ANONİM KRİPTOPARALARIN KORELASYON TABANLI MAHREMİYET ANALİZİ

Muhammet Ali Öztürk[1,2], İsa Sertkaya[3], Hüseyin Yüce[4]

[1] Marmara Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği, İstanbul, Türkiye
[2] TÜBİTAK BİLGEM Bilgi Sistemleri, Kocaeli, Türkiye
[3] MCS Labs & BCLabs, TÜBİTAK BİLGEM UEKAE, Kocaeli, Türkiye
[4] Marmara Üniversitesi, Teknoloji Fakültesi, İstanbul, Türkiye
muhammet.ozturk@tubitak.gov.tr, isa.sertkaya@tubitak.gov.tr,
huseyin@marmara.edu.tr

ÖZET

Bitcoin, açık anahtarlı adresleri kullandığı için anonimliği tamamıyla sağladığı düşünülse de bu adresler herkese açık bir kayıt defterinde tutulduğundan dolayı anonim değildir. Bu nedenle anonim kriptoparlar yayınlanmıştır. Anonim kriptoparaların teoride matematiksel olarak tamamıyla anonim olduğu düşünülse de pratikte anonimliği yeteri kadar sağlayamazlar. Bu makalede Zcash, Dash ve Monero anonim kriptoparalarının pratikte iddia edildikleri kadar anonim olup olmadığını tespit etmek amacıyla korelasyon tabanlı mahremiyet analizleri yapılmıştır. Bu makaleyle beraber ilk defa Dash ve Monero anonim kriptoparaları için korelasyon tabanlı mahremiyet analizi çalışması yapılmıştır, Zcash için daha önce yapılan bir çalışma bulunmaktadır. Zcash'in korumalı işlemleri %84,4 ve Dash'in ÖzelGönderim ile alakalı işlemleri %49.304 oranında ilişkilendirilebilmiştir. Monero işlemlerinin adres ve miktarları tamamen gizli olduğu için korelasyon tabanlı mahremiyet analizi gerçekleştirilememiştir.

Anahtar Kelimeler— Mahremiyet analizi, anonim kriptopara, zcash, dash, monero

Correlation Based Privacy Analysis of Private Cryptocurrencies

ABSTRACT

Although Bitcoin is considered to provide complete anonymity because it uses public-key addresses, these addresses are not anonymous because they are kept in a public registry. For this reason, anonymous cryptocurrencies have been published. It is stated that anonymous cryptocurrencies are mathematically anonymous in theory, for various reasons they cannot provide enough anonymity in practice. In this article, correlation-based privacy analyzes were conducted to determine whether the anonymous cryptocurrencies of Zcash, Dash and Monero are indeed as anonymous as they claim in practice. With this article, correlation-based privacy analysis was carried out for the first time for Dash and Monero anonymous cryptocurrencies, there is a previous study for Zcash. Zcash's shielded transactions were associated with the rate of 84.4% and Dash's PrivateSend-related transactions at a rate of 49.304%. Correlation-based privacy analysis could not be performed for Monero because the addresses and amounts of Monero transactions are completely confidential.

Keywords— Privacy analysis, anonymous cryptocurrency, zcash, dash, moner

I.GİRİŞ (INTRODUCTION)

Bitcoin açık kaynak kodlu, yazılım tabanlı bir çeşit dijital para birimidir. Kullanmış olduğu kriptografik yöntemlerden dolayı Bitcoin'e kriptopara, kullanılan teknolojiye de blokzincir denir. Bitcoin'i farklı kılan şey blokzincir teknolojisinin sağlamış olduğu anonimlik ve herhangi bir merkeze bağlı olmayan yapısıdır [1].

En temel tabiriyle blokzincir hiçbir merkezi otoriteye ihtiyaç olmaksızın değer olarak atfedilen çeşitli varlıkların bir veriymiş gibi aktarılmasını sağlayan veritabanına verilen isimdir [2],[3]. Blokzincirin altyapısı kendisine adını veren "bloklar (blocks)" ve bu bloklar içerisine eklenen "işlemlerden (transactions)" oluşur. Bu işlemler, ilgili blokzincire ait her türlü verinin kaydedildiği bir çeşit içerik bilgisidir. Bu kayıtlar birleştirilir ve belirli aralıklarla bloklara yazılır. Bu bloklar da sırayla art arda oluşturularak bir zinciri

oluşturur. Blokzincirdeki herbir blok (ilk blok hariç) kendisinden önceki bloğun özet (hash) bilgisini de tutar.

Bitcoin işlem, blok ve adreslerinin tamamının açık (public) veritabanlarına kaydedilmesinden dolayı Bitcoin kriptoparası düşünüldüğü kadar anonim değildir. Bu nedenden ötürü de Zcash, Dash ve Monero gibi anonimlik ve mahremiyete daha fazla önem veren anonim kriptoparalar çıkmıştır.

Anonim kriptoparaların ortak özelliği anonimliğin artırılarak mahremiyetin ihlalinin engellenmesinin sağlanmasıdır. Dolayısıyla bu kriptoparalara anonim kriptoparalar (anonymous cryptocurrencies) adı verilmiştir. Örnek olarak Zcash, anonimliği korumalı havuz ve gizli işlemeler vasıtasıyla sağlamaya çalışır.

Ne var ki, anonim kriptoparalar teoride anonimlik sağladıklarını belirtseler de pratikte bu kriptoparalar çeşitli yöntemlerle analiz edilebilmektedirler. Bu durumda da anonim kriptoparaların sağladıkları anonimlik ve mahremiyet ihlal edilebilmektedir. Anonim kriptoparaların analiz edilebileceğini tespit etmek amacıyla bu makalede Zcash, Dash ve Monero anonim kriptoparaları için korelasyon tabanlı mahremiyet analizi yapılacaktır.

Yıllar boyunca Bitcoin kriptoparasının anonimliğine odaklanan çeşitli çalışmalar ve araştırmalar yapılmıştır. Bu çalışmaların önemli bir kısmı Bitcoin adresleri, blokları ve işlemlerleri üzerinde yapılan çalışmalardır [4], [5], [6], [7], [8]. Bu çalışmalar Bitcoin adresine sahip madenciler (miners), madenci havuzları (mining pools), normal kullanıcılar (standart users) ve Bitcoin satıcıları/borsacıları (Bitcoin exchanges) gibi çeşitli kullanıcı gruplarına odaklanarak mahremiyet analizi gerçekleştirir. Başka araştırmalar ise Bitcoin kriptoparasının eşler arası ağının (peer-to-peer network) analiz edilerek çeşitli bilgilerin elde edilmesi üzerine odaklanmıştır [9],[10],[11].

Anonim kriptoparalar da Bitcoin gibi çeşitli mahremiyet analizi çalışmalarının konusu olmuşlardır. [12] ve [13] çalışmaları Dash anonim kriptoparasının mahremiyet analizine odaklanır. Monero anonim kriptoparası üzerine odaklanan [14],[15] ve [16] araştırmaları genel itibariyle çeşitli analiz yöntemleriyle anonimliğin ihlaline odaklanırken [17] çalışması tüm bu çalışmalardan farklı olarak "Makine Öğrenme (Machine Learning)" yöntemlerini kullanarak anonimliğin analizine odaklanmıştır. [2], [18], [19], [20], [21], [22], [23] çalışmalarıysa doğrudan Zcash anonim kriptoparasına odaklanır. Alex Birkuyov tarafından hazırlanan [2] çalışması bahsedilen mahremiyet analizlerinden doğrudan korelasyon tabanlı olan tek çalışmadır.

Kriptoparaların sadece blokzincirde bahsedilen özellikleri üzerinden mahremiyet analizi yapılmaz, kriptosistemdeki çeşitli öğeler de analiz edilebilmektedir. [24] ve [25] çalışmaları Bitcoin, Zcash, Dash ve Monero'nun ağ analizlerini yaparken [26] çalışması ise yine Bitcoin, Dash, Monero, ve Zcash için mobil cüzdanları (mobile wallet) üzerine mahremiyet analizi yapar.

Anonim kriptoparalar oldukça farklı araçları kullanarak blokzincirdeki işlem ve adres mahremiyetini sağlamayı amaçlar. Bu nedenle birçok farklı mahremiyet analizi yapılmıştır. Bu makalede Zcash, Dash ve Monero anonim kriptoparaları için korelasyon tabanlı mahremiyet analizi yapılmıştır. İlk olarak bu anonim kriptoparaların kullanımları gruplandırılmıştır. Daha sonra ilgili anonim kriptoparaların adresleri, işlemleri ve blokları analiz edilerek adreslerin birbirleriyle olan ilişkileri tespit edilmeye; yani anonimleştirilen para transferlerinin anonimliğinin bozulmasına (de-anonymization) çalışılmıştır. Makalede ilk olarak [2] makalesinden yola çıkılarak Zcash anonim kriptoparası için korelasyon tabanlı mahremiyet analizi çalışması yapılmıştır. Analiz sırasında Alex Birkuyov'un kullanmış olduğu algoritmalarda bazı güncellemeler yapılmıştır. Dash ve Monero anonim kriptoparaları içinse daha öncesinden herhangi bir korelasyon tabanlı mahremiyet analizi yapılmamıştır, bu analiz çalışması ilk defa bu makalede yapılmıştır.

Analiz çalışmasının ardından makalede yapılan bu analizin sonuçları paylaşılmıştır. Daha sonra elde edilen bu sonuçların nedenleri hakkında tartışma yapılmıştır. Son olarak anonim kriptoparaların kullanıcı ve geliştiricilerine bu sonuçlardan kaçınmaları için önerilerde bulunulmuştur. Kısaca bu makalede sadece analiz çalışması yapılmamış; anonim kriptoparalarlar ilgilenenler için sonuca götüren nedenler ve önerilerden de bahsedilmiştir.

II. TANIMLAR (DEFINITIONS)

2.1. Blokzincir ve Bitcoin

Blokzincirin çözüm getirdiği en önemli sorunlarda birisi de merkezi güvene dayalı sistemlerdir. Blokzincir teknolojisi, "değer (value)" olarak atfedilen verilerin dağıtık olarak veritabanlarında tutulmasıdır [1]. Bitcoin kriptoparası eşler arası teknolojisini (peer-to-peer technology) kullanarak herhangi merkezi ağ olmadan çalışır [27].

Bitcoin adreslerinin tamamıyla açık adres olması gibi sebeplerden dolayı düşünüldüğü kadar mahremiyet sağlamamaktadır. Jong-Hyouk Lee tarafından hazırlanan araştırmaya göre Bitcoin'in anonim olmamasının kısaca 3 sebebi vardır, [28]:

1. Blokzincirin açık olması (public blockchain)
2. Adreslerin açık anahtarlı olması (public key-based address)
3. Eşler arası veri paylaşımının İnternetten yapılması (peer-to-peer networking over the Internet)

2.2. Anonim Kriptoparalar

Bitcoin'in anonimlik sağlamada yetersiz olmasından dolayı anonim kriptoparalar yayınlanmıştır. Anonim kriptoparaların aşağıdaki özellikleri sağlanmış olması beklenir [28]:

- **Gizlilik:** Yapılan para transferlerindeki gönderen, alan ve gönderilen para miktarı işlemi yapan adres sahipleri haricindeki hiçbir kimse tarafından bilinmemesi için bir şekilde gizlenmesi gerekmektedir.
- **Takip Edilememezlik:** Anonim olarak yapılan para transferlerdeki paraların hiçbir şekilde işlem tarihçesinde (yani defterlerde) izlenilebilir yahut ilişkilendirilebilir olmaması gerekmektedir.
- **Birbiriyle Değiştirilebilirlik:** Tüm dijital paraların birbirlerinden ayırt edilemez olduğu, böylece karşılıklı olarak değiştirilebilir olduğu temin edilmelidir.

Makalede Zcash, Dash ve Monero anonim kriptoparaları üzerine korelasyon tabanlı mahremiyet analizi yapılacağından dolayı aşağıda kısaca bu anonim kriptoparalardan ve anonimliği nasıl sağladıklarından bahsedilecektir.

2.3. Zcash

Zerocash protokolü kullanılarak geliştirilmiş olan Zcash, Bitcoin'den çatallandırılmış (forked) bir kriptoparadır. Bitcoinden farklı olarak zk-SNAKRs kullanılarak matematiksel olarak işlemler ve adresler için anonimlik sağlar. Bitcoin gibi şeffaf işlemlerin (transparent transactions) yanında ayrıca gizli işlemleri (private transactions) de destekler. Gizli işlemlerde transfer edilen para ikinci bir havuz olan korumalı havuza (shielded pool) aktarılır [29], [30].

Zcash kriptoparasının kullanmış olduğu temel para birimine ZEC, en küçük para birimine Zatoshi denir. 1 ZEC 10^8 Zatoshiye eşittir. Varsayılan işlem ücreti (transaction fee) 10^4 Zatoshidir (10^{-4} ZEC). İlk blok ödülü (block mining reward) 12.5 ZEC (10 ZEC madenciye, 2.5 ZEC Zcash geliştiricilerine) kadardır. Zamanla bu ödül Zcash kurucuları tarafından düşürülmüştür. Şu anki blok üretme ödülü 6.25 ZEC kadardır. 1.25 ZEC Zcash kurucularına gider, kalan 5 ZEC'de bloğu oluşturan madenciye gönderilir [2].

Girdi ve çıktının görünür olduğu açık adreslere (transparent-address) t harfi ile başladıkları için kısaca t-adres, gizli ve çıktının gizlendiği gizli adreslere (private-address) de z harfi ile başladıkları için kısaca z-adres de denir. Zcash'te z-adreslerin geçtiği işlemlere EkleBöl işlemleri (JoinSplit transactions) adı verilir, kısaca EB-işlemleri (JS-transactions) de denir. Bir EB-işleminde en fazla 2 farklı z-adresi kullanılabilir. Toplamda 4 farklı EB-işlemi bulunmaktadır [29]:

1. **z'den z'ye işlemler (z-to-z transactions):** Sadece z-adresleri arasında yapılmış olan işlemlerdir. Hem gönderenin hem de alıcının adresleri gizlidir. Ayrıca gönderilen miktar ve alınan miktar tamamen gizlidir. Sadece böyle bir işlemin gerçekleştiğine dair işin ispatı vardır. Zden zye işlemde görülebilen tek veri bu işlemin bedelidir. Zcash'de gizliliğinin sağlandığı EB-işlemidir. Burada yapılan işlemler korumalı havuzdan korumalı havuza yapılan bir işlem olmasından dolayı bu işlemlere korumalı işlemler (shielded transactions) de denilir.
2. **z'den t'ye işlemler (z-to-t transactions):** Girdi olarak sadece z-adres varken çıktı olaraksa bir veya daha fazla t-adresi bulunur. Korumalı havuzdan şeffaf havuza ZEC aktarımı olduğundan dolayı bu işlemlere korumanın kaldırılması işlemleri (deshielding transactions) de denilir. Bu işlemlerde girdi miktarı 0 ZEC'tir. Çıktı değerleri defterde herkese açıktır. Toplam çıktıyla beraber işlem bedelinin toplamı korumalı havuzdan çıkan Zcash'i verir.
3. **t'den z'ye işlemler (t-to-z transactions):** Çıktı olarak sadece z-adres, girdi olaraksa bir yahut daha fazla t-adres bulunur. Şeffaf havuzdan korumalı havuza ZEC aktarımı yapıldığından dolayı bu işlemlere aynı zamanda korumanın oluşturulması işlemleri (shielding transactions) de denilir. z'den t'ye işlemlerin aksine t'den z'ye işlemlerde girdi değerleri defterde herkese açıkken çıktı değeri gizlidir, yani blokzincirde 0 ZEC olarak görülür. Girdilerin toplamından işlem bedeli çıkartıldığı zaman çıkan sonuç korumalı havuza gönderilen Zcash'i verir.
4. **tz'den tz'ye işlemler (tz-to-tz transactions):** Hem işlem girdisinde de hem de işlem çıktısında hem t-adres hem de z-adres bulunur. İşlem bedeliyle beraber çıktıların toplamının toplanır. Elde edilen toplam girdilerin toplamından çıkartılır. Çıkan sonuçta farkın pozitif çıkması durumunda korumanın sağlanması işlemi, farkın negatif çıkması durumunda korumanın kaldırılması işlemi yapılmış denilebilir. Farkın 0 çıkmasıysa bu işlemin bir çeşit korumalı işlem olmasını sağlar.

2.4. Dash

18 Ocak 2014 tarihinde Bitcoin kriptoparasındaki anonim eksikliğini farkeden Evan Duffield tarafından geliştirilmiştir [31], [32], [33].

Dash, aslında Bitcoin tabanlı yazılım olan Litecoin kriptoparası çatallanmasıdır. Bitcoin'e nazaran daha anonimleştirme odaklı coin transferi yapısı sunar. Bitcoin'e göre 2 farklı yenilik getirmiştir [34]:

2.4.1. AnaUç

Kriptoparalarda veri akışının sürekliliğini sağlamak ve eşleri ilgili ağda gerçekleşen çeşitli olaylarda güncel tutmak için P2P ağında çalışan ve tam düğüm (full node) adı verilen sunuculardır. AnaUçlar kriptosistemdeki ÖzelGönderim ve HızlıGönderim denilen iki tane çok önemli işlemden sorumludur. Bir

kullanıcının AnaUç olabilmesi için 1000 Dash'e sahip olması gerekir. Yaptıkları bu yatırıma karşılık AnaUçlar herbir üretilen bloklardan sağlanan blok ödülün yaklaşık %45'ini alır. Diğer %45'i bloğu üreten madenciye giderken kalan ödülün %10 kadarı Zcash'te olduğu gibi Dash kurucularına gider.

2.4.2. ÖzelGönderim

Bitcoin'de önerilen CoinJoin yapısının üzerine kurulmuştur. CoinJoin'de kısaca elindeki parayı anonimleştirmek isteyen bir kullanıcı yine elindeki parayı anonimleştirmek isteyen başka bir kullanıcıyla beraber Dash karıştırma işlemine girer. Burada Dash transferi rastgele başka farklı adreslere gönderilerek girdi ile çıktı arasında hiçbir ilişki bulundurulmaz. ÖzelGönderim en az 3 kullanıcının karıştırma işlemine katılması şartını koşar. Bunun yanında karıştırma işleminin toplamda 2 ile 16 sefer (round) arasında yapılmasını şart koşar. Ağda dağıtık olan AnaUçlar vasıtasıyla ÖzelGönderim işlemi gerçekleştirilir. Yapılan karıştırmalar sayesinde Dash, anonimlik şartlarından birisi olan "birbiriyle değiştirilebilirliği" sağladığını belirtir. ÖzelGönderim sadece 10 Dash'ın katlarını (en fazla 10^3 Dash ve en az 10^{-3} Dash) kullanır.

2.5. Monero

18 Nisan 2014'te yayınlanan Monero anonimlik, mahramiyet ve işlem gizliliğine odaklanan bir anonim kriptoparadır [35], [36]. Monero "gizlenmiş bir açık defterdir" (obfuscated public ledger); yani herkes işlem gönderebilir ve alabilir ancak hiçbir kimse bu işlemlerdeki adresleri ve gönderilen miktarları göremez. Diğer kriptoparalar gibi yeni madeni paralar çıkarmak ve madencileri "ağı korumak ve işlemleri doğrulamak" için teşvik etmek amacıyla işin ispatı mekanizmasını kullanır.

Para birimi XMR'dir. Blok ödülü ilk blokta 17.592169267200 XMR olarak belirlenmişken her blokla düşen bu ödül 3 Temmuz 2020 23:13:28 UTC tarihli 2134425. bloğun ödülü 1.579420370752 XMR kadardır. XMR 10^{-12} ye kadar bölünebilir, yani teknik olarak en küçük yapılabilen Monero işlemi 0.000000000001 XMR olacaktır. Anonimliği sağlamak için halka imzalar yapısından faydalanır.

Kriptografide halka imza, her birinde anahtar olan bir kullanıcı grubundaki üyelerden herhangi biri tarafından imzalanabilen bir çeşit dijital imzadır. Yani halka imza ile imzalanan bir mesaj dışarıdan bir grup kullanıcı tarafından imzalanmış gibi görünür. Ancak aslında bu mesaj, anahtara sahip olan o gruptaki sadece bir kişi tarafından imzalanmıştır. Halka imzaları işlem çıktılarının geriye doğru takip edilememesini sağlar [37].

2.6. Uygulama ve Analiz

Bu çalışmada Alex Birkuyov'un hazırlamış olduğu [2] makalesindeki yapılan çalışmalar temel alınarak Zcash, Dash ve Monero anonim kriptoparaları için korelasyon tabanlı mahremiyet analizi yapılmıştır. Bu analizler neticesinde analiz edilebilen ilgili anonim kriptoparaların ne derecede işlem ilişkilendirilmesi yapılabildiği hesaplanmıştır. Anonim kriptoparaların analizi için Bitcoin ile Bitcoin kodundan türetilme kriptoparalar için hazırlanmış olan ve Github veri deposuna (repository) yüklenmiş olan Blocksci[1] açık kaynak kodlu uygulaması kullanılacaktır. Zcash içinse Blocksci uygulamasının Zcash için hazırlanmış olan çatallanması[2] kullanılacaktır.

III. ZCASH ANALİZİ (ANALYSIS OF ZCASH)

Zcash için analize 784834. bloğun üretildiği tarih olan 04 Nisan 2020 Cumartesi 12:03:06 tarihinde başlanmıştır. Bunun anlamı Zcash anonim kriptoparası için yapılan korelasyon tabanlı mahremiyet analizi 04 Nisan 2020 tarihinden önce üretilmiş olan tüm 784834 bloğu kapsar. 784834. bloktan sonra üretilmiş ve üretilecek olan tüm bloklarla beraber Zcash için yapılacak tüm yeni güncellemeler yapılmış olan mahremiyet analizi çalışması kapsamınının dışındadır.

Mahremiyet analizi çalışmasında ilk olarak Zcash kullanıcılarının korumalı XMR aktarımı sağlayan EB-işlemlerini ne derece kullandığı Şekil 1'deki grafikte gösterildiği gibi tespit edilmiştir. Şekil 1'de gösterilmekte olan grafikte Zcash anonim kriptoparasının çıktığı tarih olan 2016 Ekim tarihinden analiz çalışmasının yapıldığı 2020 Nisan tarihine kadar Zcash kullanıcıların tercih ettikleri işlem tipleri yıl ve ay bazında toplamları gruplanarak gösterilmiştir. Şekil 1'deki x ekseninde olan *Blok Üretme Tarihi* ilgili işlem tipinin toplandığı yıl ve ayı belirtir. Grafikteki y ekseninde de işlem tipinin tercih edilme sayısını verir. Grafik incelendiği zaman kullanıcıların büyük çoğunlukla doğrudan şeffaf işlemleri tercih ettikleri görülecektir. Zcash'in ilk çıktığı aylarda, yani 2016 Ekim, Kasım ve Aralık aylarında kullanıcıların EB-işlemlerini tercihi %25-%30 oranındaydı. Zcash işlemlerinin anonimliğinin sağlanması açısından önemli bir değer olan bu oranın zaman içerisinde artması beklenirken %10-%15 oranına kadar düştüğü gözlemlenmiştir. Mart 2020 ayı için bu oran %15,91'dir. Şekil 1'deki grafikte Zcash kullanıcıları EB-işlemlerini gerektiği düzeyde tercih etmedikleri açıkça görülmektedir.

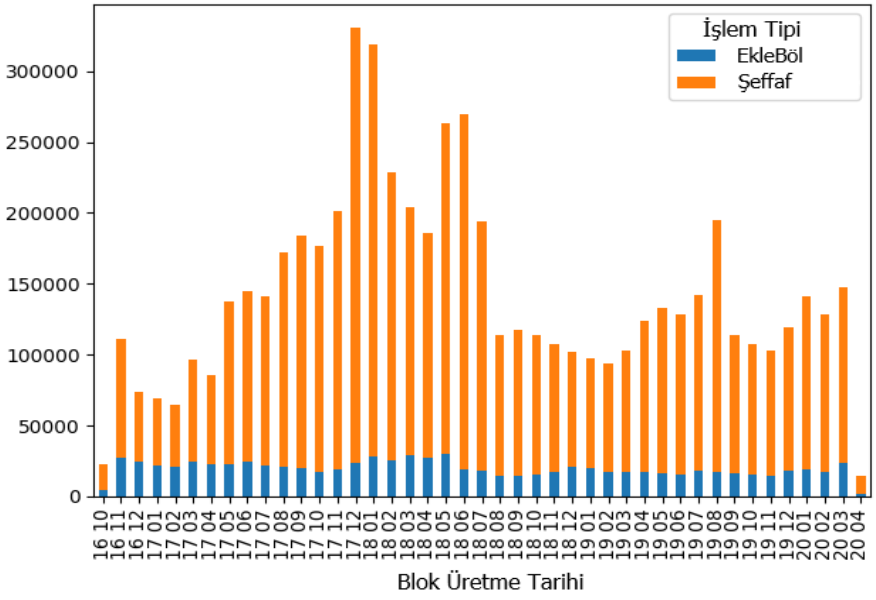
Analiz çalışması kapsamında daha yine aynı tarihler için Zcash kullanıcıların EB-işlem tiplerini tercih etme oranlarına bakılmıştır. Şekil 2'de yıl ve aylara göre tercih edilen EB-işlemi tipi grafiği gösterilmektedir.

[1] Princeton University - Center for Information Technology Policy tarafından hazırlanan Blocksci açık kaynaklı uygulama koduna https://github.com/citp/BlockSci bağlantı adresine tıklayarak ulaşabilirsiniz.

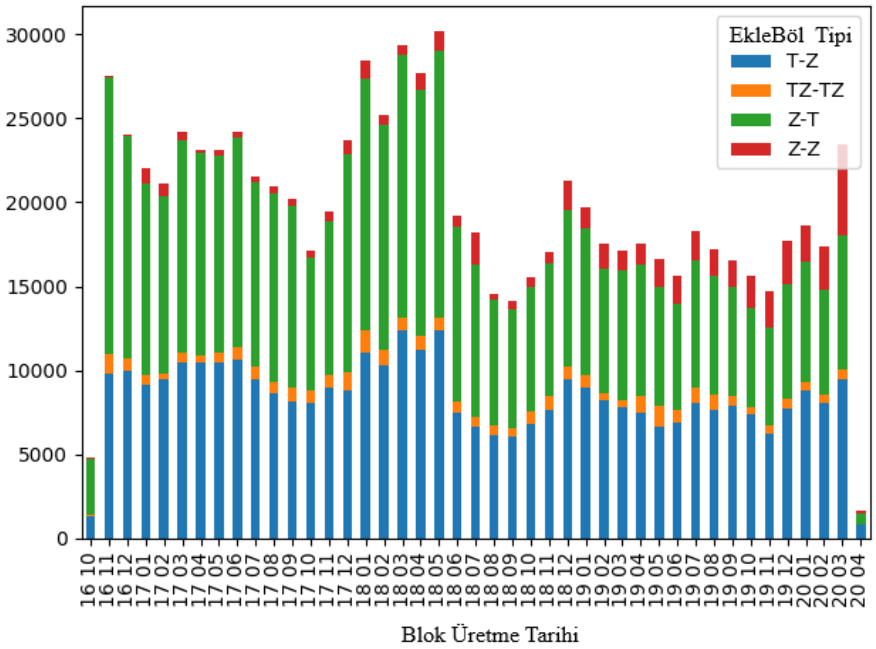
[2] CryptoLux Research Group at SnT, University of Luxembourg tarafından hazırlanmış olan Blocksci uygulamasının Zcash için hazırlanmış forkuna https://github.com/cryptolu/BlockSci bağlantı adresine tıklayarak ulaşabilirsiniz.

Şekil 2'deki x ekseninde bulunan *Blok Üretme Tarihi* Şekil 1'deki x ekseni ile aynı değeri taşır. Grafikteki y eskeni ise kullanıcıların ilgili yıl ve ayda tercih ettikleri toplam EB-işlemi tipini verir. Burada üzerinde en fazla durulması gereken EB-işlemi tipi zden zye yapılan korumalı işlemlerdir. 2016'nın son aylarına tekabül eden Zcash'in çıktığı ilk zamanlarda korumalı EB-işlemlerinin tüm EB-işlemlerine oranı %1-%3 oranındayken zaman içerisinde bu oranın önemli bir istakrarlı artış sergilediği aşikârdır. Bu oran Mart 2020'de %23,17 oranına kadar çıkmıştır. EB-işlemleri arasında üçüncü şahıslara neredesye hiçbir şekilde yapılan işlemin miktarı ve adresleri hakkında bilgi vermeyen tek EB-işlemi tipi bu korumalı işlemlerdir. Korumalı işlemlerin kullanım oranının artması Zcash kriptoparasının daha zor korelasyon tabanlı mahremiyet analizi yapılabilmesini sağlar. Bu grafik EB-işlemlerini kullanan Zcash kullanıcılarının zaman içerisinde Zcash anonim kriptoparasını kullanma konusunda iyi yönde bilinçlendikleri bilgisini verir. Çünkü ne kadar gizli adres kullanılarak yapılsalar da zden tye, tden zye ve tzden tzye yapılan işlemler sonuçta korumalı havuza giren ve korumalı havuzdan çıkan Zcash miktarları (yani işlemlerin ZEC yahut Zatoshi değerleri) hakkında bilgi verirler.

Analiz işlemi için bir sonraki adında blokzincirdeki tüm işlemler için "çıktı adresi değeri" gruplanmıştır. Çıktı adresi değerleri gruplaması için en çok kullanılan 10,000 adres çıktısı incelenmiştir. Şekil 3'te en çok kullanılan 10,000 işlem adreslerine ait çıktıların ZEC değerleri verilmiştir. Bu grafikte verilen sonuç "10,000 farklı işlem çıktısı" değeri değil "10,000 farklı çıktı adresi" değeridir. Şekil 3'teki grafikte x eksenindeki *OutputValue* çıktı adreslerinin Zatoshi cinsinden değerini verir. Grafikteki y eksenindeki *tops* ise bu değerlerin toplam kullanılma sayısını verir. Şekil 3'teki grafik incelendiği zaman grafikteki değerlerin ilginç bir şekilde 10^6 Zatoshi yani 0,01 ZEC'te yoğunlaştığı ve 10^7 Zatoshi yani 0,1 ZEC'e doğru toplam kullanılma sayısı azalan şekilde değiştiği gözlemlenmektedir. 10^6 Zatoshi değeri neredeyse 1,000,000 kez adres çıktısı olarak kullanılmıştır. Bu sonuç Zcash anonim kriptoparasında özellikle 0.01 ZEC / 10^6 Zatoshi ve 0.1 ZEC / 10^7 Zatoshi arasındaki değerlerin azımsanamayacak bir ölçüde en çok kullanılan adres çıktısı değerleri olduğunu gösterir.

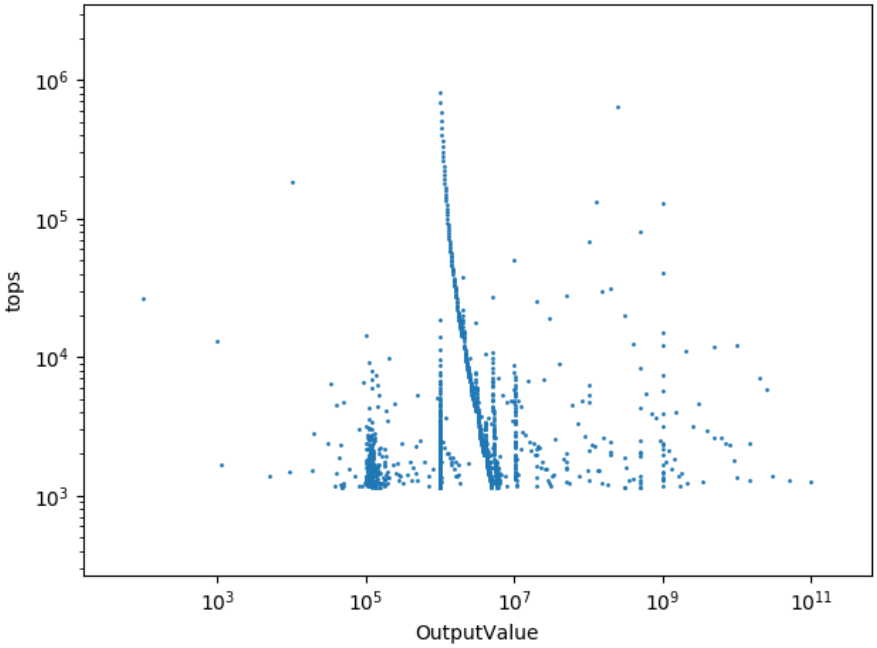


Şekil 1. Yıl ve Aylara Göre İşlem Tipi (Transaction Type) Grafiği

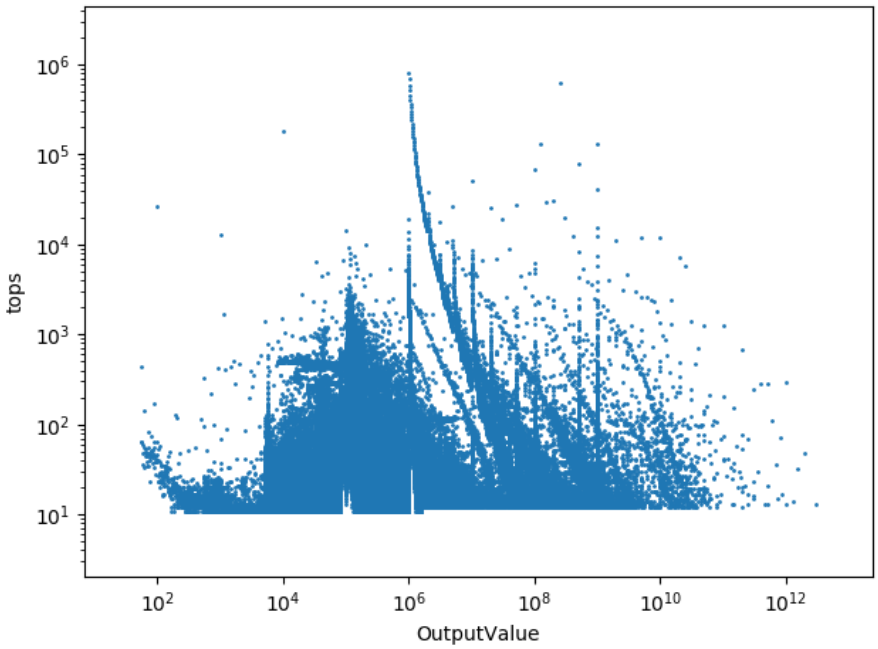


Şekil 2. Yıl ve Aylara Göre EkleBöl İşlemleri Tipi (JoinSplit Transactions Type) Grafiği

.



