve maliyet gerektirebilir. Ancak buna karşılık olarak, kullanıcıların kişisel verileri (hak ve özgürlükleri) korunur, veri sorumlusu/işleyicisinin uğrayabileceği maddi/itibar kayıpları ve kurumun kapatılması veya hapis cezasına çarptırılması gibi yasal yaptırımlar önlenebilir.

Bu bölümde bu kanun ve genelgeye ilişkin özet bilgi verilmiş ve teknik çözüm önerileri sunulmuştur.

3.1. Kişisel Veri Korunumu (KVK) Kanunu ile Uyumluluk (Compliance with Turkish Personal Data Protection Law)

Türkiye'de NesNet nesneleri ve DHT ile ödeme yapılabilmesi için cihazdan (nesneden) ve kullanıcıdan elde edilecek, işlenecek ve saklanacak kişisel verilerin KVK kanunu ile uyumlu olması gerekmektedir. Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi içermektedir [12].

Bu bağlamda NesNet uygulama ve/veya DHT veri sorumlusu tarafından aşağıdakilerin yükümlülüklerin sağlanması gerekmektedir [12, 14, 17]:

Aydınlatma Yükümlülüğü: NesNet uygulama ve/veya DHT tarafından toplanacak verinin nasıl, kimin tarafından ve hangi nedenlerle toplanacağı konusunda kişinin bilgilendirilmesi gerekmektedir.

Açık Rıza: Kişisel verilerin NesNet uygulaması ve/veya DHT tarafından işlenebilmesi için kişilerin açık olurunun alınması gerekmektedir.

Veri Güvenliği: NesNet uygulaması ve DHT tarafından toplanan, işlenen, saklanan ve erişilen kişisel verilere ait veri güvenliğinin sağlanması gerekmektedir. Bu bağlamda

- Verilerin kriptografik yöntemler kullanılarak saklanması
- Kriptografik anahtarların güvenli ve farklı ortamlarda saklanması
- Veriler üzerinde gerçekleştirilen tüm işlemlerin güvenli bir şekilde günlük tutma (logging) aracı ile kayıt altına alınması
- Verilerin bulunduğu ortamlara ait güvenlik güncellemelerin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması ve test sonuçlarının kayıt altına alınması
- Verilere yazılım aracılığı ile erişim sağlanıyorsa bu yazılıma ait kullanıcı yetkilendirmesinin yapılması, gerekli güvenlik testlerinin düzenli olarak yapılması ve test sonuçlarının kayıt altına alınması
- Verilere uzaktan erişim sağlanıyorsa en az iki kademeli doğrulama yapılması

gerekmektedir.

Anonimleştirme/Silme/Yok Etme: Kişisel verilerin işlenmesini gerektiren durumun ortadan kalkması veya kullanıcının talebi üzerine kişisel verilerin NesNet uygulama ve/veya DHT tarafından anonim hale getirilmesi, silinmesi veya yok edilmesi gerekmektedir. Bu kapsamda yapılan tüm işlemlerin kayıt altına alınması ve kayıtların en az 3 yıl saklanması gerekmektedir. Anonimleştirme için aşağıdaki teknikler kullanılabilir:

- ***Maskeleme:*** Kişisel verilerin belirli alanları silinerek veya yaldızlanarak kişinin belirlenemez hale getirilmesidir.
- ***Toplulaştırma:*** Verilerin kümülatif hale getirilerek toplam değerinin yansıtılmasıdır.
- ***Veri Türetme:*** Mevcut verinin daha genel hali ile değiştirilmesidir.
- ***Veri Karması:*** Verilerin karılarak veriden kişinin belirlenemez hale getirilmesidir.

Sicil'e Kayıt Yükümlülüğü: Kişisel verilerin işlenmesine başlamadan önce, NesNet uygulama ve DHT veri sorumluları Veri Sorumluları Sicili'ne (VERBİS) kayıt olmakla yükümlüdür.

Yapılan Başvuruların Cevaplanması Yükümlülüğü: Kişiler, NesNet uygulama ve/veya DHT tarafından işlenen kendi kişisel verilerine ilişkin bilgi edinme hakkına sahiptir. Yapılan başvurulara ilişkin cevapların NesNet uygulama ve/veya DHT tarafından 30 gün içerisinde cevap verilmesi gerekmektedir.

Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü: Kişiler tarafından kendi verilerine ilişkin başvuruların reddedilmesi, cevabın uygun bulunmaması veya cevap alamaması gibi durumlarda kişiler kurula başvurabilir. Kurul tarafından yapılacak değerlendirme sonucunda kurul kararının NesNet uygulama ve/veya DHT veri sorumlusu tarafından 30 gün içerisinde yerine getirilmesi gerekmektedir.

Kişisel Verilerin Yurt Dışına Aktarılması: Kişisel veriler, ilgili kişinin açık rızası olmadan yurt dışına aktarılamaz.

KVK kanunun "Suçlar" başlıklı madde uyarınca Türk Ceza Kanunu'na (TCK) göre aşağıdaki yaptırımlar uygulanır [12, 13, 14, 26]:

- ***TCK 135:*** Kişisel verilerin hukuka aykırı olarak kaydedilmesi kişisel verileri hukuka aykırı olarak kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. Özel nitelikli kişisel veri işlenmesi halinde ceza yarısı oranında artırılır.
- ***TCK 136:*** Verileri hukuka aykırı olarak verme veya ele geçirme kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.
- ***TCK 137:*** Bu suçlar, kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenirse ceza yarı oranında artar.
- ***TCK 138:*** Verileri yok etmeme kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.
- ***TCK 140:*** Tüzel kişiler hakkında güvenlik tedbiri uygulanması yukarıdaki suçların işlenmesi dolayısıyla tüzel kişiler hakkında onlara özgü güvenlik tedbirlerine hükmolunacağı belirtilmiştir.

- ***KVK Kanunu Madde 17/f.2:*** KVK Kanunu'nun 7'nci (136) maddesine aykırı olarak kişisel verilerin silinmemesi veya anonim hale getirilmemesi halinde bir yıldan iki yıla kadar hapis cezası verilir.

Yukarıda özetlenen ve KVK kanunu nedeni ile doğabilecek olası hukuki sorunlara yönelik KVKK ve Türkiye Bilişim Vakfı tarafından önerilen teknik çözümlerin [14, 17] Nesnelerin İnterneti ve DHT ile dijital ödemeler için değerlendirmesi aşağıda verilmiştir:

Siber Güvenliğin Sağlanması: NesNet – DHT sistemin siber güvenliğinin sağlanması için güvenlik duvarı, internet ağ geçidi, rol ve yetkilendirme politikaları, anti-virüs ve anti-spam yazılımı, güncel yazılım sürümleri, güçlü şifre ve parola, güvenli iletişim teknikleri, vb. bileşenlerin ve yöntemlerin kullanılması, kullanılmayan yazılım ve servislerin kaldırılması önerilmektedir.

Kişisel Veri Güvenliğinin Takibi: NesNet –DHT sisteminde kişisel veri güvenliğin takibinde günlük tutma ve raporlama araçları ile sistemde gerçekleşen işlemler, kullanılan yazılım ve servisler, güvenlik sorunları ve anomalileri kayıt altına alınabilir.

Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması: Kişisel verilerin kaybolması veya çalınmasına engel olmak için gerekli fiziksel (kilitli dolapta saklama, yedekleme, vb.) ve/veya siber güvenlik (şifreleme ile güvenli veri saklama ve erişim sağlama, rol ve yetkilendirme ile erişimi sınırlandırma, vs.) önlemlerinin alınması önerilmektedir.

Kişisel Verilerin Bulutta Saklanması: Kişisel verilerin tutulduğu bulut depolama hizmeti sağlayıcısı tarafından gerekli güvenlik önlemlerinin alınması (verilerin kriptografik yöntemlerle şifreli olarak saklanması ve erişimin sağlanması, her bulut çözümü için farklı şifreleme anahtarların kullanılması, vs.), uzaktan erişim için en az iki kademeli doğrulama yapılması gerekmektedir.

Bilgi Teknolojileri Sistemleri Tedariki, Geliştirme ve Bakımı: Yeni sistemlerin tedariki, geliştirme ve bakım süreçlerinde veri sorumlusu tarafından güvenlik gereksinimlerin göz önüne alınması ve gerekli güvenlik önlemlerinin alınması (örneğin geliştirilecek yeni bir sistemin güvenlik tasarımın KVK kanunu gereksinimlerini sağlaması, sistem bileşeni bakım veya onarım için 3. partiye göndermeden önce kişisel verilerin bulunduğu disklerin çıkartılması, vb.) gerekmektedir.

Kişisel Verilerin Yedeklenmesi: Kişisel verilerin zarar görmesi, çalınması, kaybolması veya kötü amaçlı yazılımlar tarafından erişimin engellenmesi durumunda en kısa zaman içerisinde yedeklenen veriler ile tekrar faaliyete geçmesi. DHT veri değişmezliğini sağladığından DHT'deki veriler için yedekleme ihtiyacı olmayacaktır, ancak NesNet uygulaması özelinde kullanılan veriler için yedekleme önem arz etmektedir.