Şekil 3. En Çok Kullanılan 10,000 Adres Çıktısı



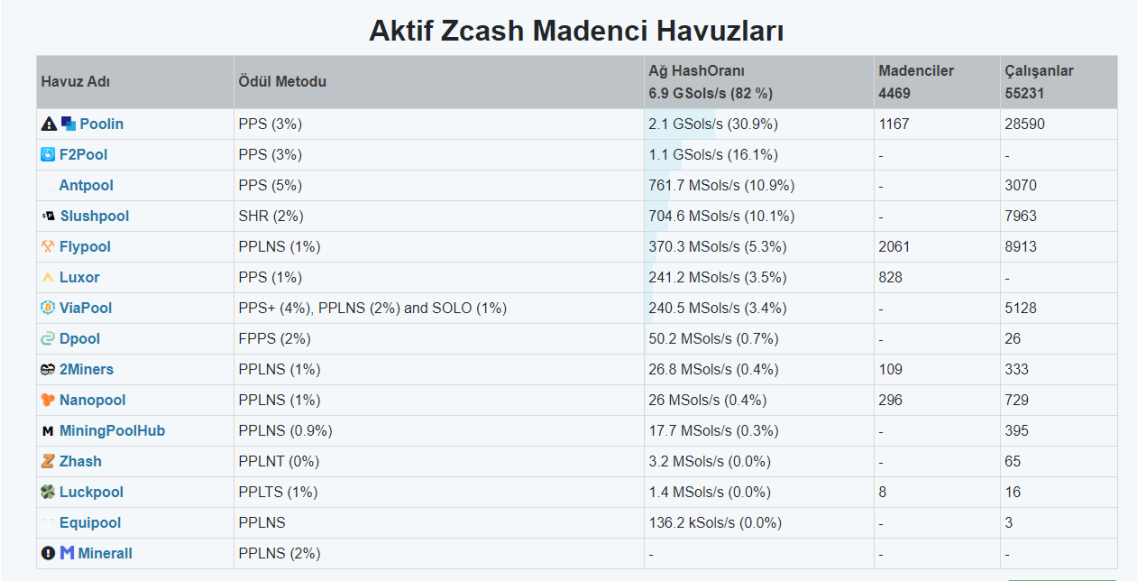
Şekil 4. En Çok Kullanılan 1,000,000 Adres Çıktısı

Analiz çalışmasında bir sonra grafikte en çok kullanılan 1,000,000 çıktı adresi değeri incelenmek istendiğinde Şekil 4'teki grafik sonuç olarak çıkmıştır. Grafikteki *OutputValue* ve *tops* eksenleri Şekil 3'teki eksenlerin aynısıdır. Şekil 3'te olduğu gibi Şekil 4'te de 0.01 ZEC/10^6 Zatoshi ve 0.1 ZEC/10^7 Zatoshi arasındaki değerlerin azımsanamayacak bir ölçüde en çok kullanılan adres çıktısı değerleri olduğu açıkça gözlemlenmektedir. Madenci havuzlarının bünyesinde bulundurdukları madencilere genellikle en az 0.01 ZEC/10^6 Zatoshi katılım payı verdikleri bilinmektedir. Madenci havuzları madencilerin yapmış oldukları işlemci gücü destek payına göre 0.01 ZEC'in üstüne Zatoshi seviyesinde ekleme yaparlar. Misal olarak bir madenciye 0.01022 ZEC ödeme yapılırken daha fazla işlemci gücü tedarik eden başka bir madenciye 0.01322 ZEC ödeme yapılabilir. Bu bilgiler ışığında Şekil 3 ve Şekil 4'teki grafiklerde gözlemlenen yoğunlaşmanının madenci havuzlarının yaptıkları madenci ödemelerinden kaynaklandığını sonucuna varılabilir. Aynı zamanda elde edilen bu sonuç madenci ve blok ödülü üretme kaynaklı işlemlerin Zcash kriptoparasındaki işlemlerin önemli bir bölümüne tekabül ettiği anlamına da gelir. Ancak bazı madenci havuzları madencilerine blok üretme ödülünden düşen paylarını zden zye korumalı işlemler aracılığıyla gönderdiğinden kesin olarak bu konuda bir şey söylenemez.

3.1. Madenci Havuzları ve Madencilerin Analizi

Şekil 5'te Aktif Zcash madenci havuzları gösterilmektedir. Şekil 5'teki madenci havuzları ağ özetleme oranının (network hashrate) %82'sini kapsarken Poolin isimli madenci havuzu ağ özetleme oranının %30,9 kadarını kapsadığı görülmektedir. Bu durum "merkezisizleştirilmiş" olarak bir merkezi otorite olmaksızın işlem yapan blokzincirler için oldukça tehlikeli bir durumdur. Gerçekten de Nisan 2020'de yapılan madenciler analizinde en fazla blok üretme ödülü alan madencinin Poolin madenci havuzu olduğu ve F2Pool ve Antpool ile bu üç madenci havuzunun madenci ödülü pastasından en fazla payı aldıkları gözlemlenmiştir.

Hem zamanla Zcash kriptoparası için ciddi değişiklikler manasına gelen Overwinter gibi güncellemeler nedeniyle, hem de madenci havuzlarınının madencilerinin sürekli madenci havuzu değiştirmesi ve yeni madenci havuzlarının maden üretme yarışına dâhil olması sebebiyle aşağıda detaylı olarak açıklanacak işlem analizleri tüm 784834 blok için baştan sona olacak şekilde yapılmamıştır. Ayrıca belki de milyonlarca işlemle beraber bu işlemlerde ZEC gönderip alan on milyonlarca adresi sürekli olarak korelasyon tabanlı mahremiyet analizi işlemine girdirmek analizin performansı açısından etkili sonuçlar almayı zorlaştırır. Bu gibi nedenlerden dolayı analizlerin tamamı belirli bir blok aralığında yapılmasının daha doğru olacağı kanaatine varılmıştır. Bunun için de son 10,000, 25,000 ve 50,000 blok kısaca temel analizlere sokularak hız ve performans ile elde edilen sonuçların etkileri ve yüzdeleri bakımından karşılaştırılmışlardır. Karşılaştırma sonucunda korelasyon tabanlı mahremiyet analizinin son 25,000 blok aralığı için yapılmasında karar kılınmıştır.



Aktif Zcash Madenci Havuzları

Havuz Adı	Ödül Metodu	Ağ HashOranı 6.9 GSols/s (82 %)	Madenciler 4469	Çalışanlar 55231
Poolin	PPS (3%)	2.1 GSols/s (30.9%)	1167	28590
F2Pool	PPS (3%)	1.1 GSols/s (16.1%)	-	-
Antpool	PPS (5%)	761.7 MSols/s (10.9%)	-	3070
Slushpool	SHR (2%)	704.6 MSols/s (10.1%)	-	7963
Flypool	PPLNS (1%)	370.3 MSols/s (5.3%)	2061	8913
Luxor	PPS (1%)	241.2 MSols/s (3.5%)	828	-
ViaPool	PPS+ (4%), PPLNS (2%) and SOLO (1%)	240.5 MSols/s (3.4%)	-	5128
Dpool	FPPS (2%)	50.2 MSols/s (0.7%)	-	26
2Miners	PPLNS (1%)	26.8 MSols/s (0.4%)	109	333
Nanopool	PPLNS (1%)	26 MSols/s (0.4%)	296	729
MiningPoolHub	PPLNS (0.9%)	17.7 MSols/s (0.3%)	-	395
Zhash	PPLNT (0%)	3.2 MSols/s (0.0%)	-	65
Luckpool	PPLTS (1%)	1.4 MSols/s (0.0%)	8	16
Equipool	PPLNS	136.2 kSols/s (0.0%)	-	3
Minerall	PPLNS (2%)	-	-	-

Şekil 5. Aktif Zcash Madenci Havuzları (*https://www.poolwatch.io/coin/zcash bağlantı adresini kullanarak ulaşabilirsiniz. 1 Temmuz 2020 01:37 tarihinde erişilmiştir.*)

Tablo 1, tüm Zcash madenci ve madenci havuzlarının toplamda üretmiş oldukları blok sayısıyla beraber elde ettikleri blok ödüllerini Zatoshi cinsinden verir. Bazı t-adresleri için t-Havuz, bazıları için de t-Madenci olarak bahsedilmiştir. Bunun tek nedeni t-Havuz olarak bahsedilen t-adresleri çeşitli Zcash gezginleri (Zcash explorer) kullanılarak tespit edilebilirken t-Madenci olarak bahsedilen t-adresleri bu gezginlerde tespit edilemeyen diğer madencilerdir. Bunlara havuz denmeyişinin tek sebebi de bu adreslerin madenci havuzuna mı yoksa doğrudan bir madenciye mi ait olduğu tespit edilemediğinden dolayıdır. Bunun yanında listede bazı t-adreslerinin yanına (1) ve (2) sayılarının olduğu görülmektedir; bu rakamlar işaret ettikleri üç t-adresinin aynı maden üretme ödülü işleminde aynı ödülü paylaştıklarını belirtmek için konulmuşlardır. Bu kullanıcıların neden bu şekilde bir kullanıma gittikleriyle alakalı herhangi bir bilgiye ulaşılamamıştır. Ayrıca ödülü paylaşan bu t-adresler yüzünden en alttaki TOPLAM'da üretilen 25,000 blok olması gerekirken 25,395 blok üretilmiş gibi görünmektedir. (1) ve (2) olarak belirtilen adresler blok sayısının çoklanmasına ve TOPLAM'ın 25,000'den çok olmasına sebep olmuştur.

Madenciler edindikleri maden ödülünü ilk olarak korumalı havuzdan aktarır. Bu ödülü korumalı havuza aktardıktan sonra harcarlar. Bu nedenle elde edilen tüm ödüller bir şekilde korumalı havuza aktarılır, yani bu ödülleri en azından bir kere EB-işlemi kullanılarak harcanırlar/aktarılırlar. Madenci havuzları da ilk olarak ödülü korumalı havuza gönderir. Daha sonra madencilere ödeme için pay ederler. Yukarıdaki madenci havuzları incelendiği zaman üç farklı şekilde bünyelerindeki madencilere blok ödülünden pay verdikleri görülmüştür:

Tablo 1. Son 25,000 Blok İçin Madenci Havuzları ve Madencilerinin Ürettikleri Blok Sayıları ve Kazandıkları Toplam Blok Ödüllerinin Tablosu

Muhtemel Madenci Havuzu	Üretilen Blok Sayısı	Elde Edilen Ödül (Zatsohi)
t-Havuz$_1$	6689	3,344,969,017,139
t-Havuz$_2$	4064	2,032,320,097,793
t-Havuz$_3$	3473	1,736,716,892,093
t-Havuz$_4$	3116	1,558,218,911,897
t-Havuz$_5$	1984	992,096,545,245
t-Havuz$_6$	1844	903,249,641,532
t-Havuz$_7$	1671	835,613,483,844

t-Havuz$_8$	1005	502,575,066,265
t-Madenci$_{1.1}$ (1)	192	94,800,000,000
t-Madenci$_{1.2}$ (1)	192	1,200,000,000
t-Madenci$_{1.3}$ (1)	192	0
t-Madenci$_2$	123	61,504,294,873
t-Havuz$_9$	119	59,505,023,033
t-Havuz$_{10}$	114	57,002,644,529
t-Madenci$_3$	110	55,003,940,580
t-Madenci$_4$	108	54,001,092,756
t-Madenci$_5$	59	29,503,685,602
t-Madenci$_6$	54	27,000,610,772
t-Madenci$_7$	48	24,010,592,681
t-Havuz$_{11}$	48	24,001,376,828
t-Madenci$_8$	40	20,002,890,351
t-Havuz$_{12}$	40	20,001,576,991
t-Madenci$_9$	28	14,000,407,478
t-Madenci$_{10}$	26	13,000,740,130
t-Madenci$_{11}$	16	8,000,755,908
t-Madenci$_{12.1}$ (2)	11	5,502,394,915
t-Madenci$_{12.2}$ (2)	11	0
t-Madenci$_{13}$	10	5,000,690,720
t-Madenci$_{12.3}$ (2)	6	3,000,067,198
t-Madenci$_{14}$	2	1,000,003,838
TOPLAM	**25395**	**12,482,802,444,991**

1. İlk yöntemde madenci havuzları korumalı havuzdan ZEC'leri bir t-adrese aktarır daha sonra madencilerine ödeme yaparlar. Yani zden tye bir EB-işlemi gerçekleştikten sonra ödeme tamamen şeffaf işlemler olan tden tye işlemlerle gerçekleştirilir. Bu şekilde ödeme yapan madenci havuzlarına TMadenciler denilir.
2. İkinci yöntemde madenci havuzları korumalı havuzdan doğrudan pay etme işlemi yaparlar. Bu yöntemin en çarpıcı özelliği zden tye yapılan işlemde adres ve miktarı görünmeyen bir girdiden sayısı yüzleri bu t-adreslere ödeme yapılmasıdır. Bu şekilde bir ZEC gönderimini madenci havuzları dışında hemen hemen hiçbir kimsenin yaptığı gözlemlenememiştir. Bu şekilde payı dağıtan madenci havuzlarına ZMadenciler denilir.
3. Üçüncü ve son yöntemde madenci havuzları pay dağıtımını tamamen korumalı zden zye işlemler vasıtasıyla yaparlar. Korumalı işlemleri analiz etmek mümkün olmadığı için de bu madenci havuzları korelasyon tabanlı mahremiyet analizi kapsamında incelenemişlerdir. Bu durum her ne kadar makalede elde edilecek sonuç açısından üzücü olsa da anonimliği birinci önceliği olan Zcash kriptoparası için oldukça mühim ve sevindirici bir durumdur.

3.1.1. TMadencilerin analizi

Alex Birkuyov tarafından hazırlanan [2] makalesinde bahsedilen yöntemlerden yola çıkarak TMadencilerin analizi yapılmıştır. Makalede bahsedilmiş olan ilgili analiz algoritması yüzeysel olduğundan dolayı bu algoritmadan yola çıkılarak yeni bir TMadenci bulma algoritması yazılmıştır. Bu algoritma Ek-A'da Algoritma I: TMadencilerinBulunması başlığıyla gösterilmiştir.

Algoritma 1'de yapılan analiz çalışmasından sonra bulunan *korumaliHavuzdanCoinAlanGruplanmisListesi* ile daha önce tespit edilmiş olan madenci havuzları listesi karşılaştırılır. Karşılaştırma, blok üretme ödüllerini korumalı havuza koyan madenci havuzlarının yaptıkları tden zye işlemleri çıktı toplamlarıyla *korumaliHavuzdanCoinAlanGruplanmisListesi*'ndeki muhtemel TMadencilerin yaptıkları zden tye işlemlerinin toplamı karşılaştırılır. Bu karşılaştırma sonucunda bulunan veriler aşağıdaki Tablo 2 de detaylı olarak gösterilmiştir. Ödül Adresi olarak belirtilen adresler blok ödülünü alan adreslerdir. Ödeme adresleri olarak belirtilen adresler ise ödülü alan madenci havuzunun bünyesinde bulundurdukları madencilere ödeme yaptıkları adreslerdir.

Bir madenci havuzu için birden fazla ödeme adresi olabilir. Analiz sırasında bazı adreslerin çarpraz bir şekilde birbirlerine ödeme yaptıkları gözlemlenmiştir. Bu da analiz sırasında hangi adreslerin gerçekten ödeme yapılan adres olduğu, hangi adreslerin ödeme yapılan adres olduğunu anlamayı zorlaştırmıştır. Bu nedenle bir önceki tabloda bulunan bazı madenci havuzlarının TMadenci kategorisine girdikleri tespit edildiği halde Tablo 2'deki listede yer alamamışlardır.

Aşağıdaki Tablo 2'de Ödül Adresi'nin sağındaki Blok Sayısı alanı o adresin toplamda kaç blokta tden zye EB-işlemi yaptığını verir. O alanın sağında bulunan Zatoshi Değeri alanı da o bloklarda gönderilen toplam Zatoshi cinsinden değerlerini verir. Bazı madenci havuzları blok ödüllerini biriktirip göndermeyi tercih ederken bazı madenci havuzları aldığı ödülleri doğrudan göndermeyi tercih etmişlerdir. Ödeme Adresi alanının sağındakı Blok Sayısı alanı muhtemel TMadenci adresinin yaptığı zden tye EB-işlemlerinin toplam sayısını, o alanın sağında bulunan Zatoshi Değeri alanı da bu işlemlerin toplam gönderilen Zatoshi cinsinden değerini verir.

Tablo 2. Algoritma 1 Kullanılarak Bulunan Muhtemel TMadenciler Tablosu

Ödül Adresi	**Blok Sayısı**	**Zatoshi Değeri**	**Ödeme Adresi**	**Blok Sayısı**	**Zatoshi Değeri**
t-Madenci$_{12.1}$ (2)	11	5,502,394,915	MuhtemelTMadenci$_1$	11	5,502,174,915
t-Havuz$_6$	1864	991,096,475,562	MuhtemelTMadenci$_2$	1848	991,559,348,012
t-Madenci$_2$	10	64,504,511,838	MuhtemelTMadenci$_3$	9	64,500,000,000
t-Havuz$_2$	46	2,049,331,846,484	MuhtemelTMadenci$_4$	22	2,049,331,406,484
TOPLAM	1931	1,061,103,382,315	**TOPLAM**	1890	1,061,561,522,927

Son 25,000 blok içerisinde toplamda 17,656 EB-işlemi yapılmıştır. TMadenci analizi ile yukarıdaki tabloya göre toplamda 3,821 EB-işleminin birbirleriyle ilişkisi ortaya çıkmaktadır. Bunun anlamı bütün EB-işlemlerinin %21,6'sının korumalı havuza girmelerine rağmen hangi adresten gelip hangi adrese gittiği izlenebilmekte; ayrıca hangi madenci adresinin hangi madenci havuzu bünyesinde bulunduğu tespit edilebilmektedir. TMadencilerin analizi ile son 25,000 blok için tüm EB-işlemlerinin %21,6'sının anonimliği ve mahremiyeti analiz edebilmiştir. Son 10,000 ve 50,000 blok analizi yapıldığında da yine benzer oranlar elde edilmiştir.

3.1.2. ZMadencilerin analizi

TMadenci olarak adlandırılmış olan madenci havuzları bünyesindeki madencilere ödül paylaşımını korumalı havuzdan ZEC'i çektikten sonra şeffaf işlemler vasıtasıyla yaparlar. ZMadencilerse araya fazladan bir şeffaf işlem koymaksızın ödemeleri doğrudan korumalı havuzdan madencilerine olacak şekilde yaparlar. Yani ödemeler zden tye EB-işlemleri vasıtasıyla gerçekleştirilir. ZMadencileri bulmak için kullanılmış olan algoritma Ek-B'de Algoritma II: ZMadencilerinBulunması başlığıyla gösterilmiştir. TMadenciler algoritmasında olduğu gibi ZMadenciler kullanılan algoritmada da [2] makalesinde bulunan ilgili algoritma temel alınmış ve üzerinde bazı güncellemeler yapılmıştır.

Algoritma sonucunda Muhtemel ZMadenciler bulunduktan sonra TMadencilerde yapıldığı gibi ilk olarak Tablo 1'deki madenci havuzları tablosunda tespit edilen madenci havuzlarının blok üretme ödülleri toplamıyla muhtemel ZMadencilerin gruplanmış haldeki zden tye işlemlerinin girdi değerleri toplanarak karşılaştırılır ve eşleşen kayıtlar listelenir. Yapılan karşılaştırmanın sonucu aşağıdaki Tablo 3'teki gibidir. Tablo 3'teki listede Tablo 2'deki gibi bir Ödeme Adresi alanı bulunmamasının tek nedeni ZMadencilerin ödemeyi aracı bir t-adresi olmadan doğrudan yapmalarıdır. Gruplandırılabilecek bir t-adresi olmadan, z-adresleri de gruplandırılamayacağından dolayı tespit edilen işlemler gruplandırılmıştır, bu nedenle bir Ödeme İşlemi Grubu oluşturulmuştur. Bu grup 30 ve daha fazla aynı adrese (madencilerin adresleri) sahip olan işlemlerin oluşturduğu gruptur. ZMadenciler için algoritma sonucunda ikiden fazla "işlem grubu" bulunmuştur. Ancak karşılaştırma sonucunda herhangi bir Tablo 1'deki t-adresin değeriyle eşleşme olmadığından aşağıdaki listede diğer işlem grupları

gösterilememiştir. Bunun yanında bir diğer madenci havuzu tespit etme yöntemi olan "madenci adresinden yola çıkarak madenci havuzlarını bulma yöntemi" kullanılmaya çalışılmış; ancak bu madenci havuzları yine de tespit edilememiştir. Bu durumun nedeni madenci havuzları kendi sitelerinde artık madenci adreslerini gizlemeyi tercih etmektedirler.

Tablo 3. Algoritma 2 Kullanılarak Bulunan Muhtemel ZMadenciler

Ödül Adresi	Blok Sayısı	Zatoshi Değeri	Ödeme İşlemi	Blok Sayısı	Zatoshi Değeri
t-Havuz$_{10}$	100	57,002,644,529	İşlemGrubu$_1$	98	56,955,178,696
t-Havuz$_9$	111	59,004,988,098	İşlemGrubu$_2$	109	58,828,420,000
TOPLAM	211	116,007,632,627	**TOPLAM**	207	115,783,598,696

ZMadencileri bulma algoritması sonuçlara göre toplamda 418 korumalı işlem muhtemel ZMadenci kategorisinde birbirleriyle ilişkilendirilmiştir; bu da son 25,000 bloktaki korumalı işlemlerin %02,4'ünün birbirleriyle bir ilişkisi olduğu anlamına gelir. Böylece TMadenci havuzu analizi sonuçları ile ZMadenci analizi sonuçları birleştirildiği takdirde şimdiye kadar son 25,000 bloktaki tüm korumalı işlemlerin %24'ü için korelasyon tabanlı mahremiyet analizi yapılabilmiş demektir.

TMadencilerle veya ZMadencilerle ilişkilendirilememiş toplamda 24 madenci daha bulunmaktadır. Bu madencilerden bir kısmı muhtemelen madenci havuzu değil ciddi miktarda işlemci gücü toplamış madenci adresleridir. Ayrıca bahsedilen madencilerin TMadenci ve ZMadenci algoritmalarında tespit edilememesinin en önemli nedeni yukarıda da bahsedildiği gibi bazı madenci havuzlarınının bünyesinde bulundurdukları madencilere blok ödülünden payı zden zye korumalı işlemler vasıtasıyla gerçekleştirmesidir. Kalan madencilerin 2,158 EB-işlemi daha bulunmaktadır ki, bu da tüm EB-işlemlerinin %12,2'sidir. Her ne kadar bu işlemler takip edilememiş olsa da toplamda tüm EB-işlemlerinin %36,2'sinin madenciler ve madenci havuzları ile bir şekilde ilişkili olduğu söylenebilir.

3.2. Gidiş-Geliş İşlemleri

Zcash kriptoparasını kullanan ve yaptıkları ZEC aktarımlarına mahremiyet kazandırmak isteyen Zcash kullanıcıları bunu EB-işlemleri vasıtasıyla gerçekleştirirler. Her ne kadar bir nebze anonimlik ve mahremiyet kazandırsa da bazı Zcash kullanıcıları kısa süre içerisinde tden zye, sonra da zden tye ZEC aktarımı gerçekleştirirler. Yapılan bu işlemler sonucunda da ZEC aktarımlarında tden zye işlemin değeriyle zden tye işlemin değeri aynı yahut yakın olduğu için bu iki adres arasında ilişki kurulabilmektedir. Bu ilişki sonucunda korumalı havuza giren ve korumalı havuzdan çıkan iki farklı EB-işlemi arasında doğrudan bir ilişki elde edilmiş olur. Bu şekilde analiz edilerek bulunan EB-işlemlerine gidiş-geliş işlemleri (round-trip transaction-RTT / kısaca GGİ) denir [2], [19].

Gidiş-geliş işlemleri 3 farklı yöntemle analiz edilmektedir, [2]. Bu yöntemlerin hepsinde bir ya da daha fazla tden zye işlemin girdi değeriyle bir ya da daha fazla zden tye işlemin çıktı değerleri karşılaştırılır. İlk yöntemde kısaca birer tden zye ve zden tye işlemin değerleri birbirine eşit mi değil mi diye bakılır. Bu iki değer birbirine eşitse arada bir ilişki vardır denilebilir. İkinci yöntemde bir tden zye işlem iki farklı z'ten t'ye işlemin toplamına eşit mi değil mi diye kontrol edilir. Eşitlik bulunursa yine bu işlemler arasında bir ilişki olduğu söylenebilir. Üçüncü ve sonunca yöntemde de yine bir tden zye ve zden tye işlemin değerlerinin son 4 rakamı karşılaştırılır. Son 4 rakamında benzerlik olan değerler, değerlerin kendisi birbirine yakınsa aralarında bir ilişki vardır denilir.

3.2.1. Temel karşılaştırma

Temel karşılaştırma yönteminde korumalı havuza Z aktarımı yapan bir tden zye işlem (bundan sonra t-z işlemi olarak bahsedilecektir) ile korumalı havuzdan çıkan zden tye işlem (bundan sonra z-t işlemi olarak bahsedilecektir) karşılaştırılacaktır. Karşılaştırmada basitçe korumalı havuza giren ZEC değeri ile korumalı havuzdan çıkan ZEC değeri karşılaştırılır ve birbirlerine eşit olmaları halinde bu iki işlem arasında bir ilişki olduğu varsayılır. Bu karşılaştırmadaki tek koşul t-z işleminin z-t işleminden önce gerçekleşmiş olmasıdır (yani ZEC ilk önce korumalı havuza girmiş, daha sonra korumalu havuzdan çıkmıştır).

Yapılan karşılaştırmada ilk olarak birbirine eşit değerler karşılaştırılmıştır. Daha sonra t-z işlemiyle korumalı havuza ZEC girdirdikten sonra zden zye işlem (bundan sonra z-z işlemi denilecektir) yapıp daha sonra bu ZEC'leri havuzdan z-t işlemiyle çıkartan Zcash kullanıcılarının işlemlerinin de analizi yapılmıştır. Zcash kullanıcıları burada doğrudan bir t-z işlemi yapıp hemen ardından z-t işlemi yapmak yerine bu iki işlem arasında korumalı bir (yahut daha fazla) z-z işlemi yaparak karıştırma yaparlar. Korumalı z-z işlemlerinde daha önce de bahsedildiği gibi sadece işlem bedelleri görülmektedir. Bunun için karşılaştırmaya ayrıca işlem bedelleri de dâhil edilmiştir.

Bahsedilen ilk temek karşılaştırmada karşılaştırma denklemi "t-z girdi değeri = z-t çıktı değeri" şeklindedir. İkinci karşılaştırmadaki denklem arada yapılmış olması muhtemel olan z-z korumalı işlemleri de dâhil etmek amacıyla "t-z değeri = z-t değeri + işlem

bedeli * (yapılan muhtemel z-z işlemi sayısı veya değiştirlen işlem bedeli – kullanıcılar ayrıca işlem bedellerini de değiştirebilirler)" şeklinde değiştirilmiştir. İşlem bedellerinde ilk olarak sadece varsayılan işlem bedeli olan 10^5 Zatoshi değerindeki işlemler dâhil edilmiştir. Ancak işlem bedelleri ZEC aktaran kişiler tarafından değiştirilebileceğinden yahut ZEC aktarımı yapan kişilerin birden fazla karşılaştırma işlemi (z-z işlemi) yapabileceklerinden işlem bedelleri $2*10^5$, $3*10^5$, $4*10^5$, $5*10^5$ ve $6*10^5$ olarak belirlenmiştir. En fazla işlem bedelinin $2*10^5$ olarak seçildiği yapılan karşılaştırmalarda tespit edilmiştir. Yukarıda yapılan temel gidiş-geliş işlemleri karşılaştırmalarında toplamda 1,516 farklı t-z ve z-t işlemi arasında ilişki tespit edilmiştir; bu da toplam EB-işlemlerinin işlemlerin %08,6'sına tekabül eder.

3.2.2. Alt-küme toplamlarının karşılaştırılması

Korumalı havuzda z-z işlemi yaparak "*ZEC karıştırması yapmak*" z-z işlemlerini hiç kullanmamaya nazaran daha fazla anonimlik sağlamaktadır. Ancak sonuçta doğrudan korumalı havuza giren değerle aynı yahut yakın bir değeri korumalı havuzdan çıkararak şeffaf havuzda Zcash işlemlerine devam etmek de bir önceki kısımda yapılan analiz çalışmasında da gözlemlendiği gibi yine düşünüldüğü kadar anonimlik sağlamamaktadır. Bu durumda Zcash kullanıcıları korumalı havuzdan çıkarken ellerinde bulundurdukları ZEC'leri iki yahut daha fazla parçaya bölüp bu parçaları farklı t-adreslere göndererek anonimlik ve işlem gizliliğinin artırmayı amaçlarlar. Ne var ki, ZEClerini iki parçaya bölerek korumalı havuzdan çıkartan kullanıcıların işlemlerini analiz etmenin de yöntemi bulunmaktadır.

Alt-küme Toplamlarının Karşılaştırılması durumunda iki farklı z-t işlemi çıktı değerleri toplamıyla bu değerlerin işlemlerinden önce gerçekleşmiş olan herhangi bir t-z işleminin girdi değeri birbirleriyle karşılaştırılır. Burada kullanıcı korumalı havuza t-z işlemi ile ZEC aktarmıştır, bu ZEC'i iki farklı z-adrese bölerek bu adresler aracılığıyla iki farklı z-t işlemi gerçekleştirmiştir.

Karşılaştırma sonrası bu iki değer eşleştiği takdirde bu değerler arasında bir ilişki olması muhtemeldir. Karşılaştırma işlemine başlamadan önce bir önceki yöntemde yapıldığı gibi Z-madenciler ve T-madenciler karşılaştırılacak işlemlerden çıkartılmıştır. Ayrıca buna ek olarak bir önceki karşılaştırmada tespit edilen işlemler de karşılaştırılacaklar listesinden çıkartılır. Aynı şekilde girdi ve çıktı değerlerinden yine üç defadan fazla karşılaştırmaya giren değerleri olan işlemler de listeden çıkartılır. Kalan çıktı değerlerinin hepsi toplanır, toplanan değerlerden yine üç defadan fazla çıkan değerler bulunacak karşılaştırma sonuçlarının çoklanmasını engellemek adına çıkartılır. Son olarak bir önceki yöntemin ikinci karşılaştırmasında yapıldığı gibi muhtemel z-z ara-işlemlerinin işlem bedeli değerleri z-t işlemlerinin çıktılarının toplamıyla ayrıca toplanır ve t-z işlemlerinin girdi değerleriyle karşılaştırılır.

Yapılan alt-küme toplamları karşılaştırması sonucunda 1,613 farklı girdi ve çıktı işleminin eşleştiği tespit edilmiştir. Bu da tüm EB-işlemlerinin işlemlerin %09,1'ine tekabül eder.

3.2.3. Parmak izi değerleri karşılaştırması

Zcash kullanıcıları t-z işlemi yahut z-t işlemi kullanarak ZEC aktarımı yaparken bazen gönderilecek değerdeki EB-işlemlerinin varsayılan işlem ödülü değeri olan 10.000 Zatoshi'den daha az olan kısmını görmezden gelme hatasına düşerler. "Parmak izi değeri" adı verilen bu değer kullanılarak iki farklı işlemin girdi ve çıktı değerleri arasında bir ilişki kurmak mümkün olmaktadır. Daha önceki karşılaştırma denklemlerinde olduğu gibi bu karşılaştırma denkleminde de T-Madencilerin işlemleri, Z-Madencilerin işlemleri ve daha önceki her iki yöntemdeki karşılaştırmalarda tespit edilen işlemler karşılaştırılacaklar listesinden çıkartılır. Ayrıca parmak izi değeri üç kereden daha fazla kez listeye giren değerlere ait işlemler de parmaz izi değerleri karşılaştırması analizindeki karşılaştırılacaklar listesinden çıkartılır. Bu karşılaştırmada t-z işlemi girdi değeriyle z-t işlemi çıktı değeri son 4 rakamı eşit olan tüm işlemler bulunur. Burada dikkat edilmesi gereken en önemk-li nokta girdi değerinin çıktı değerinden büyük olması; ancak çok büyük olmamasıdır. Bu nedenle karşılaştırılarak bulunan işlemlerin değerleri (Girdi_Değeri / Çıktı_Değeri) -1<0.01 olacak şekilde bir denkleme sokulur. Bu denklem sonucunda 593 farklı t-z ve z-t işlemi bulunur. Bu da tüm EB-işlemlerinin %03,4'üne tekabül eder.

3.3. Zcash Analizi Sonuçları

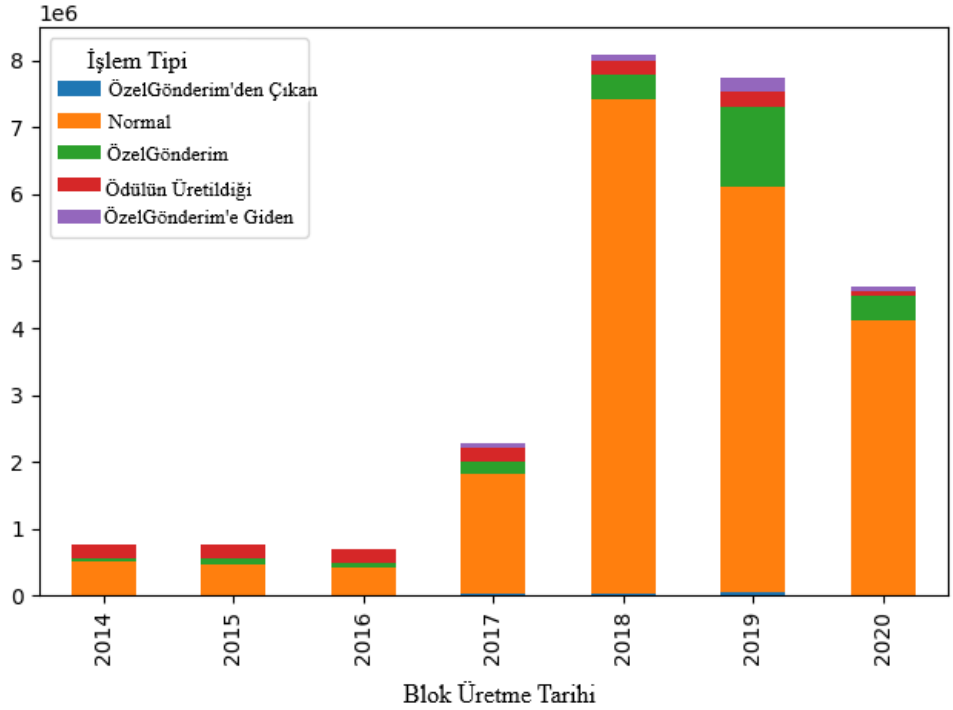
Yukarıda detaylı bir şekilde anlatılan korelasyon tabanlı mahremiyet analizi işlemlerinin sonucunda son 25,000 bloktaki toplam 7,961 EB-işleminde tam olarak bir ilişki tespit edilebilmiştir ki, bu da tüm EB-işlemlerinin %45,1'idir. Bu ilişkiler haricinde 2,158 ödülü alan madenci havuzu yahut madencinin yapmış olduğu t-z işlemi, 325 Zcash sahiplerinin yapmış olduğu t-z işlemi, 783 TMadenci şartlarına uyan z-t işlemi ve 23 ZMadenci şartlarına uyan z-t işlemi tespit edilmiştir. Bu adresler ve işlemler tek taraflı analiz edilebilen ancak kime ait olduğu "kesinlikle" belli olan ve toplam EB-işlemlerinin %18,6'lık kısma tekabül eden adres ve işlemlerdir. Toplamda bu şekilde olan 3,289 işlem tespit edilmiştir.

Zcash kriptoparası için son 25,000 bloktaki EB-işlemlerinin tam olarak 4,302 tanesi, yani %24,6'sı z-z işlemidir. Bu işlemleri mevcut yöntemlerle analiz etmek mümkün değildir. Bu nedenle analiz edilebilme ihtimali olan EB-işlemlerinden z-z işlemleri çıkartıldığı takdirde kalan tüm EB-işlemlerinin %84,4'ü için bir şekilde ilişkilendirilme yapılmıştır. Sonuç olarak Zcash anonim kriptoparası pratikte istenilen seviyede anonim değildir.

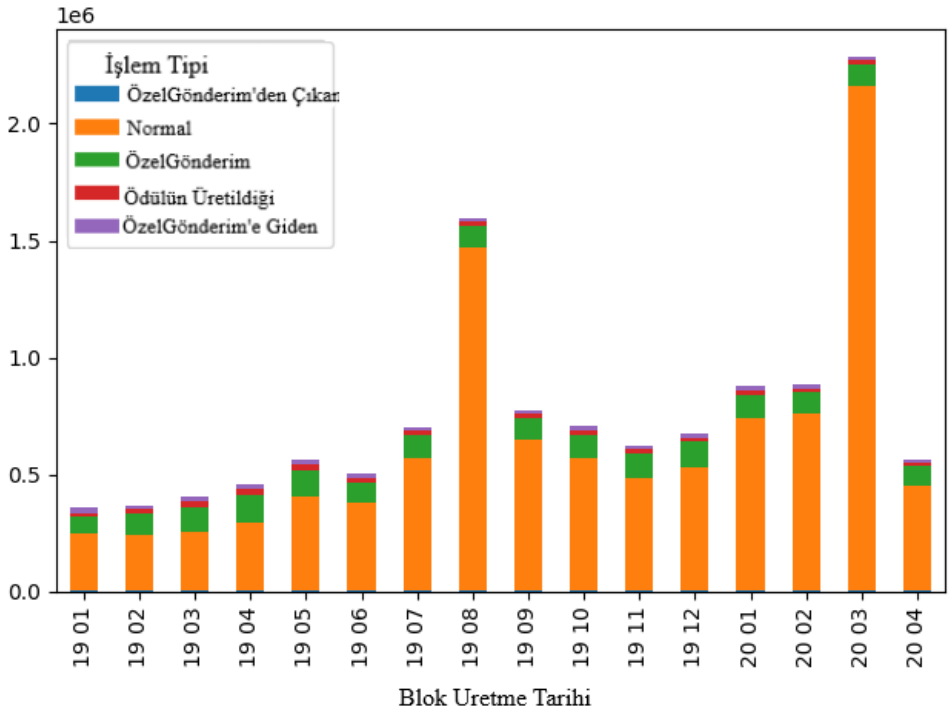
IV. DASH ANALİZİ (ANALYSIS OF DASH)

Dash analizi 26 Nisan 2020 16:23:44 tarihinde başlatılmıştır. Bu tarihte üretilen en son blok 1297693. bloktur. Zcash analizinde olduğu gibi 1297693. bloktan sonra üretilmiş bloklar ve bloklara ait işlemler analize dâhil edilmeyecektir. Korelasyon tabanlı mahremiyet analizinde yapılacak olan madenci havuzu analizleriyle gidiş-geliş işlemleri analizi yine aynı şekilde Zcash anonim kriptoparasında yapıldığı gibi son 25,000 blok temel alınarak yapılacaktır.

Zcash'teki işlemler EB-işlemleri ve şeffaf işlemler olarak ikiye ayrılırken tüm işlemleri şeffaf olan Dash'in işlemleri, ÖzelGönderim kullanılarak anonimlik sağlayan karıştırma işlemleri (mixing transactions) ve normal işlemler olmak üzere ikiye ayrılır. Doğrudan bu karıştırma işlemlerini analiz etmek, karıştırmada kullanılan adreslerin sadece o işleme özel (tek kullanımlık) olmaları nedeniyle gruplandırılamayacaklarından dolayı mümkün değildir. ÖzelGönderim işlemleri bu nedenle bir nevi Zcash'teki zden zye korumalı işlemlerine benzer. Zcash için yapılan analiz korumalı havuza giren tden zye ve korumalı havuzdan çıkan zden tye işlemler kullanılarak mümkün olmaktadır. Bu nedenle Dash'in analiz edilebilmesi için ÖzelGönderim dışındaki normal işlemleri analiz edilebilecek şekilde gruplandırmak gerekmektedir.



Şekil 6. Yıllara Göre Kullanıcılar Tarafından Dash İşlem Tiplerinin Tercih Edilme Oranları



Şekil 7. 2019 ve 2020 Yılları İçin Aylara Göre Kullanıcılar Tarafından Dash İşlem Tiplerinin Tercih Edilme Oranları

Dash anonim kriptoparası için korelasyon tabanlı mahremiyet analizi gerçekleştirebilmek adına tüm işlem tipleri aşağıdaki gibi 5 parçaya bölünmüştür:

1. **Normal İşlemler:** Bitcoin'deki işlemlerin aynısıdır. Zcash anonim kriptoparasında bu işlemler şeffaf işlemler olarak geçer. Dash'te bulunan bu normal işlemler mahremiyet analizine dâhil edilmeyecektir.
2. **Ödül İşlemleri:** Bloğu oluşturan madenciyle beraber AnaUç'a blok ödülünün verildiği işlemdir. Bitcoin ve Zcash gibi tüm kriptoparalarda bu işlemler bulunur. Girdi adresi daima boştur ve işlem ücreti sıfırdır. Girdi değeri üretilen blok ödülüyle blok içerisinde geçen işlemlerin işlem bedeli değerlerinin toplamıdır. Normal işlemlerde olduğu gibi analize dâhil edilmez.
3. **ÖzelGönderim İşlemleri:** Dash anonim kriptoparası için "anonimliğin" gerçekleştirildiği işlemlerdir. 2.4 Dash bölümünde detaytlı bir şekilde anlatılmışlardır. Yapılan korelasyon tabanlı mahremiyet analizi açısından incelendiği zaman Zcash'teki zden zye korumalı işlemlere benzerler. Girdi sayısı ile çıktı sayısı ve girdi değeri toplamı ile çıktı değeri toplamı daima aynıdır, işlem ücreti sıfırdır. Korelasyon tabanlı mahremiye analizini gerçekleştirmek adres gruplaması yapılamadığından mümkün değildir, bu nedenle mahremiyet analizine dâhil edilmezler.
4. **ÖzelGönderim'e Giden İşlemler:** Elindeki Dash'i anonimleştirmek isteyen kullanıcı, bu Dash'leri yukarıdaki 3. maddede anlatılan ÖzelGönderim işlemlerine dâhil eder. Dash gezginleri incelendiği zaman ÖzelGönderim işlemlerinden hemen önceki işlemde ilgili Dash değerinin parçalanıp farklı adrese bölündüğü gözlemlenecektir. Dash'lerin ÖzelGönderim öncesi parçalandığı işlemlere ÖzelGönderim'e Giden İşlemler adı verilir. İşlem ücreti sıfırdan büyüktür. Bu işlemleri tespit etmek çıktı adreslerinin değerlerine bakılır. Eğer 2 ya da daha fazla 1.00001 sayısına bölünen çıktı adresi değeri varsa bu işlem ÖzelGönderim'e Giden İşlemdir. Zcash anonim kriptoparasındaki tden zye işlemlere benzerler. Dash anonim kriptoparası için mahremiyet analizine dâhil edilmiş olan ilk işlem tipidir.
5. **ÖzelGönderim'den Çıkan İşlemler:** ÖzelGönderim'e Giden İşlemlerin aksine ÖzelGönderim kullanılarak anonimleşmesi sağlanan Dash'lerin sahipleri tarafından harcanmak vs. gibi sebeplerle kullanıcının cüzdanlarına geri ödendiği işlemlerdir. Yani anonimleştirilen Dash'lerin tekrardan bir adrese kümelendirildiği işlemlerdir. İşlem ücreti sıfırdan büyüktür. Bu işlemleri tespit etmek için bu sefer girdi adreslerinin girdi değerlerine bakılır. Eğer 2 ya da daha fazla 1.00001 sayısına bölünen girdi adresi değeri varsa bu işlem ÖzelGönderim'den Çıkan İşlemdir. Zcash anonim kriptoparasındaki zden tye işlemlere benzerler. Dash anonim kriptoparası için mahremiyet analizine dâhil edilmiş olan bir diğer işlem tipidir.

Yukarıda gösterilmekte olan Şekil 6 ve Şekil 7'de Dash işlem tiplerinin iki farklı zaman aralığı için grafikleri verilmiştir. Şekil 6'da Dash'in ilk çıktığı 2014 yılından analiz için belirlenen en son blok olan 1260895 nolu bloğa kadar olan, yani 26 Nisan 2020 tarihine kadar üretilmiş olan tüm bloklarının işlem tiplerine göre toplam kullanılma sayılarının grafiği verilmiştir. Şekil 7'de ise 2019 ile 2020 yılları içinde 01 Ocak 2019 tarihinde üretilen ilk bloktan yine 1260895. bloğa kadar aylara ve yıllara göre tüm bloklarının işlem tiplerine göre toplam kullanılma sayılarının grafiği verilmiştir. Her iki grafikte de sol üstte görünen *1e6* ifadesi y eksenindeki değerlerin 1,000,000'ın katları olduğunu belirtir. Mesela Şekil 6'da 2017 yılı için x ekseninde bulunan Normal İşlem verisinin y eksenindeki değeri ortala 2'dir. Bunun anlamı 2017 yılında Dash kullanıcıları yaklaşık 2,000,000 civarında Normal İşlem gerçekleştirmişler demektir.

Şekil 6'daki grafik incelendiği zaman Dash kullanımının 2017 yılında bir anda ciddi bir şekilde arttığı açıkça görülmektedir. Grafikte tüm yıllar için ÖzelGönderim işlemlerini kullanıcılar tarafından çok fazla tercih edilmediği aşikârdır. Aynı durum Şekil 7'de bulunan grafikte de görünmektedir. Bu iki grafik incelendiği zaman anlaşılacağı üzere Dash kullanıcıları büyük çoğunlukla normal işlemleri yapmayı tercih etmektedir. Tablo 4'te Şekil 6'da gösterilmekte olan ilk bloktan 1260895. bloğa kadar yapılan tüm işlemlerin işlem tipine göre toplam kullanılma/tercih edilme sayıları verilmiştir. ÖzelGönderim işlemleri, ÖzelGönderim'e Giden işlemler ve ÖzelGönderim'den Gelen işlemler; yani ÖzelGönderim ile alakalı işlemlerin "toplamının" tüm işlemlerin toplamına oranı Tablo 4'te görüldüğü gibi %11.79 olmaktadır.

Tablo 4. 129769. Bloğa Kadar Tiplere Göre Dash İşlemleri Sayıları ve Yüzdeleri

Dash Blokzinciri İşlem Tipi	**Toplam İşlem Sayısı**	**Toplam İşlem Sayısı Yüzdesi**
ÖzelGönderim'e Giden	493,818	1.976501384
ÖzelGönderim'den Gelen	147,193	0.589138444
ÖzelGönderim	2,305,085	9.226078621
Normal	20,732,384	82.98115028
Blok Ödülü	1,305,970	5.227131276
TOPLAM	24,984,450	100.00

Dash anonim kriptoparası için daha efektif bir korelasyon tabanlı mahremiye analizi yapabilmek adına Zcash anonim kriptoparasında da yapıldığı gibi ilgili analiz çalışması son 25,000 blok için yapılmıştır. Tablo 5'te son 25,000 blok için kullanıcıların tercih ettikleri toplam işlem tipi sayıları ve yüzdeleri verilmiştir. Son 25,000 blokta ÖzelGönderim ile alakalı işlemler toplamda 179,995 işlemdir (ÖzelGönderim işlemleri, ÖzelGönderim'e Giden işlemler ve ÖzelGönderim'den Gelen işlemler). ÖzelGönderim ile alakalı işlemler toplamının tüm işlemler toplamına oranı %6,81 oranına gerilemiştir.

Korelasyon tabanlı mahremiyet analizi çalışması Dash anonim kriptoparası için ise sadece ÖzelGönderim'e Giden işlemler ve ÖzelGönderim'den Gelen işlemler için yapılacaktır. Bu iki işlem tipinin toplam sayısıysa tüm işlemler sayısının %1.13'üne tekabül eden 29,894 tane işlemdir. Yani korelasyon tabanlı mahremiyet analizi tüm işlemlerin sadece %1,13'ü için yapılacaktır. %5,68 oranında olan ÖzelGönderim işlemleri için korelasyon tabanlı mahremiyet analizi yapılamamaktadır. Kalan %93,19 oranındaki Normal işlemler ve Blok Ödülü işlemlerini analiz etmeye gerek bulunmamaktadır.

Tablo 5. Son 25,000 Blok İçin Tiplere Göre Dash İşlemleri Sayıları ve Yüzdeleri

Dash Blokzinciri İşlem Tipi	**Toplam İşlem Sayısı**	**Toplam İşlem Sayısı Yüzdesi**
ÖzelGönderim'e Giden	23,558	0.890872471
ÖzelGönderim'den Gelen	6,336	0.239603021
ÖzelGönderim	150,101	5.676239443
Normal	2,436,524	92.13991667
Blok Ödülü	27,855	1.053368396
TOPLAM	2,644,374	100.00

4.1. Madencilerin Analizi

Zcash'den farklı olarak Dash kriptoparasında blok ödülleri madencilerle beraber aynı zamanda AnaUçlara da gönderilir. Ancak hangi adresin AnaUça, hangi adresin madenciye ait olup olmadığını bilmek doğrudan mümkün değildir. Bu nedenle madenci havuzlarının mahremiyet analizine madenci havuzlarına ait adreslerle beraber mecburen AnaUçlara ait olan adresler de eklenmişitr. Madenci havuzlarını ve yaptıkları anonim işlemlerini tespit etmek için Zcash'te olduğu gibi yine bünyesinde bulundurdukları madencilere yaptıkları ödemeler gruplandırılarak analiz işlemi yapılmıştır. Madenci havuzu, Dashleri "normal işlemleri" kullanarak ödeme yapıyorsa TMadenci, "ÖzelGönderim'den çıkan işlemleri" kullanıyorsa ZMadenci olacaktır.

İlk olarak tüm Ödül İşlemlerine çıktı olan tüm adresler AnaUç olup olmadığını bakılmaksızın madenci olarak varsayılmıştır. Daha sonra bu adreslerden yine aynı 25,000 bloğu içerisinde ÖzelGönderim'e Giden İşlemler listesinde girdi adresi olarak tespit edilen adresler listelenir. Ödülü alan olası madenci havuzlarının tespitinden sonra sıra ödülü madencilere dağıtan TMadencilerle ZMadencileri tespit etmeye gelir. Bu işlem Zcash için uygulanan algoritmaya benzer bir algoritmayla gerçekleştirilir. İlk olarak yapılan TMadencilerin bulunması analizi sonrası elde edilen sonuçlar aşağıdaki tablodaki gibidir:

Tablo 6. Dash İçin Muhtemel TMadenciler

Havuz Adresleri	Dash Değeri	İşlem Sayısı	TMadenci Adresleri	Dash Değeri	İşlem Sayısı
$HavuzGrubu_1$	852,530,786	6	$MuhtemelTMadenci_1$	852,476,979	1
$HavuzGrubu_2$	10,899,071	6	$MuhtemelTMadenci_2$	10,840,118	1

Yukarıdaki gösterilen Tablo 6'da TMadenci olarak tespit edilen kayıtlar gösterilmektedir. ZMadenci olaraksa hiçbir kayıt bulunamamamıştır. Ödül adresini ÖzelGönderim'e gönderen toplamda 12 işlem ve ÖzelGönderim'den ödülleri alarak madencilere paylaştıran toplam 2 işlem tespit edilmiştir. Toplamda bulunan 14 işlem son 25,000 bloktaki analiz edilecek olan ÖzelGönderim'e Giden işlemlerle ÖzelGönderim'den Çıkan işlelerim toplamının %0.468321402 kadarına denk düşmektedir. Oldukça düşük bir değer tespit edilmesinden dolayı madenci analizi işlemleri Dash için maalesef gözardı edilecek, mahremiyet analizi sonuçlarına dâhil edilmeyeceklerdir.

4.2. Gidiş-Geliş İşlemleri

Gidiş-Geliş işlemleri Dash kriptoparası için "t" zamanında gerçekleşmiş bir ÖzelGönderim'e Giden İşlemle (bundan sonra "ÖGG işlemi" denilecektir) "$t+t_1$" zamanında (yani daha sonraki herhangi bir zamanda) gerçekleşmiş bir ÖzelGönderim'den Çıkan İşlemin (aynı şekilde bundan sonra "ÖGÇ işlemi" denilecektir) karşılaştırılmasıdır. Yani aslında Zcash'te yapılmış olan gidiş-geliş işlemleri analizine benzer bir yöntem uygulanır. Zcash'de yapılan girdi ve çıktı değerleri karşılaştırmasına Dash için de ÖGG işleminin çıktı toplamı ve ÖGÇ işleminin girdi toplamı değerleri karşılaştırılır.

4.2.1. Temel Karşılaştırma

Gidiş-geliş işlemleri karşılaştırmasında ilk olarak temel karşılaştırma yapılır. Yine Zcash analiznde olduğu gibi"t" zamanında ÖzelGönderim'e giden "ÖGG" işlemiyle "$t+t_1$" zamanında ÖzelGönderim'den çıkan başka bir "ÖGÇ" işlemi karşılaştırılır. ÖGG işleminin 10'un katsayılarına ayrılmış çıktı adresleri değerleri toplamıyla ÖGÇ işleminin 10'un katsayılarına ayrılmış girdi adresleri değerleri toplamı karşılaştırılır ve birebir eşleşen kayıtlar listelenir.

Karşılaştırma işlemi sonrasında toplamda 8795 farklı işlemin listeye girdiği gözlemlenmiştir. Liste incelendiği zaman bazı Dash miktarı adres sayısı ikililerin onlarca defa listeye girdiği görülmektedir. Örnek vermek gerekirse 24002972. numaralı indekse sahip işlem toplamda 64 farklı başka işlemle ilişkilendirilmiştir. Bu durumda 100 kez yahut daha az listeye giren 4427 işlem, 25 kez yahut daha az listeye giren 1400 işlem ve 7 kez yahut daha az listeye giren 510 işlem tespit edilmiştir. Birebir eşleşen girdi adres toplamı ve çıktı adres toplamı olan işlemlerin sayısı ise 76'dır.

4.2.2. Alt-küme toplamlarının karşılaştırılması

Diğer bir gidiş-geliş işlemleri karşılaştırması olan "Alt-küme Toplamlarının Karşılaştırılması" Dash anonim kriptoparası Zcash'te yapılana benzer bir mantık uygulanarak gerçekleştirilir. İlk olarak "t" zamanında gerçekleştirilmiş bir ÖGG işleminin 10'un katsayısı olan çıktı adresleri değerleri toplamıyla "$t+t_1$" ve "$t+t_2$ ($t+t_1$ ile $t+t_2$ zamanları aynı yahut farklı zamanlar olabilir) zamanlarında gerçekleştirilmiş 2 farklı ÖGÇ işlemlerinin 10'un katsayısı olan girdi adreslerinin değerlerinin toplamı karşılaştırılır. Karşılaştırma sonucunda birebir eş olan işlemler kümesi listeye eklenir.

Karşılaştırma sonucunda toplamda 10417 farklı işlemin listeye girdiği gözlemlenmiştir. İlk gidiş-geliş işlemleri karşılaştırılması listesinde olduğu gibi bu listede de aynı Dash miktarına sahip bazı işlemlerin onlarca defa listeye girdikleri gözlemlenmiştir. Bu sefer $ÖGÇ_1$ girdi değeri, $ÖGÇ_2$ girdi değeri ve bu iki değerlerin toplamıyla $ÖGÇ_1$ işlem indeksi ve $ÖGÇ_2$ işlem indeksleri temel alınarak tüm liste gruplandırılır.

Gruplandırma sonucunda hala aynı işlemlerin onlarca hatta daha fazla kez karşılaştırma sonucu listesine girdiği görülmüştür. Listedeki toplam görünme sayıları (count) gruplandığı zaman 100 kez yahut daha az listeye giren 10392 işlem, 25 kez yahut daha az listeye giren 10183 işlem ve 7 kez yahut daha az listeye giren 9954 işlem tespit edilmiştir. Birebir eşleşen girdi adres toplamı ve çıktı adres toplamı olan işlemlerin sayısı ise 7832'dir. Her iki listenden çıkan sonuçlar Tablo 7'de aşağıdaki gibi verilmiştir:

Tablo 7. Dash Gidiş-Geliş İşlemleri Karşılaştırma Sonuçları Tablosu

Karşılaştırmada Adres Görülme Sayısı	Temel Karşılaştırma	Temel Karşılaştırma Yüzdesi	Alt Küme Toplamları Karşılaştırması	Alt Küme Toplamları Karşılaştırması Yüzdesi	Karşılaştırma Toplamı	Karşılaştırma Toplamı Yüzdesi
Sadece 1 Defa	76	%0.254	7,832	%26.199	7,833	%26.202
7 ve Daha Az	510	%1.706	9,954	%33.298	9,971	%33.354
25 ve Daha Az	1,400	%4.683	10,183	%34.064	10,387	%34.746
100 ve Daha Az	4,427	%14.808	10,392	%34.763	11,698	%39.131
Hepsi	8,795	%29.421	10,417	%34.846	14,739	%49.304

Tablo 7'de ilk olarak her iki listede sadece bir kez karşılaştırmada görünen işlemlerin sayısı gösterilmiştir. Daha sonra sırayla 7 kez ve daha az görünen, 25 kez ve daha az görünen, 100 kez ve daha az görünen işlemlerin sayısı gösterilmiş; en sonda da listede bulunan tespit edilmiş tüm işlemlerin sayısı verilmiştir. Her bir sayının yanındaki "Yüzde" olarak belirtilen alan ÖGG ve ÖGÇ işlemlerin toplamı olan 29894 sayısına göre ilgili karşılaştırma sayısının yüzdesini verir.

Korelasyon tabanlı mahremiyet analizinden olan alt-küme toplamları karşılaştırması sonucunda birebir karşılaştırılabilme ihtimali olan %26.202 oranında işlem bulunmuştur. Bu karşılaştırmalardaki önemli olan nokta şudur; gruplandırma sırasında listede görünme sayısı arttıkça iki işlem arasında tutarlı bir ilişkilendirme yapıp işlemin takip edilebilmesi azalmaktadır. Bunun yanında yapılan ilişkilendirmenin geçerliliği (yani gerçekten de iki işlem arasında ilişki olup olmadığının tespit edilmesi) ÖzelGönderim'den çıkan işlemde olan tüm karıştırmalardaki adreslerden geriye giderek anlaşılabilir. Mesela X_1 işlemi ÖGG işlem ve X_2 ÖGÇ işlemi olsun. Listede bu iki işlem arasında ilişki olması ihtimalinin belirtilmesi durumunda X_2 işlemine girdi olan $X_{1.A}$, $X_{1.B}$, $X_{1.C}$ şeklindeki tüm adreslere bakılır. Daha sonra bunların çıktısı olduğu ÖzelGönderim işlemlerinde bulunan tüm işlemlerin $X_{1.A.1}$, $X_{1.A.2}$, $X_{1.A.3}$, $X_{1.b.1}$ $X_{1.b.2}$, $X_{1.b.3}$, $X_{1.c.1}$, $X_{1.c.2}$ ve $X_{1.c.3}$ şeklindeki girdi adreslerine gidilir. Her bir geriye gidilen seferin bir önceki muhtemel ilişki yolu sayısıyla mevcut ÖzelGönderim işleminin girdi adresi sayısı çarpılır. Yukarıdaki durumda ilk ÖzelGönderim işleminde 3 ilişki ihtimali varken ikincisinde 9, üçüncüsünde 27 ve dördüncüsünde 81 ilişki ihtimali olacaktır, bu durum her bir ÖzelGönderim işlemi tam olarak 3 adresle yapıldığı varsayılarak hesaplanmıştır. Yapılan sefer sayısı arttıkça ilişkilendirmeyi doğrulamanın zorluğu da yine ciddi bir şekilde artacaktır. Buna karşılaştırma sonuç listelerindeki işlemin görünme sayılarının artmasını da eklersek özellikle 7 defadan daha fazla listeye giren işlemlerin doğrulanmasını ne derece zorlaştığı daha iyi anlaşılacaktır. Yine de bu durum bütün ÖzelGönderim işlemlerinde girdi-çıktı ikililerinin tamamını teker teker deneyerek ÖGG işlemleriyle ile ÖGÇ işlemleri arasındaki ilişkiyi körlemesine bir yöntem ile bulmaktan daha kolay ve hızlı olacaktır. Bu durum şu şekilde düşünülebilir; Kaba Kuvvet (Brute Force) kullanarak bir şifreleme algoritmasını kırabilmek için m*n*t değer zaman kadar sürdüğü varsayılsın. Bu süreyi n birim zaman kadar azaltarak m*t kadar süreye düşürmek algoritmanın çok daha kolay kırılmasına olanak sağlayacaktır ki, şifreleme algoritmasını kırmak tam olarak bu durumu ifade eder. Yapılan analiz çalışması sayesinde bir Dash işleminin mesela x*y sayıda Dash işlemiyle olabilecek olası ilişki sayısı ihtimali mahremiyet analizi sayesinde x Dash işlemine düşürülmüştür.

Daha sonra, gidiş-geliş işlemleri mahremiyet analizi çalışmasına ek olarak Zcash anonim kriptoparasından farklı olarak Dash anonim kriptoparası için ÖGG işlemlerinin çıktı adresleri sayısıyla ÖGÇ işlemlerin girdi adresleri sayısı karşılaştırmaya eklenmiştir. Çünkü kullanıcılar, ÖzelGönderim'e girdikleri Dash miktarının tamamını olduğu gibi cüzdanlarındaki bir adreste toplayıp harcayabilmek istedikleri takdirde parçalanan tüm Dash'lerin bulunduğu adresleri girdi olarak yeni bir ÖGÇ işlemine dâhil etmeleri gerekir. Bu durumda ÖGG işleminin toplam çıktı sayısı ile ÖGÇ işleminin toplam girdi sayısı aynı olacaktır. Bu nedenle toplam Dash değerlerinin eşit olmasının yanında toplam girdi-çıktı adres sayılarının eşit olması koşulu da analiz karşılaştırılmasına eklenmiştir. Adres sayılarının eş olması koşulunun karşılaştırma analizine eklenmesiyle çıkan sonuçlar Tablo 8'de aşağıdaki gibi verilmiştir.

Tablo 8. Adres Sayıları Dâhil Dash Gidiş-Geliş İşlemleri Karşılaştırma Sonuçları Tablosu

Karşılaştırmada Adres Görülme Sayısı	Temel Karşılaştırma	Temel Karşılaştırma Yüzdesi	Alt Küme Toplamları Karşılaştırması	Alt Küme Toplamları Karşılaştırması Yüzdesi	Karşılaştırma Toplamı	Karşılaştırma Toplamı Yüzdesi
Sadece 1 Defa	41	%0.137	3,187	%10.661	3,201	%10.708
7 ve Daha Az	289	%0.967	6,160	%20.606	6,188	%20.700
25 ve Daha Az	843	%2.820	6,992	%23.389	7,216	%24.139
100 ve Daha Az	2,743	%9.176	7,280	%24.353	8,417	%28.156
Hepsi	4,861	%16.261	7,607	%25.447	10,688	%35.753

Yapılan yeni gidiş-geliş işlemleri mahremiyet analizleri neticesinde hem temel karşılaştırma için hemn de alt-küme toplamları karşılaştırması için elde edilen toplam işlem sayısı yüzdesinin önemli ölçüde azaldığı gözlemlenmektedir. Örnek olarak sadece 1 defa eşleşen toplam işlem sayısı 7,883'en 3,201'e düşmüştür. Yine toplamda 14,739 işlem değil 10,688 işlem tespit edilmiştir. Her ne kadar toplam bulunan sonuç açısından bir azalma olduğu düşünülse de bu muhtemel ilişkilerin gerçekten var olup olmadığı tespit etmek isteyen için bu durum kolaylık sağlayacaktır.

4.2.3. Parmak izi değerleri karşılaştırması

ÖzelGönderim'e girebilecek en küçük değer 0.001 Dash olduğundan ve bu değer de varsayılan işlem ücretinden büyük olduğundan parmak izi gidiş-geliş işlemleri analizi Dash için yapılmayacaktır.

4.3. Dash Analizi Sonuçları

Gidiş-geliş işlemleri mahremiyet analiz çalışmasında ilk aşamada sadece işlemlerin toplam girdi ve çıktı değerleri karşılaştırması yapılmış ve bu karşılaştırma sonucunda tüm ÖzelGönderim'e giden ve ÖzelGönderim'den gelen işlemlerin %49,304'ü için ilişkilendirilme yapılmıştır. İlgili mahremiyet analizine işlemlerde bulunan girdi ve çıktı adreslerinin toplam sayılarının eşit olması koşulu da eklendiğinde bu oranın %35,753'e düştüğü gözlemlenmiştir. Yapılan ilişkilendirmeler "ÖGG Xt_1 ve ÖGÇ Xt_2 işlemlerinin adres sayıları ve işlem değerleri birbirine eşittir; bu nedenle aralarında bir ilişki olması muhtemeldir." varsayımı temel alınarak yapılmıştır. Ne var ki, ilişkinin doğrulaması tez konusu kapsamında olmadığı için detaylıca açıklanmamış ve ilişkiyi doğrulayan herhangi bir çalışma yapılmamıştır. Dash kriptoparası tamamıyla umumi yani herkese açık bir kriptopara olduğundan, ilişkilendirmenin doğru olmasını kontrol etmek amacıyla ÖGÇ Xt_2 işleminden tüm ÖzelGönderim adresleri kullanılarak geriye doğru gitmek yeterli olacaktır.

Dash anonim kriptoparası için madenci havuzları kullanılarak bir analiz yapılmamıştır. Bu nedenle mahremiyet analizi sonuçları sadece gidiş-geliş işlemlrinde bulunan sonuçlardır.

V. MONERO ANALİZİ (ANALYSIS OF MONERO)

2.5 Monero alt-kısmında kısaca anlatıldığı gibi Monero oldukça popüler bir anonim kriptoparadır ve Bitcoin'den sonra en önemli ilk 10 kriptoparadan birisi olduğu bazı kaynaklar tarafından belirtilir[3]. Ne var ki, korelasyon tabanlı mahremiyet analizi çalışması kapsamında bir analiz çalışması yapılamamıştır. Bunun temel nedeni şudur; yapılan tez çalışması farklı zamanlarda, yani farklı bloklarda gerçekleştirilmiş olan işlemlerin toplam işlem değerlerinin birbirleriyle karşılaştırılarak arada bir ilişki bulunması üzerine odaklanır. Mesela Zcash için t_1 zamanında yapılmış bir t-z işleminin toplam girdi değeriyle $t_1 + t_i$ zamanında (yani daha sonra) yapılmış bir z-t işleminin çıktı değerleri toplamı karşılaştırılır. İki değerin birbirine eş olması durumunda arada bir ilişki vardır denilebilir. Monero'daki ödül işlemleri hariç tüm işlemlerin girdi ve çıktı değerlerinin herkese açık olan kayıt defterlerinde özetlenerek yahut tamamıyla gizlendiği için bu değerleri herhangi bir şekilde gruplandırarak veya gruplandırmadan doğrudan karşılaştırmak mümkün olmamaktadır. Sonuç olarak Monero anonim kriptoparası için korelasyon tabanlı mahremiyet analizi yapılamamıştır.

VI. TARTIŞMA VE ÖNERİLER (DISCUSSION AND SUGGESTION)

6.1. Tartışma

Bitcoin kriptoparası her ne kadar ilk çıktığında anonim olduğu düşünülse de açık anahtarlı adres kullandığı için hiçbir şekilde anonim olmadığı zaman içerisinde anlaşılmıştır. Çünkü bu açık anahtarlı adres kullanılarak Bitcoin defterinde tüm işlem geçmişini rahatlıkla görüntülenebilmekter. Bu nedenle Bitcoin için daha fazla anonimlik sağlaması adına çeşitli yöntemler

[3] https://www.investopedia.com web sayfasında bu iddia detaylı olarak belirtilmiştir.

önerilmiştir. Bu yöntemlerin de arzu edilen anonimliği sağlamadığı anlaşılınca korelasyon tabanlı mahremiyet analizi çalışmasının temel konusu olan anonim kriptoparalar yayınlanmıştır.

Bahsedilen bu anonim kriptoparalar teoride çeşitli kriptografik yöntemler yahut Zerocash gibi protokollerle çeşitli şekillerde güçlü bir anonimleştirme sağlarlar. Ne var ki, kriptosistemde bulunan ve blokzincir teknolojisi bünyesindeki elemanları haricindeki cüzdanlar yahut eşler arası ağ gibi elemanları analiz edildiğinde [24] ve [26] makalelerinde belirtilen örneklerinde olduğu gibi anonimliği bozma yapılabilmektedir. Bunun yanında anonim kriptoparalarla işlem yapan çeşitli kullanıcı adresleri analiz edildiğinde de yine anonimliği bozma yapılabildiği gözlemlenmiştir. Bu anoninmliği bozma yöntemine "korelasyon tabanlı mahremiyet analizi" adı verilir.

Zcash ve Dash gibi anonim kriptoparaların anonimsizleştirilebilmesinin temel sebeplerini aşağıdaki gibi listelemek mümkündür:

- Bilgi güvenliğinde en zayıf halkanın "insan" olduğu her zaman vurgulanmıştır. Kriptoparalarda da bu durum maalesef farklı değildir. Zcash ve Dash analizi sırasında normal kullanıcıların anonim işlemleri yaparken yeterince bilinçli davranmadıkları gözlemlenmiştir. Örnek vermek gerekirse kullanıcının t_1 zamanında yapmış olduğu X_1 işlemini işlem gizliliğini sağlamak adına anonimliğin sağlandığı EkleBöl yahut ÖzelGönderim yöntemi kullandıktan sadece saatler sonra, $t_1 + t_i$ zamanında X_2 işlemini yaparak aynı değerle ilgili anonimliği sağlayan yöntemden çıkıp kendisine ödeme yapması bu iki işlem arasında bir ilişki kurulmasına neden olmaktadır.
- Kriptoparalarda farklı kullanıcı grupları bulunmaktadır. Bu kullanıcı gruplarından madenciler kriptoparalar için en önemli görevlerden birisi olan blokzincire yeni blokların eklenmesi görevini belli bir blok ödülü karşılığında icra ederler. Bundan dolayı madenci havuzları ve madenciler için hususi olarak yapılan anonimsezliştirme yöntemleri geliştirilmiştir. Gerçekten de madenci havuzlar Zcash kriptoparasında olduğu gibi sürekli olarak benzer şekilde madencilere ödeme yaparlar. Korumalı havuzları kullandıkları halde bu madenci havuzlarını analiz etmek mümkün olmaktadır. Sonuç olarak madenci havuzlarının yaptığı işlemler daha kolay analiz edilerek anonimsizleştirilebilir olur.
- Zcash kriptoparası için işlemlerin kolay takip edilebilir olmasının en temel sebeplerinden birisi z-z korumalı işlemlerin sayısının olması gereken seviyelerde olmamasıdır. Sadece korumalı işlemin yapılması da takip edilememezliğin, dolayısıyla anonimliğin ve mahremiyetin sağlanması için yeterli olmaz. Korumalı havuza girdirilen değerlerin korumalı havuzun dışarısına çıkartıldığında hiçbir şekilde birleştirilemeyecek şekilde parçalanarak çıkartılması alternatif olarak önerilir.
- Dash kriptoparası düşünüldüğü zaman ÖzelGönderim işlemleri 10'un katsayılarına bölündüğünde kullanıcılar aynı şekilde bu bölünmüş değerleri tek bir adres üzerinde muhtemelen "harcaması daha kolay olacağı" gibi sebeplerden dolayı toplamaktadırlar. Bu da yine işlem anonimliğinin ve mahremiyetinin ihlal edilmesine neden olmaktadır.