Kapalı ve İzin Gerektiren DHT Kullanmak: Kişisel ve ödeme verileri gibi kritik verilerin paylaşımının sınırlandırılması açısından kapalı ve izin gerektiren DHT kullanılabilir.

Kritik Verinin Saklanmaması ve Anonim Hale Getirilmesi: DHT'de saklanan veriler silinemeyeceğinden kişisel ve ödeme bilgisi içeren kritik verilerin saklanmaması, yalnızca anonim veri tutulması, gerekli olması durumunda kritik verinin, tercihen gizli ve özel bir ağda bulunan zincir-dışı sistemde tutulması (örneğin banka sunucusu) tercih edilmeli ve veri güvenliğinin sağlanması için veri gizleme, şifreleme, birleştirme gibi teknikler kullanılmalı.

Hata Kaydının Saklanması: Veri düzeltilmeye ilişkin talep gelmesi durumunda, konu verinin düzeltildiğine dair bilgi kayıt altına alınmalıdır. DHT'de silme işlemi yapılamadığından hata kayıt işlemi DHT yerine NesNet uygulama tarafında bir günlük tutma aracı ile yapılması tercih edilebilir.

3.2. 2019/12 Sayılı Bilgi ve İletişim Güvenliği Tedbirleri Cumhurbaşkanlığı Genelgesi ile Uyumluluk

(Compliance with the Turkish Presidential Circular Number 2019/12 on Information and Communication Precautions)

Kamu kurum ve kuruluşları ve kritik altyapı hizmeti veren işletmeler (Bankacılık ve Finans alanında kamu hizmeti veren işletmeler bu kategoriye dâhil) için geçerli olan genelgeye göre ve ödeme hesap bilgilerinin ve işlemlerin gizlilik derecesine sahip olduğu ve kritik veri içerdiği göz önüne alınarak, banka gibi kritik bir altyapı sağlayıcısı tarafından geliştirilecek bir NesNet – DHT sistemi tarafından aşağıda sıralanan isterler karşılanmalıdır.

Veri Depolama: Banka hesap bilgilerinin aralarında bulunduğu nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve verilerin yurtiçinde güvenli bir şekilde depolanması gerekmektedir. Bu veriler, kurumların kendi özel bulut veya kurum kontrolündeki yerli bulut hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanamaz.

Veri Erişimi ve Günlük Tutma: Ödeme ve kişisel bilgiler gibi kritik verilerin internete kapalı ve fiziksel güvenliği sağlanmış bir ortamda bulunan güvenli bir ağda tutulması, gerekmektedir. Bu ağda kullanılacak cihazlara erişimin kontrollü olarak sağlanması ve sistem günlük kayıtlarının değiştirilmeye karşı önlem alınarak saklanması gerekmektedir. Sisteme erişim yetkilendirmelerinin, yapılan iş ve ihtiyaca göre yapılması gerekmektedir. Ayrıca ödeme sistemin internete açık olan tarafta (örneğin NesNet cihazı ile ödeme işlemi yapabilmek için uygulama ve uygulama sunucusu arasındaki bağlantı) gerekli güvenlik önlemlerinin (güvenlik duvarı, uçtan uca tünelleme yöntemleri, yetkilendirme ve kimliklendirme mekanizmaları vb.) alınması gerekmektedir.

NesNet Cihaz Güvenliği: NesNet cihazla ödeme yapılabilmesi için, mevzuatta kodlu veya kriptolu

haberleşmeye yetkilendirilmiş kurumlar tarafından geliştirilecek yerli uygulamaların kullanılması gerekmektedir. NesNet cihazların kurum sistemlerine bağlanabilmeleri için kaynağından emin olunması gerekmektedir. Banka tarafından, örneğin beyaz listeme yöntemi ile, yalnızca onay verilen cihaz tipleri (örneğin Android ve iOS işletim sistemine sahip mobil cihazlar) ödeme yapabilecektir.

Veri Paylaşımı ve Haberleşme: Sosyal medya üzerinden ödeme bilgileri gibi kritik verilerin paylaşımı ve haberleşmesi yapılamayacaktır. Yerli ve milli kripto sistemlerinin geliştirilmesi teşvik edilerek, kurumlara ait gizlilik dereceli haberleşmenin bu sistemler üzerinden gerçekleştirilmesinin sağlanması gerekmektedir. Ödeme sistemlerinde hâlihazırda kullanılan kriptografik yöntemlerin bu bağlamda yeniden değerlendirilmesi gerekebilir.

Genelgeye göre ayrıca e-posta sistemlerinin ayarları güvenli olacak biçimde yapılandırılmalı, e-posta sunucuları, ülkemizde ve kurumun kontrolünde bulundurulması ve sunucular arasındaki iletişimin şifreli olarak yapılması sağlanmalıdır. Kurumsal olmayan şahsi e-posta adreslerinden kurumsal iletişim yapılmayacak, kurumsal e-postalar şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır.

Yayma ve Veri Güvenliği: Genelgeye göre ödeme gibi gizlilik dereceli bilgilerin işlendiği yerlerde nesnelerden elektromanyetik dalga yayılmasının önlenmesi konusundaki güvenlik (TEMPEST) veya benzeri güvenlik önlemlerinin alınması gerekmektedir.

Hâlihazırda dijital ödeme sistemlerinde hizmet uluslararası yüksek veri güvenliği sağlayan Payment Card Industry (PCI) Data Security Standard (DSS) standardı [27] ile sağlanmaktadır. Ayrıca, ödeme işlemlerinin gerçekleştirildiği sunucu ve ödeme hizmet noktası (POS cihazı ve ATM) arasındaki iletişim kablolu ve kriptografik yöntemlerle şifreli olarak gerçekleşmektedir. NesNet cihaz ile ödeme işleminde cihaz ve POS cihazı arasında gerçekleşen temassız (Near Field Communications, NFC) ödeme işlemleri şifreli olarak yapılmaktadır.

NesNet-DHT uygulaması şifreleme işlemlerinde veri güvenliğinin sağlanması için sunucu (backend) tarafında Hardware Security Module (HSM) donanımı kullanılabilir. HSM cihazı, fiziksel güvenlik, mantıksal güvenlik kontrolleri ve güçlü şifreleme yöntemleri kullanarak hassas verilerin güvenli bir şekilde iletilmesini, işlenmesini ve saklanmasını sağlamaktadır. PCI DSS uyumluluğu için ödeme sistemlerinde kullanılan HSM cihazlarına ait güvenlik seviyesinin Federal Information Processing Standard (FIPS) 140-2 seviye 3 veya üzeri olması önerilmektedir.

NesNet-DHT sisteminde son kullanıcı tarafından kullanılan NesNet (cihaz ve mobil/web, vs. uygulaması) tarafındaki veri güvenliğinin arttırılması için yazılımsal tedbir olarak whitebox kriptografi [28] gibi veri gizleme (data obfuscation) yöntemleri kullanılabilir. Whitebox kriptografi, veriyi gizleyerek ve rastgele saklayarak ödemede kullanılan kriptografik anahtarlar gibi hassas verilerin çalınmasını önleyebilmektedir. Ayrıca cihaz içerisinde hassas verinin güvenli bir şekilde saklanması, işlenmesi ve korunması için donanımsal tedbir olarak Trusted Execution Environment (TEE) veya Secure Environment (SE) ortamları kullanılabilir. TEE, cihazın "Rich" işletim sisteminde gerçekleşen güvenlik saldırılarından koruyan, cihazın ana işlemci içerisindeki güvenli bölgedir (yazılımsal ve donanımsal bileşen) [29]. SE ise hassas veriyi güvenli bir şekilde korumaya ve güvenilir uygulamaları koşturmaya yarayan, cihazın içerisinde bulunan mikroişlemci çiptir (donanımsal bileşen) [30]. Mobil uygulama ile ödeme işlemlerinin yapıldığı cihazlar ise PCI PA-DSS uyumlu olmak zorundadır. PIN girişinin yapıldığı cihazlar ile PCI PTS uyumlu olarak işlem gerçekleştirilmektedir. DHT ile ödemeler için bu standartları ile uyumluluk gerekli olmayacaktır, ancak güvenlik tasarımında faydalanılabilir.

Fiziksel ve Siber Güvenlik: Ödeme bilgilerinin işlendiği sunucu odası gibi kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında mobil ve/veya veri transferi özelliğine sahip cihazların bulundurulmaması gerekmektedir.

Genelgeye göre temin edilecek yazılım veya donanımların kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) açıklığı içermediğine dair üretici ve/veya tedarikçilerden taahhütname alınması gerekmektedir.