6.2. Öneriler

Anonim kriptoparaların en önemli özelliği isimlerinden de anlaşılacağı gibi kullancılar için anonimlik ve mahremiyet sağlamalarıdır. Korelasyon tabanlı mahremiyet analizi sonucundan anlaşılacağı gibi bu anonim kriptoparaları teoride anonimliği sağladıklarını belirtirlerken pratikte istenildiği ölçüde anonimliği yakalayamamaktadırlar. Kriptoparalarda mahremiyet ve anonimliğini artırabilmek adına sadece Zcash ve Dash değil tüm anonim kriptoparalara geliştiricileri ve kullanıcılarına öneriler aşağıda verilmiştir:

- Anonim kriptopara geliştiricileri kullanıcıları "anonim özelliklerinin nasıl kullanılması" gerektiğiyle alakalı bilgilendirme yapmaları önerilir. Örneğin en iyi pratikler (best practices) şeklinde bir web sayfası oluşturulup kullanıcılar için en doğru bir şekilde nasıl EkleBöl işlemi yahut ÖzelGönderim işlemi yapabilecekleri basitçe bilgilendirilebilir.
- Kullanıcılar beklendiği gibi kendileri için en kolay ve en ucuz olan yöntemi seçeceklerdir. Hem anonim hem de normal işlem seçeneği sunan kriptoparalar, anonim işlem yapmaları için kullanıcıları zorlayamacaklarından kullanıcıları teşvik amaçlı çeşitli alternatif yöntemlere gidebilirler.
- Zcash kriptoparası için, kullanıcılar korumalı bir işlem yaptıkları zaman korumalı işleme girerken kullandıkları işlem miktarını korumalı işlemden çıkarken kullanmamaları önerilir. Bunun yerine kullanıcılar sadece ihtiyacı olan miktarı korumalı havuzdan çıkarmaları daha doğru olacaktır.
- Yine Zcash kullanıcılarının EB-işlemlerinin tamamıyla anonimlik sağlamadığını bilmeleri gerekir. Korumalı havuza ZEC aktardıkları zaman bu korumalı havuzda ZEC'i farklı z-adreslere parçalamaları ve farklı z-adresleri üzerinden işlem yapmaları daha fazla anonimlik ve takip edilememezlik sağlayacaktır.
- Zcash kullanıcıları son olarak işlem yaparken Zatoshi cinsinden 10.000'in (varsayılan işlem bedeli) katsayısı olacak yuvarlak değerler üzerinden işlem yapmaktan kaçınmalıdırlar. Böylece kötü niyetli kişiler göz ardı edilen ve

analiz çalışmasında parmak izi değeri de denilen değerleri kullanarak işlem geçmişini takip edemeyeceklerdir.

- Zcash madenci havuzları bünyesinde bulundurdukları madencilere ödemeli hep aynı adres üzerinden yapmaktan kaçınmalıdırlar. Yapılan analizde bazı madenci havuzlarının en azından 6-7 farklı adres kullandıkları tespit edilmiştir ki bu da iyiye işarettir. Ayrıca madenci havuzlarının TMadenci yahut ZMadenci kategorilerine girmekten kaçınmaları için madencilerine ödemeleri doğrudan z-z korumalı işlemler üzerinden yapmaları tavsiye edilir. Misal vermek gerekirse SlushPool, Bitfly ve Luxor Mining isimli madenci havuzları doğrudan z-adrese sahip madencilere ödeme yapmaya imkân sunduklarını belirtilir[4].
- Dash kullanıcıları, Zcash kullanıcıları örneğinde olduğu gibi ÖzelGönderim işlemleri yaptıkları miktarın birebir aynısını, karıştırma seferleri sonunda farklı bir ikinci adrese olduğu gibi toplamamaları önerilir. Çünkü bu şekilde yapıldığında karıştırma sırasında 10'un katsayısına bölünen bir değer tekrardan bölünmediğinden karıştırma sonrası işlem miktarı aynı olduğu gibi toplam girdi adresi sayısı da birebir aynı olur. Dolayısıyla Dash kullanıcılarının ÖzelGönderim öncesi işlemleriyle ÖzelGönderim sonrası işlemleri birbirinin aynısı veya benzeri olmaması gerekir.
- Yine Dash kullanıcılarının ÖzelGönderim sonrası işlemlerinde başka bir adrese ödeme yapacakları zaman ÖzelGönderim'e girdikleri tüm adresleri kullanmak yerine ihtiyacı olan miktarı kullanmaları tavsiye edilir. Bunun yanında, ÖzelGönderim'de kullanılan miktarın tamamına ihtiyaç olması durumunda anonimliği artırmak adına ÖzelGönderim sonrası işlemler farklı şekillerde parçalandıktan sonra o parçaların ödeme yapılacak adrese farklı işlemlerde ödenmesi daha sağlıklı olacaktır.
- Monero ve Verge için doğrudan analiz çalışması yapılmadığı için bu kriptoparalarda doğrudan bir tedbir açıklaması yapılmayacaktır. Ancak anonim yahut anonim değil tüm kriptopara kullanıcılarının şahsi adreslerini gerekmeyen hiçbir yerde açıklamamaları tavsiye edilir. Ayrıca kriptopara geliştiricilerinin bu durumu ihlal eden (veya kendilerinden dijital para satın alan kullanıcıların adreslerini uygulama açıklığı nedeniyle sızdıran) Online marketler yahut forumları izlemeleri; gerekirse bu yerlere geçici veya kalıcı engelleme koymaları önerilir.
- Son olarak Zcash ve Dash geliştiricilerinin, kullanıcı gruplarının genel olarak yapmış olduğu hataları gruplandırmaları önerilir. Böylece her yapılan yanlışı engellemek imkânsız olsa da kullanıcıların en çok yaptığı yanlışlar için düzeltmeler, güncellemeler yahut alternatif yöntemler geliştirmek mümkün olacaktır.

VII. SONUÇ (RESULT)

2008 yılının Ekim ayında Satoshi Nakamoto, yayınlamış olduğu [1] makalesinde anlattığı blokzincir teknolojisiyle beraber Ocak 2009'da tüm İnternet kullanıcılarının hizmetine sunduğu Bitcoin kriptoparası bilişim teknolojilerinde yeni bir çağı beraberinde getirmiştir. Dağıtık yapısı ve güven odaklı olmayan mekanizması sayesinde blokzincir farklı birçok kişi, grup ve kuruluş tarafından ilgi odağı olmuştur. Geçen 11 yılda blokzincir teknolojisinin önemini artarak korumuştur.

Bitcoin, ilk çıktığı yıllarda her ne kadar tümüyle anonim olduğu düşünülse de yapılan çalışmalarla hiçbir şekilde anonim olmadığı anlaşılmıştır, [4], [5], [6], [7], [8]. Bu durumda çeşitli geliştiriciler farklı zamanlarda Bitcoin'e alternatif "anonim kriptoparalar" da denilen ve anonimliğe odaklanan kriptoparalar geliştirmişlerdir. Bu kriptoparalar teoride gerçekten de ciddi anlamda anonimlik ve mahremiyet sağlar. Zcash ve Monero kriptografik yöntemler kullanarak istenilen anonimliği sağlarken Dash ve PIVX AnaUçlar ve CoinJoin tabanlı karıştırma mekanizmaları kullanarak yapar. PIVX ayrıca Zcash'in kullanmış olduğu Zerocash protokolünü de kullanır. Verge ise ToR altyapısını kullanarak IP adreslerini gizlemeye odaklanır. Ancak Zcash ve Dash anonim kriptoparalarının yapılan korelasyon tabanlı mahremiyet analizi sonucunda pratikte, yani günlük kullanımlarda düşünüldüğü kadar anonimlik sağlamadığını yapılan analizler neticesinde anlaşılmıştır.

Zcash ve Dash için bu tez içerisinde işlem miktarı (ve Dash için ayrıca toplam adres sayısı) bakımından mahremiyet analizi çalışması yapılmıştır. Analiz çalışması sonucunda Zcash için%84,4 oranında ve Dash için %49,3 oranında (toplam adres sayısı parametresi mahremiyet analizine eklendiğinde bu oran %35,75'e düşmüştür) anonim işleminin birbirleriyle ilişkisi olma ihtimalinin bulunduğu sonucuna varılmıştır. İlgili kriptoparaların anonimlik seviyesinin artırılması için hem kullanıcılarına hem de geliştiricilerine çeşitli görevler düşmektedir. Mahremiyet analizi sonrasında tüm kullanıcı grupları ve anonim kriptopara geliştiricileri için çeşitli önerilerden bahsedilmiştir.

Sonuç olarak şu söylenebilir, anonim kriptoparalar her geçen gün gelişen ve değişen bilişim teknolojilerinin önemli bir parçası olmuşlardır. Özellikle hiçbir şekilde güven odaklı olmayan kriptoparalar gibi bilgi güvenliğinin ve mahremiyetin olduğu "para" odaklı sistemlerde gizlilik ve mahremiyetin ihlalinin ciddi

[4] zcashcommunity.com

seviyelerde yaşanması beklenen bir durumdur. Burada önemli olan nokta kriptopara geliştiricilerinin güvenlik ihlallerinin anlaşılmasının ardından hızlı bir şekilde müdahele edip yapılan yanlışlardan ve ihlallerden ders çıkartabilmesidir. Anonim kritpoparalarda korelasyon tabanlı mahremiyet analizi çalışması sonucunda Zcash ve Dash anonim kriptoparaları için anonimliğin analiz edilebileceği ve işlem geçmişinin tespit edilebileceği gösterilmiş; bunun yanında analiz yapılmasını engellemek yahut çıkan sonuçları daha kabul edilebilir hale getirebilmek için çeşitli önerilerden bahsedilmiştir.

KAYNAKLAR (REFERENCES)

[1] Satoshi, N., Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/, 1–9, 2008

[2] Birkuyov A., Daniel, F., Deanonymization of Hidden Transactions in Zcash, University of Luxembourg, 1-15, 2018

[3] TÜBİTAK BİLGEM UEKAE, Blokzincir, Blokzincir Araştırma Laboratuvarı, https://blokzincir.bilgem.tubitak.gov.tr/blok-zincir.html, Erişim: 2020-03-27

[4] Birkuyov A., Dmitry K., Ivan P., Deanonymisation of Clients in Bitcoin P2P Network, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14), 15-29, 2014

[5] Sarah M., Marjori P., Grant J., Kirill L., Damon M., Geoffrey M. V., Stefann, S., A fistful of bitcoins: Characterizing payments among men with no names, Proceedings of the 2013 conference on Internet measurement conference ACM, University of California and San Diego George Mason University New York USA, 127-140, 2013

[6] Dorit, R., Adi S., Quantitative Analysis of the Full Bitcoin Transaction Graph, International Conference on Financial Cryptography and Data Security, The Weizmann Institute of Science Department of Computer Science and Applied Mathematics Israel, 6-24, 2013

[7] Androulaki1 E., Karame G. O., Roeschlin1 M., Scherer1 T., Capkun1 S., Evaluating User Privacy in Bitcoin, International Conference on Financial Cryptography and Data Security, ETH Zurich 8092 Zuerich Switzerland ve NEC Laboratories Europe 69115 Heidelberg Germany, 34-51, 2013

[8] Reid F., Harrigan M., An Analysis of Anonymity in the Bitcoin System 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, IEEE, Clique Research Cluster Complex & Adaptive Systems Laboratory UniversityCollege Dublin Ireland, 1318-1326, 2011

[9] Spagnuolo M., Maggi F., Zanero S., BitIodine: Extracting Intelligence from the Bitcoin Network, International Conference on Financial Cryptography and Data Security, Springer Berlin Heidelberg, 457-468. 2014

[10] KoshyEmail P., Koshy D., McDaniel P., An Analysis of Anonymity in Bitcoin Using P2P Network Traffic, International Conference on Financial Cryptography and DataSecurity FC 2014: Financial Cryptography and Data Security, Springer Berlin Heidelberg, 469-485, 2014.

[11] Birkuyov A., Ivan, P.: Bitcoin over tor isn't a good idea, IEEE, Symposiumon Security and Privacy SP 2015. 122-134. IEEE, University of Luxembourg, Esch-sur-Alzette, Luxemburg, 2015

[12] Harry K., Steven G., Alishah C., Malte M., Arvind N., Blocksci: Design andapplications of a blockchain analysis platform, 29th {USENIX} Security Symposium ({USENIX} Security 20), Princeton University, 2721 – 2738, 2020

[13] Atlas, K., An analysis of darkcoin's blockchain privacy via darksend, 1–25, 2014

[14] Abraham H., Bernhard H., An empirical analysis of monero cross-chain traceability, International Conference on Financial Cryptography and Data Security FC 2019: Financial Cryptography and Data Security, Austrian Institute of Technologyand Vienna University of Technology, 150 – 157, 2019

[15] Möser M., Soska K., Heilman E., Lee K., Heffan H., Srivastava S., Hogan K., Hennessey J., Miller A., Narayanan A., Christin N., An empirical analysis of traceability in the monero blockchain, Proceedings on Privacy EnhancingTechnologies, Vol 2018, Iss 3, 143-163, 2018

[16] Amrit K., Clement F., TolePrateek S., A traceability analysis of monero's blockchain, 22nd European Symposiumon Research in Computer Security Proceedings 2017, National University of Singapore, 153-173, 2017

[17] Borggren N., Yoon Kim H., Yao L., Koplik G., Simulated blockchains for machinelearning traceability and transaction values in the monero network, Geometric Data Analytics Inc. Durham NC, 1–10, 2020

[18] Kappos G., Yousaf H., Maller M., Meiklejohn S., An empirical analysis ofanonymity in zcash, 27th USENIX Security Symposium (USENIX Security'18), Cornell University - University College London, 1 – 15, 2018

[19] Quesnelle J., On the linkability of zcash transactions, 27th USENIX SecuritySymposium (USENIX Security '18), Cornell University Esch-sur-Alzette Luxemburg, 1 – 5, 2017

[20] Erik D., Elias R., Florian T., Map-z: Exposing the zcash network in times of transition, IEEE, 44th Conference on Local Computer Networks (LCN), Cornell University Distributed Security Infrastructures Technical University of Berlin, 84 – 92, 2019

[21] Kappos G., Piotrowska A. M., Extending the anonymity of zcash, Cornell University - University College London United Kingdom, 1 – 2, 2019

[22] Alex B., Daniel F. Privacy and linkability of mining in zcash, IEEE, Conference on Communications and Network Security (CNS), University of Luxembourg Esch-sur-Alzette Luxemburg, 118 – 123, 2019
[23] Alex B., Daniel F., Giuseppe V., Privacy aspects and subliminal channelsin zcash, CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, University of Luxembourg Esch-sur-Alzette Luxemburg, 1813–1830 2019
[24] Alex B., Sergei T., Deanonymization and linkability of cryptocurrency transactionsbased on network analysis, IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, , 172 – 184, 2019
[25] Alex B., Sergei T., Transaction clustering using network traffic analysis for bitcoinand derived blockchains, INFOCOM 2019 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2019, University of Luxembourg Esch-sur-Alzette Luxemburg, 204 – 209, 2019,
[26] Alex B., Sergei T., Security and privacy of mobile wallet users in bitcoin, dash,monero, and zcash. Elsevier University of Luxembourg Esch-sur-Alzette Luxemburg, 1 – 11, 2019
[27] Bitcoin, Bitcoin'e başlarken, bitcoin.org, https://bitcoin.org/tr/, Erişim: 2020-03-27
[28] Jong-Hyouk L., Rise of anonymous cryptocurrencies: Brief introduction, IEEEConsumer Electronics Magazine IEEE Consumer Electron. Mag. Consumer Elec-tronics Magazine, IEEE, SangmyungUniv. - Cheonan South Korea, 20 – 25, 2019
[29] Daira H., Sean B., Taylor H., Nathan W., Zcash protocol specification, Zcash Protocol Specification, Zcash, 1–151, 2020
[30] Zcash documentation, Zcash Basics, Zcash, https://zcash.readthedocs.io/en/latest/rtd_pages/basics.html, Erişim: 2020-03-28
[31] Dash, Dash documentation, dash.org, https://docs.dash.org/en/stable/, Erişim: 2020-07-01,
[32] Dash, What is dash cryptocurrency? The most comprehensive guide ever!, dash.org, https://blockgeeks.com/guides/what-is-dash/, Erişim: 2020-05-05
[33] Dash, Dash cryptocurrency: Complete dash coin guide, dash.org, https://www.bitdegree.org/tutorials/dash-cryptocurrency/, Erişim: 2020-05-05
[34] Dash, Dash features, dash.org, https://docs.dash.org/en/stable/introduction/features.html, Erişim: 2020-07-01
[35] Wikipedia, Monero. wikipedia.org, https://en.wikipedia.org/wiki/Monero, Erişim: 2020-07-04
[36] Monero, Monero technical specs, Monero Documentation, https://monerodocs.org/technical-specs/, Erişim: 2020-07-04,
[37] Monero, Ring signature, web.getmonero.org, https://web.getmonero.org/resources/moneropedia/ringsignatures.html, Erişim: 2020-07-04

EK-A: Algoritma 1 - TMadencilerin Bulunması
(APPENDIX-A: Algorithm 1 - FindingTMiners)

```
TMadencileriBul(blokZincir)
{
    blokListesi[] = blokZincir[-25000]
    //blokzincirdeki son 25,000 blok çekilir
    işlemListesi[] = blockListesi.işlemler
    muhtemelTMadenciListesi[] = Ø
    korumaliHavuzdanCoinAlanListesi[] = Ø
    korumaliHavuzdanCoinAlanGruplanmisListesi = Ø
    for (işlem in işlemListesi)
    {
     if (işlem.ciktiSayisi > 30 and işlem.KorumalıİşlemMi == false)
    {
            muhtemelTMadenciListesi = işlem.girdiAdresi
    }
        else if (işlem.KorumaliİşlemMi == true)
        {
            korumaliHavuzdanCoinAlanListesi = işlem.ciktiAdresi
        }
    }
    muhtemelTMadenciListesi = muhtemelTMadenciListesi $in$
    muhtemelTMadenciListesi.adres = korumaliHavuzdanCoinAlanListesi.adres
    korumaliHavuzdanCoinAlanListesi = korumaliHavuzdanCoinAlanListesi $in$
    korumaliHavuzdanCoinAlanListesi.adres = muhtemelTMadenciListesi.adres
    odemeYapilanMadenciListesi = blokListesi.islem.ciktiAdresi $in$
    blokListesi.islem = muhtemelTMadenciListesi.islem
    for (muhtemelTMadenci in muhtemelTMadenciListesi)
    {
        TMadencileriGrupla(muhtemelTMadenciListesi, muhtemelTMadenci,
        odemeYapilanMadenciListesi,
        korumaliHavuzdanCoinAlanGruplanmisListesi)
            }
    return korumaliHavuzdanCoinAlanGruplanmisListesi
    }

    TMadencileriGrupla (muhtemelTMadenciListesi,
    muhtemelTMadenci,
    odemeYapilanMadenciListesi,
    korumaliHavuzdanCoinAlanGruplanmisListesi)
```

```
{
    mevcutHavuzunMadenciAdresleri =
    odemeYapilanMadenciListesi in
    odemeYapilanMadenciListesi.islem =
    muhtemelTMadenci.islem
    for (girdi in muhtemelTMadenciListesi)
    {
        girdiIslemMiners =
    odemeYapilanMadenciListesi in
    odemeYapilanMadenciListesi.islem =
    girdi.islem
        if(exists(girdiIslemMiners in
    mevcutHavuzunMadenciAdresleri))
        {
            korumaliHavuzdanCoinAlanGruplan
        misListesi =
        korumaliHavuzdanCoinAlanListesi in
        korumaliHavuzdanCoinAlanListesi.adres
        = girdi.adres
            }
    }
}
```

EK-B: Algoritma 2 - ZMadencilerin Bulunmasi
(APPENDIX-2: Algorithm 2 – Finding ZMiners)

```
ZMadencileriBul(blokZincir)
{
    blokListesi[] = blokZincir[-25000]
    //blokzincirdeki son 25,000 blok çekilir
    muhtemelZMadenciler[] = Ø
    for (blok in blokZincir)
    {
     if (işlem.ciktiSayisi > 30 and
işlem.KorumalıİşlemMi == false)
    {
            muhtemelZMadenciler = blok.islem
        }
    }
    odemeYapilanMadenciListesi =
blokListesi.islem.ciktiAdresi $in$
blokListesi.islem = muhtemelZMadenciler.islem
```

KARAR DESTEK SİSTEMLERİNİN MOBİL CİHAZ ADLİ BİLİŞİMİ SÜREÇLERİNE UYGULANMASINA YÖNELİK BIR ÖNERİ ÇALIŞMASI

Furkan Yılmaz*[1] ve Hüseyin Çakır[2]

[1] Gazi Üniversitesi, Bilişim Enstitüsü Adli Bilişim ABD, Ankara
[2] Gazi Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Ankara
furkanyilmaz89@hotmail.com, hcakir@gazi.edu.tr

ÖZET

Bu çalışmada, diğer dijital materyal türlerine göre nicelik ve nitelik açıdan daha ön plana çıkan mobil cihaz adli bilişimi üzerinde durulmuştur. Karar destek sistemlerinin mobil cihaz süreçlerine entegresi için iş akışına ilişkin sorular ve kurallar çıkartılmıştır. Türkiye'de adli bilişimde karşılaşılan sorunlar ele alınarak, mobil cihaz adli bilişimi ile ilgilenen personelin karşılaştığı problemlerle ilgili en hızlı, en doğru ve en verimli şekilde karar destek sistemleri aracılığıyla çözüme ulaşmasını sağlayacak bir model önerisi sunulmuştur. Bu model önerisi ile yüksek iş hacmine sahip ve kamu sektöründe ya da özel sektörde faaliyet gösteren adli bilişim laboratuvarlarının mobil cihaz adli bilişimine ilişkin süreçlerini en etkili şekilde hızlandırarak, zaman ve maliyet açısından tasarruf sağlamaları öngörülmektedir. Mobil cihaz adli bilişimi uygulayıcısı olan personele katkı sağlaması, potansiyel riskleri azaltması, süreci hızlandırması ve hukukilik çerçevesinde delil bütünlüğünün korunması beklenmektedir.

Anahtar Kelimeler— adli bilişim, adli bilişim laboratuvarı, karar destek sistemleri, mobil cihazlar, mobil cihaz adli bilişimi

A Proposal Study on the Application of Decision Support Systems to Mobile Forensics Processes

ABSTRACT

In this study, it is presented a model proposal in which the digital forensics applications, which is a method of obtaining evidence that is frequently used in actual criminal investigations, is proposed for law enforcement units to accelerate the process in the most efficient and effective way due to the volume problem; mobile device forensics is emphasized in terms of quantity and quality compared to other types of digital materials. Questions and rules regarding the workflow have been drawn up to integrate decision support systems into mobile forensics processes. By handling the problems in digital forensics in Turkey, a model proposal is presented to the personnel who work in mobile forensics to get the solution in the fastest, most accurate and most efficient way through the decision support systems. With this model proposal, it is foreseen that digital forensics laboratories, which have huge backlog and operate in the public or private sector, will accelerate the processes related to mobile device forensic computing in the most effective way and save time and cost. It is expected to contribute to the mobile forensic personnel, reduce potential risks, accelerate the process and protect the integrity of evidence within the framework of legality.

Keywords— decision support systems, digital forensics, digital forensic laboratory, mobile devices, mobile forensics

I. GİRİŞ (INTRODUCTION)

Çağımızda teknolojinin ve internetin günlük yaşamın vazgeçilmez bir parçası haline gelmesinin sonucunda, kişilerin yaşamlarına ilişkin en önemli bilgiler dijital olarak tutulmaya başlanmıştır. Artık suç soruşturmalarında ve kovuşturmalarında en önemli bulgular, dijital materyallerden elde edilmekte, hatta adli bilişim işlemlerine yetki veren Ceza Muhakemesi Kanunu (CMK) Madde 134'te "…somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde …" ifadesi olmasına ragmen keşif araması haline gelmiş durumdadır. Bununla birlikte sahip olunan dijital veri depolama birimleri çeşitlenmekte niceliksel ve niteliksel büyüme göstermektedir. Bu durumun tabii sonucu olarak bir suç dolayısıyla hakkında soruşturma yapılan şüpheliden elde edilen dijital materyaller: kişisel bilgisayarı, tableti, cep telefonu, sim kat, hafıza kartı, harici harddiski, USB bellek, CD/DVD vb. şeklinde çeşitlenmekte, bunların delil olarak analiz edilmesi gerekmektedir. Doğal olarak her geçen gün artan veri hacimlerinden kaynaklanan ve aynı zamanda çeşitli işletim sistemleri, dosya formatları vb. barındıran artan sayıda ve türdeki kaynakları inceleme ve analiz için standart tekniklerden yoksun olmanın sonucu olarak çeşitli sorunlar meydana gelmektedir [1].

Özellikle cep telefonları gibi mobil cihazların, kişinin sürekli yanında taşıması ve en mahrem anlarına dahi tanıklık ediyor olmasından dolayı diğer dijital materyallere göre suça konu bulguları taşıma ihtimali daha yüksektir.

Bu noktada adli bilişim faaliyetleri devreye girmekte; ancak oluşan bu dijital delil yığını tüm dünyada olduğu gibi (İrlanda Ulusal Polisi tarafından hazırlanan rapora göre dijital materyalin raporlanıp inceleme süresi 4 yılı aşmıştır [2].) Türkiye'de de önemli bir duruma gelmektedir. Hatta Türkiye'de 2018 yılında Kasım ayına kadar incelenen dijital material sayısı yaklaşık 630 bin olmuş, Avrupa kıtasının yıllık inceleme sayısıyla neredeyse denk olması Türkiye'deki durumun ciddiyetini daha da net ortaya koymaktadır [3].

Ayrıca Türkiye'de adli bilişim faaliyetlerine yetki veren temel mevzuat olan CMK'da ilgili madde metni 2005 yılında yürülüğe girmiştir. Her ne kadar madde metninde günümüze kadar bazı ufak değişiklikler yapılmış olsa da, mevcut ihtiyaçları karşılamamakta ve uygulamaya ilişkin bir çok soru işareti barındırmaktadır.

Bu çalışmayla ülkemiz mevzuatı içerisinde gün geçtikçe artan çeşitliliği, hızla değişen teknolojisi, karşılaşma sıklığı ve içinde barındırdığı veriler ile adli bilişim alanında önemli bir zorluk olarak karşımıza çıkan mobil cihazlardan delil elde etme aşamasında karar destek sisteminin uygulanmasına ait pragmatik, yapısal ve disiplinler arası bir yaklaşım ile bir model önerisi oluşturulacaktır.

Kolluk kuvvetleri tarafından uygulanabilecek ulusal bazda mobil cihazlara ilişkin detaylı ve net bir iş akışı bulunmamaktadır. Bu model sayesinde mobil cihaz adli bilişimi ile ilgilenen personelin, en doğru kararı en kısa sürede vermesi ve bunun sonucu olarak maliyet ve zaman tasarrufu sağlanması hedeflenmektedir. Mobil cihaz adli bilişimi uygulayıcısı olan personele katkı sağlaması, potansiyel riskleri azaltması, süreci hızlandırması ve hukukilik çerçevesinde delil bütünlüğünün korunması beklenmektedir.

II. PROBLEM (PROBLEM)

Dijital deliller yapısı gereği çok hassas olduklarından dolayı tüm süreç dikkatle ve belli prosedürlere uyularak icra edilmelidir. Dellilerin karartılması ya da zarar görmesine sebebiyet verecek uygulamalar, adli makamların delillerin reddi kararına yol açmaktadır [4].

Türkiye'de adli bilişim faaliyetleri yürütülürken bazı sorunlarla karşılaşılmaktadır. Farklı sebeplerle ortaya çıkan sorunlar dijital delilin geçerliliği konusunda şüphe uyandıracağından, bu sorunların çözülmesi gerekmektedir. Başlar, bu sorunları; adli bilişim sürecine ilişkin potansiyel riskler, ağ trafiği analizi delillerinin sorunları, mobil cihazlara ilişkin sorunlar, adli bilişim ilke ve standartlarının belirlenememesi, laboratuvarların yetersizlikleri, uygulayıcı eğitimsizliği, hukuka aykırıllk halleri olmak üzere yedi başlık altında saymıştır [5].

Ülkemizde uluslararası standartlara önem verilmektedir; ancak dijital delilin elde ediliş sürecine ilişkin işlemlerin nasıl olacağıyla ilgili düzenlemelerin olmaması, henüz elde ediliş aşamasında geri dönülmeyecek hasarlara zemin hazırlamaktadır [6]. Yapısı gereği hassas olan dijital verilerin, elde edildiği ilk andan itibaren delil zincirinin oluşması gerekmektedir. İmaj alma işlemlerindeki eksiklik, inceleme ve raporlama aşamasında ortaya konan delilleri görlgelemektedir.

Bir diğer problem ise, bilişim sistemlerinin gittikçe artan kapasitelerinin büyüklüğüdür. Şöyle

ki, delil olarak kullanılabilecek veri, elde edilen tüm sistemdeki verinin on binde biri kadar düşük seviyededir. Bu açıdan her türlü verinin değil, sadece yargılama konusu olayla ilgili, faili ve fiili ispat edecek verinin elde edilmesi gerekmektedir [7]. Bu da artan iş yüküne sebep olmakta, oluşan bu yığınları eritebilmek için daha akıcı süreçlerin oluşturulması ihtiyacı doğmaktadır.

Adli bilişim faaliyetini yerine getiren kolluk ve bilirkişilerin yeterince eğitilemesi de adli bilişim süreçleri açısından sorun teşkil etmektedir. Adli bilişim alanında görev alan personel, her bir dijital delilin farklılıklarını bilmesi gerekir [8]. Ayrıca bu personel, bilişim sistemleriyle ilgili ileri düzey bilgiye sahip, bunu koruyacak şekilde teknolojiyi takip eden ve gerekli hukuki bilgiyi haiz olmaları gerekmektedir [9]. Uzman personel eksikliği neticesinde veri elde etme imkanının olmadığı, manyetik alan etkisinden soyutlanmadan taşındığı, veri bütünlüğünü korumaya yönelik tedbirler alınmadan işlemlerin yapıldığı görülmektedir [10]. Gelinen noktada kolluk birimlerinde dahi adli bilişim personeli sayısı binlere ulaşmışken, bu sayıda personeli aynı nitelikte eğitmek ve aynı nitelikte iş ve işlemleri icra etmesini sağlamak da diğer bir problemdir.

Çeşitliliği gün geçtikçe artan mobil cihazlarla ilgili olarak, mobil cihaz adli bilişim süreçlerinde veri çıkarımına ilişşkin standardizasyon eksikliği görülmektedir [11]. Ayrıca mobil cihazlardaki ve mobil işletim sistemlerindeki çeşitlilik kesinlik barındıran bir standartlaşmanın önündeki en büyük engeldir. Mobil cihazlardan en fazlaya veriyi elde etme yöntemi olan fiziksel imaj alma işlemine ilişkin uygulanan teknikler pahalı, çok fazla teknik bilgiyle zaman istemektedir [11].

Ceza muhakemesi hukuku kapsamında yapılan adli bilişim faaliyetleri özünde temel hak ve özgürlüklere müdahale niteliği taşıdığından, yapılan işlemlerin hukukiliği önem arz etmektedir. Teknik açıdan ne kadar mükemmel bir çalışma ortaya konsa da, hukukiliğindeki problem elde edilen veriyi delil hukuku açısından geçersiz kılınmasına sebep olacaktır. Ceza Muhakemesi Kanunu Madde 134, adli bilişim faaliyetleri açısından temel mevzuat uygulamayla ilgili bir çok boşluğu barındırmakta ve uygulayıcılar bu alanları nasıl doldurcağı konusunda yeterli bilgiye sahip değillerdir.

III. SINIRLILIKLAR (LIMITATIONS)

Mobil cihazlar yapısı gereği çok çeşitlidir. Bu çeşitlilik adli bilişim uygulamalarını olumsuz etkilemektedir. Üretici firmaların, işletim sistemlerinin, kullanılan donanımlar ve hafıza çiplerinin çeşitlenmesi, adli bilişim için standart uygulama oluşturmayı zorlaştırmaktadır. Hatta piyasadaki bazı cihazların herhangi bir adli bilişim yazılımıyla dahi desteklenmediği görülmektedir.

Mobil cihaz adli bilişiminin amacı veriye ulaşmak iken, üretici firmaların veriyi cihazda kriptolu olarak tutma eğiliminde oldukları bilinmektedir. Bu da mobil cihaz adli bilişiminde fiziksel imaj almak için kullanılan bazı yöntemleri işlevsiz kılmaktadır.

İlk müdahale süreçleri ele alınırken, olay yerinin mobil cihaz dışındaki unsurları göz ardı edilmiştir. Olay yerleri için karşılacak senaryoların ve uyulacak prosedürler çalışma kapsamı dışında tutularak, mobil cihazlar için uygulanması gereken adımlara odaklanılmıştır.

Mobil cihaz adli bilişimi için ilk müdahale ve imaj alma aşamalarından sonra inceleme ve raporlama aşamaları gelmektedir. Ancak bu çalışmada başarılı şekilde imaj almak için bir model oluşturulduğundan, bu aşama sonrası yapılması gerekenler de çalışma kapsamı dışında tutulmuştur.

Personelin, modelde bahse konu işlemleri de nasıl uygulayacağını biliyor olması gerekmektedir. İşlemi yapacak mobil cihaz adli bilişimi uygulayıcısının konudaki bilgi eksiliğine ragmen işlem yapma ihtimali ve bu işlemler sonucunda delililn zarar görmesi ihtimali göz ardı edilmiştir

Mobil cihazların imajının alınabilmesi için gerekli olan yazılım, donanım ve uzmanlık konusunda çokça seçenek mevcuttur. Hatta uygulanabilecek yöntemler için teknolojik açıdan bir sınır koymanın da mümkün olmadığı değerlendirilmektedir. Bu sebeple modelin başarılı şekilde işlemesi için gerekli olan yazılım, donanum ve uzmanlık için Türkiye'de adli bilişim faaliyeti yürüten bir kolluk biriminin haiz olduğu kaynaklar esas alınmıştır.

IV. ADLİ BİLİŞİM (DIGITAL FORENSICS)

Digital Forensics Research Workshop (DFRWS), adli bilişimi suç teşkil ettiği tespit edilen olayların yeniden canlandırılmasını kolaylaştırmak veya ilerletmek veya planlanan operasyonları aksattığı görülen yetkisiz eylemlerin tahmin edilmesine yardım etmek amacıyla dijital kaynaklardan elde edilen dijital delillerin korunması, toplanması, doğrulanması, tanımlanması, analizi, yorumlanması, dokümantasyonu ve sunumuna

yönelik bilimsel olarak türetilmiş ve kanıtlanmış yöntemlerin kullanılması olarak tanımlamaktadır [12]. Literatür'de de adli bilişime için bir çok tanım bulunmaktadır.