Yazılımların güvenli olarak geliştirilmesi ile ilgili tedbirler alınması gerekmektedir. Bu bağlamda Open Web Application Security Project (OWASP), ISO/IEC 27002, ISO/IEC TR 13335, NIST SP 800-14, SP 800-64, Common Criteria gibi standartlar ile uyumlu yazılım geliştirme yapılması önerilmektedir.

Temin edilen veya geliştirilen yazılımların kullanılmadan önce güvenlik testlerinden geçirilmesi gerekmektedir. Otomasyon ile kurum kendisi veya TÜBİTAK BİLGEM gibi güvenilir 3. parti kurumlar tarafından sızma testi, kaynak kod analizi, yük testi, dağıtık hizmet dışı bırakma (distributed denial of service (DDoS)) testi, sürekli zafiyet analizi testi, uygulama güvenlik testi, vb. uygun görülen siber güvenlik testleri yapılmalıdır. Ödeme sistemlerinde ayrıca canlıya geçişten önce PCI ve ödeme ağlarına ait uygulama ve sunucu güvenlik testleri de yapılmaktadır. Ayrıca genelgeye göre siber tehdit bildirimleri ile ilgili gerekli tedbirin alınması gerekmektedir.

BİGT'de belirtilen güvenlik tedbirlerinin uygulanmasına ilişkin yılda en az bir kere denetim yapılacak olup, denetim sonuçları ile yapılan düzeltici faaliyetleri içeren raporlar Dijital Dönüşüm Ofisi'ne iletilecektir. Söz konusu tedbirlere uyulmaması nedeniyle bir zafiyet oluşması

durumunda hâlihazırda ilgili mevzuatta belirlenen yaptırımlar geçerlidir. Örneğin arka kapı zafiyetinin duyurularak alımın iptali ve firmanın yasaklı duruma düşürülmesi gibi yaptırımlar uygulanabilecektir. Oluşabilecek zararın boyutuna göre gerek duyulması durumunda kurum içi adli veya idari soruşturma süreçleri işletilebilecektir [15].

4. TÜRKİYE'DE GÜVENLİ DİJİTAL ÖDEMELER İÇİN NESNET – DHT SİSTEM TASARIMI ÖNERİLERİ (IOT-DLT SYSTEM DESIGN RECOMMENDATIONS FOR SECURE DIGITAL PAYMENTS SYSTEMS IN TURKEY)

Bölüm 3'te belirtilen NesNet – DHT ödeme sistemlerin KVK Kanunu ve Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ile uyumluluk çerçevesindeki sistem tasarım önerilerine bu bölümde yer verilmiştir. Geliştirilmesi amaçlanan NesNet-DHT ödeme sisteminin fiziksel olarak Türkiye sınırları içerisinde bulunduğu ve hizmet verdiği varsayılmıştır. Benzer şekilde, veri sorumlusunun ve veri işleyicisinin ülkemizde bulunduğu ve yalnızca Türkiye'deki kullanıcılara ait kişisel verilerin işlendiği varsayılmıştır.

Ülkemiz hukukuna uygun bir NesNet - DHT ödeme sistemi geliştirebilmek için kişisel verilerin yönetilebilmesine ve sistemin kişiselleştirilmesine olanak sağlayan DHT altyapıları kullanılmalıdır.

Hyperledger Fabric sürüm 1.2 ve üzeri platformunda kişisel verilerin yönetilmesi için 'Private Data Collection' (Özel Veri Toplama) fonksiyonu ile özel veri toplama olanağı sağlanmaktadır. Bu fonksiyon sayesinde kişisel veri, ağdaki belirli bir düğümde bulunan harici bir veritabanında saklanabilir. Blokzincirde yalnızca verinin özet değeri saklanır ve üyelerle paylaşılır.

IBM özet bulutu üzerinde çalışan Hyperledger Fabric blokzincir tabanlı IBM Blockchain platformu, sağladığı veri şifreleme yeteneği ve Hardware Security Module (Donanım Güvenlik Modülü) desteği ile şifreleme anahtarlarının güvenli bir şekilde saklanması ve verilerin blokzincirde ve veritabanda güvenli bir şekilde saklanmasını sağlar. Güvenli Servis Sandığı (Secure Service Container) ile işletim sisteminin güvenlik ataklarına maruz kalma riski azaltılır.

R3 Corda, izinli blokzincir yapısına sahip olup kişisel verinin yönetilmesine olanak sağlayan kurumsal blokzincir uygulama geliştirme platformudur. Veri gizliliği ve kişisel veri güvenliği korunumu için aşağıdaki hizmetler sağlanmaktadır:

• ***Kapıcı hizmeti (doorman service):*** Ağa katılan kullanıcılara ve operatörlere ait ad, telefon numarası, e-posta adresi gibi kişisel verileri toplar. Bu veriler özel ve güvenli bir veritabanında saklanır, ağdaki üyelerle paylaşılmaz. Gerektiği durumda kişisel veriler veritabanından silinir.

• ***Ağ haritası (network map):*** Üyelerin birbirleriyle iletişim kurmalarını sağlar. Bu hizmet kapsamında ağ üyeleri ile kişisel veri paylaşılmaz.

• ***Noter hizmeti (notary service):*** Ağda konsensüs (uzlaşma) sağlar ve işlemlerin eşsiz ve kesin (final) olduklarını garanti eder. Bu hizmet kapsamında kişisel veri işlenmez.

Ayrıca veri ihlalinin tespit edilmesi durumunda ilgili tarafların zamanında bilgilendirilmesi için gerekli yöntemler bulunmaktadır.

IBM ve R3 Ekim 2020'de birlikte çalışarak IBM LinuxONE ile yerel (on-premise) ve IBM Cloud'den oluşmak üzere hibrit bulut hizmetinin 2021 yılının ilk üç ayı içinde 'IBM Cloud Hyper Protective Services' altında hizmete sunmayı planlandıklarını duyurdu.

Ülkemiz hukukuna uygun bir NesNet–DHT sistemi geliştirebilmek için ya yerel (on-premise) Hyperledger Fabric, R3 Corda, IBM Blockchain gibi kişisel verilerin yönetilmesine olanak sağlayan DHT tabanlı sistemlerin kullanılması ya da yerli bir NesNet-DHT ödeme sisteminin geliştirilmesi önerilmektedir.

Hyperledger Fabric, R3 Corda, IBM Blockchain gibi platformlar kullanılarak KVK kanunu ile uyumluluk sağlanması mümkün olabilir. Ancak yerli/milli kripto haberleşmesi, yerel bulut hizmet sağlayıcısı, yerel e-posta sunucusu, yerli mobil uygulamanın kullanılması vb. kısıtlarından dolayı BİTG ile uyumluluk sağlanamayabilir. Bu bağlamda söz edilen mevcut DHT platformları tabanlı veya sıfırdan NesNet-DHT ödeme sistemi geliştirilmesi için sistem tasarım önerileri aşağıda sunulmuştur.

4.1. Üst Düzey Sistem Mimarisi (High Level System Architecture)

NesNet-DHT platformun katmanlı mimarisindeki (bkz. Şekil 1) katmanlar aşağıdaki özelliklere sahiptir:

• ***Kullanıcı Ara Yüzü:*** Son kullanıcının NesNet cihazını kullanarak NesNet-DHT platformu uygulama katmanı ile etkileşimine olanak sağlayan bileşendir. Kullanıcı ara yüzü, örneğin, NesNet cihaz düğmesi, ekranı, sesli komut vermeye yarayan sensörü veya NesNet cihaz üzerinde kurulu olan web/mobil, vb. uygulama olabilir.

• ***Uygulama Katmanı:*** NesNet cihazı kullanıcı ara yüzü (web/mobil, vb.) uygulamaların işlevselliklerini sağlayan katmandır.

• ***İşleme Katmanı:*** NesNet iletim katmanından alınan verileri işleyen, analiz eden ve saklayan katmandır. Veritabanı, büyük veri işleme, bulut bilişim, vb. modüllere sahiptir.

• ***İletim Katmanı:*** Telli / telsiz ağlarda ilgili haberleşme teknolojisi (Wireless Fidelity (Wi-Fi), Bluetooth, Radio Frequency Identifer (RFID), Local Area Network (LAN),

vb.) ile sezim ve işleme katmanı arasındaki veri iletimini sağlayan katmandır.

• ***Sezim Katmanı:*** NesNet cihaz sensörleri ile veri sezimleyen ve iletim katmanına ileten fiziksel katmandır.