"Adli Bilişim, bilişim sistemleri ve üzerinde bulunan depolama ünitelerinin, herhangi bir suçu işlemede veya yasaklanmış bir faliyette kullanılıp kullanılmadığını tespit etmek amacıyla yapılan çalışmaların tümüdür." [13].

"Adli Bilişim (Computer Forensics – Bilgisayar Kriminalistiği) bilimi; suçun aydınlatılabilmesi için bilimsel metotlar kullanılarak, çeşitli varyasyonlardaki dijital medyalar üzerinde bulunan, suçla ilgili dijital delillerin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde adalet önüne sunulmaya hazır hale getirilmesini sağlayan ve başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünüdür" [14].

"Adli Bilişim en basit tanımıyla, bir yargılama esnasında kullanılabilecek potansiyel delillerin belirlenmesi için bilgisayar araştırma ve analiz tekniklerinin kullanılmasıdır. Bilgisayardaki verilerin korunması, tanılanması, çıkarılması, dökümü ve yorumunu içerir ancak bunun yanında hukuki kurallar, süreçler, delillerin bütünlüğü gibi konulara da riayet ederek bulunan veriler hakkında rapor yazılmasını da kapsar" [15].

"Adli Bilişim, bilişim sistemlerine iletilen, işlenen ve/veya depolanan dijital verinin adli talimat üzerine elde edilerek bulgu olarak tespit edilmesinden, raporlanarak delil olarak değerlendirilmesi amacıyla mahkemeye sunulmasına kadar geçen süreçte delil zinciri her aşamada uygulanarak gerçekleştirilen multidisipliner (çoklu disipinli) ve interdisipiliner (disiplinler arası) halde işletilen teknik ve hukuki adımlar ile işlemler bütünüdür [16].

Her türlü veri depolayan, ileten veya işleyen bilişim sistemleri üzerinde, yazılım veya donanım kullanılarak verilerin ortaya çıkartılması, kurtarılması, analiz edilmesi ve ilgili makamlara sunulması amacıyla yürütülen ilk müdahale, muhafaza, adli kopya alma, inceleme, raporlama ve benzeri faaliyetlerin her biri veya bütünü olarak tanımlanabilir.

Adli soruşturmalarda bu faaliyetlere yetki veren temel mevzuat soruşturmalarla sınırlı olmak üzere Ceza Muhakemesi Kanununun 134. maddesidir. Başlığındaki "bilgisayar, bilgisayar programları ve kütükleri" ifadesinin mobil cihazları karşılayıp karşılamadığı bile zamanında tartışma konusu olmuş olan bu maddeyi uygulayanlar çok iyi bilirler ki; adli bilişim faaliyetlerinin uygulanmasına ilişkin ihtiyaçları karşılamamaktadır.

V. MOBİL CİHAZ ADLİ BİLİŞİMİ (MOBILE FORENSICS)

Adli bilişim bazı alt dallara ayrılmaktadır. Bunlar temelde dört ana başlık altında toplamak mümkündür. Bunlar bilgisayar adli bilişimi (computer forensics), mobil cihaz adli bilişimi (mobile forensics), ağ adli bilişimi (network forensics) ve bulut adli bilişimidir (cloud forensics) [17].

Telefon, tablet, gps cihazları gibi elde kullanılması mümkün olan son kullanıcı düzeyindeki bilgisayar sistemleri olarak tanımlayabileceğimiz mobil cihazlardan yazılım veya donanım kullanılarak içindeki verilerin ortaya çıkartılması, kurtarılması, analiz edilmesi ve ilgili makamlara sunulması amacıyla yürütülen ilk müdahale, muhafaza, adli kopya alma, inceleme, raporlama ve benzeri faaliyetlerdir.

Mobil cihazlar üzerinde adli bilişime konu olabilecek donanım bileşenleri, öncelikle verinin depolandığı donanımlardır. Bunlar hafıza çipi, hafıza kartı ve sim karttır. Somut olayın konusuna göre wi-fi, bluetooth gibi kablosuz bağlantılar da delil kaynağı haline gelebilir [18].

Mobil cihazlar kişilere ait arama kayıtları, mesajlar, e-postalar, resimler, videolar, müzikler, ses dosyaları, sosyal medya hesapları, yüklü uygulamalar, konumlar, dökümanlar, wi-fi bağlantıları gibi hassas bilgileri barındırmaktadır.

5.1. Cihaza İlk Müdahale

Suça konu cihaz muhafaza altına alınmadan önce Ceza Muhakemesi Kanununu Madde 134 uyarınca hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından verilmiş kararın varlığı teyit edilmelidir.

Muhafaza altına alınan cihazın, ilk önce marka, model, imei numarası gibi ayırt edici özellikleri ve kim tarafından kullanıldığı bilgisiyle beraber not alınır. Buna müteakip fiziksel bir hasarının olup olmadığı ve cihazın açık olup olmadığı kontrol edilir.

Cihaz açıksa kapatılmaz ve şifreli olup olmadığı teyit edilir, şifreli ise olay yerinde temin cihetine gidilir. Ayrıca cihazın dış bağlantılarını kesmek için faraday çantası kullanılır ya da uçak moduna alınır. Cihazda bulunan sim kart ve hafıza kartı gibi aparatların da marka, operatör, seri numarası,

ICCID gibi ayırt edici özellikleriyle beraber tespiti yapılır. Cihaz ve aparatlarıyla beraber fotoğrafı çekilir. Eğer dıştan görünen fiziksel arızası varsa, fotoğraflar arızanın belli olacağı şekilde de çekilir.

5.2. İmaj Alma

Dijital delil niteliğindeki bir veri depolama biriminin veya dosya içeriğinin veri bütünlüğü korunarak, adli bilişim yöntemleriyle bire bir (bit-to-bit) kopyalanması işlemidir. Veriyi elde etmek için uygulanan yöntemler gerektirdiği teknik bilgi ve maliyet açısından sınıflandırmaya Şekil 1'deki gibi tutulmaktadır [19].

Şekil 1. Mobil Cihaz Adli Bilişimi Araçları Sınıfladırması [19]

5.2.1. Manuel İnceleme

Kullanıcı arayüzü kullanılarak ulaşılan bilgilerin kaydedilmesi sürecini içerir [19]. Bu yöntem adli bilişim araçları arasında en az teknik bilgi gereksinimi olan yöntemdir. Cihazın çalışıyor olması ve şifresiz, şifresi biliniyor ya da şifresinin bir şekilde aşılmış olması gerekmektedir. Her ne kadar en temel ve en sınırlı yöntem gibi gözükse de bazı adli bilişim yazılımlarının anlamlandırmadığı uygulamaların veritabanlarına erişme imkanı sağlamaktadır.

5.2.2. Mantıksal imaj alma

Bir çok mobil cihaz adli bilişimi yazılımının sunduğu en fazla sayıda mobil cihazı destekleyen hızlı bir ayıklama yöntemidir. Orta düzey teknik bilgiyle ve temel düzeyde bir eğitimle mantıksal çıkarım yapmak mümkündür [19]. Bir kaynak cihazdan ayıklanabilecek veri türleri olan arama kayıtları, telefon defteri, SMS'ler, takvim etkinlikleri, çoklu ortam dosyaları (resimler, videolar, ses dosyaları) ve uygulama verileri gibi verilerinin elde edilmesidir. Çoğu durumda, kilitli cihazlar için mantıksal ayıklama mümkün değildir.

Mantıksal seviyede veri elde etmenin literatürde dosya sistemli çıkarım (file-system extraction) olarak da geçen yöntemle alınacak bir imajda, mantıksal bir uzantı ile görünmeyecek gizli sistem dosyalarına da erişilebilmektedir. Sistemde yüklü bulunan ya da kullanıcı tarafından sonradan yüklenen uygulamaların çoğu bu yöntemle ayıklanan veritabanı dosyalarında saklanmaktadır. Parolalara, uygulama verilerine, telefon defteri girdilerine, arama kayıtlarına, mesajlara ve kullanıcıya tahsis edilmiş alanlardaki verilere ulaşılabildiğinden, cihazın yedeğini alma (backup) işlemi niteliğinde olarak değerlendirilmektedir.

5.2.3. Fiziksel imaj alma

En geniş ve kapsamlı ayıklama yöntemidir. Mobil cihazın hafıza çipinin kart üzerindeyken verisinin elde edilmesini kapsayan ve ileri düzey uzmanlık gerektiren yöntemdir [19]. Ayrılmış alan dahil olmak üzere mobil cihaz üzerinde "bit to bit" yöntemi ile binary seviyesinde veriye erişilmesidir. Raw formatta alınan bu imaj sayesinde silinmiş alandaki verilere de ulaşılabilmektedir. Alınan veri binary yapıda olduğundan dolayı, maliyeti ne kadar düşük olsa da gerektirdiği uzmanlık düzeyi yüksektir [20].

Ancak her ne kadar maliyetinin düşük olduğu düşünülse de, veriyi elde etmek mobil cihazların marka, model hafıza çipi gibi bileşenlerinin çeşitliliğinden dolayı geniş ar-ge ihtiyacı oluştumaktadır. Veriyi anlamlandırma konusunda da benzer şekilde kullanılan mobil uygulamaların farklı yazılım dilleriyle, farklı veri tabanlarını kullanması ya da farklı algoritmalar kullanmasından dolayı çeşitliliği benzer bir zorluk olarak karşımıza çıkmaktadır. Teoride uzmanın veriyi fiziksel düzeyde elde edip anlamlandırsa dahi, mobil cihazların günümüzde geldiği noktadan dolayı pratikte lisanslı mobil cihaz yazılımı olmazsa olmaz haline gelmiştir.

5.2.4. Chip-off

Adli bilişimde uygulamada son seçenek olarak kullanılan yöntemlerden biridir. Kart üzerindeki kalıcı veri tutan hafıza çipinin sökülerek, özel donanımlarla iletişim kurulması ve binary düzeyinde veriye ulaşılmasıdır. Bu yöntemle cihazda bütünsel olarak neler olup bittiğinin daha iyi bir resmini verir [21]. Ancak yeni gelişen teknoloji ile yeni model Android işletim sistemine sahip cihazlarda veriler cihazın kendisine ait bir şifreleme algoritması ile tutulduğundan dolayı anlamlandırma konusunda sıkıntılar yaşanmaktadır. Aynı şekilde iOS işletim sistemine

sahip cihazlar da veriler şifreli tutulduğu için chip-off işleminde başarılı sonuçlar elde edilememektedir. Bu yöntemin diğer bir zorluğu da bellek çipinin, kontrollerdan ayrı çipler olması durumunda, hafıza çipindeki verinin decrypt (şifresinin çözülmesi) edilemesidir.

5.2.5. Mikro düzeyde okuma

Mikro düzeyde okuma yöntemleri, yüksek güçlü mikroskop vasıtasıyla çipte bulunan fiziksel kapıların durumunu görüntülemek için kullanılmasıdır [19]. Bu görüntüleme neticesinde 0 ve 1'lere dönüştürülerek, tüm veri çipindeki her bir bitin çıkartılması amaçlanmaktadır. Bu bitleri bir araya getirerek dosya sistemine, dosyaların üstverilerine ve veri alanlarına erişilmesi hedeflenmektedir. Piyasada bulunabilecek en düşük kapasiteli telefonun 32 GB olduğunu düşünürsek, tüm bitlerin okunması için bu işlemin 270 milyar kez yapılması gerekmektedir. Bu sebeple gerektirdiği donanımlar ve emek açısından en pahalı yöntemdir. Dünyada bu yöntemin uygulandığı laboratuvarların olduğu bilinmektedir; ancak Türkiye'de uygulandığına ilişkin bir veri bulunmamaktadır.

5.3. Kullanılan Yöntemler

5.3.1. Kullanılan yazilimlar

Mobil cihaz adli bilişiminde dünya genelinde sıklıkla kullanılan yazılımlar aşağıda belirtilmiştir [22].

XRY: 1984 yılından beri İsveç'te bulunan MSAB firmasına ait mobil cihaz incelemelerinde kullanan dünya genelinde kabul görmüş bir çözümdür. Dronelar da dahil olmak üzere yaklaşık 25.000 farklı cihazı destekleyen XRY yazılımı, MTK, Spreadtrum, Coolsand & Infineon gibi Çin menşeili telefonlarda kullanılan çip setler için uygun çözümlerden biridir. Literatürde XRY ismiyle genel olarak anlamlandırılmasına rağmen bu ürün XRY ve XAMN olarak iki farklı fonksiyona sahiptir. XRY yazılımı cihazdan verinin çıkartılmasında; XAMN ise çıkartılan verinin analiz edilmesinde kullanılan yazılımdır. Mobil cihaz adli bilişiminde önemli olan cihazlardan verinin elde edilmesi süreci olduğu için bu firmanın XRY ürünün ön plana çıkması da kaçınılmazdır. Ayrıca Türkçe dil desteğini bulunması Türk adli bilişim incelemecileri için tercih sebebidir [23].

UFED: 1999 yılında İsrail'de kurulan Cellebrite şirketinin en bilinen mobil cihaz inceleme ve imaj alma yazılımı olan UFED, dünya çapında da kullanılan bir yazılımdır. 2018 yılında Forensic 4:Cast tarafından verilen "En iyi mobil adli bilişim donanımı" ödülünü UFED Touch2 ile, "En iyi mobil adli bilişim yazılımı" ödülünü ise UFED 4PC ve UFED Physical Analyzer (PA) ürünleri ile kazanmıştır [24].

UFED Touch ürünü sahada bu yazılımı kullanmamıza imkân veren bir donanımdır. Bu sayede olay yerinde imaj alma ve çıkarım yapma imkânı sunan bu cihazla arama kayıtları, resim, video gibi soruşturma açısından önem arz eden verilere anında ulaşma imkânınız olacaktır.

UFED 4PC ürünü ise kullanılan özel kitlerle mobil cihazların normal bilgisayarlar vasıtasıyla imajının alınmasını sağlarken; UFED PA ürünü ise alınan imajın anlamlandırılması ve incelenmesi için kullanılan ürünüdür.

Magnet Axiom: 2009 Yılında Kurulan Magnet Forensics firmasının ürünü olan Axiom, ilk olarak piyasaya IEF (Internet Evidence Finder) olarak çıkmıştır. İnternet kalıntılarını analiz etme konusundaki başarısı ile oldukça popüler hale gelmiş ve daha kapsamlı olan Axiom ürününü 2016 yılında piyasaya sürmüştür. Axiom hem bilgisayarlarda hem de mobil cihazlarda analiz imkanı sağlamaktadır.

Axiom, gelişmiş kazıma ve üçüncü parti uygulamalar için kapsamlı desteği sayesinde daha fazla silinmiş, kodlanmış ve şifreli veriye ulaşılmaktadır. Öte yandan diğer mobil adli bilişim yazılım kitleri ile chip-off ve J-tag gibi yöntemlerle alınan imajları desteklemektedir.

Magnet Acquire isimli aracıyla da mobil cihazların imajları alınabilmektedir. Ayrıca bu alınan imajlar Cellebrite'ın UFED ürünüyle ve Guidance Software'in Encase ürünüyle de analiz edilebilmektedir [25].

Oxygen Forensic Detective: Oxygen Software şirketi, 2000 yılında bilgisayardan mobil telekomünikasyona yazılım şirketi olarak kurulmuştur. Rus menşeili bu şirketin merkezi Amerika Birleşik Devletleri'ndedir.

Diğer mobil adli bilişim yazılımlarından farklı olarak, Jet-Imager ismini verdikleri modülle Android cihazlar için en hızlı fiziksel çıkarım seçeneğini sunmaktadır. %25'e varan süre avantajı sağlayan bu yöntem ile 16 GB bir telefonun imajı 5 ila 7 dakika arası sürmektedir. Ayrıca LG cihazlara özel olarak, bazı modellerinde tek klik ile ekran kilidini aşma özelliğini desteklemektedir. Bunun için ilave kablo veya araca ihtiyaç duymayan yöntem,

sadece standart USB kablosuna ihtiyaç duymaktadır. Hem Android hem de iOS işletim sistemine sahip cihazlar için, yüklü olan casus yazılımları tespit eden Oxygen Forensic Detective, casus yaılımların log ve konfigürasyon dosyalarını prosesleme imkanın sahiptir. Bu sayede konfigürasyon verisi, kullanılan servisler, uygulamanın kullanıcı adı, data transferinde kullanılan cell ID gibi bilgilere ulaşabilmektedir [26].

Paraben: 2001 yılından beri Amerika Birleşik Devletleri Merkezli bu firma, mobil cihazlar, akıllı telefonlar, bilgisayarlar, eposta, oyun sistemleri ve bulut adli bilişimi üzerine çözümler üretmektedir. Mobil cihaz adli bilişimi ile ilgili E3:DS ürünü bulunmaktadır. E3:DS ürünü, mantıksal imaj alma, fiziksel imaj alma, Çin menşeili cihaz desteği, bulut desteği, veri analizi, uygulama anlamlandırması ve kilitli cihazların kilidini aşma özelliklerine sahiptir [27].

Mobiledit: 1991 yılında kurulan Compelson firması, mobil cihaz adli bilişimi ile ilgili çalışmalarına 1996 yılında başlamıştır. 20 yılı aşkın süredir bu alanda kolluk kuvvetlerine, askeri kuvvetlere ve soruşturmalara destek olmaktadır. MOBILedit Forensic, MOBILedit Forensic Express, Sim Cloning Tool ve Camera Ballistics, ürünlerine sahip olan MOBILedit, mobil cihazlarda kullanılan yazılımları veri çıkarımı yapma, rehber, mesajlar, takvim, hatırlatıcılar, notlar, şifreler, uygulama verileri gibi birçok bilgiye ulaşılmasını sağlamaktadır [28].

Blackbag: Blackbag Technologies firması adli bilişim alanında Apple cihazlarına ilişkin sunduğu çözümlerle öne çıkmaktadır. Bu firmanın mobil cihaz adli bilişimi üzerine olan araçları, Blacklight ve Mobilyzedir. Blacklight hem Mac hem de Windows işletim sistemleri üzerinde çalışan kapsamlı incelemeyi sağlayan bir yazılımdır. Bu yazılımlar Windows, iOS ve Android işletim sistemine sahip cihazlardan bilinen internet kalıntıları, backup dosyaları gibi veri yapıları, sanal imajlar ve Windows registry dosyaları gibi verileri analiz edebilmektedir [29]. Mobilyze aracı ise, iOS ve Android cihazlarından imaj alma, triyaj yapma ve raporlama özelliklerine sahiptir.

Andriller: Andriller yazılımı Android cihazların şifrelerini aşmasıyla ön plana çıkmış bir mobil cihaz inceleme yazılımıdır. Mobil cihazlardan veri çıkarımı yapabilmekte, bunu yaparken bazen root işlemiyle bazen de root işlemi olmaksızın veriyi çıkartabilmektedir. Ayrıca Whatsapp uygulamasının kriptolu veritabanlarını aşabilmekte, Android backup dosyalarını çıkartabilmektedir [30].

Katana Forensics: Birleşik Devletler menşeili Katana Forensics firmasının mobil cihaz adli bilişimi ile ilgili ürünleri bulunmaktadır. Bunlar Lantern Triage ve Lantern 4'tür. Lantern Triage, mobil cihazlar için bir triyaj yazılımı olup, olay yerinde veri çıkarımı fonksiyonu vardır. Adnroid ve iOS işletim sistemli cihazlarından çıkarım özelliği sayesinde dosya sistemleri, mesajlar, bulut verisi, harita verisi, geolokasyon verileri ile çağrı kayıtları gibi bilgileri sunmaktadır. Lantern 4 ürünü ise mobil cihazlar için bir imaj alma ve analiz yazılımıdır. iOS ve Android cihazlarda mantıksal, iOS cihazlarda fiziksel çıkarım özelliklerine sahiptir. Dosya sistemi, dosya imza bilgisi, anahtar kelime araması gibi özelliklere de sahip olan bu yazılım Mac cihazlarda çalışabilmektedir [31].

5.3.2. Teknik yöntemler

Mobil cihaz adli bilişiminde bazı zorluklarla karşılaşılmaktadır. Veriye normal yöntemlerle ulaşılamama sorununu gündeme getirmektedir. Bu verinin normal yöntemlerle elde edilememesi fiziksel müdahaleyi de gerekli kılan Chip-off, JTAG, rooting ve jailbreak gibi ileri düzey teknik yöntemlerin uygulanmasını gerektirmektedir" [16].

Cihazlarla yukarıda sayılan araçlarla iletişim kurulamaması halinde, cihaza bazı teknik müdahalelerin yapılması gerekebilir. Sıklıkla yapılan teknik müdahaleler aşağıdaki gibidir.

Tamir: Cihaz ile arıza sebebiyle iletişim kurulamadığı durumlarda, teknik müdahalelerle ile cihazın arızasının tespiti, onarılması, eski haline getirilmesi süreçleridir. Bu yöntem diğer yöntemlere göre daha az maliyetli ve veri güvenliği açısından daha az risklidir.

Chip-off: Kart üzerindeki kalıcı veri tutan hafıza çipinin sökülerek binary düzeyinde veriye ulaşılmasıdır. Yöntem olarak çipi karta bağlayan bacakları ısıtılarak, kart ile bağlantısı kesilmektedir. Sökülen çipin pin-outu çıkartılarak ve veri yolları temizlenerek uygun apparat vasıtsaıyla bilgisayara gösterilmektedir. Bu şekilde fiziksel imaj alınmış olmaktadır. Ancak yeni gelişen teknoloji ile Apple cihazlardan sonra, Android işletim sistemine sahip cihazlarda veriler cihazın kendisine ait bir şifreleme algoritması ile tutulduğundan dolayı anlamlandırma problemleri chip-off yönteminin etkinliğini azalmıştır. Hafıza çipinin, kontrollerdan ayrı durumda board

üzerinde olması da, chip-off'u etkileyen bir diğer unsurdur.

J-tag: (Joint Test Action Group) İşlemcilerin kart üzerinden sökülmeden, kart üzerindeki j-tag pinleri üzerinde lehimleme işlemi yapılarak veriye erişilmesi işlemidir. Adli bilişim standartlarına uygun olarak Android cihazlarda anakart üzerinden test uçlarına lehimlemeler yapılarak j-tag işlemi yapılmaktadır. Fakat yeni gelişen teknoloji ile yeni model Android işletim sistemine sahip cihazlarda veriler cihazın kendisine ait bir şifreleme algoritması ile tutulduğundan dolayı anlamlandırma konusunda sıkıntılar yaşanmaktadır. Bunlar dışında diğer Android cihazlarda anakart üzerinde yol kopukluğu vb. gibi fiziksel bir arıza olmaması durumlarında cihazın anakartı üzerine lehimlemeler yapılarak veri alışverişi mümkün olabilmektedir.

ISP: (in system programming) çipin sisteme kurmadan önce programlanmasını gerektirmek yerine, bazı programlanabilir mantık aygıtlarının, mikro denetleyicilerin ve diğer gömülü aygıtların tam bir sistemde kurulurken programlanabilmesidir. Yeni model ufs çip diye tabir ettiğimiz çiplerde j-tag işlemini desteklemediği onun yerine ISP yönteminin kullanıldığı bilinmektedir

Root: Telefon, tablet gibi Android cihazların verisine ulaşmak için kök klasörüne erişim sağlanması işlemidir.

VI. KARAR DESTEK SISTEMI (DECISION SUPPORT SYSTEMS-DSS)

Karar destek kavramı ilk olarak Carnegie Teknoloji Enstitüsü'nde 1950'li yıllarda gerçekleştirilen teorik organizasyonel karar verme çalışmaları ve Massachusetts Institute of Technology (MIT) tarafından 1960'lı yıllarda etkileşimli bilgisayar sistemlerinde gerçekleştirilen çalışmalar sonucunda ortaya çıktığı bilinmektedir [32].

Gorry ve Scott Morton'a göre ise karar destek sistemi bireylerin enteklektüel kaynakları ile bilgisayarların karar iyileştirme yeteneklerini birleştiren ve yarı-yapısal problemlerle ilgilenen yönetim düzeyindeki karar alması gerekenler için bilgisayara tabanlı olarak destek sağlayan sistemler olarak vurgulanmıştır [33].

Karar destek sistemleri için yapılan en genel tanımlardan biri Gökçen tarafından "yönetici konumundaki karar vericilerin karar vermelerinde yardımcı olan sistemlerdir. Diğer bir deyişle, verilmesi gereken kararlarla ilgili veriyi daha iyi anlayarak, daha etkin karar seçeneklerini oluşturma, alternatifleri belirleme ve değerlendirme işlevlerinde destek sağlayan ve doğru karar verme olasılığını artıran sistemlerdir" şeklinde yapılmıştır [34].

Karar destek sistemleri genel olarak karar verici uzman kişilerin kararlarını vermede daha etkin ve verimli olmalarını sağlamak amacıyla geliştirilmiş olan bilgisayar destekli araçlar veya yazılımlar olarak tanımlanabilir [35].

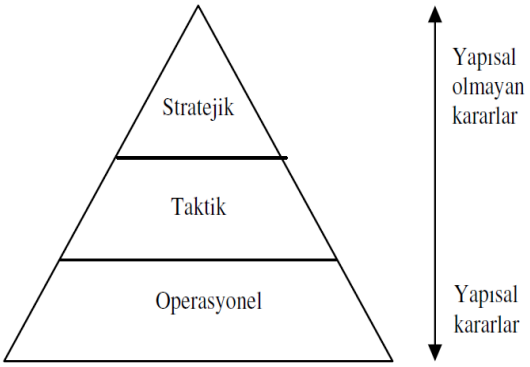
Karar Destek Sisteminde; "Karar" kelimesi, problem çözümünü; "Destek", karar verme sürecinde, bilgisayar ve yazılım teknolojileri kullanımıyla karar vericilerin desteklenmesini; "Sistem"; insan-makine arasındaki etkileşim ve bunun dizayn ve tanımlanmasını ifade etmektedir [32].

Tüm organizasyonların faaliyetinde sıklıkla kapsamlı veya basit kararlar alması gerekmektedir. Bunlar yatırım yapma-yapmama, kapasite artırma-azaltma, işçi alma-çıkarma, çalışma saatlerini artırma, ürün yelpazesini artırma-azaltma, üretim teknolojilerini değiştirme-değiştirmeme gibi faaliyetleri içerir. Bu kararları vermek her zaman kolay değildir ve bu kararlardan sonra her zaman doğru sonuçlar elde edilmeyebilir [36].

Karar verme süreci, stratejik, taktik ve operasyonel seviyelerde olabilir. Bunlar karar verecek yöneticinin seviyesine göre şekillenir. Yöneticilerin seviyelerine ve problemlerin niteliğine göre yapısal, yarı-yapısal ve yapısal olmayan kararlar şeklindedir. Şekil 1'de gösterildiği üzere yönetim seviyelerine göre karar tipleri alt kademeye doğru indikçe yapısal olmayandan yapısala doğru bir geçiş olmaktadır [37].

Karar destek sistemleri kullanılırken sıklıkla kullanılan algoritmalar aşağıdaki şekilde sıralanabilir [38]:

- Genetik Algoritmalar
- Doğrusal Programlama
- Yapay Sinir Ağları (YSA)
- Uzman Sistemler (US)
- Bulanık Önermeler mantığı
- Zaman Serileri
- Bayes Algoritması
- Analitik Hiyerarşi Prosesi (AHP)



Şekil 2. Yönetim Seviyelerinde Karar Tipleri [37]

Mobil cihaz adli bilişiminde karar destek sisteminin uygulanması bir uzmandan alınan bilgilerin karmaşık problemi çözmek için kullanılması mahiyetinde olacağı için yukarıda sayılan algoritmalardan uzman sistemler kullanılması daha uygun olmaktadır.

VII. MOBİL CİHAZ ADLİ BİLİŞİMİ VE KARAR DESTEK SİSTEMLERİ (MOBILE FORENSICS AND DSS)

Adli inceleme yapan tüm uzmanlar, kendilerini bekleyen artan iş yığını, büyük miktarda delil ve veri yığını problemiyle karşı karşıyadır [39]. Mobil cihaz adli bilişimi sürecinde, uzman sistemler yaklaşımıyla yapısal kararların ele alınması hedeflenmektedir. Yapısal kararlar, tanımlanmış kararlar olarak da belirtilebilirler. Yapısal kararlarda, sorunların çok iyi tanımlanmasının yanında, belirlilik seviyesi yüksek olması ve karar verici için öznel bir esneklik söz konusu değildir. Bu tip kararlar için bireyden bağımsız bilgisayar tarafından da alınabilen kararlar denilebilir [37]. Bu sayede ileri derece uzmanlık ve tecrübe isteyen bu süreçlerin uzman sistemler yardımıyla, bu süreçte yeni başlamış olan adli bilişim personelleri için hem karar alma süreçlerini hızlandırması hem de en doğru karara hata yapmadan ulaşması hedeflenmektedir.

Literatürde, adli bilişim iş akışına ilişkin kural koyma çalışmaları yapılmıştır. Effiong, çalışmasında adli bilişime ilişkin bütün süreci ele alan bir yapı ortaya koymuştur. Süreçler adım adım ele alınmıştır. Bu çalışmada bilgisayarlar üzerin yoğunlaşılmış ve adımlar genel nitelkikte olup daha yüzeysel olduğu görülmüştür [12].

Mobil cihazlar üzerine Faheem vd. tarafından yapılan çalışmada mobil cihaz adli bilişimi koruma, elde etme, inceleme, analiz ve raporlama olarak beş adımda ele elınmıştır. Bu adımlar daha genel nitelikte olup, doğrudan uygulayıcı için yol gösterici olarak görülmesi mümkün olmamaktadır. Ayrıca bu çalışma da mobil cihaz adli bilişiminde very çıkarımına ilişkin standardizasyon eksikliği ve mobil cihazlardan veriyi elde etmeye yönelik tekniklerin zorluğu ile maddi ve zaman yönünden maliyeti de vurgulanmıştır. Bu çalışmada mobil bulut verileri üzerine de yoğunlaşılmış; ancak mobil cihaz adli bilişimine ilişkin adımlar genel nitelikte kalmış ve mobil cihaz adli bilişiminde uygulamadli alt düzey problemler göz ardı edilmiştir [11].

Al Mutawa vd., tarafından yapılan adli bilişime yönelik model önerisi olan çalışmada ise, adli bilişim süreçlerinin davranışsal delil analizi konu alınmıştır. Buradaki model önerisinde ise laboratuvar ortamındaki inceleme, analiz ve raporlama süreçlerine odaklanılmıştır [40]. Post-mortem yani olay yeri sonrası olan sürece odaklanılarak, adli bilişim personeli için yapılan hataların telafisinin olmadığı ilk müdahale süreçleri göz ardı edilmiştir.

NIST (National Institute of Standard and Technology) tarafından hazırlanan mobil cihaz adli bilişimi için rehberde de mobil cihaz teknolojisi ve adli bilişim süreçleri baştan sona detaylı ele alınmıştır. Mobil cihaz adli bilişimiyle ilgilene herkesin başvurması gereken nitelikteki bu çalışmada, mobil cihaz incelemede kullanılan araçların çalışma prensipleri dahil, bir çok önemli noktaya değinilmiştir. Mobil cihaza müdahaleye ilişkin oluşturulan karar ağacı diyagramında cihazın durumuna ilişkin kilitli olup olmadığı ve batarya durumu gibi sınırlı bazı unsurlar dile getirilmiştir. Çalışmada da belirtildiği üzere bu diyagram başlangıç niteliğindedir. Detaylara girilmemiş problemler için uzmandan destek alınması gerektiği şeklinde çözümler önerildiği görülmüştür [19].

Akalın, mobil cihaz inceleme sürecine yoğunlaşarak bir model önerisi geliştirmiştir. Bu modelde literatürün genelinde yer alan koruma, elde etme, inceleme-analiz ve raporlama aşamaları üzerinden oluşturmuştur. Bu aşamaları toplamda on dokuz alt adımda ele almış ve alt adımların gerçekleşmesine dair kontrol listeleri oluşturmuştur. Ayrıca iki farklı adli bilişim yazılımıyla mobil cihaz incelemesine de yer verilmiştir. Detaylara girilen bu çalışmada da mobil cihaz adli bilişiminin en önemli problemlerinden olan imaj alma safhasında karşılaşılan engellere girilmemiş ve çözümler sunulmamıştır [20].

Mobil cihaz adli bilişiminin uygulanmasına ilişkin Türkiye'deki en kapsamlılardan sayılabilecek eserde Doğanay, zorluklar ve delil zincirine odaklanmıştır. Ancak mobil cihazlardan delil elde edilmesine ilişkin bir iş akışına yer vermiştir. Bu iş akışı her ne kadar diğer çalışmalara göre detaylı bir çıktı vermiş olsa da, adli bilişim uygulayıcısı için yapılması gerekenleri saymış ancak hangi sorunların nasıl çözüleceğine ilişkin detaylar yüzysel kalmıştır [41].

Anlaşıldığı üzere adli bilişime ilişkin çıkarılan modeller, daha yüksek seviyedeki süreçlere odaklanmıştır ve alt seviyedeki temel ilkelerle ilgili fazla detaya yer verilmemiştir. Ayrıca yapılan çalışmalar laboratuvar ortamında yürütülen adli bilişim süreçlerine ele alınmış ve olay yerindeki süreçler ve hukuki süreçler mevzuat ülkeden ülkeye farklılık gösterdiği için göz ardı edildiği görülmüştür. Bunlara ilave olarak mobil cihaz adli bilişiminin en önemli problemlerinden olan imaj almayla ilgili olarak mobil cihazların kendi içinde barındırdığı zorluklardan dolayı detaylı bir süreç modeli ortaya konulamadığı görülmüştür.

Bu çalışmada pragmatik, yapısal ve disiplinler arası bir yaklaşım ile mobil cihazların imaj alınmasına en önemli faktörler belirlenerek, hukuki açıdan karşılaşılan sorunların çözümünü de barındıran bir model önerisi geliştirilmiştir. Karar destek sistemiyle de mobil cihaz adli bilişim uygulayıcılarının cihaza ilk müdahale aşamasından başlayarak bir soru-kural diyagramı çıkartılmıştır.

7.1. Mobil Cihaz Adli Bilişiminde Soruların Belirlenmesi

Mobil cihaz adli bilişimi; cihaza ilk müdahale, imaj alma ile inceleme ve raporlama olmak üzere üç temel aşamada ele alınmıştır. Sorular belirlenirken mobil cihazlar üzerine çalışan adli bilişimcinin durumu net bir şekilde ortaya koyması, bunları detaylandırması ve varsa sorunları belirlenmesi hedeflenmiştir. Bu sorular özellikle Türkiye Cumhuriyeti mevzuatına göre hareket eden kolluk birimlerini yönlendirecek şekilde tasarlanmıştır. Model, pratikte mobil cihazların genelinde adli bilişim faaliyeti uygulayan kolluk birimlerine fayda sağlayacak adımları içerecek şekilde tasarlanmış olup sorular ve açıklamaları aşağıda verilmiştir.

7.1.1. Cihaza ilk müdahale

Cihaza ilk müdahale aşaması suça konu olduğu değerlendirilen bulgunun tespitiyle başlamaktadır. Cihaz tespitinden sonra olay yerine giden adli bilişim personelinin yetkileri de dahil olmak üzere kontrol etmesi gereken hususları da barındıran bir soru-cevap süreci ortaya konulmaya çalışılmıştır. Sorulara yetkinin olup olmadığının kontrolüye başlanıp, cihazın fiziksel durumunun tespiti ile devam edilmektedir. Bir sonraki aşama olan imaj alma işlemi için gerekli tedbileri alacak şekilde son verilmektedir. Oluşturulan diagram Şekil 2 ve Şekil 3'te gösterilmiştir.