Şekil 1. NesNet-DHT platformu katmanlı mimarisi
(Layered architecture of IoT-DLT platform)

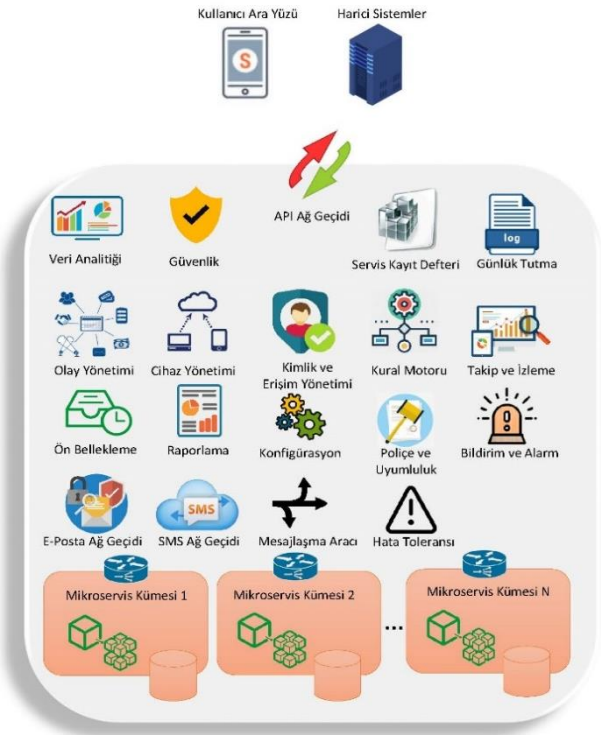
4.2. NesNet-DHT Düğümü Mimarisi (IoT-DLT Node Architecture)

BİTG'ye uyumluluk için NesNet-DHT düğümü uygulama sunucusunun kurum içerisinde veya KVK kanunu ve BİTG'ye uygun ve kurum kontrolündeki yerli bulut hizmet sağlayıcı tesisinde barındırılması gerekmektedir. Maliyet, güvenlik ve gizlilik, otomasyon, ölçekleme, esneklik / özelleştirilebilme ve iş sürekliliği gibi avantajları nedeni ile özel bulut mimarisi tercih edilebilir. Bulut mimariyi destekleyen ve dağıtık yapılar için uygun olan mikroservis yazılım mimarisi [31] kullanılabilir.

Mikroservis yazılım mimarisinin avantajları aşağıdaki gibidir:

- Ölçeklenir, esnek ve modüler yapıya sahip
- Platform (veritabanı, yazılım dili, işletim sistemi, vb.) bağımsız
- Farklı teknolojileri aynı çatı altında kullanma imkânı
- NesNet ve DHT gibi dağıtık mimarili yapılar için uygun
- Bulut mimariye uygun
- Yazılımı hızlı sahaya yerleştirme (deployment)
- Bir mikroservis güncellendiğinde diğer mikroservisler etkilenmez, spesifik bir mikroservisi yatay ölçeklendirmek mümkün

Mikroservis, küçük, otonom ve bir arada çalışan servislerdir. Servisler birbirinden bağımsız olarak çalışır ve her servisin kendisine ait veritabanı (sanal veya fiziksel)



Şekil 2. NesNet-DHT düğümü uygulama sunucusu yazılım mimarisi (IoT-DLT node application server software architecture)

bulunur. NesNet-DHT düğümüne ait önerilen yazılım mimarisi Şekil 2 ile gösterilmektedir.

Mikroservis mimarisi konteyner yapısı üzerinde yerleştirilebilir. Konteyner yapısının avantajları aşağıdaki gibidir [32]:

- İşletim sistemi düzeyinde sanallaştırma sağlamaktadır.
- Uygulamaları birbirinden ve altyapıdan izole etmeye yarar.
- Platform bağımsızdır; herhangi bir sunucu, altyapı veya bulut yapısı üzerinde çalışabilir.
- Kolay ve hızlı bir şekilde ölçekleme yapmaya olanak sağlamaktadır.

Uygulama sunucusu katman (istemci (client) sunum katmanı, iş katmanı, veri aktarım katmanı, vb.) ve/veya kiracı (tenant), örneğin aynı bankanın farklı şubesi, bazında ayrı konteyner yapıları kullanılabilir.

Konteynerlar arasında ortak olabilecek (cross-cutting) bileşenler (bkz. Şekil 2):

- ***API Ağ Geçidi:*** NesNet-DHT uygulama sunucusuna internet üzerinden kullanıcı ara yüzü ve/veya harici sistemler tarafından Application Programming Interface (API) ağ geçidi ile tek noktadan bağlanılır. İnternet üzerinden kritik veri paylaşımı yapılmamalıdır.
- ***Bildirim ve Alarm Yönetimi:*** Veri analitiği sonucunda ve/veya günlük tutma ***esnasında*** tespit edilebilecek

anomali ve güvenlik tehditleri ile ilgili alarm yönetimi. Kullanıcılara alarm veya gerçekleştirilen işlemler ile ilgili kullanıcı ara yüzüne mobil/web uygulama, SMS, e-posta, vb. yöntem ile bildirim gönderimi.

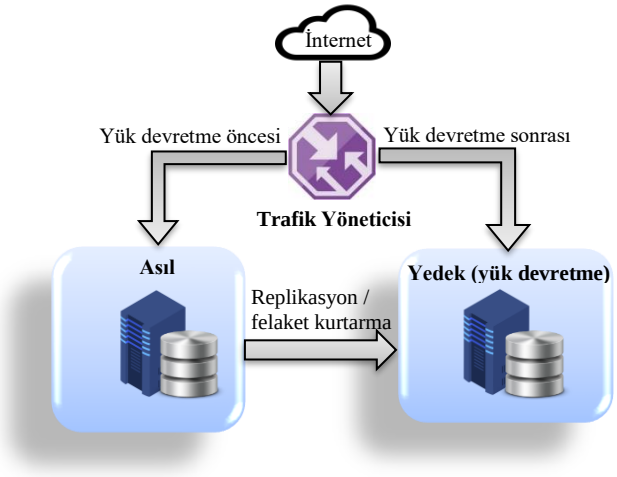
- ***E-posta Ağ Geçidi:*** Türkiye'de bulunan ve kurumun kontrolündeki e-posta sunucusuna şifreli olarak bağlanmak için kullanılacak olan e-posta ağ geçidi. E-posta ile ödeme veya kişisel veri gibi hassas verilerin iletimi yapılmamalıdır. Anti-virüs ve spam filtresi gibi güvenlik önlemleri bulunmalıdır. Kurumsal olmayan şahsi e-posta adreslerinden kurumsal iletişim yapılmamalı, kurumsal e-postalar şahsi amaçlarla kullanılmamalıdır.
- ***Kimlik ve Erişim Yönetimi:*** Uygulamalara erişim için dijital kimlik yönetimi, kimlik doğrulama, rol ve yetkilendirme poliçelere uygun bir şekilde yapılmalıdır. Uzaktan erişim için en az iki kademeli doğrulama yapılmalıdır. Geleneksel kimlik doğrulama yöntemleri (identity authentication management) yerine NesNet cihazları için daha uygun olan kimlik ilişki yönetimlerinin (identity relationship management) kullanılması önerilmektedir. Kimlik doğrulama işlemci gücü sınırlı NesNet cihazı üzerinde gerçekleştirmek yerine NesNet cihazın bağlı olduğu akıllı mobil cihaz üzerinde yapılabilir [33]**.** Şifresiz doğrulama özelliği sayesinde tüm NesNet cihazları için uygun olan, çoklu kademeli (multi-factor) doğrulama, karşılıklı (mutual) doğrulama ile güçlü doğrulama özelliklerine sahip, Fast Identity Online (FIDO) gibi doğrulama yöntemleri tercih edilebilir. Internet Engineering Taskforce (IETF) NesNet cihazları için optimize edilmiş ve "Authentication and Authorization for Constrained Environments (ACE)" isimli doğrulama standartları üzerine çalışmalar yürütmektedir, bu çalışmalardan da sistem tasarımında faydalanılabilir. Ayrıca NesNet cihazları için optimize edilmiş (örneğin IEEE 1609.2 standartlı) dijital sertifikaların kullanılması tercih edilebilir.
- ***Konfigürasyon Yönetimi:*** Sistemdeki donanım ve yazılımları (veritabanı, uygulama, haberleşme kanalları, mikroservisler, vb.) tespit eder ve bileşenleri yapılandırır. Sistem üzerinde yapılan değişiklikleri kontrol ve dokümante ederek sistemin doğru konfigürasyonda olmasını ve yapılan değişikliklerin takip edilebilmesini sağlar. Bu nedenle siber güvenlik ve yedekleme açısından önem taşımaktadır.
- ***Kural Motoru:*** NesNet cihaz, veri, iletişim, uygulama, vb. tipleri için tanımlanmış poliçelerin uygulanması için sistemin uçtan uca (iş akışı, olay yönetimi, rol ve yetkilendirme, alarm yönetimi, mesajlaşma, vb. için) yapılandırılmasını ve kuralların uygulanmasını sağlar.
- ***Cihaz Yönetimi:*** NesNet cihazların uçtan uca yaşam döngülerini yönetir (NesNet cihaz erişim yönetimi ve doğrulama, yapılandırma ve kontrol, uzaktan yönetim, izleme ve tanı, yazılım güncellemeleri ve bakım, vb.).
- ***Güvenlik:*** NesNet cihazlarına ilişkin risk analizin yapılması (cihaz keşfi, donanım yazılımı risk analizi, cihaz özelinde risk analizi, vb.), otomatik poliçe üretimi, mevcut poliçelerin uygulanması ve uygunluk kontrollerinin yapılması, bilinen ve sıfır gün ağ ve NesNet cihaz saldırı tehditlerinin önlenerek uçtan uca NesNet-DHT sistemin siber güvenliği sağlanmalıdır. Bu amaçla, NesNet cihazları ile bütünleşik çalışan bilgi güvenliği ve olay yönetimi (Security Information and Event Management (SIEM)) aracı [34] kullanılabilir. SIEM aracı, veri analitiği, olay yönetimi, günlük tutma, raporlama, poliçe, bildirim ve alarm yönetimi araçları, vb. araçlar ile bütünleşik çalışarak veya içererek, sistemin uçtan uca gerçek-zamanlı bilgi güvenliğini sağlamaktadır.
- NesNet cihaz keşfinde, kurum tarafından belirlenecek poliçelere uygun beyaz liste ve/veya kara liste kullanılarak beyaz/kara listeme yöntemi kullanılabilir. NesNet cihazında kullanılacak uygulama, mevzuatta kodlu veya kriptolu haberleşmeye yetkilendirilmiş kurumlar tarafından geliştirilecek yerli uygulamalar olmalıdır. Uygulama whitebox kriptografi gibi veri gizleme yöntemi kullanılarak geliştirilmeli ve ödeme işlemleri için kullanılacak kriptografik anahtarların SE veya TEE gibi cihazın güvenli alanında saklanması gerekmektedir.
- ***Hata Toleransı:*** Hata toleransı, bir mikroservisin arıza yapması durumunda sistemin olumsuz etkilenmemesi için önlem olarak yedeğinin bulunmasıdır.
- ***Günlük Tutma:*** Sistemde gerçekleşen işlemler günlük tutma (logging) aracı ile kayıt altına alınmalı ve değiştirilmeye karşı önlem alınarak saklanmalıdır. Yetkisiz erişimin önlenmesi için rol ve yetkilendirme ile günlüklere erişim sağlanmalıdır. Sistem günlük kayıtları üzerinde yapılan tüm işlemler (erişim, değişiklik, silme, vb.) kayıt altına alınmalı ve en az 3 yıl saklanmalıdır. Kişisel veri işlemeye ilişkin rıza kayıtları (rıza verme veya geri çekme), tarih, zaman damgası, IP adresi, vb. bilgiler ile birlikte tutulmalıdır.
- ***Mesajlaşma Aracı:*** Günlük tutma gibi sistemde dağıtık gerçekleştirilen işlemlerin merkezi olarak işlenebilmesi için mesajlaşma aracı kullanılabilir.
- ***Olay Yönetimi:*** NesNet cihazları ile ilgili olayların (cihaz NesNet-DHT ağına katıldı, çıkartıldı, kendisi ile ilgili bilgi talep etti, vb.) poliçelere uygun olarak yönetimi, ilgili işlem veya süreçlerin yürütülmesini sağlar. Güvenlik olay yönetimi SIEM ile birlikte yapılabilir.
- ***Ön Bellekleme:*** Ön bellekleme, geçici bir depolama alanında verinin saklanması ile veritabanı üzerindeki iş yükünü, veri erişimindeki gecikmeyi ve ağ trafiğini azaltarak sistem başarımını ve dayanıklılığını arttırmaya yarar. Ön bellekte mümkün olduğunca hassas veri saklanmamalı, yetkisiz erişimin engellenebilmesi için rol ve yetkilendirme ile erişim sağlanmalı. Veri gizliliği ve bütünlüğün sağlanması için ön bellekte tutulan her obje için farklı şifreleme anahtarı kullanılarak veri şifreleme yapılmalı ve TLS ile sunucu ve istemci arasında uçtan uca kanal şifreleme ile veri iletişimi gerçekleştirilmelidir.
- ***Poliçe ve Uyumluluk:*** NesNet cihazları dâhil olmak üzere NesNet-DHT sistemin uyması gereken poliçelerin ve uyumluluk kıstasların tanımlanması güvenlik açısından gerekmektedir. Poliçeler, veri, mesaj, kullanıcı, cihaz, uygulama, iletişim, vb. tipine göre belirlenebilir. Güvenlik servisi ile entegre çalışabilir.

- ***Raporlama:*** Günlük tutulan verilerin rapor haline getirilmesi için (statik/dinamik) raporlama araçları kullanılabilir. Yetkisiz erişim ile kişisel verilerin görüntülenmesi ve/veya raporlar üzerinde değişiklik yapılmasının önlenebilmesi için rol ve yetkilendirme tanımlarına uygun ve doğrulama yapılarak raporlama aracına erişim sağlanmalıdır. Güvenlik ihlallerine ilişkin raporlar, güvenlik servisi ile entegre ve otomatik olarak yetkili mercilere gönderimi sağlanabilir.
- ***Servis Kayıt Defteri:*** Oto-ölçekleme, arıza veya güncelleme sonucunda mikroservislerin çalışma durumları ve ağ konumları dinamik olarak değişebilmektedir. Mikroservislerin değişen ağ konumlarının takibini kolaylaştırmak için servis keşfi otonom olarak yapılmalıdır. API ağ geçidi (veya ayrı bir servis keşif bileşeni) tarafından yapılan servis keşfi esnasında tespit edilen mikroservislerin ağ konumları servis kayıt defterine kaydedilir. Böylece API ağ geçidi, servis kayıt defterine göre ağ trafiğini ilgili mikroservislere yönlendirir.
- ***SMS Ağ Geçidi:*** Kullanıcılara SMS ile bildirim göndermek için SMS sunucusuna bağlanmak için kullanılan SMS ağ geçidi. SMS ile hassas bilgi iletimi yapılmamalıdır.
- ***Takip ve İzleme:*** Dağıtık yapıya sahip NesNet-DHT sisteminde, mikroservisler birbirleri ile senkron ve asenkron olarak haberleşmektedir. Bu nedenle sistemde gerçekleşen olaylarla ilgili izlemenin dağıtık olarak yapılması gerekmektedir. Dağıtık izleme, olayların uçtan uca takibine olanak sağlaması neden ile sistem başarımın takibi ve arıza giderme açısından önemlidir.

Geleneksel yedekleme yöntemleri (bkz. Şekil 3) mikroservis mimarili dağıtık sistemler için uygun/yeterli olmayabilir. Mikroservis mimariye sahip bir uygulamanın yedeklenmesinde tutarlılık, erişebilirlik ve bölümleme (consistency, availability and partition tolerance (CAP)) teoremi [31] göz önüne alınmalıdır. Bu teoreme göre, dağıtık veritabanların bulunduğu mikroservis mimarisinde erişilebilirlik tutarlılık, erişebilirlik ve bölümleme arasında ödünleşim bulunmaktadır. Durum tutarlılığın ve erişebilirliğin aynı anda sağlanabilmesi için örneğin birden fazla mikroservis küme haline getirilerek (bkz. Şekil 2) uyumlu biçimde (lockstep) yedeklenebilir. Öte yandan bölümlemenin ve erişebilirliğin aynı anda sağlanması tercih edilirse, sistemde tutarlılık garanti edilemeyebilir veya nihai (eventual) tutarlılığa sahip olabilir.

4.3. NesNet Cihaz Mimarisi (IoT Device Architecture)

Genel NesNet cihaz mimarisi Şekil 4 ile gösterilmiştir. NesNet cihazlarında kullanılan haberleşme protokolleri, veri formatları ve işlemci gücü nedeniyle her cihaz için geçerli olabilecek tek siber güvenlik çözümü bulunmamaktadır. Sınırlı işlem gücü, batarya ömrü ve hafızaya sahip olmalarından dolayı standart güvenlik yöntemlerini destekleyemeyebilirler ve aşağıdaki güvenlik tehditlerine maruz kalabilirler [35], [36]:



Şekil 3. NesNet-DHT düğümü veri tabanı altyapısı ve felaket kurtarma (IoT-DLT node database infrastructure and disaster recovery)

- ***Gizlilik:*** Hassas verinin cihaz üzerinden görüntülenmesi, cihazın çalınması veya klonlanması
- ***Hizmet Hırsızlığı:*** Kimlik doğrulama zafiyetlerinin kötüye kullanımı sonucunda yetkisiz cihazların veri veya hizmetlere erişimin sağlanması
- ***Veri Bütünlüğü:*** Yetkisiz mesajlar gönderilmesi veya yetkisiz biri tarafından cihazın ele geçirilmesi ile bilgi kirliliğin oluşması
- ***Erişebilirlik:*** Hizmet engelleme (denial of service) saldırısı sonucunda NesNet cihazın mesaj gönderimine engel olunması

Saldırganın bakış açısı ile maliyet ve fayda bakımından, en çok aşağıdaki tipteki saldırıların gerçekleşmesi beklenir [35]:

- ***Yazılım Saldırıları:*** Kötü amaçlı yazılım, sosyal mühendislik
- ***Haberleşme Saldırıları:*** İki bağlantı noktası arası bağlantıyı izleme saldırısı (man-in-the-middle attack), zayıf rastgele sayı üreteci (weak random number generator), kod zafiyetleri

NesNet cihazların yazılım ve haberleşme saldırılarından korunabilmeleri için, NesNet cihaz tasarımında göz önüne alınabilecek bazı güvenlik önlemleri aşağıda verilmiştir.