1. Bir soruşturma kapsamında mı hareket ediliyor?

Türkiye'de adli bilişim açısından temel yetki veren mevzuat olan Ceza Muhakemesi Kanunu Madde 134'te belirtildiği üzere bu tedbir yalnızca soruşturma aşamasında uygulanmaktadır. Bu sebeple soruşturma kapsamında ve hakim kararı olmadan kişilerin temel hak ve özgürlüklerini barındıran alana müdahale Türk Ceza Kanununa göre sorumluluk doğurabilmektedir.

2. Adli bir soruşturma mı?
3. İdari bir soruşturma mı?
4. Yetkili makamlarca verilmiş bir karar var mı?

Soruşturmanın adli bir soruşturma olması durumunda hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından verilmiş karar olması gerekmektedir. Bu kararlar olmadan yapılan arama TCK Md. 120'ye göre Haksız arama suçunu oluşturabilecektir.

5. Verilen kararda arama yapılacak yere, aramanın konusuna ve şüpheliye ilişkin bilgiler uyuşuyor mu? (CMK md. 116 vd. ve CMK md. 134)
6. Kamuya ait bir cihaz mı?

İdari soruşturma kapsamında yalnızca kamuya ait cihazlara ilişkin adli bilişim incelemesi yapılabilirken, kişilere ait cihazlarda adli bilişim incelemesi yapabilmek için bir adli soruşturma kapsamında karar alınmış olması gerekmektedir.

7. Yetkili müfettiş veya denetim yetkisine sahip amir tarafından verilmiş bir karar var mı?
8. Adli bilişim dışında farklı bir kriminal analize ihtiyaç var mı?

Deliller üzerinde parmak izi, DNA analizi gibi çalışmalara ihtiyaç duyulacak olursa adli bilişim faaliyetlerine başlamadan önce ilgili birimle irtibata geçilerek gerekli önlemlerin alınması gerekmektedir.

9. Cihazın gözle görülen bir fiziksel arızası var mı?

Cihazdaki arızanın olay yerinde tespiti ileride oluşacak ihtilafların, delil karartma gibi şüphelerin ortadan kaldırılması için önem arz etmektedir.

10. Cihaz sıvı içinde mi?

Cihazın sıvı içinde olması durumunda içerideki akımı kesmek için engellemek amacıyla bataryanın sökülmesi gerekmektedir.

11. Sıvı tahrip edici bir sıvı mı?

Sıvı tahrip edici sıvıysa cihazı korumak için bir an önce o sıvıdan arındırmak gerekmektedir. Tahrip edici sıvı olmayan durumlarda oksitlenmeyi başlatmamak için mevcut sıvıyla muhafaza edilmesi gerekmektedir.

12. Cihaz açık mı?

Cihazın açık olması durumunda saat, tarih, kullanıcı gibi bazı bilgilerin kontrölü ve uçucu verilerin alınması gerekir. İlk önce uçucu verilerin kayda alınması önem arz etmektedir [41]. Cihazın açık halde laboratuvar ortamına nakli için powerbank gibi güç kaynağı ile desteklenmeli ve şarjın bitmesi durumuyla karşılaşılmasını engelleyici tedbirlerin alınması gerekmektedir.

13. Ekipman içerisinde faraday çantası var mı?

Mobil cihazlar yapısı gereği kablosuz iletişime açık olduğundan radio frekanslarını keserek, dışarıdan gelecek delil karartmaya ilişkin sinyalleri engellemek amacıyla faraday çantası kullanılması gerekmektedir. Faraday çantasının bulunmadığı durumlarda cihazın uçak moduna alınması da bir diğer çözümdür.

14. Cihaz içerisinde sim kart ve hafıza kartı gibi başka aparatlar var mı?

Cihaz içerisindeki diğer aparatların mutlak surette tespit edilmesi gerekmektedir. Daha sonradan ortaya çıkan sim kart ve hafıza kartları aidiyetle ilgili şüphe doğurabilmektedir.

15. Bu aparatları çıkartmak için bataryayı sökmek gerekiyor mu?
16. Cihaz evrensel bağlantı portlarına mı sahip?

Cihazın standartlar portlar dışında farklı, nadir bulunan veri ya da güç portuna sahip olması ara kabloları bulma konusunda ileride farklı sıkıntılara sebebiyet vermektedir. Adli bilişim incelemesi yapılması için cihazla iletişim kurulması en temel unsurlardan biridir.

7.1.2. İmaj alma

Cihaza ilk müdahale aşamasından sonra geçilen mobil cihazlar için imaj alma aşaması genellikle olay yerinde değil de laboratuvar ortamında gerçekleşirilmektedir. İmaj alma aşaması otuz dört sorudan oluşmakta ve bu sorularla cihazın içindeki anlamlı veriye ulaşılması hedeflenmektedir. Bu aşamada sorulan sorularla sırasıyla cihazın çalışıp çalışmadığı, varsa arızası, arızanın nasıl giderilebileceği, imajın nasıl alınabileceği tespit edilmesi amaçlanmaktadır.

1. Cihaza ait bilgilerin tespiti tam ve eksiksiz yapılmış mı?

Bu adım cihaza ilk müdahale eden, el koyan kişiyle laboratuvar ortamındaki uzmanın farklı kişi olması durumunda delil zincirinin korunması için önem taşımaktadır.

2. Cihaz açılıyor mu?

Cihazın açılmaması durumunda, eletriksel zararların meydana gelmemesi için içindeki elektrik enerjsini kontrollü şekilde deşarjı gerekmektedir.

3. Batarya var mı?

Bataryanın olup olmadığına göre, cihazın çalıştırılması için gereken yöntem değişmektedir. Batarya varsa osiloskop ile kontrolü gerekirken, yoksa farklı bir güç kaynağı ile enerji sağlanması gerekmektedir.

4. Sim kart olmadan açılan modellerden mi?

Bazı eski telefonların sim kart olmadan farklı bir fonksiyon barındırmamasından dolayı, sim kartsız çalışmama özellikleri mevcuttur. Bu engelin, sim kart klonlanarak aşılması mümkündür.

5. Cihaz ile normal yollardan iletişim kuruluyor mu?

Cihaz ile normal yollardan iletişim kurulması halinde, imajı alınabilir. İletişim kurulmaması halinde çözümü için adımlar atılması gerekmektedir.

6. Cihaz şifreli mi?

Cihazın şifresi olması durumunda şifreyi aşmaya yönelik işlemler yapılabilmekte iken, cihazın şifresi olmadığı halde iletişim kurulamaması halinde arıza olup olmadığına yönelik tespitlerin yapılması gerekmektedir.

7. Cihaza şifre kırma atağı yapılabiliyor mu?

Eğer cihaza şifre kırma atağına müsait olan bir cihazsa, hatalı denemeler neticesinde kendini wipelama riski de göz önüne alınarak bu işlem gerçekleştirilir. Ancak cihazın kendini tamamen silmesi olmayı, ileride şifrenin farklı yollardan

temini yoluyla aşılması imkanını da kapatacağından, bu hususa ayrıca önem gösterilmesi gerekmektedir.

8. Cihazın bootloader ile fiziksel imajı alınabiliyor mu?

Bootloader yöntemiyle cihazın kullanıcı arayüzüne ve buradaki şifreyle karşılaşmadan veriye erişilmesi mümkün olmaktadır.

9. Root işlemi ile imajı alınabiliyor mu?

Eğer cihazın şifresinin aşılması yönetici hakları elde edilince mümkün ise, cihazdaki yönetici haklarını elde etmek için root işlemi uygulanması gerekmektedir.

10. İmajı alınmasına rağmen başlangıç kriptosu var mı?

İmaj alındıktan sonra başlangıç şifrlemesi mevcutsa, veri kaybı riski olmadan atak yapılabilir. Çünkü imaj alma işlemi gerçekleştirildiğinden, asıl cihaza ilişkin delili bütünlüğü zaten sağlanmış durumdadır.

11. Cihazın arızası var mı?

Cihazın arızası varsa cihazın arızasının tespiti ve sonrasında giderilmesine yönelik işlemler yapılmalıdır.

12. Arıza bağlantı portlarında mı?

Arızanın bağlantı portlarında olması durumunda lehimleme ile giderilmesi çalışılmalıdır.

13. Lehimleme ile arıza giderildi mi?

Lehimleme ile de bağlantı kurulamadıysa, bunun çözümü portu değiştirmekten geçmektedir.

14. Arıza ekranda mı?

Ekran arızası durumunda ekranın çalışır hale getirilmesi çok müümkün olmadığından, yerine sağlam ekran takılarak cihazla iletişim kurulmaya çalışılması gerkemektedir.

15. Arıza board üzerinde mi?

Bileşenleri elinde tutan ve bunlar arasındaki iletişimi sağlayan kartın arızalı olması durumunda arızanın tespitine yönelik çalışma gerekir.

16. Board üzerindeki arıza tespit edilebiliyor mu?

Eğer kart üzerindeki arıza tespit edilemiyorsa, çözümü için başkaca yapılacak işlem bulunmamaktadır.

17. Kısa devre mi?

Kısa devre olması durumunda, kısa devrenin bulunduğu yer lehimlenerek, elektrik devresnin tamamlanması sağlanmalıdır.

18. Yanmış mı?

Eğer kart üzerinde yanma neticesinde bir tahribat oluşmuş ise, veriye ulaşmak için hafıza çipine odaklanılması gerekmektedir.

19. Hafıza çipi sağlam mı?

Hafıza çipinde de bir arıza veya hasar durumu varsa veriye ulaşılması pratikte imkansız hale geldiği söylenebilir. Bundan sonra yapılacak başkaca işlem bulunmamaktadır.

20. Arıza giderildi mi?

Eğer sayılan yöntemlerle arıza giderildiyse, cihazın verisine ulaşılıp ulaşılmadığının kontrolü ve ardından imajı alınması aşamasına geçilmesi, eğer arıza giderilememişse yapılan işlemler raporlanarak tutanak altına alınıp işlemin sonlandırılması gerekmektedir.

21. Cihazdaki veri kriptolu olarak mı tutuluyor?

Cihazın hafıza çipindeki veri kriptolu olarak tutulmuyorsa, chip-off işlemiyle çipi sökülerek, çiple iletişim kurularak verinin ham hali elde edilir. Bu şekilde cihazın fiziksel imajı alınmış olmaktadır.

22. Yapılan işlemler neticesinde arıza giderilerek veriye ulaşıldı mı?

Her ne kadar arıza giderilse de cihaz içindeki veriye ulaşılamadıysa, yapılan işlemler raporlanarak tutanak altına alınıp işlemin sonlandırılması gerekmektedir.

23. Adli bilişim yazılımları ile fiziksel imajı alınabiliyor mu?

Mobil cihaz adli bilişimin en temel hedefi sayılabilecek olan fiziksel imaj alındıysa işlemler tamamlanmış anlamına gelmektedir.

24. Adli bilişim yazılımları ile dosya sistemli ya da mantıksal imajı alınabiliyor mu?

Eğer fiziksel imaj alınamadıysa daha az miktarda ve daha yüzeysel veriye ulaşılmasını sağlayan diğer imaj alma yöntemleri denenir.

25. Adli bilişim yazılımında cihazın modeli destekleniyor mu?

Adli bilişim yazılımlarının imaj alma yöntemleri ve destekleri cihazdan cihaza değiştiğinden, destek verilen cihaz olmaması durumunda android

işletim sistemlerinin genel (generic) niteliklerinden imaj alma yönteminin denenmesi gerekmektedir.

26. Destekleyen farklı bir yazılım mevcut mu?

Her ne kadar adli bilişimde kullanılan yazılımların çoğu NIST gibi standartları haiz de olsa, tüm çözümleri kapsayan bir ürün bulunmamaktadır. Bu sebeple alternative yazılımların desteklerinin kontrol edilmesi gerekmektedir.

27. Cihaz piyasada sıkça bulunmayan Çin menşeili telefonlardan mı?

Cihazın piyasada bilinmeyen Çin menşeili bir cihaz olması, bu tip cihazlara özgü özel yazılımlara yoğunlaşılmasını gerektirmektedir.

28. İmajı alınması gereken SIM kart var mı?

Sim kart, da her ne kadar telefonun doğrudan bir parçası olmasa da bütünleyici parçası olup içerisinde veri barındırdığından imajı alınması gerekmektedir.

29. Pin veya Puk koruması var mı?

Şifreli olan sim kartların hatalı girilmesi durumunda kendini bloklamasından dolayı atak yapılamadığından, pin veya puk koruması imajı engelleyici unsurlardandır.

30. Pin veya Puk şifreleri elde mi?

Şifreli olması halinde şifrelerin temin edilmesi, olay yerindeyken tespitinin yapılması önem arz etmektedir.

31. Sim kart yerli bir operatöre mi ait?

Şifrelerinin olmaması durumunda, ülke egemenlik sınırları içerisindeki operatörlerden CMK Md. 134 kapsamında talebi yapılmalıdır.

32. İmajı alınması gereken hafıza kartı var mı?

Hafıza kartları da belirli bir kapasiteye sahip olduğundan kimi zaman cihazla birlikte kimi zaman tek olarak imajının alınması ve içerisindeki veriye erişilmesi gerekmektedir.

33. Hafıza kartı cihaz tarafından korumalı mı?

Bazı cihaz modellerinde üzerinde takılı bulunan hafıza kartını korumaya alarak, başka cihazla çalışmasını engelleyebilir. Bu durumlarda hafıza kartının imajı, cihaza takılı vaziyette olarak cihazla birlikte alınması gerekmektedir.

34. İmaj alındı mı?

Cihazın imajı alındıktan sonra, hash (veri özeti) değeri hesaplatılır, bu zamana kadar ki tüm işlemler tutanak altına alınır.

7.2. Mobil Cihaz Adli Bilişimden Kuralların Belirlenmesi

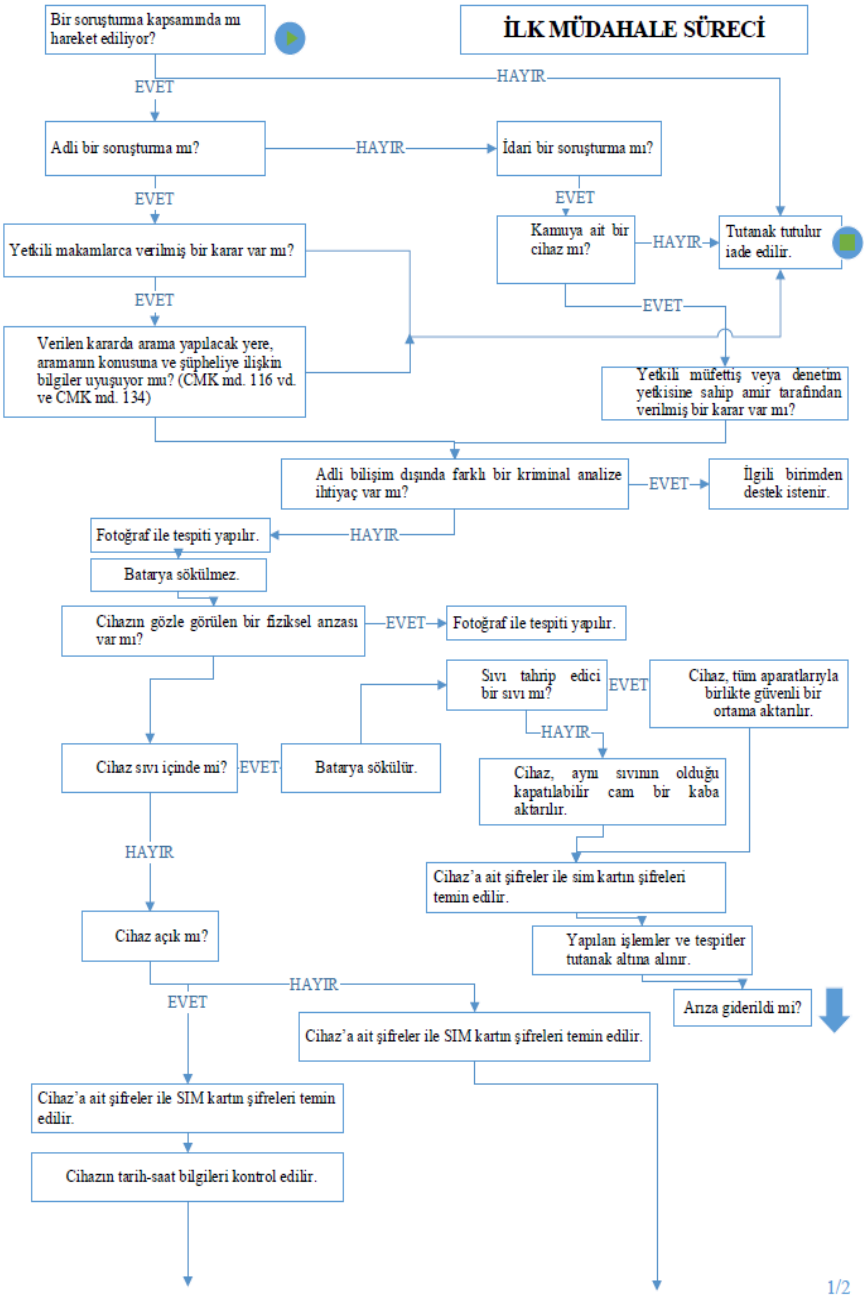
Uygulanacak kurallar belirlenirken günümüz şartlarındaki Türkiye Cumhuriyeti mevzuatı ve mevcut imkanlar dikkate alınmıştır. Adli bilişim personeline yapılacak işlemi nasıl gerçekleştireceği veya yukarıda sayılan yöntemlerin nasıl uygulanacağı değil, hangi işlemin en uygun olduğu yönünde tavsiye verecek şekilde planlanmıştır. Uygulanacak yöntemlerin detayları personelin kendi uzmanlığı olup, bunların bilgisayar sistemlerine aktarılmasına ilişkin bir öneri bulunmamaktadır.

Bu süreçler cihaza ilk müdahale ve imaj alma aşamalarından oluşmaktadır. Bütün süreçte toplamda 49 farklı soruyla mobil cihaz adli bilişimi süreçleri ele alınmış, bu sorular karşısında uygulanacak kurallar da iki farklı şekilde belirlenmiştir. Bu kuralların nasıl uygulanacağı konunun uzmanları tarafından belirlenecektir. Bu diyagramın belirlenmesinde kolluk kuvvetlerinin uygulamaları esas alınmıştır.

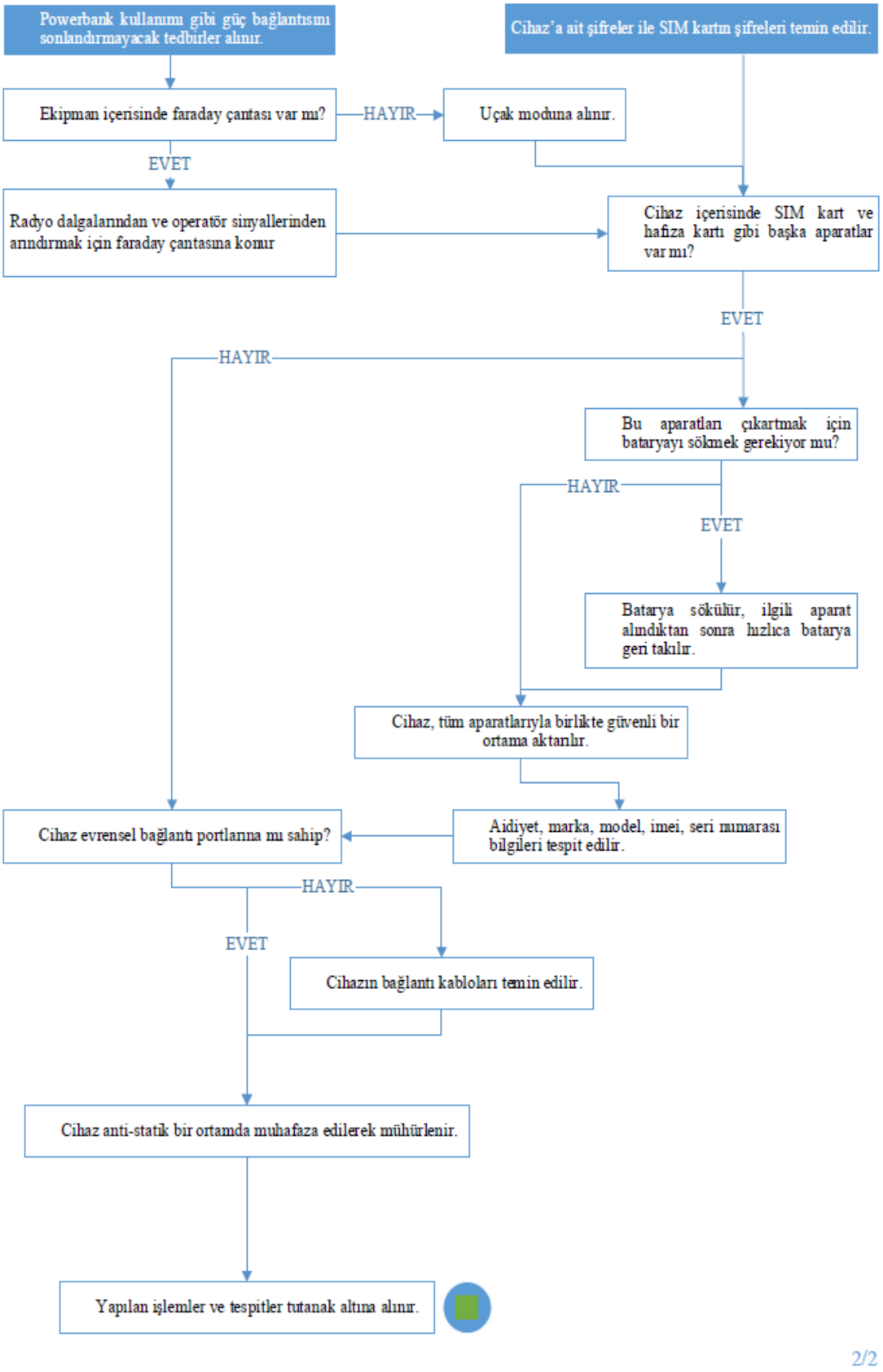
Mobil cihazların yapısı gereği, diyagramın iş akışının doğrusallığı sürekli olarak devam edememiştir. Bu sebeple bazı işaretler ile diyagramın uygulanabilir hale getirilmesi amaçlanmıştır. Bu kapsamda, soru-kural diyagramı içerisinde kullanılan mavi daire içerisindeki yeşil üçgen ile, önceki sorulardan ve verilmiş kurallardan bağımsız olarak sorulması gereken soruyu, mavi daire içerisindeki yeşil dikdörtgen ile, bu aşamadan sonra devam edilecek bir adımın olmadığı belirtilmiştir. Yatay mavi ok işareti ile o sorunun diyagramdaki daha önceki veya daha sonraki bir adımda sorulduğunu ancak soruya cevabın burada olduğu, yukarı ok işareti ile bu soruya cevabın daha yukarıdaki bir aşamada verildiği, aşağı ok işareti ile bu soruya cevabın daha aşağıdaki bir aşamada verildiği tanımlanmıştır.

7.2.1. Cihaza ilk müdahale

Cihaza ilk müdahale aşamasında sorulan on altı farklı soru için on yedi farklı kural tanımlanmıştır. Yetkilerin kontrolü sonucunda yapılacak işlemler, karşılaşılan duruma göre yapılacak işlemler ve ilk müdahale süreci tamamlandığında yapılacak işlemler Şekil 3 ve Şekil 4'te sıralanmıştır.



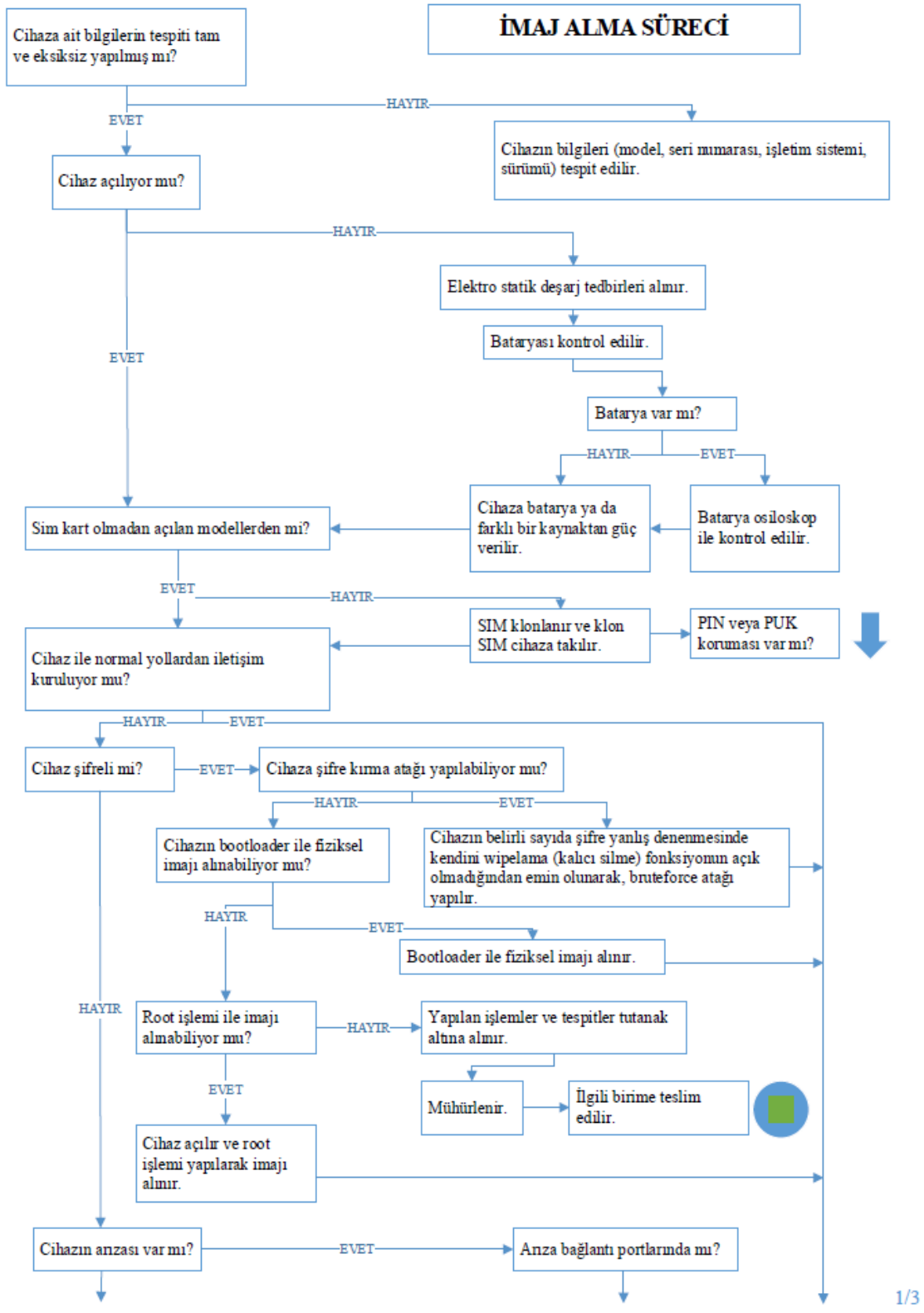
Şekil 3. Cihaza ilk müdahale süreci-1



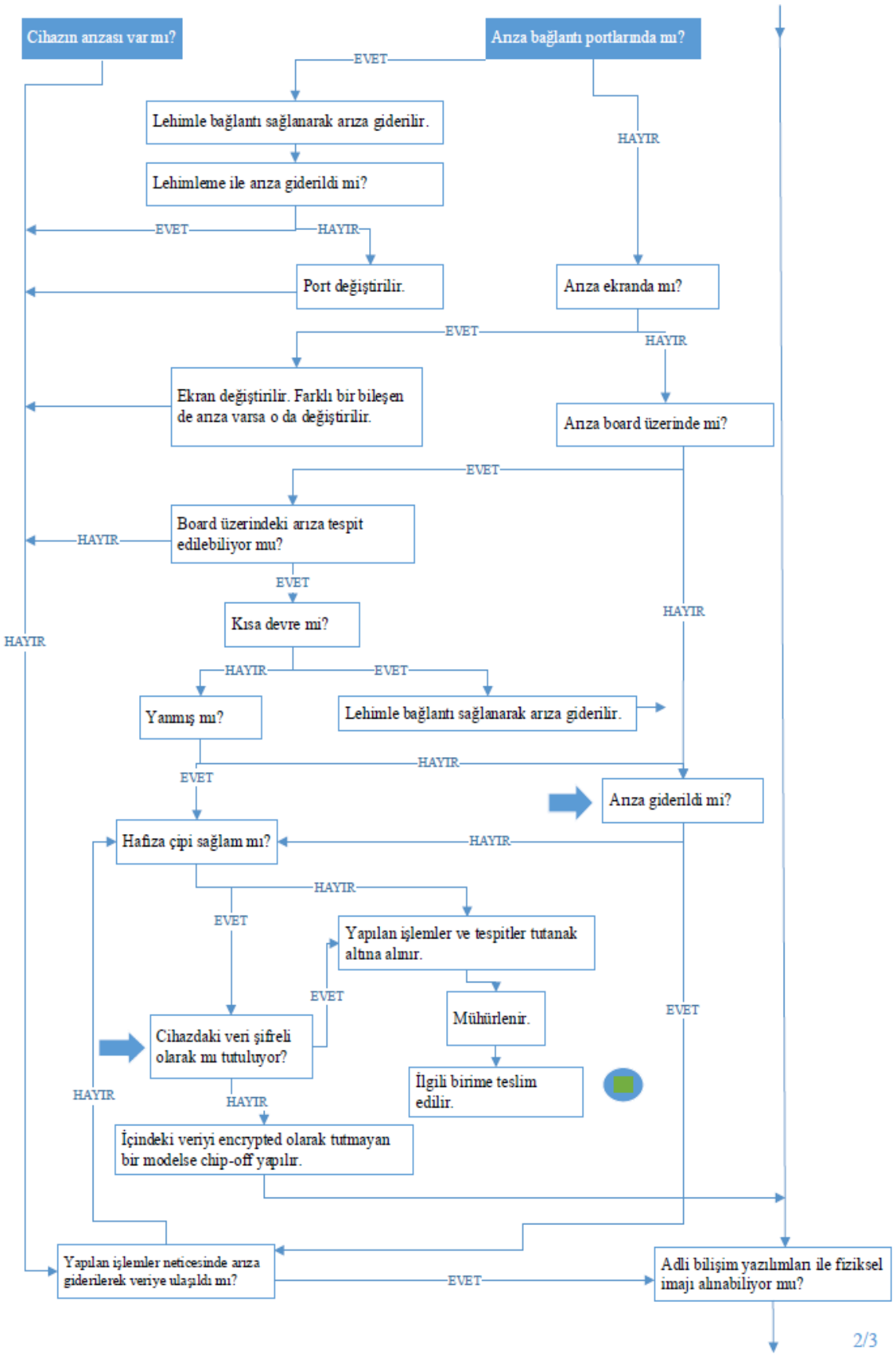
Şekil 4. Cihaza ilk müdahale süreci-2

7.2.2. İmaj alma

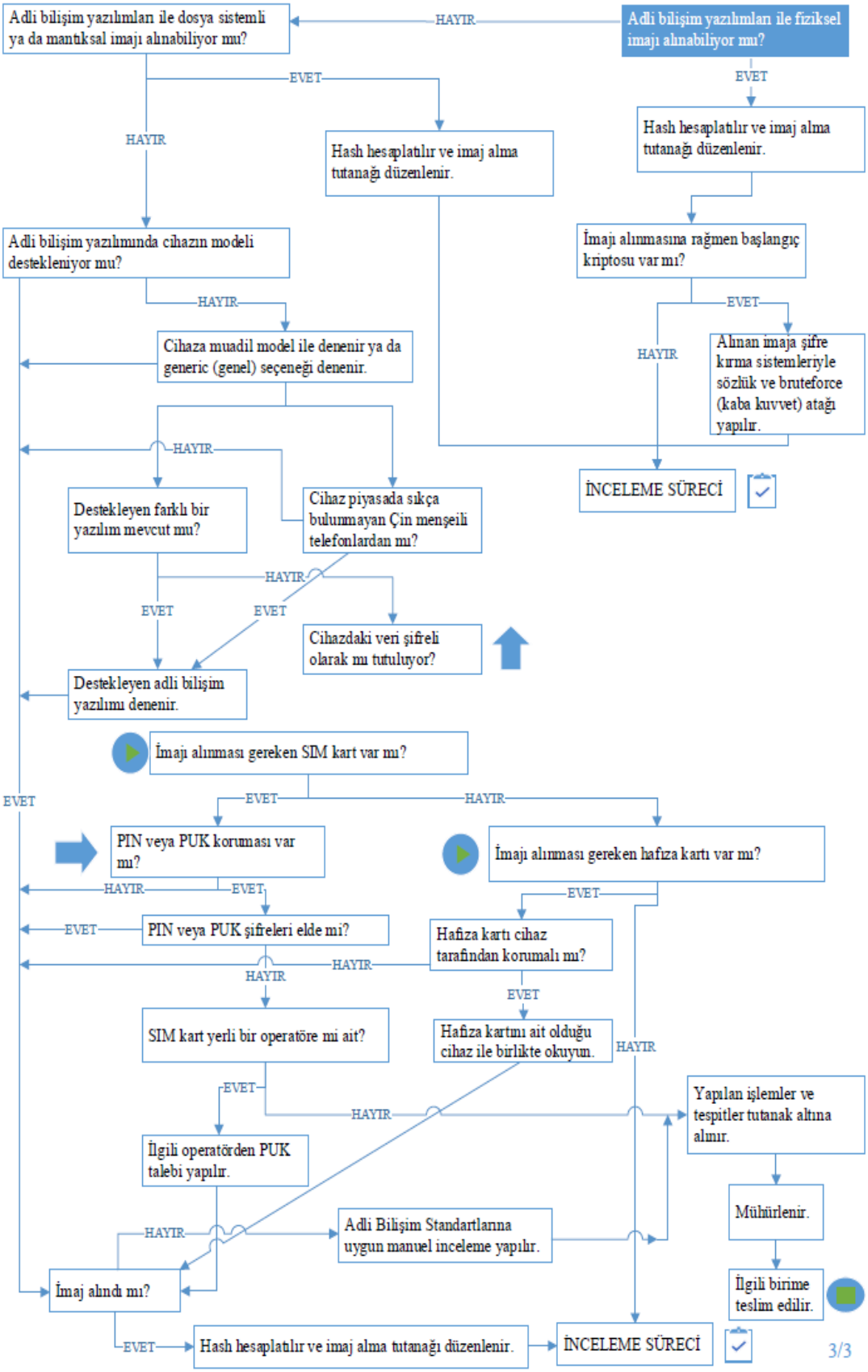
İmaj alma aşaması için hazırlanan otuz dört soruya 30 farklı kural belirlenmiştir. Bu aşama adli bilişimin en önemli adımı sayılabilir ve bu aşamada cihazın içindeki anlamlı veriye ulaşılması hedeflenmektedir. İmaj almaya ilişkin diyagramlar Şekil 5, Şekil 6 ve Şekil 7'de belirtilmiştir.



Şekil 5. İmaj alma süreci -1



Şekil 6. İmaj alma süreci -2



Şekil 7. İmaj alma süreci - 3

Bir karar destek siteminin uygulanması modeli olarak gün geçtikçe artan çeşitliliği, hızla değişen teknolojisi, karşılaşma sıklığı ve içinde barındırdığı veriler ile adli bilişim alanında önemli bir zorluk olarak karşımıza çıkan mobil cihazlardan delil elde etme aşaması ele alınmıştır.

Bu süreçler cihaza ilk müdahale ve imaj alma aşamalarından oluşmaktadır. Bütün süreçte toplamda 50 farklı soruyla mobil cihaz adli bilişimi süreçleri ele alınmış, bu sorular karşısında uygulanacak kurallar da 3 farklı şekilde belirlenmiştir. Bu kuralların nasıl uygulanacağı konunun uzmanları tarafından belirlenecektir. Bu diyagramın belirlenmesinde kolluk kuvvetlerinin uygulamaları esas alınmıştır.

VIII. MODELİN DOĞRULANMASI (VERIFICATION OF THE MODEL)

Modelin geçerliliği için, kamu kurumları, üniversite ve özel sektörden adli bilişim uzmanlarından modelin değerlendirilmesi istenmiştir. Modelin genel olarak geçerliliği ile ilk müdahale ve imaj alma aşamaları için ayrı ayrı değerlendirmeler gerçekleştirilmiştir.

8.1. İlk müdahale aşamasının değerlendirilmesi

İlk müdahale aşamasıyla ilgili olarak uzmanların hukuki açıdan bir problem olmadığı, uygulanacak adımların yeterli olduğu, cihazın imaj alınması sürecine etki edecek unsurlara yeterince önem verildiği, cihazın delil bütünlüğünü korumaya ilişkin unsurlara yeterince önem verildiği yönünde görüş birliğine vardıkları anlaşılmıştır.

İlk müdahale aşamasındaki potansiyel hataları azaltması ve ilk müdahale sürecini hızlandır beklendiği belirtilmiştir. İlk müdahale süreçlerinin uygulanabilmesi için daha fazla ayrıntıya gerek olmadığı yönünde hakim görüş oluşmuştur. Bir uzman, ayrıntılara ilişkin özellike adli bilişim işlemlerine yeni başlamış personelin kullanımı için video, resim vb. içeren ek bir dökümantasyon olmasının faydalı olacağını belirtmiştir.

8.2. İmaj alma aşamasının değerlendirilmesi

Hukuki açıdan ele alındığında bir problem teşkil etmeyeceği belirtilmiştir. Model önerisinde belirtilen imaj alma işleminde uygulanacak adımların yeterli olduğu belirtilmiştir. Cihazın imaj alınması sürecine etki edecek unsurlar ile cihazın delil bütünlüğünü korumaya ilişkin unsurlara yeterince önem verildiği yönünde görüş birliğine varıldığı anlaşılmıştır. Bu model önerisinin imaj alma aşamasındaki potansiyel hataları azaltması ve imaj alma sürecini hızlandıracağının beklendiği belirtilmiştir.

İmaj alma süreçlerinde uygulanabilmesi için daha fazla ayrıntıya gerek olmadığı yönünde hakim görüş oluşmuştur. Bir uzman, imaj alma sürecinin ayrıntılara ilişkin uzman olmayan personelin kullanımını kolaylaştıran görsel yönden desteklenmiş ek bir dökümantasyon olmasının faydalı olacağını belirtmiştir.

İmaj alma aşamasında uygulanacak adımların yeterli olduğu görüşünde de olsa, bir uzman imajı alınacak cihazın işletim sistemleri sürümlerinin de kontrol edilmesi gerektiği belirtmiştir. Ayrıca rooting gibi ileri düzey yazılımsal müdahalelerin sürece dahil edilmesinin faydalı olacağı görüşünü bildirmiştir. İmaj alma işleminin başarısız olması durumunda işlemlerin sonlandırılması yoluna gidilmekteyken; son bir yöntem olarak cihazın adli bilişim standartlarına göre manuel inceleme ile delil tespiti yapılabileceği de belirtlmiştir.

8.3. Modelin genel değerlendirilmesi

Uzmanların genel görüşü mobil cihaz adli bilişim süreçlerini yansıtıldığı ve başarılı şekilde karar verme süreçlerinin anlaşıldığı yönündedir. Diyagramın anlaşılırlığı ile ilgili de genel görüş olumlu olmakla birlikte, bazı uzmanlar daha anlaşılır hale getirilmesinin faydalı olacağını belirtmiştir.

Önerilen modelin mobil cihaz adli bilişimi uygulayıcısına katkı sağlayacağı konusunda görüş birliği bulunmaktadır. Ancak her seviyede mobil cihaz adli bilişimi uygulayıcısı için yeterli sadelikte olmadığını vurgulamışlardır. Bazı işlemlerin uygulanabilmesi için temel düzeydeki mobil cihaz adli bilişimi uygulayıcısı için eğitim verilmesinin gerekebileceği vurgulanmıştır. Ayrıca temel düzeydeki mobil cihaz adli bilişimi uygulayıcısı için resim veya video gibi bazı görsellerle dökümantasyonun takviye edilmesinin faydalı olacağı görüşü de bir uzman tarafından sunulmuştur.

8.4. Değerlendirme

Modelin mobil cihaz adli bilişimine katkı sağlayacağı anlaşılmıştır. Ancak bunun daha sağlıklı işlemesi için uzmanlardan gelen öneriler değerlendirilmiştir. Bu kapsamda belirtilen modelin anlaşılırlığı, uygulayacak personelin yeterliliği, imaj alınamama durumunda manuel inceleme yapılabileceği, işletim sistemi sürümlerinin de kontrol edilmesi gerektiği ve

rooting işlemlerinin de belirtilmesi gerektiği konularında öneriler gelmiştir.

Modelin anlaşılırlığı ile ilgili olarak diyagram mobil cihaz adli bilişimi faaliyeti işinin doğası gereği çok fazla bağlantı barındırmaktadır. Bu bağlantıların ilişkisi kimi zaman doğrusal olmadığından farklı işaretlerle bu ilişki kurulmaya çalışılmıştır. Ancak bu öneriye istinaden diyagramın doğrusal akışı dışındaki iş akışlarını tanımlamakta kullanılan işaretlere ilişkin açıklmaya ilave olarak yer verilmiştir.

Uygulayacak personelin yeterliliği ile ilgili olarak ise, personelin bu işlemleri yerine getirmesi için belirli bir teknik bilgi birikimine sahip olması gerektiği aşikardır. Ancak personelin yetiştirilmesi, gereken eğitimin nitelikleri bu çalışmanın konusu olmadığından, personelin eğitimi göz ardı edilmiştir. Bu işlemleri uygulayacak personelin yeterli teknik bilgi birikimini haiz olduğu kabul edilmiştir.

İmaj alınmama durumunda manuel inceleme yapılabileceği önerisi ile ilgili olarak; çalışma ilk müdahale ve imaj alma aşamalarıyla sınırlı olarak yapılmıştır. Manuel inceleme işlemi, imaj alma sonrası gerçekleştirilen inceleme ve raporlama alanlarında kaldığı değerlendirildiğinden çalışmanın başında göz ardı edilmiştir. Ancak öneriyle tekrar değerlendirilmiş ve manuel inceleme işlemi esası itibariyle bir inceleme işlemi olsa da, imaj alma işleminin başarısız olması durumunda başvurulan bir yöntem olduğundan, imaj alma işlemini yürüten personelin de bu işlem esnasında dikkate alması gereken bir adımdır. Bu sebeple adli bilişim standartlarına uygun olarak manuel incelemenin yapılması gerektiği modele işlenmiştir.

İşletim sistemlerinin kontrol edilmesi ve rooting işleminin uygulanması önerisiyle ilgili olarak, bu işlemler mobil cihaz adli bilişimi açısından önem arz etmektedir. Ancak imaj alma işleminde kullanılan mobil cihaz adli bilişimi yazılımları, imaj alma işlemlerini gerçekleştirirken işletim sistemlerini, çip setlerini, yazılımın root atılması ihtiyacı gibi unsurları değerlendirildiğinden bu hususlar, mobil cihaz adli bilişim yazılımlarının desteği altında çözüme kavuşturulmasının gerektiği beklenmektedir. Ayrıca desteklenen sürümler ve root ihtiyacı yazılımların güncellemelerine göre değişiklik gösterebileceğinden, model önerisinin genel geçer niteliğini olumsuz etkileme ihtimalinden dolayı bu önerilere ilave olarak yer verilmemiştir.

IX. SONUÇLAR (CONCLUSIONS)

Genel olarak karar verici uzman kişilerin kararlarını vermede daha etkin ve verimli olmalarını sağlamak amacıyla geliştirilmiş olan bilgisayar destekli araçlar veya yazılımlar olarak tanımlanabilen karar destek sistemlerinin [19] adli bilişim alanında mobil cihaz adli bilişim sürecinde nasıl entegre olabileceğine ilişkin bir çalışma gerçekleştirilmiştir.

Bu çalışmayla gün geçtikçe artan çeşitliliği, hızla değişen teknolojisi, karşılaşma sıklığı ve içinde barındırdığı veriler ile adli bilişim alanında önemli bir zorluk olarak karşımıza çıkan mobil cihazlardan delil elde etme aşamasında karar destek sisteminin uygulanmasına ait bir model önerisi sunulmuştur. Mobil cihaz adli bilişiminde en sık karşılaşılan durumlara ilişkin hazırlanan soru-kural akış diyagramı ile mobil cihaz adli bilişimi ile ilgilenen personelin, en doğru kararı en kısa sürede vermesi ve verdiği kararları sonuçlarıyla birlikte kaydederek, sistemin daha efektif hale getirilmesi amaçlanmıştır.

Bu kapsamda mobil cihaz adli bilişimine ilişkin 50 farklı soru oluşturulmuş ve bu sorular karşısında uygulanacak kurallar geliştirilmiştir. Sorular cihaza ilk müdahale ve imaj alma aşamalarına ayrılarak sorulmuştur. Özellikle cihaza ilk müdahale aşaması diğerlerinden farklı olarak olay yerinde uygulanması gereken protokolleri kapsamaktadır. Bu sebeple aşamalara ayrıştırabilen bu soru-kural akış diyagramı, teknik birimler dışında olay yerinde delillere el koyan kolluk birimleri tarafından da özellikle cihaza ilk müdahale aşaması uygulanabilmesi mümkündür.

Bu model önerisinin doğrulanmasıyla ilgili olarak, üniversitelerde, kamu kurumlarında ve özel sektörde görev yapan adli bilişim uzmanlarıyla görüşmeler gerçekleştirilmiştir. Bu modelin mobil cihaz adli bilişimi süreçlerini yansıttığı, karar vermeyle ilgili süreçlerin anlaşıldığı, mobil cihaz adli bilişimi uygulayıcısı için katkı sağlayacağını belirtmişlerdir. İlk müdahale ve imaj alma süreçlerini hızlandırmasının ve potansiyel hataların azaltılmasının beklendiği konusunda görüş bildirilmiştir. Ayrıca Türkiye'deki adli bilişim uygulamasında karşılaşılan sorunlardan olan hukukilik ve delil bütünlüğü konularına gereken önemin verildiği de vurgulanmıştır.

Uzmanların üzerinde durduğu unsurlardan biri de tecrübeli personelin süreci rahatça işletebileceği iken, yeni başlayan personelin resim veya video

gibi görsellerle desteklenmesinin ve modelin anlaşılırlığının artırılmasının faydalı olacağıdır. Ayrıca temel düzeydeki mobil cihaz incelemecisinin bazı iş ve işlemler uygularken eğitimlerle desteklenmesi gerektiği yönünde görüş bildirilmiştir. Ancak personelin eğitimi bu çalışmanın konusu olmadığından, bu öneriler göz ardı edilmiştir.

Ancak anlaşılır hale getirilmesiyle ilgili açıklamalar eklenmiş ve manuel inceleme yapılmasıyla ilgili olarak da model önerisinde yer verilmiştir. İmaj alınamaması durumunda adli bilişim standartlarına uygun manuel inceleme yapılmasına ilişkin diyagrama bir adım eklenmiştir.

Teknik açıdan ihtimallerin binlerce olduğu mobil cihaz adli bilişimi süreçlerinde, anlaşılır bir model sunulabilmesi için bazı unsurlar göz ardı edilmiştir. Olay yeriyle ilgili mobil cihazın dışındaki unsurlar bu süreç dışında tutulmuştur. Ayrıca yazılımsal işlemlerle ilgili olarak adli bilişim yazılımlarının sunduğu imkanlarla sınırlı kalınmıştır. Box cihazları gibi üçüncü parti yazılımlarla cihazın tüm admin haklarına erişilip cihazın her türlü sistem alanına erişilmesi mümkünken, önerilen modelde uzmanın adli bilişim yazılımının sunduğu kadarıyla rooting işlemini gerçekleştirmesi öngörülmüştür. Ayrıca modeli uygulayacak personelin, modelde bahse konu işlemleri de nasıl uygulayacağını biliyor olması gerekmektedir. İşlemi yapacak mobil cihaz adli bilişimi uygulayıcısının konudaki bilgi eksiliğine ragmen işlem yapma ihtimali de göz ardı edilmiştir.

Özetle bu önerilen modelin, yüksek iş hacmiyle adli bilişim faaliyeti yapan kamu veya özel laboratuvarlarda uygulanması halinde maliyet ve zaman tasarrufu sağlanması hedeflenmektedir. Ayrıca olay yerinde delil toplayan kolluk görevliler ve bilirkişiler için de kullanılmasının hem ülke geneli adli bilişim açısından iş ve işlemlerin standarda kavuşmasına hem de belirlenmiş kurallar sayesinde olası potansiyel riskleri azaltmaya ve sorunlar karşısında hızlı çözüm üretebilmesine fayda sağlayacaktır.

KAYNAKLAR (REFERENCES)

[1]. M. Scanlon and M. T. Kechadi. “Digital Evidence Bag Selection for P2P Network Investigation”. In Proceedings of the 7th International Symposium on Digital Forensics and Information Security (DFIS-2013), pages 307–314. Springer, Gwangju, South Korea, 2014.

[2]. D. Lillis, et al. “Current Challenges and Future Research Areas for Digital Forensic Investigation”. arXiv preprint arXiv:1604.03850, 2016.

[3]. “Soylu, incelenen dijital materyal sayısını açıkladı: 2018'de, ortalama 45 binden, 631 bin 233'e yükseldi” [Online]. Available: https://t24.com.tr/haber/soylu-incelenen-dijital-materyal-sayisini-acikladi-2018de-ortalama-45-binden-631-bin-233e-yukseldi,749982 Yayın Tarihi: 16.11.2018 Erişim Tarihi: 06.12.2020

[4]. K. Say, “Bilişim Suçlarında Olay Yeri İncelemesinin Hukuki Boyutu”, L. Bayram (ed.), Ses Görüntü ve Data İncelemeleri içinde (251-260), Adalet Yayınevi, Ankara, 2008, s. 259.

[5]. Y. Başlar, “Adli Bilişim Sürecinde Karşılaşılan Sorunlar ve Çözüm Önerileri”. 2019.

[6]. İ. Çiçek, “Ülkemizde Adli Bilişim Laboratuarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları”, Yayınlanmamış Yüksek Lisans Tezi, Haliç Üniversitesi Fen Bilimleri Enstitüsü, 2008, s. 14.

[7]. O. Değirmenci, “Ceza Muhakemesinde Sayısal (Dijital) Delil”, Seçkin Yayıncılık, Ankara, 2014, s. 121.

[8]. K. Say, “Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi”, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2006.

[9]. Ş. Sağıroğlu, M. Karaman, “Adli Bilişim”, Teletapi Haberleşme ve Bilişim Teknolojileri Dergisi, 2012, S. 203, s. 67.

[10]. Ö. Özbey, “Adli Bilişim ve Sayısal Deliller (5271 sayılı CMK’nın 134. maddesi)”, Yargıtay Dergisi, 2010, C. 36, S. 3, ss. 61-126

[11]. M. Faheem, M. T. Kechadi, N. Le-Khac, “The State of the Art Forensic Techniques in Mobile Cloud Environment: A Survey, Challenges and Current Trends”, International Journal of Digital Crime and Forensics, Vol. 7, Issue 2, Pg.1-19, April 2015

[12]. E. Ndarake, “Computer Forensics Investigation (Step by step guide)”, 2013 https://baixardoc.com/documents/computer-forensics-investigation-techniques-effiong-effiong--5c9d2edf8ef6d Yayın Tarihi: 2013 Erişim tarihi: 20.04.2021

[13]. T. Henkoğlu, “Adli bilişim: Dijital delillerin elde edilmesi ve analizi”, Pusula, 2014.

[14]. A. H. Ekizer, Adli Bilişim. Erişim adresi: https://www.ekizer.net/adli-bilisim-computerforensics/ , 2014. Yayın Tarihi: 2014 Erişim Tarihi: 18/4/2021

[15]. H. Aydoğan, “Adli Bilişimde Yeni Elektronik Delil Elde Etme Yöntemleri” Yayınlanmamış Yüksek Lisans Tezi, Ankara, Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2009.

[16]. H. A. Doğanay, "Mobil Adli Bilişiminin Önemi Bağlamında Hukuki Süreç ve Delil Zinciri Kavramı ile Yeni Nesil Mobil Cihazların İncelenmesinde Karşılaşılan Güncel Zorlukların Değerlendirilmesi", Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimler Enstitüsü, 2019.

[17]. I. L. Lin, H. C. Chao, ve S. H. Peng, "Research of digital evidence forensics standard operating procedure with comparison and analysis based on smart phone". In 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 386-391), 2011.

[18]. H. Çakır ve M. S. Kılıç, "Mobil Cihazların İncelenmesi" Adli Bilişim ve Elektronik Deliller 1. Baskı, Ankara, 2014, 373-409.

[19]. W. Jansen, R. Ayers, ve S. Brothers, "Guidelines on Mobile Device Forensics". NIST Special Publication 800-101 Revision 1, Springfield, VA, USA, 2014.

[20]. U. Akalın, "Mobil Cihazlarda Adli Bilişim Çalişmalarina Yönelik Bir Model Önerisi" Gazi Üniversitesi Yayınlanmamış Yüksek Lisans Tezi, 2016.

[21]. A. Zareen, S. Baig, "Mobile Phone Forensics Challenges, Analysis and Tools Classification", in the Proceedings of the 2010 International Workshop on Systematic Approaches to Digital Forensic Engineering, May 2010, pp. 47-55, 2010.

[22]. "The Digital Investigator's Resource for Mobile Device Forensic Information" [Online]. Available: https://www.mobileforensicscentral.com/mfc/products_software.asp Erişim Tarihi: 03.12.2020

[23]. "XRY" [Online]. Available: https://www.msab.com/products/xry/ Yayın Tarihi: 2020 Erişim Tarihi: 03.12.2020]

[24]. "Cellebrite" [Online]. Available: https://www.cellebrite.com/en/home/ Yayın Tarihi: 2020 Erişim Tarihi: 02.12.2020

[25]. "Magnet Forensics" [Online]. Available: https://www.magnetforensics.com/axiom-smartphone/#leader Erişim Tarihi: 02.12.2020

[26]. "Oxygen Forensics" [Online]. Available: https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective Erişim Tarihi: 02.12.2020

[27]. [27] "Paraben Corporation" [Online]. Available: https://paraben.com/ Yayın Tarihi: 2020 Erişim Tarihi: 02.12.2020

[28]. "MOBILEdit" [Online]. Available: https://www.mobiledit.com/mobiledit Yayın Tarihi: 2020 Erişim Tarihi: 02.12.2020

[29]. "BlackBag Technologies" [Online]. Available: https://www.blackbagtech.com/software-products.html Yayın Tarihi: 2020 Erişim Tarihi: 02.12.2020

[30]. "Andriller" [Online]. Available: https://www.andriller.com/ Yayın Tarihi: 2020 Erişim Tarihi: 02.12.2020

[31]. "Katana Forensics" [Online]. Available: https://katanaforensics.com/lantern.php Yayın Tarihi: 2020 Erişim Tarihi: 02.12.2020

[32]. B. Bilgen, "Kurumsallaşma Üzerine Bir Karar Destek Sistemi Oluşturulması -Türk İnşaat Sektöründe Örnek Uygulama (Kural Tabanlı Kds Modeli)" Yayımlanmamış Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, İstanbul Teknik Üniversitesi, İstanbul, 2011.

[33]. E. Turban, Decision Support Systems and Expert Systems: Management Support Systems, 2nd ed., Macmillan Publishing Company, 6-30, 105-131, New York, 1990.

[34]. H. Gökçen, "Yönetim Bilgi Sistemleri", Palme Yayıncılık, Ankara, 2007.

[35]. E. Güvenç, "Zeki Karar Destek Sistemi Kullanılarak Muğla Sıtkı Koçman Üniversitesi Uzaktan Eğitim Öğrencilerinin Ders Performanslarının Değerlendirilmesi" Yayımlanmamış Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Muğla Sıtkı Koçman Üniversitesi, Muğla, 2018.

[36]. M. A. Tokaylı, "Zaman Pencereli Araç Rotalama Problemi İçin Karar Destek Sistemi," Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Gazi Üniversitesi, Ankara, 2005.

[37]. Türkiye Bilişim Derneği (TBD), Kamuda Karar Destek Sistemlerinin Kullanımı ve Bir Model Önerisi, Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği, Kamu Bilişim Platformu XII, Antalya, 2010.

[38]. N. Demirci, Karar Destek Sistemlerinin Bir Durum Çalışmasına Uygulanması. Yayımlanmamış Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Trakya Üniversitesi, Edirne, 2012.

[39]. N. M. M. Noor, A. F. Ghazali and Y. M. Saman "Decision Support Systems for Forensic Science in Crime Investigation" International Journal of Digital Content Technology and its Applications, 2013, 7.16: 26.

[40]. N. A. Mutawa, J. Bryce, Virginia N.L. Franqueira, A. Marrington, J. C. Read, Behavioural Digital Forensics Model: Embedding Behavioural Evidence Analysis into the Investigation of Digital Crimes Digital Investigation, Volume 28, Pp 70-82, 2019.

[41]. H. A. Doğanay, "Mobil Cihaz Adli Bilişiminde Karşılaşılan Güncel Zorluklar ve Delil Zinciri", Legem Yayıncılık, 2020.

BULUT BİLİŞİM GÜVENLİĞİ ETKİ DÜZEYLERİNİN DEĞERLENDİRİLMESİ

Buse Uslu[1], Tamer Eren[2*], Evrencan ÖZCAN[3]

[1,2,3] Kırıkkale Üniversitesi, Endüstri Mühendisliği Bölümü, Mühendislik ve Mimarlık Fakültesi, Kırıkkale

buseuslu03@gmail.com, tamereren@gmail.com, evrencan.ozcan@kku.edu.tr

ÖZET

Bulut bilişim, kullanıcıya uzak bir sunucu üzerinden internet aracılığı ile esnek zamanda erişim sağlama, veri depolama, veri transferi işlemlerini yapmasına imkân sağlamaktadır. Bu tür imkânlarının yanında çoklu kullanım, ölçeklenebilirlik, esneklik ve kullandıkça öde politikasına sahip olması şirketler için önemli hale gelmiştir. Bulut bilişimin sunduğu avantajların yanı sıra kullanıcıların neredeyse tüm işlerini dijital bir ortama aktarması ve depolama sağlaması, sahip oldukları gizli bilgilere erişmek isteyen diğer kullanıcıların saldırı risk faktörünü de ortaya çıkarmıştır. Bulut hizmet sağlayıcıları ve kullanıcıları güvenlik üzerine sıkı tedbirler almalıdırlar. Bu süreçte bulut hizmet sağlayıcıları güvenlik üzerine tedbirler alsa da kullanıcıların da tedbirler alması gereklidir. Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Ofisi, kullanıcılar için bulut bilişim güvenliği çerçevesinde 14 genel güvenlik tedbirini açıklamıştır. Şirketler seçim süreçlerinin karmaşıklığı ve bu süreç kapsamında oluşabilecek fazla maliyet ve zaman gibi operasyonel engelleri en az seviyede tutmak için değerlendirme faktörlerini önceliklerine göre sıralamalıdırlar. Bu çalışmada, şirketlerin bulut hizmet seçimi sürecinde 14 genel güvenlik tedbirini hangi öncelikle dikkate alması gerektiğinin belirlenmesi amaçlanmıştır. Bulut bilişim alanında uzman 5 kişinin görüşleri doğrultusunda çok kriterli karar verme yöntemlerinden AHS (Analitik Hiyerarşi Süreci) ve BAHS (Bulanık Analitik Hiyerarşi Süreci) yöntemleri ile öncelik değerleri elde edilmiş ve değerlendirilmiştir.

***Anahtar Kelimeler*—** Bulut bilişim, bulut bilişim güvenliği, çok kriterli karar verme, analitik hiyerarşi süreci, bulanık analitik hiyerarşi süreci

Evaluation of Cloud Computer Security Effect Levels

ABSTRACT

Cloud computing allows the user to access, store and transfer data in a flexible time via the internet over a remote server. It has become important for companies to have multi-use, scalability, flexibility and pay as you go policy, as well as such opportunities. Besides these advantages offered by cloud computing, transfer of almost their work to a digital environment and provides storage has also revealed the attack risk factor of other users who want to access the confidential information they have. Cloud service providers and users should take strict security measures. In this process, although cloud service providers take measures on security, users must take precautions in their users. Digital Transformation Office of the Presidency of Republic of Turkey has announced the 14 general security measures in the framework of cloud computing security for users. Companies should prioritize the evaluation factors in order to minimize the operational obstacles such as the complexity of the selection processes and the excess cost and time that may occur during this process. In this study, it is aimed to determine which priority companies should consider 14 general security measures in the cloud service selection process. In line with the opinions of 5 experts in the field of

cloud computing, priority values were obtained and evaluated with multi-criteria decision making methods, Analytical Hierarchy Process and Fuzzy Analytical Hierarchy Process methods.

Keywords— Cloud computing, cloud computing security, multi criteria decision making, analytical hierarchy process, fuzzy analytical hierarchy process

I. GİRİŞ (INTRODUCTION)

21. yüzyılda verilerin sanal ortam aracılığı ile erişim sağlama, depolama ve aktarma gibi durumlar için yaygın kullanılması, bulut bilişim alanlarında gelişime yol açmıştır. Şirketlerin ve bireysel kullanıcıların neredeyse tüm işlerini dijital bir ortama aktarması ve depolama sağlaması, sahip oldukları gizli bilgilere erişmek isteyen diğer kullanıcıların saldırı risk faktörünü de ortaya çıkarmıştır. Sahip olunan veri depolama alanlarına saldırı faktörünün gerçekleşmemesi için bulut hizmeti sunan şirketler güvenlik üzerine sıkı tedbirler almaktadır [1, 2]. Bu doğrultuda bulut hizmet kullanıcılarının bulut bilişim güvenliği çerçevesinde aldıkları tedbirlerin önem düzeyleri belirlenerek etki düzeyi yüksek bulut bilişim güvenlik aşamaları belirlenmelidir.

Bulut bilişimin sağladığı avantajlar, her geçen gün daha çok şirketin bilgi teknolojisi uygulamalarını ve verilerini buluta taşımasına yol açmaktadır. Bulut bilişim sayesinde, şirketler, bilgi teknolojileri altyapısının yönetimi ve işletilmesini başka sunucudan temin ederek daha düşük maliyet ve daha az işgücünden yararlanabilmektedir [3]. Ayrıca bulut bilişim teknolojisinin sunduğu özelliklerin hepsini satın almak ya da kiralamak yerine şirketler bulut hizmet modeli ve tipini ihtiyaçlarına göre şekillendirilebilmektedirler.

Bulut bilişimin etkin kullanıma sahip olması, günlük hayatın her alanına girmesine neden olmuştur. Şirketlerin dijital ortamlara dâhil olması, literatürde yapılan çalışmalara yön vermesi ve bulut bilişime olan bu ilgi devlet teknoloji ofisinin de dikkatini çekmiştir.

Bulut bilişimin sunduğu birden fazla faktörün olması ve her geçen gün bu faktörlerin artması, bulut bilişim seçim süreçlerinde karmaşıklığa ve kritik önem faktörlerinin belirlenmesinde sorunlar yaşanmasına sebep olmaktadır. Bu durumları ortadan kaldırma amacı ile literatürde çok kriterli karar verme yöntemleri kullanılarak faktörlerin önceliklendirilmesi ile ilgili yapılan çalışmalar bulunmaktadır.

Literatürde bulut bilişim ile ilgili çalışmalar incelendiğinde, farklı sektör ve alanlarda bulut bilişim hizmet sağlayıcı seçiminde etkili olan CPU kullanımı, hizmet, güvenirlilik, veri hızı, müşteri memnuniyeti, maliyet, kullanılabilirlik, güvenlik, ölçeklenebilirlik, birlikte çalışabilirlik, adapte olabilirlik, hafıza kullanımı, tepki süresi, işlem hızı, veri merkezi konumu, taşınabilirlik, uygunluk, şeffaflık ve ağ gecikme süresi gibi faktörlerin tespit edildiği ve bu faktörlerin çok kriterli karar verme yöntemleri kullanılarak ve önem dereceleri belirlenerek sıralamalar elde edildiği görülmektedir.

Afify vd. [4] bulut hizmet seçimi için literatürde yapılan yöntemleri inceleyerek etkin hizmet tanımlama modeli, keşif ve seçim mekanizmalarına sahip eksiksiz bir sistemin var olması gerektiğini vurgulamışlardır. Böylelikle, kullanıcıya işlevsel ve işlevsel olmayan gereksinimlerini karşılayan en iyi SaaS hizmet seçimi için anlamsal tabanlı bir SaaS seçim sistemini önermişlerdir. Zheng ve Xu [5] belirledikleri 3 hizmet sağlayıcının güvenlik ve gizlilik, işletim sistemine olan uyumluluğu ve kullanılabilirlik kriterlerini bulanık çok nitelikli karar verme yöntemlerinden biri olan üçgen sezgisel bulanık sayılar (TIFN) yöntemi kullanarak değerlendirmişlerdir. Çalışma sonucunda üçgensel sezgisel bulanık sayılar için yeni bir sıralama yaklaşımını önermişlerdir.

Garg vd. [6] belirledikleri hizmet sağlayıcıları arasında en iyi seçimi yapmak için işlevsel olmayan gereksinimlere (NRF) dayalı ve AAS ve TOPSIS (Technique for Order Prefence by Similarity To An Ideal Solutıon) yöntemi tabanlı TrAdeCIS yöntemini uygulamışlardır. Uygulama sonucunda TrAdeCIS yöntemini önermişlerdir. Khowfa ve Silasai [7] bulut hizmet sağlayıcı seçiminde QoS özelliklerine uygun değerlendirmeler yapabilmek için çalışma kapsamında tepki süresi ve maliyeti, maliyet ve tepki süresi, güvenlik ve maliyet, güvenlik ve tepki süresi ikili belirlemişlerdir. En

uygun bulut hizmet sağlayıcı seçimi için ise AHS yöntemini kullanmışlardır.

Khurana ve Bawa [8] verimlilik, kullanılabilirlik, güvenilirlik, tepki süresi kriterlerini Microsoft Azure, Amazon ve Rackspace bulut hizmet sağlayıcıları arasındaki etki düzeylerini belirlemişler ve SLA (hizmet seviyesi anlaşması) tabanlı sıralamasını yapmışlardır. Çalışmada sundukları bulut hizmet aracı programını ile bulut hizmet sağlayıcı seçiminde kaliteli bir sıralama elde etmişlerdir. Al-Faifi vd. [9] bulut hizmet sağlayıcı seçiminde etkili olan hafıza kullanımı, tepki süresi, maliyet ve CPU kullanımı kriterlerinin AAS (Analitik Ağ Süreci) ve DEMANTEL (The Decision Making Trial and Evaluation Laboratory) yöntemleri ile önceliklerini belirlemişlerdir. K-means algoritması ile bulut hizmet sağlayıcıları kümelendirilmiştir.

Sohaib vd. [10] bulut hizmetlerin sunduğu özellikleri 3 ana kriter ve 12 alt kriter olarak belirlemişlerdir. Bulut hizmet modelleri üzerindeki kriter etkileri TOPSIS yöntemi ile değerlendirilmiştir. Teknoloji, organizasyon ve çevre ana kriterlerinin SaaS, PaaS ve IaaS bulut hizmet türlerine etkilerini belirlemişlerdir. Uslu vd. [11] literatür taraması ve uzman görüşler doğrultusunda bulut hizmet sağlayıcısı seçiminde etkili olan kriterleri 5 ana ve 17 alt kriter şeklinde belirlemişlerdir. Belirlenen kriterlerin etkinlik düzeyleri uzmanların değerlendirmeleri ile AAS yöntemi kullanılarak tespit edilmiştir. Uslu vd. [12] çalışmasında ise kriterleri eşit ve Uslu vd. [11] çalışmasındaki AAS yönteminde elde edilen ağırlıklar kullanılarak 6 bulut hizmet sağlayıcısını TOPSIS ve PROMETHEE yöntemleri kullanarak sıralamalar karşılatırmışlardır. Devi ve Shanmugalakshmi [13] literatürde yer alan çalışmaların haricinde, kullanılabilirlik, maliyet, depolama ve güvenlik faktörlerini AHS yöntemi kullanarak değerlendirmişlerdir. Ayrıca doğrusal programlama modeli kullanarak elde edilen kriter ağırlıklarını yorumlamışlardır.

Gireesha vd. [14] bulut hizmet sağlayıcı seçiminde Geliştirilmiş Aralıklı Değerli Sezgisel (GADS) bulanık küme ağırlıklı toplam ve ürün değerlendirmesi tabanlı seçim model yaklaşımından bahsetmişlerdir. Liu vd. [15] bulut hizmet sağlayıcı seçiminde etkili olan maliyet, tepki süresi, kullanılabilirlik, güvenirlilik ve müşteri memnuniyeti kriterlerini dikkate alarak belirledikleri 8 bulut hizmet sağlayıcısını Entropi-GRA-ELECTRE III ile bulut hizmet sağlayıcı seçimi gerçekleştirmişlerdir. Youssef [16] bulut hizmet sağlayıcı seçimi için TOPSIS ve en iyi en kötü yöntem (BWM) ile tercih sırası tekniğini içeren bir model önermiştir. Önerdiği yaklaşımı ve AHS yöntemini uygulayarak elde edilen sıralamalar karşılaştırılmıştır. Youssef çalışmasında önerdiği modelin AHS'den daha iyi performans gösterdiği ve bu sebeple AHS'ye göre daha verimli ve güvenli olduğunu belirmiştir.

Tiwari ve Kumar [17] ise TOPSIS yöntemine benzer bir sıralama yöntemi tekniği geliştirmişlerdir. Önerilen yöntemde, bulut hizmet sağlayıcıları tarafından sağlanan hizmet kalitesi ve bulut hizmet kullanıcısının öncelikleri dikkate alınarak duyarlılık analizi sonucunda bir sıralama elde edilmektedir. Bu çalışma için önerdikleri yöntem ile GTOPSIS, TOPSIS ve türevleri yöntemlerini uygulayarak karşılaştırmışlardır. Nacer vd. [18] bulut hizmet sağlayıcıların sundukları özelliklerdeki çeşitlilik göz önüne alındığında bulut hizmet seçimini doğru sağlamanın oldukça güç olduğundan bahsetmişlerdir. Bulut hizmet sağlayıcılarını karşılaştırarak bulut ilişkisel veri tabanları ve bulut kuyruğu hizmetleri üzerinde durmuşlardır. Uslu [19] çalışmasında ise literatür taraması ve uzman görüşlerini dikkate alarak bulut hizmet sağlayıcı seçiminde etkili olan kriterleri gruplandırarak aralarındaki ilişkilere göre değerlendirmiştir. Uzmanların belirlemiş olduğu 7 bulut hizmet sağlayıcısı üzerinde çok kriterli karar verme ve bulanık yöntemler uygulanarak değerlendirmiştir.