Haberleşme Saldırıları Güvenlik Önlemleri [35], [36]**:**

- ***Paket şifreleme:*** Düşük karmaşıklıklı olan bu yöntemde amaç, şifreleme ile verinin yetkisiz taraflar tarafından erişilmesine ve değiştirilmesine engel olarak gizliliği sağlamak ve veri bütünlüğünü korumaktır.
- ***Tekrarlama (replay) önleme:*** Düşük karmaşıklıklı bu yöntemde amaç, kayıtlı mesajların tekrar gönderimine engel olmaktır.
- ***Hafif mesaj doğrulama kodu:*** Düşük karmaşıklığa sahip bu yöntem ile düşük kapasiteli NesNet cihazları

için optimize edilmiş hafif (düşük karmaşıklıklı) kriptografi ile üretilecek mesaj doğrulama kodu (message authentication code (MAC)) kodu ile mesajların değiştirilmesine engel olunması amaçlanmaktadır.

Şekil 4. NesNet cihaz mimarisi (IoT device architecture)

- ***Bağlantı noktası (port) koruma:*** Düşük karmaşıklıklı bu metotta, Saldırgan tarafından bağlantı noktasına erişimine engel olunması hedeflenmektedir. Kullanılmayan portlar kapatılmalıdır.
- ***Çoklu önceden paylaşılan anahtar:*** Düşük karmalıklıklı bu yöntemde, amaç düşük kapasiteli başsız (headless) NesNet cihazları için, Wi-Fi ağlarında Wi-Fi Protected Access 3 (WPA3) ile, şifrelemeli haberleşme yapılabilmesi için önceden çoklu simetrik/gizli anahtarın paylaşılmasıdır. WPA3 standardında cihaz ve grup spesifik parola belirlenebilmekte, ve aynı SSID için çoklu önceden paylaşılan anahtar desteklenebilmektedir. Kullanıcı ve cihaz arasında bire bir ilişki sağlayarak kullanıcı takibine olanak sağlamaktadır. Böylece NesNet cihazların güvenliği arttırmakta ve yazılımı sahaya yerleştirmede esneklik sağlamaktadır.
- ***Karşılıklı doğrulama:*** Orta yükseklikte karmaşıklığa sahip bu yöntemde, NesNet cihazları için optimize edilmiş karşılıklı doğrulama yöntemleri (FIDO, Physically Unclonable Function (PUF), vb.) kullanılarak güvenli haberleşme ve cihaz ve kişi takibi yapılması amaçlanmaktadır [33].
- ***Açık anahtar paylaşımı:*** Yüksek karmaşıklığa sahip bu yöntemde, kötü amaçlı iletişime engel olunması hedeflenmektedir.
- ***Kanal şifreleme:*** Yüksek karmaşıklıklı Secure Shell (SSH), Transport Layer Security (TLS), vb. kanal şifreleme yöntemleri kullanılarak istemci ve sunucu arasındaki haberleşmede kanal şifrelemesi kullanarak kötü amaçlı iletişime engel olunması amaçlanmaktadır.

Yazılım Saldırıları Güvenlik Önlemleri [37]**:**

- ***Güvenli bootloader:*** Orta yükseklikte karmaşıklığa sahip olan bu yöntemde amaç, Yalnızca yetkili donanım yazılımı firmaları tarafından erişimi sağlamaktır.
- ***Güvenli hafıza:*** Orta yükseklikte karmaşıklığa sahip bu yöntemde, NesNet cihazı içerisindeki TEE, vb. güvenli yazılım alanında ödeme ve haberleşme için kullanılan kriptografik anahtarların saklanması hedeflenmektedir.
- ***Veri/bellek karma, bağlantı zamanı yeniden sıralama:*** Orta karmaşıklıklı bu yöntemde, NesNet cihazında bulunan dosyaların veya program içerisindeki verilerin veya belleğin sırasının değiştirilerek işletim sistemine yönelik saldırıların önlenmesi amaçlanmaktadır.
- ***Bütünlük doğrulama:*** Orta karmaşıklığa sahip bu yöntemde amaç, USB gibi takılır cihazların NesNet'e bağlanmasına izin vermeden önce bütünlüğün doğrulanarak malware, virüs gibi kötücül yazılımları engellemektir.
- ***Kurcalama tespiti:*** Yüksek karmaşıklıklı bu yöntemde, NesNet cihaza kaba kuvvet saldırısı ile izinsiz girişin önlenmesi amaçlanmaktadır. NesNet cihazın yazılımsal hata nedeni ile çökmesi, vb. hataların sistem günlüklerinden tespit edilerek saldırıların önlenmesi hedeflenmektedir.
- ***Veri ve kod gizleme:*** Yüksek karmaşıklığa sahip olan bu yöntemde amaç, whitebox kriptografi ile veri ve kod gizleyerek uygulama güvenliğini arttırmaktır. NesNet için optimize edilmiş hafif whitebox kriptografi ile NesNet cihazında ödeme ve haberleşme gibi işlemlerde kullanılacak şifreleme anahtarları güvenli bir şekilde cihazda saklanabilir. NesNet cihazındaki whitebox uygulaması ile birlikte çalışacak olan sunucu tarafındaki hızlı blackbox kriptografi uygulaması ile uçtan uca güvenliği sağlanabilir [38], [39].

4.4 Nesnelerin İnternetinde Kişisel Verilerin Kullanımı (Usage of Personal Data in IoT)

Bir NesNet cihazın NesNet-DHT ağına bağlanabilmesi için öncelikle ağa kayıt olmalıdır. Bu amaçla, NesNet cihazı, kendisi ile ilgili bilgileri içeren cihaz parmak izini (device fingerprint) oluşturur ve NesNet-DHT düğümüne iletir.

Parmak izi oluşturma işlemi, büyük bir veri setinin daha küçük bir bit dizgisine eşleştirilmesidir (bkz. Şekil 5). Parmak izi fonksiyonu olarak yaygın olarak bir özet (hash) fonksiyonu kullanılır. Parmak izinden girdinin eşleştirilebilmesi için parmak izin eşsiz olması gerekmektedir. Literatürde parmak izi algoritmaları arasında Rabin's algoritması gibi kriptografik olmayan

özet fonksiyonları ve Message Digest (MD) ve Secure Hash Algorithm (SHA) ailelerine ait kriptografik özet fonksiyonları yaygın olarak kullanılmaktadır. Rabin's algoritması gibi kriptografik olmayan özet fonksiyonları, kriptografik özet fonksiyonlarına göre daha hızlıdır, ancak kötü amaçlı saldırılara karşı koruma sağlamamaktadırlar. Kriptografik özet fonksiyonları, aşağıda belirtilen özelliklerinden dolayı cihaz parmak izi fonksiyonu olarak tercih edilmektedirler [40]:

- ***Deterministik*:** Rastgele olmayan şekilde parmak izi oluşturma; aynı mesaj ile aynı parmak izi üretilmektedir.
- ***Tek yönlü*:** Özet değerinden girdiyi elde etmek mümkün değildir.
- ***Çığ etkisi (avalanche effect)*:** Girdide ufak bir değişiklik özet değerinde büyük bir değişikliğe neden olmaktadır
- ***Çarpışmaya dayanıklı (collision resistant):*** Aynı özet değerinden iki farklı girdi elde etmek mümkün değildir.
- ***Öngöründü (pre-image) saldırısına dayanıklı*:** Belirli bir özet değerine sahip girdiyi elde edilmesi olan öngöründü saldırısına karşı dayanıklıdır.

Şekil 5. Parmak izi oluşturma işlemi (Fingerprinting)

Cihaz parmak izi, cihaz ve kullanıcı takibi amacı ile kullanılmaktadır. Güvenilir olmayan cihazları ve güvenilir bir cihaz ile ağa erişmeye çalışan yetkisiz kullanıcıları tespit etmek ve engellemek açısından önemli bir güvenlik unsurdur.

Parmak izi aşağıdakiler cihaz ve ağ bilgilerini içerebilir:

- ***Ağ Bilgileri*** (Ağ konfigürasyonu, Internet Protocol (IP) adresi, Media Access Control (MAC) adresi, Wi-Fi Service Set Identifier (SSID), GSM şebeke adı, vb.)
- ***Batarya Bilgileri*** (cihazın şarj edilme sıklığı gibi pil kullanım profili)
- ***Cihaz Aygıt Yazılımları*** (yüklü olan sanal klavyeler, ses ve video kod çözücüleri, mevcut sensörler, ekran, vb.)
- ***Cihaz Bilgileri*** (Cihaz tipi, adı, üreticisi, oryantasyonu)
- ***Cihaz Kimliği*** (International Mobile Equipment Identity (IMEI), Universally Unique Identifier (UUID), Object Identifier (OID), Unique Device Identifier (UDID), Advertising Identifer (ADID), vb.)
- ***Dil ve Zaman*** (yerel dil, yerel saat dilimi)
- ***Donanım Bilgileri*** (Hafıza, bellek, çekirdek ve işlemci bilgileri)
- ***Ekran Bilgileri*** (çözünürlük, parlaklık, vb.)
- ***Güvenli Haberleşme Protokol Bilgileri*** (Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) versiyonu ve el sıkışma bilgileri)
- ***İşletim Sistemi*** (işletim sistemi adı ve versiyonu, boot, jailbreak/rooted olma durum)
- ***Uygulamalar*** (cihazda kurulu olan uygulamaların listesi)

Cihaz bilgileri ile kişi ve davranışı tespit edilebileceğinden, bu bilgiler kişisel veri olarak nitelendirilmektedir. Kişisel veri olmasından dolayı ve DHT'de silme işlemi yapılamadığından cihaz parmak izinin DHT üzerinde saklanmaması gerekmektedir. Cihaz parmak izi, NesNet-DHT uygulama sunucusunda KVK kanunu ve BİTG ile uyumlu bir şekilde saklanabilir. Bu verilerin cihazdan elde edilmesi ve işlenmesi için öncelikle kullanıcının açık rızası alınmalıdır. Kullanıcı rızası alındıktan sonra elde edilecek verilerin işlenmesi ve saklanması için kriptografik parmak izi oluşturma fonksiyonları ve yöntemleri kullanılabilir.

Cihaz parmak izi ile birlikte kullanılan kriptografik yöntemler aşağıdaki gibidir [41]:

- ***Kimlik doğrulama (authentication):*** Kriptografik doğrulama algoritmaları ile cihaz parmak izinden cihazın ve/veya cihazı kullanan kişinin doğruluğu tespit edilir.
- ***Şifreleme ve güvenli haberleşme*:** Cihaz parmak izi, gizli veya simetrik anahtar olarak kullanılabilir. Şifreleme anahtarı olarak kullanılarak güvenli haberleşme yapılabilir. Parmak izi, özet fonksiyonundan geçirilerek yeni kriptografik anahtarlar üretilebilir.

Güvenlik açısından cihaz parmak izin klonlanamaz bir şekilde oluşturulması önem arz etmektedir. Bu bağlamda fiziksel klonlanamaz fonksiyon (physically unclonable function (PUF)) [41] kullanılabilir. Bu yöntem ile eşsiz kimliği bulunmayan NesNet cihazları için kriptografi ile eşsiz güvenlik anahtarı oluşturularak cihaz parmak izinin klonlanması engellenir. PUF, hafif ve maliyet etkin olması ve NesNet cihazlarında kriptografik anahtar gibi varlıkları saklamayı gerektirmeden güvenli doğrulama yapabilmesi nedeni ile NesNet için cazip bir yöntemdir.

NesNet cihazlarında aşağıdaki güçlü PUF protokolleri tercih edilebilir:

- ***Gizlenmiş zorluk-tepki:*** Makine öğrenmesi saldırılarına karşı koruma sağlayan PUF doğrulama algoritması.
- ***Karşılıklı doğrulama:*** NesNet cihazlarında karşılıklı doğrulamayı destekleyen PUF protokolü.

5. SONUÇ VE ÖNERİLER (CONCLUSION AND SUGGESTION)

NesNet ekosistemindeki güvenlik açıkları nedeni ile ülkemizde DHT üzerinden güvenli dijital ödemelerde yaygınlaşabilmesi için henüz yeterince olgunlaşmadığı değerlendirilmektedir. Düşük işlemci gücüne sahip NesNet

nesnelerinde geleneksel kriptografik yöntemler desteklenemediğinden, kişisel verilerin güvenli bir şekilde işlenebilmesi için NesNet özelinde geliştirilecek güvenlik yöntemlerin kullanılması gerekmektedir.

Hukuka uygun yeterli güvenlik önlemleri bulunmayan NesNet - DHT ödeme sistemlerinde meydana gelebilecek güvenlik ve kişisel veri ihlalleri nedeniyle kullanıcıların gizlilik ve mahremiyeti zarar görebilir, maddi, manevi kayıplara yol açabilir, hak ve özgürlükleri sınırlanabilir. Bunun sonucunda, veri işleyen kuruma ve/veya veri sorumlusuna para cezası, hapis cezası, kurum kapatılma cezası, vb. yaptırımlar uygulanabilir. Bu yaptırımlar kurum ve/veya veri sorumlusunda iş kaybı, ciddi maddi zarar ve itibar kayıplarına yol açabilir.

Bu çalışmada, ülkemizdeki NesNet ve DHT ödeme sistemlerine ilişkin mevut durum hakkında özet bilgi sağlandı, KVK kanunu ve BİTG'nin NesNet ve DHT ödeme sistemlerine etkisi ele alındı ve KVK kanunu ve BİTG nedeni ile doğabilecek olası hukuki sorunlara yönelik teknik çözümlerine yer verildi. Türkiye'de hukuka uygun, güvenli NesNet – DHT ödeme sistemi geliştirebilmek için sunulan sistem tasarım önerileri, sistemin geliştirilmesi için harcanması gereken ek efor, süre ve maliyete karşın olası kişisel veri ihlallerin önüne geçilerek veri işleyen kurum ve ve/veya veri sorumlusu açısından iş kaybı, maddi zarar ve itibar kayıplar önlenebilir, kişilerin hak ve özgürlükleri korunabilir.

Türkiye'de blokzincir ödeme sistemleri bulunmakla birlikte, KVKK ve BİTG ile uyumlu, NesNet nesneleri ile DHT üzerinden dijital ödemelerin yapılabildiği bir platform henüz bulunmamaktadır. Kişisel ve kritik verilerin güvenliğinin sağlanabildiği, KVKK ve BİTG ile uyumlu, NesNet nesneleri ile DHT üzerinden dijital ödemelerin yapılabildiği bir platformun geliştirilebilmesi için NesNet-DHT sistem tasarım önerilerinde bulunuldu. Bu bağlamda Hyperledger Fabric, R3 Corda, IBM Blockchain gibi kişisel verilerin yönetilebildiği blokzincir tabanlı olarak veya yerli bir NesNet-DHT ödeme sistemi geliştirilmesi önerildi. Mevcut blokzincir platformlarının KVK kanunu ile uyumlu olduğu ancak BİTG ile uyumlu olmadığı değerlendirilmektedir. Bu platformların hukuka uyumlu hale getirilebilmesi veya ülkemiz hukukuna uygun yeni bir NesNet-DHT ödeme sisteminin geliştirilmesi için sistem tasarım önerileri sunuldu. NesNet cihaz mimarisi, NesNet-DHT düğüm mimarisi ve NesNet cihazlarındaki kişisel verilerin hukuka uygun olarak toplanması, saklanması ve işlenmesi konuları ele alındı.

NesNet-DHT düğüm uygulama sunucusu için maliyet, güvenlik ve gizlilik, otomasyon, ölçekleme, esneklik ve iş sürekliliği gibi avantajları nedeni ile özel bulut mimarisi tercih edilebilir. Bulut mimariyi destekleyen ve dağıtık yapılar için uygun olan mikroservis yazılım mimarisi önerilmektedir. Mikroservis mimaride KVK kanunu ve BİTG ile uyumluluk için kullanılabilecek bileşenler tarif edilmiştir. Dağıtık veritabanların bulunduğu mikroservis mimarisinde erişilebilirlik, bölümleme ve tutarlılık arasında ödünleşim bulunmaktadır. NesNet-DHT düğüm mimarisi, erişilebilirlik, tutarlılık ve bölümlemeye ilaveten maliyet, gecikme, aktif kullanıcı sayısı, işlem sayısı, vb. başarım ölçütleri de göz önüne alınarak tasarlanmalıdır.

NesNet nesnelerin düşük işlemci gücüne sahip olmaları nedeni ile yüksek işlemci gücü gerektiren geleneksel kriptografik yöntemleri destekleyememektedirler. Bu nedenden dolayı ve saldırganın maliyet-faydası açısından NesNet nesnelerin yazılım ve haberleşme saldırılarına maruz kalma ihtimalleri daha yüksektir. Bu tür saldırılardan korunabilmeleri için, NesNet cihazların tasarımında göz önüne alınabilecek bazı güvenlik önlemlerine yer verildi.

NesNet cihazın NesNet-DHT ağına tanımlanmasında kullanılan cihaz parmak izi, cihaz ve ağ bilgilerini içerebilmektedir. Cihaz bilgileri ile kişi ve davranışı tespit edilebileceğinden, bu bilgiler kişisel veri olarak nitelendirilmektedir. DHT'de silme işlemi yapılamadığından cihaz parmak izinin DHT üzerinde saklanmaması gerekmektedir. Cihaz parmak izin KVK kanununa uygun olarak işlenebilmesi için kullanılabilecek kriptografik parmak izi oluşturma fonksiyonları ve yöntemleri özetlenmiştir. Cihaz parmak izin klonlanamayacak bir şekilde oluşturulması için fiziksel klonlanamaz fonksiyonun kullanılması önerilmektedir.

NesNet ile DHT ödeme sistem güvenliğinin iyileştirilmesi için gelecekte, siber saldırı tespitinde, otomatik poliçe ve siber güvenlik test senaryoları üretiminde makine öğrenmesi tekniklerinin incelendiği araştırma faaliyetlerin ağırlık kazanacağı öngörülmektedir.

KAYNAKLAR (REFERENCES)

[1] Q. F. Hassan, **Internet of Things A to Z: Technologies and Applications,** John Wiley & Sons, Hoboken, New Jersey, A.B.D., Mayıs 2018.

[2] S. S. Sabry, N. A. Qarabash, H. S. Obaid, "The Road to the Internet of Things: a Survey", **2019 9th Annual Information Technology, Electromechanical Engineering and Microelectronics Conference (IEMECON)**, Jaipur, Hindistan, 290-296, 2019.

[3] N. K. Yilmaz, H. B. Hazar, "The Rise of Internet of Things (IoT) and its Applications in Finance and Accounting", **Istanbul Finance Congress PressAcademia Procedia (PAP)**, Istanbul, Türkiye, 10, 32-35, Kasım 2019.

[4] Internet: IoT Analytics, https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/, 01.07.2020.

[5] Internet: S. Wasserman, 80% of IoT Connected Devices Aren't Secure. Is Apple Increasing this Number?, Engineering, https://www.engineering.com/IOT/ArticleID/11743/80-of-IoT-Connected-Devices-Arent-Secure-Is-Apple-Increasing-this-Number.aspx, 01.07.2020.

[6] O. Taş, F. Kiani, "Nesnelerin interneti (IoT) ve kablosuz algılayıcı ağların güvenliğine yapılan saldırıların tespit edilmesi ve önlenmesi", *Politeknik Dergisi*, 24(1), 219-235, 2021.

[7] IBM, **Device Democracy: Saving the future of the Internet of Things**, IBM, 2015.

[8] A. Panarello, N. Tapas, G. Merlino, F. Longo, A. Puliafito, "Blockchain and IoT Integration: A Systematic Survey", *Sensors*, 18(8), 2575, Ağustos 2018.

[9] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities", *Future Generation Computer Systems*, 88, 173-193, 2018.

[10] F. Şen, "Dağıtık Kayıt Teknolojisi", *Gümrük Ticaret Dergisi*, 17, 85-94, 2019.

[11] E. Ünsal, Ö. Kocaoğlu, "Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri", *Avrupa Bilim ve Teknoloji Dergisi*, 13, 54 - 64, Ağustos 2018.

[12] T.C. Cumhurbaşkanlığı, "Kişisel Verilerin Korunması Kanunu", *Resmî Gazete*, 57(5), 2016.

[13] Internet: Kişisel Verileri Koruma Kurumu, Kişisel Verileri Koruma Kurumu (KVKK), www.kvkk.gov.tr, 01.07.2020.

[14] Kişisel Verileri Korunumu Kurumu, **Kişisel Veri Güvenliğİ (Teknik ve İdari Tedbirler)**, Kişisel Verileri Korunumu Kurumu, Ankara, Türkiye, 2018.

[15] T.C. Cumhurbaşkanlığı, "Cumhurbaşkanı Kararı", *Resmî Gazete*, 30938(1733), Türkiye, 2019.

[16] Internet: TÜBİTAK BİLGEM Blokzincir Araştırma Laboratuvarı, https://blockchain.bilgem.tubitak.gov.tr/, 05.01.2021.

[17] Türkiye Bilişim Vakfı, **Kişisel Verilerin Korunması Hukuku ve Blokzincir Teknolojisi Raporu**, Blockchain Türkiye Platformu, Türkiye, 2019.

[18] "Regulation (EU) 2016/679 of the European Parliament and of the Council: General Data Protection Regulation (GDPR)", *Official Journal of the European Union*, 59, Mayıs 2016.

[19] Takas İstanbul, **BİGA Projesi**, Takas İstanbul, İstanbul, Türkiye, 2019.

[20] Internet: Akbank, Akbank'ta Ripple Üzerinden Sterlin Transferleri Başladı!, Akbank Lab, https://www.akbanklab.com/tr/guncel/basinda-biz/akbankta-ripple-uzerinden-sterlin-transferleri-basladi, 05.01.2021.

[21] BKM, **Keşif: Blockchain'in Sırları**, BKM, Türkiye, 2018.

[22] Internet: T2 Software, http://blockchain.t2.com.tr/, 05.01.2021.

[23] Internet: Global Miles, https://www.globalmiles.com/, 05.01.2021.

[24] Internet: NETAŞ, Netaş'tan AB'nin bağımsız ödeme kanallarının güvenliğinde Türkiye'yi pay sahibi yapacak blokzincir projesi, http://www.netas.com.tr/medya/netas-tan-ab-nin-bagimsiz-odeme-kanallarinin-guvenliginde-turkiye-yi-pay-sahibi-yapacak-blokzincir-projesi/, 05.01.2021.

[25] Internet: Proofstack, https://tr.proofstack.io/, 05.01.2021.

[26] Türk Ceza Kanunu, *Resmi Gazete*, 43(5), Türkiye, 2004.

[27] Internet: PCI Security Standards Council, PCI Security Standards, **https://www.pcisecuritystandards.org/**, 05.01.2021.

[28] S. Chow, P. Eisen, H. Johnson, P. C. V. Oorschot, "White-Box Cryptography and an AES Implementation", **Selected Areas in Cryptography (SAC) 2002: 9th Annual International Workshop,** 250-270, St. John's, Newfoundland, Kanada, 2002.

[29] Global Platform, Inc., **Introduction to Trusted Execution Environments**, Global Platform, 2018.

[30] Global Platform, Inc., **Introduction to Secure Elements**, Global Platform, Inc., 2018.

[31] L. A. Monteiro, R. R. Hazin, A. C. D. Lima, F. Ferraz, W. H. C. Almeida, "Survey on Microservice Architecture -Security, Privacy and Standardization on Cloud Computing Environment", **The Twelfth International Conference on Software Engineering Advances (ICSEA 2017)**, 198-205, Athens, Yunanistan, Ekim 2017.

[32] S. Newman, **Building Microservices: Designing Fine-Grained Systems**, O'Reilly, Cilt: 1, California, A.B.D., 2015.

[33] IoT Working Group, **Identity and Access Management for the Internet of Things - Summary Guidance**, Cloud Security Alliance (CSA), 2017.

[34] N. Miloslavskaya, A. Tolstoy, "New SIEM System for the Internet of Things", **WorldCIST'19 2019: Advances in Intelligent Systems and Computing**, La Toja Island, Galicia, İspanya, 931, 317-327, Nisan 2019.

[35] NXP, **IoT Device Security: Built-In, Not Bolt-On,** DIGI, 2018.

[36] European Union Agency for Network and Information Security (ENISA), **Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures**, ENISA, Kasım 2017.

[37] A. Koivu, L. Koivunen, S. Hosseinzadeh, S. H. S. R. Samuel Lauren, V. Leppanen, "Software Security Considerations for IoT", **2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom)**, Chengdu, Çin, 392-397, Aralık 2016.

[38] D. G. V. Albricci, M. Ceria, F. Cioschi, N. Fornari, A. Shakiba, A. Visconti, "Measuring Performances of a White-Box Approach in the IoT Context", *Symmetry*, 11(1000), 2019.

[39] Y. Shi, W. Wei, Z. He, H. Fan, "An ultra-lightweight white-box encryption scheme for securing resource-constrained IoT devices", **ACSAC '16: Proceedings of the 32nd Annual Conference on Computer Security Applications**, Los Angeles, California, A.B.D., 16–29, Aralık 2016.

[40] P. Gauravaram, L. R. Knudsen, "Cryptographic Hash Functions", **Handbook of Information and Communication Security**, Springer-Verlag Berlin Heidelberg, Almanya, 59-79, 2010.

[41] C. Wang, R. M. Gerdes, Y. Guan, S. K. Kasera, **Digital Fingerprinting**, Cilt 1, Springer-Verlag New York, A.B.D., 2016.