Bulut bilişime güvenin artırılması için güvenlik ve gizliliğin sağlanması büyük önem taşımaktadır [20]. Keskin vd. [21] bulut güvenlik gereksinimlerine göre çok kriterli karar verme yöntemlerinden AHS, TOPSIS ve AAS (Analitik Ağ Süreci) yöntemleri kullanılarak bulut bilişim hizmetlerini sıralamışlardır. Bulutta depolanan verilerin silinebilmesi, diğer bir buluta transfer işlemi, kullanıcıların kontrollü verilere erişim sağlaması gibi önemli güvenlik faktörleri bulunmaktadır [22]. Bulut bilişim sağlayıcılara güvenlik ve gizlilik alanlarında yeni tedbirler oluşturulması,

kullanıcılara da bu alanlarda tedbirlere dikkat etmeleri konusunda büyük rol düşmektedir.

Bu çalışmada ise literatürden farklı olarak, TC Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin [23] Bilgi ve İletişim Güvenliği Rehberinde sunmuş olduğu bulut bilişim kullanıcılarının dikkat etmesi gereken 14 genel güvenlik tedbiri ele alınmıştır. Bu güvenlik tedbirleri dikkate alınarak kullanıcıların bulut bilişim seçiminde tedbir önceliklerinin belirlenmesi ve daha kolay bulut bilişim seçimi yapılmasına yardımcı olunması amaçlanmıştır. Çalışma kapsamında bulut bilişim alanında uzman 5 kişinin görüşleri dikkate alınarak çok kriterli karar verme yöntemlerinden AHS ve BAHS yöntemleri ile öncelik değerleri tespit edilmiştir. Çalışmanın sonuç bölümünde elde edilen öncelik değerleri yorumlanarak şirketler için önemi vurgulanmıştır. Böylece şirketler bulut hizmet seçiminde bulut bilişim güvenliklerinin belirlenmesi ve seçim aşamasındaki önem etki düzeylerinin belirlenmesi için nasıl bir yol izlemesi gerektiğini görebileceklerdir. Bu sayede, dijital dönüşüm ofisinin belirlediği tedbirler doğrultusunda tedbirlerin profesyonel bir bakış yardımıyla bulut hizmet seçiminde gizlilik ve güvenliğe üst düzey önem vererek daha güvenilir bir seçim yapma kolaylığı elde edeceklerdir.

Çalışma 5 bölümden oluşmaktadır. İkinci bölümde bulut bilişim hakkında genel bilgilerden bahsedilmektedir. Üçüncü bölümde çok kriterli karar verme problemlerinden AHS ve BAHS yöntemlerinden bahsedilmiştir. Dördüncü bölümünde bulut bilişim güvenlik tedbirlerinin öncelik değerleri belirlenmiş ve karşılaştırılmıştır. Son bölümde ise yapılan çalışmanın sonuçları verilmiş ve gelecekte yapılabilecek çalışmalar hakkında önerilerde bulunulmuştur.

II. BULUT BİLİŞİM (CLOUD COMPUTING)

Bulut bilişim, kullanıcıya ait verilerin uzak bir sunucu üzerinden esnek zamanda erişim sağlama, depolama ve aktarma işlemlerini yapabilmesine ya da internet ortamında bulunan uzak bir sunucu üzerinden çalışan uygulamaları kullanarak işlemler yapabilmesine olanak sağlayan bir platformdur. Bulut bilişim sayesinde, sahip olunan yetki doğrultusunda istenilen veriye her yerden ve her türlü elektronik iletişim cihazını kullanarak ulaşmak mümkün olabilmektedir [3, 12].

2.1. Bulut Bilişim Tipleri

Bulut hizmet tipleri kullanım biçimlerine göre melez, özel, genel ve topluluk olmak üzere 4 tipten oluşmaktadır. Genel bulut, bulut servis sağlayıcıları tarafından internet üzerinden web ara yüzü aracılığıyla kullanıcılara genel kullanım imkânı sağlayan bir hizmet tipidir [24].

Özel bulut, şirketlerin veri güvenliğinin önemli olduğu durumlarda kullanıcıların güvenlik önlemlerinin diğer bulut tiplerinden yüksek olan bir hizmet tipidir. Şirketler genellikle kurum dışında ki tüm erişim yollarını kapatılarak sadece kurum içi hizmet alınımını tercih etmektedir [3, 25].

Melez bulut, iki veya daha fazla bulutun bir arada kullanıldığı bir hizmet tipidir. Melez bulut tipi, özel, genel ve topluluk bulut tiplerinin ihtiyaca göre şekillenmesi ile oluşan bulut kümesi şeklinde belirtilmektedir [26,27].

Topluluk bulut, belirli ikiden fazla kurumun bir arada kullandığı bir bulut tipidir. Burada amaç ortak çalışma alanlarında bulunan kurumların bir arada olmasıdır [19]. Türkiye'de kullanılan e-devlet sistemi topluluk bulut tipine en iyi örnektir.

2.2. Bulut Bilişim Modelleri

Bulut bilişim üç ana hizmet modeline ayrılmaktadır. Bulut bilişim hizmet sağlayıcıları, kullanıcılarına kullanım türlerine göre yazılım (SaaS), platform (PaaS) ve altyapı (IaaS) modellerinden birini ya da aynı anda birkaçını kullanmasına imkân sağlamaktadır.

Bulut yazılım hizmeti, kullanıcılarına web tabanlı çeşitli yazılım ve uygulamaları sunarak yazılım yüklemesi yapmadan kullanma imkânı sağlamaktadır. Bu hizmet modeli kullanıcılara pratik, hızlı ve hazır bir platform sunduğundan dolayı zaman ve maliyet açısından oldukça tercih edilen bir bulut modelidir [28].

Bulut platform hizmeti, kullanıcılarına yeni uygulamalar geliştirmesine ve yazılımlarını yönetebilmesine olanak sağlamanın yanında yazılım geliştirme ortamı için gerekli tüm yazılım ve donanım platformu sunmaktadır [29, 30].

Bulut altyapı hizmeti, kullanıcılar arasında kaynak bulutu olarak ifade edilen bulut hizmet modelidir. Kullanıcının ihtiyacı olan ağ türüne göre güvenli erişim imkânı sunarak dinamik veri depolama alanı, kullanılacak işlemci kaynaklarının sanal olarak kullanıcıya sunulması ve ağ hizmetleri gibi servisler imkânı sağlayan bir hizmet modelidir [20, 31].

III. TEORİK METOD (THEORETICAL METHOD)

İnsanoğlu yaşamı boyunca karşılaştığı problemlerde seçim yapması gerekmektedir. Bu seçim süreçlerinde çeşitli sebeplerden dolayı karar vermekte zorluk çekmektedir. Karar vericilerin karşılaştıkları karmaşık problemlerde, anlaşılır, kolay ve objektif analiz yaparak daha profesyonel kararlar verilmesi için çok kriterli karar verme yöntemleri geliştirilmiştir [32]. Bu çalışmada çok kriterli karar verme yöntemlerinden AHS ve BAHS yöntemleri kullanılarak bulut bilişim güvenliği tedbirleri önem düzeyleri belirlenmiştir.

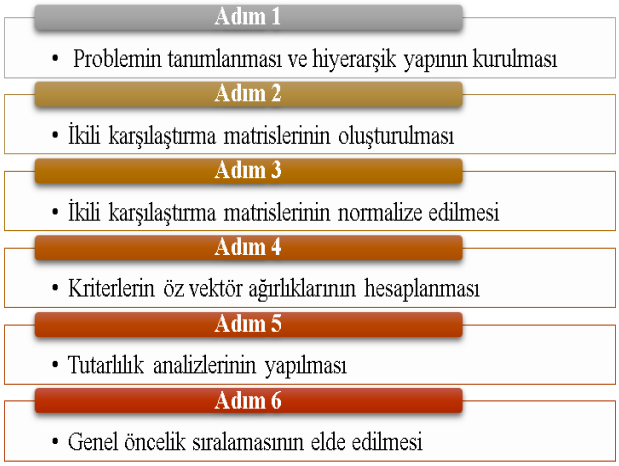
Literatürde AHS ve BAHS yöntemi ile ilgili çalışmalara bakıldığında, bilişim teknolojileri [32, 33-40], ulaşım [41, 42], enerji [43] ve sağlık [44] alanlarında da kullanıldığı görülmektedir.

3.1. Analitik Hiyerarşi Süreci

AHS yöntemi, karmaşık problemlerin çözüm sürecini kolaylaştırmak için Saaty tarafından 1980 yılında geliştirilmiştir. AHS yöntemi ele alınan problemi hiyerarşik bir yapıda modelleyerek, problemin kriterler ve alternatifler arasındaki ilişkiyi daha iyi tespit edilmesini mümkün kılmaktadır [45]. Problemde ele alınan kriterler kendi aralarında karşılaştırılarak öncelik değerleri belirlenir. Bu süreçte ortak bir skala olarak, Saaty [46] tarafından geliştirilen 1-9 skalası ile uzman kişilerin ya da karar vericilerin değerlendirmeleri kullanılmaktadır. AHS yöntem adımları Şekil 1'de gösterildiği gibi 6 adımdan oluşmaktadır. AHS yönteminde kullanılan 1-9 skalası ise Tablo 1'de gösterilmektedir [47].

3.2. Bulanık Analitik Hiyerarşi Süreci

Karar vericiler, karar verme aşamasında içinde bulunduğu durumun avantaj ve dezavantajlarına göre stratejik çalışmaktadırlar. Karar verme süreçlerinin karmaşıklığının yanı sıra belirsizliğin çok olduğu ve net sayıların verilemediği problemler için bulanık mantık yöntemleri tercih edilmektedir [47]. BAHS, hiyerarşik yapıdaki problemleri sözel ifadeler ile tanımlanmasında yardımcı olan en yaygın yöntemdir [42]. Literatürde BAHS için birçok farklı uygulama tekniği geliştirilmiştir. Bu teknikler arasında en yaygın kullanılan "Genişletilmiş Analiz Yöntemi'dir. Çalışmada kullanılan genişletilmiş analiz yöntemi, Chang tarafından 1996 yılında geliştirilmiştir [48]. Karar vericilerin ikili karşılaştırma matrislerinde kullandıkları sözel ifadelerin üçgensel bulanık sayı karşılığı Tablo 2'de gösterilmektedir. BAHS yöntem adımları Şekil 2'de gösterildiği gibi 4 adımdan oluşmaktadır.



Şekil 1. AHS adımları (AHP steps)

Tablo 1. AHS 1-9 skalası (AHP 1-9 scale)

Önem Derecesi	Tanımı
1	Eşit derecede önemli
3	Orta derecede önemli
5	Güçlü derecede önemli
7	Çok güçlü derecede önemli
9	Son derecede önemli
2,4,6,8	Ara değerler

IV. UYGULAMA (EXPERIMENT)

Bulut bilişim teknolojisi sayesinde internet aracılığı ile sahip olunan yetki dâhilinde dünyanın her yerinden verilere ulaşmak mümkün hale gelmektedir. Bulut bilişim, şirketleri veri merkezi

kurma masrafından kurtarmanın yanında zaman kaybı ve bakım ücreti gibi faktörlerden de kurtarmaktadır. Ancak şirket ve bireysel kullanıcıların neredeyse tüm işlerinin dijital bir ortama aktarması, sahip oldukları verilere erişmek isteyen diğer kullanıcıların saldırı risk faktörünü de ortaya çıkarmıştır.

Şekil 2. BAHS adımları (BAHP steps)

Tablo 2. Sözel ifadelerin üçgen bulanık sayı türünden karşılıkları (Verbal expressions in the triangle fuzzy number type)

Üçgensel Bulanık Sayılar	Sözel İfade
(1,1,1)	Eşit önemli
(2/3,1,3/2)	Daha fazla önemli
(3/2,2,5/2)	Kuvvetli derecede önemli
(5/2,3,7/2)	Çok kuvvetli derecede önemli
(7/2,4,9/2)	Tamamıyla önemli

Bulutta saklanan verilerin gizliliğinin ve güvenliğinin sağlanması konusunda hizmet sağlayıcılar daha iyi politikalar ve uygulamalar oluşturmalıdırlar. Kullanıcılar da bulut hizmet sağlayıcı seçiminde veri gizliliğinin ve güvenliğinin sağlanması için gerekli tedbirleri belirlemeli ve bu tedbirlere bulut bilişim teknolojileri uygulamalarında dikkat etmelidirler. Uygulama kapsamında, Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Ofisinin [23] sunmuş olduğu bilgi ve iletişim güvenliği rehberinde bulut bilişim güvenliği çerçevesinde belirlenen genel güvenlik tedbirleri ele alınmıştır. Ele alınan tedbirler Tablo 3'te gösterildiği gibidir. Şirketler bulut bilişim güvenliği çerçevesinde sunulan tedbirleri dikkate alarak bulut bilişim seçiminde uygulamalıdırlar. Çalışma kapsamında, bilişim sistemleri alanında uzman 3 doktora ve 2 yüksek lisans eğitim seviyesinde toplam 5 uzmanın görüşleri doğrultusunda 14 tedbir çok kriterli karar verme yöntemlerinden AHS ve BAHS yöntemleri kullanılarak kendi aralarındaki baskınlık düzeyleri belirlenmiştir. Böylelikle bulut bilişim güvenliği çerçevesinde dikkate alınacak tedbirlerin, hizmet seçiminde öncelik değerlerinin bulunması amaçlanmıştır. Çalışma kapsamında yer alan problem akış şeması Şekil 3'te gösterilmektedir.

4.1. AHS Yöntemi ile Tedbirlerin Önceliklenmesi

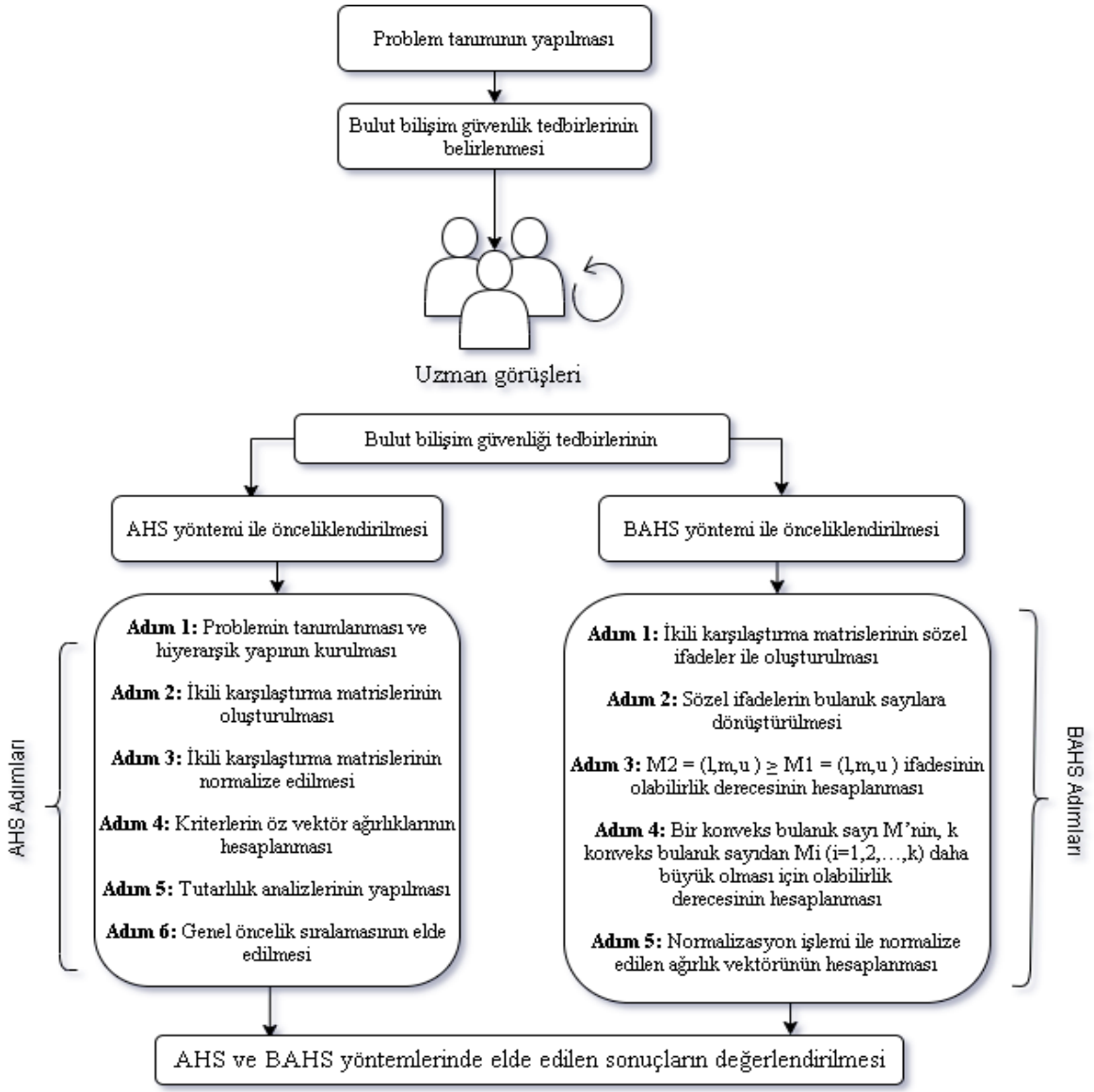
Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Ofisinin [23] bulut bilişim güvenliği üzerine belirlediği tedbirleri kendi aralarında incelendiğinde çok kriterli karar verme yöntemleri arasında kolay, anlaşılır ve pratik bir yöntem olan AHS yöntemi tercih edilmiştir. AHS yöntemde kullanılan Saaty 1-9 skalası kullanılarak ele alınan 14 tedbir, bulut bilişim alanında uzman 5 kişi tarafından değerlendirilmiştir. Uzmanların ikili karşılaştırmaları Tablo 4'te gösterilmektedir.

İkili karşılaştırma matrisi kullanılarak AHS yönteminde bulunan ikili karşılaştırma matrisinin normalize etme, öz vektör hesaplama ve tutarlılık oranı hesaplama adımları uygulanmıştır. AHS yönteminde tutarlılık oranı %10'dan küçük olması gerekmektedir. Uzman görüşleri doğrultusunda değerlendirilen kriterlerin tutarlılık oranı %8,9 elde edildiği için AHS uygulaması tutarlı sonuç vermektedir. AHS yönteminde elde edilen tedbirlerin öncelik değerleri Tablo 5'te gösterilmektedir.

Elde edilen bu sonuçlara göre %18,7 oranında öncelik değeri ile bulut hizmet kullanımı (BK) en etkili kriter olarak belirlenirken bu sırayı %16,3 öncelik değeri ile bulut ortam güvenliği (BG), %16 öncelik değeri ile erişim yetkilerinin yönetiminin sağlanması (ES) kriteri takip etmektedir.

4.2. BAHS Yöntemi ile Tedbirler Baskınlıklarının Belirlenmesi

BAHS, karmaşık ve net sayıların kullanılamadığı problemlere sözel ifadeler kullanılarak ikili karşılaştırmaların yapılmasını sağlaması ve AHS yöntemine benzer bir metot uygulaması sebebiyle karar verme süreçlerinde yaygın olarak kullanılan bir yöntemdir. Uzmanların kriter değerlendirme aşamasında sözel ifadeler kullanması ve kriterlerin birbirlerine çok yakın öneme sahip olması karar verme sürecini zorlaştırmıştır. Bu süreçte BAHS yöntemi kullanılarak kriterlerin kendi aralarındaki baskın değerleri elde edilmiştir. Kriterlerin ikili karşılaştırma matrisi için uzmanların değerlendirdiği sözel ifadeleri Tablo 2'de yer alan üçgensel bulanık sayılara dönüştürülmüştür. İkili karşılaştırma matrisinin üçgensel bulanık sayılar ile gösterimi Tablo 6'da gösterilmektedir. Tablo 6 incelendiğinde veri iletimi güvenliği (VG) kriteri sanal makineye ait belleklerin imhası (SBİ) kriterine kuvvetli derecede önemli iken imajların imha edilmesi (İE) kriterine çok kuvvetli derecede önemli olduğu görülmektedir.



Şekil 3. Problem akış şeması (Flowchart of the problem)

Tablo 3. Bulut bilişim güvenliği tedbirleri [23]

Tedbir adı	Açıklaması
Bulut Hizmeti Kullanımı (BK)	Kritik verilerin yurt içinde depolandığı ve kurumlara ait özel bulut sistemleri haricinde, yer, sunucu veya servis tabanlı bulut hizmeti kullanılacaksa; Personel, yetki ve yetkinlik düzeyleri; Erişim, işlem ve ağ trafiği iz kayıtlarının izlenmesi; Güncelleme durum alarmları; Siber olay alarmları; Performans ve kapasite göstergeleri kurum tarafından kontrol edilmelidir.
Hizmet Kapsamı ile Rol ve Sorumlulukların Belirlenmesi (HB)	Bulut bilişim hizmeti kapsamında hizmet veren ve alan kurum arasında, karşılıklı yükümlülükleri ve gizlilik maddelerini içeren bir sözleşme yapılmalıdır. Alınan hizmetin kapsamı sözleşme içerisinde tam olarak belirtilmeli ve hizmet kapsamında işlenen verinin kritikliği doğrultusunda yeterli seviyede güvenlik önlemleri alınmalıdır.
Veri İletimi Güvenliği (VG)	Bulut bilişim kapsamında çalışan tüm sistemler arasındaki veri trafiği güvenli ve güncel iletişim protokolleriyle gerçekleştirilmelidir. Bulut ortamına doğru veri iletimi sağlanırken iletimin tek yönlü olması sağlanmalı ve kurumsal ağ bulut ortamından gelecek tehditlere karşı izole olmalıdır.
Kaynakların İzole Edilmesi (KE)	Aynı bulut ortamını kullanan kurumların sistemleri ağ seviyesinde birbirlerinden mantıksal ve/veya fiziksel olarak izole edilmelidir. Kurumların yalnızca kendilerine ait veriye erişim imkânı sağlanmalıdır.
İmajların İmha Edilmesi (İE)	Bulut hizmeti kapsamında, ihtiyaç olması durumunda şablon olarak kullanılan imajların geri döndürülemeyecek şekilde silinmesine servis sağlayıcı tarafından imkân tanınmalıdır.
Sanal Makineye Ait Belleklerin İmhası (SBİ)	Bulut hizmeti kapsamında herhangi bir sanal makinenin hizmetinin sonlandırılması durumunda, sanal makinenin bulut bilişim sunucularında bulunan bellek bölgeleri otomatik olarak servis sağlayıcı tarafından geri döndürülemeyecek şekilde silinmelidir.
Bulut Ortamı Güvenliği (BG)	Servis sağlayıcılar kendi kaynaklarını DDoS saldırılarına karşı koruyabilmeli ve kapasitesinin üzerinde gelen yüksek boyutlu DDoS saldırılarına karşı iş ve hizmet sürekliliğini sağlayabilmelidir. Hizmet alan taraf ile imzalanan sözleşme ve taahhütlerde bu husus yer almalıdır. Servis sağlayıcılar, servis verdikleri herhangi bir hizmet alanına gelen bir siber saldırıdan (servis dışı bırakma, zararlı yazılım vb.) veya saldırının sistemlerde oluşturabileceği performans problemlerinden diğer hizmet alanlarının etkilenmemesi için güvenlik duvarı, saldırı tespit sistemi gibi güvenlik önlemlerini almalıdır. Servis sağlayıcıların verdikleri hizmetler ile ilgili hizmet seviye taahhüt koşulları belirlenmeli, ölçülmeli ve raporlanabilmelidir. Kurumlar, varlık gruplarının kritiklik derecesine uygun güvenlik tedbirlerini uygulayan ve periyodik güvenlik denetimlerini gerçekleştiren bulut hizmeti sağlayıcılarından hizmet almalıdır. Operatörler tarafından sunuculara erişimde trafiğin yurt içinde kalmasına yönelik tedbirler uygulanmalıdır. Bulut hizmeti kullanımında kuruma ait şifreleme anahtarları hizmeti alan kurum tarafından yönetilmelidir. Bulut yönetim arayüzü üzerinden işlem yapmak için IPSec veya SSL VPN geçidi kullanılmalı ve bulut yönetim arayüzüne erişim sadece bu kanallardan yapılmalıdır
Sanal Makineye Ait Disk Bölgelerinin İmhası (SDİ)	Bulut hizmeti kapsamında herhangi bir sanal makinenin hizmetinin sonlandırılması durumunda, sanal makinenin bulut bilişim sunucularında bulunan disk bölgeleri otomatik olarak servis sağlayıcı tarafından geri döndürülemeyecek şekilde silinmelidir.
İş Sürekliliğinin Sağlanması (İS)	Bulut bilişim hizmeti sunacak servis sağlayıcı iş sürekliliğini sağlamak amacıyla felaket kurtarma merkezi veya yedekleme mekanizmaları ile ilgili yeterlilikleri kurumun bilgi güvenliği gereksinimlerine uygun olarak sağlamalıdır
Erişim Yetkilerinin Yönetiminin Sağlanması (ES)	Bulut hizmet sağlayıcısının, hizmet alan kurumun sistemine giriş yapması gerektiğinde önceden belirlenmiş kurum yetkililerinden onay almalıdır. Yetkilendirme süreli olmalı ve sorun giderildiğinde erişim yetkisi kaldırılmalıdır. Hizmet sağlayıcı bu süreçte yapılan tüm işlemleri kayıt altına almalı ve bunları raporlamalıdır. Hizmet sağlayıcının bu süreci sistem üzerinde yönetecek ve raporlayacak özellikleri ve tanımlı süreçleri olmalıdır.
Hizmetin Sonlandırılması Hususları (HH)	Paylaşımlı/bulut ortamdan hizmet sağlayan servis sağlayıcılar hizmetin sonlanması durumunda hizmet alan tarafa ait profil ayarları, hizmet raporları vb. hizmete ilişkin tanımları silmelidir. Bulut sistemlerde barındırılan veriler, kullanımının sonlandırılması durumunda sistemlerden geri getirilemeyecek şekilde silinmelidir.
Güvenli Veri Depolama Politikasının Uygulanması (GU)	Bulut bilişim hizmeti sunacak servis sağlayıcının veri güvenliğini (ifşa, değiştirme, bozulma vb. durumlara karşı) sağlamak adına güvenli veri depolama politikası bulunmalıdır.
Bulut Ortamı İşlem Kayıtlarının Tutulması (BT)	Bulut sistemlerde gerçekleştirilen yönetimsel işlemler kayıt altına alınmalı ve değişmezliği sağlanmalıdır.
Kaynakların Fiziksel Olarak İzole Edilmesi (KFE)	Bulut sistemler üzerinde kuruma ait kritik veri bulundurulacaksa, kritik veriler kurum dışı başka kaynaklar ile aynı fiziksel cihaz üzerinde bulundurulmamalıdır.

Tablo 4. AHS ikili karşılaştırma matrisi

Kriter /Kriter	BK	HB	VG	KE	İE	SBİ	BG	SDİ	İS	ES	HH	GU	BT	KFE
BK	1,000	7,000	2,000	8,000	9,000	9,000	1,000	3,000	6,000	2,000	9,000	4,000	5,000	8,000
HB	0,143	1,000	0,250	2,000	4,000	3,000	0,143	0,200	0,500	0,200	5,000	0,250	0,500	3,000
VG	0,500	4,000	1,000	5,000	8,000	7,000	0,500	2,000	3,000	0,333	9,000	2,000	3,000	6,000
KE	0,125	0,500	0,200	1,000	3,000	2,000	0,125	0,200	0,500	0,167	4,000	0,250	0,333	2,000
İE	0,111	0,250	0,125	0,333	1,000	0,500	0,111	0,143	0,250	0,125	2,000	0,143	0,167	0,333
SBİ	0,111	0,333	0,143	0,500	2,000	1,000	0,111	0,143	0,333	0,125	3,000	0,167	0,200	0,500
BG	1,000	7,000	2,000	8,000	9,000	9,000	1,000	2,000	6,000	1,000	9,000	2,000	5,000	9,000
SDİ	0,333	5,000	0,500	5,000	7,000	7,000	0,500	1,000	4,000	0,250	8,000	3,000	3,000	6,000
İS	0,167	2,000	0,333	2,000	4,000	3,000	0,167	0,250	1,000	0,200	4,000	0,333	0,500	3,000
ES	0,500	5,000	3,000	6,000	8,000	8,000	1,000	4,000	5,000	1,000	9,000	3,000	4,000	7,000
HH	0,100	0,200	0,111	0,250	0,500	0,333	0,100	0,125	0,250	0,111	1,000	0,143	0,167	0,333
GU	0,250	4,000	0,500	4,000	7,000	6,000	0,500	0,333	3,000	0,333	7,000	1,000	3,000	5,000
BT	0,200	2,000	0,333	3,000	6,000	5,000	0,200	0,333	2,000	0,250	6,000	0,333	1,000	4,000
KFE	0,125	0,333	0,167	0,500	3,000	2,000	0,111	0,167	0,333	0,143	3,000	0,200	0,250	1,000

Tablo 5. Kriter öncelik değerleri

Kriter	Öncelik Değeri
BK	0,187
HB	0,033
VG	0,105
KE	0,025
İE	0,013
SBİ	0,016
BG	0,163
SDİ	0,100
İS	0,037
ES	0,160
HH	0,010
GU	0,079
BT	0,052
KFE	0,020

Kriterlerin kendi aralarındaki karşılaştırma önem düzeyinin çok yakın olması, 14 kriterin baskınlık düzeylerinin belirlemesini oldukça güçleştirmektedir. BAHS yöntemi adımlarının uygulanması sonucunda elde edilen kriter öncelik değerleri Tablo 7'de gösterilmektedir. Kriter baskınlık değerleri incelendiğinde, %14,4 oranında baskınlık değeri ile bulut hizmet kullanımı (BK) en etkili kriter olarak belirlenirken bu sırayı %13,1 baskınlık değeri ile bulut ortam güvenliği (BG), %11,8 baskınlık değeri ile erişim yetkilerinin yönetiminin sağlanması (ES) kriteri takip etmektedir.

4.3. Sonuçların Değerlendirilmesi

Çalışma kapsamında, Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Ofisi [23] bilgi ve iletişim güvenliği rehberinde, bulut bilişim kullanıcıları bulut bilişim güvenliği üzerine alınması gereken tedbirler 5 uzman görüşü ile kendi aralarında değerlendirilmiştir. İlk olarak, ele alınan 14 tedbirin çok kriterli karar verme yöntemlerinden AHS yöntemi kullanılarak öncelik değerleri belirlenmiştir. Kriterlerin ikili karşılaştırılması aşamasında, uzmanların kesin nicel ifadeler kullanamaması ve "daha fazla önemli", "kuvvetli derecede önemli", "çok kuvvetli derecede önemli" gibi ifadeleri tercih etmeleri sebebiyle BAHS yönteminin de kullanılmasını gerektirmiştir.

Tablo 6. BAHS ikili karşılaştırma matrisi (BAHP binary comparison matrix)

	BK	HB	VG	KE	İE	SBİ	BG	SDİ	İS	ES	HH	GU	BT	KFE
BK	**1**	3/2,2,5/2	2/3,1, 3/2	3/2,2,5/2	5/2,3,7/2	3/2,2,5/2	1,1,1	3/2,2,5/2	3/2,2,5/2	1,1,1	7/2,4,9/2	3/2,2,5/2	3/2,2,5/2	(5/2,3,7/2
HB		**1**	2/5,1/2,2/3	1,1,1	3/2,2,5/2	3/2,2,5/2	2/5,1/2,2/3	2/3,1,3/2	1,1,1	2/5,1/2,2/3	5/2,3,7/2	2/3,1,3/2	2/3,1,3/2	2/3,1,3/2
VG			**1**	3/2,2,5/2	5/2,3,7/2	3/2,2,5/2	2/3,1,3/2	1,1,1	2/3,1,3/2	2/3,1,3/2	7/2,4,9/2	1,1,1	2/3,1,3/2	3/2,2,5/2
KE				**1**	5/2,3,7/2	2/3,1,3/2	2/5,1/2,2/3	2/5,1/2,2/3	2/3,1,3/2	2/5,1/2,2/3	7/2,4,9/2	2/5,1/2,2/3	2/3,1,3/2	1,1,1
İE					**1**	2/7,1/3,2/5	2/7,1/3,2/5	2/9,1/4,2/7	2/5,1/2,2/3	2/9,1/4,2/7	2/3,1, 3/2	2/5,1/2,2/3	2/5,1/2,2/3	2/9,1/4,2/7
SBİ						**1**	2/5,1/2,2/3	2/5,1/2,2/3	2/5,1/2,2/3	2/5,1/2,2/3	7/2,4,9/2	2/7,1/3,2/5	2/5,1/2,2/3	1,1,1
BG							**1**	2/3,1, 3/2	3/2,2,5/2	1,1,1	7/2,4,9/2	3/2,2,5/2	3/2,2,5/2	3/2,2,5/2
SDİ								**1**	2/3,1,3/2	2/3,1,3/2	7/2,4,9/2	1,1,1	2/3,1,3/2	3/2,2,5/2
İS									**1**	2/3 , 1, 3/2	5/2,3,7/2	2/3,1,3/2	1,1,1	3/2,2,5/2
ES										**1**	5/2,3,7/2	3/2,2,5/2	2/3,1,3/2	3/2,2,5/2
HH											**1**	2/9,1/4,2/7	2/7,1/3,2/5	2/9,1/4,2/7
GU												**1**	1,1,1	3/2,2,5/2
BT													**1**	3/2,2,5/2
KFE														**1**

AHS yönteminde elde edilen öncelik değerleri incelendiğinde, ilk sırada %18,7 ile bulut hizmet kullanımı kriterinin, ikinci sırada %16,3 bulut ortam güvenliği kriterinin, üçüncü sırada ise %16 ile erişim yetkilerinin yönetiminin sağlanması kriterinin yer aldığı görülmektedir.

Tablo 7. Kriter öncelik değerleri

Kriter	Baskınlık Değeri
BK	0,144
HB	0,058
VG	0,111
KE	0,044
İE	0
SBİ	0,015
BG	0,131
SDİ	0,105
İS	0,070
ES	0,118
HH	0
GU	0,095
BT	0,076
KFE	0,034

BAHS yönteminde elde edilen baskınlık değerleri incelendiğinde ise, %14,4 ile bulut hizmet kullanımı, %13,1 ile bulut ortam güvenliği ve %11,8 erişim yetkilerinin yönetiminin sağlanması kriteri takip ettiği görülmüştür. Her iki yöntemde de benzer bir öncelik sıralaması elde edilse de, BAHS yönteminde bulanık değerlerin kullanılması, imajların imha edilmesi ve hizmetin sonlandırılması hususları kriterlerinin diğer kriterlerden çok daha az baskın olması sebebiyle baskınlık değerleri sıfır olarak elde edilmiştir.

V. SONUÇLAR (CONCLUSIONS)

Çalışma kapsamında bulut bilişim güvenliği üzerine alınması gereken tedbirlerin kendi aralarında öncelik değerleri belirlenmiştir. Bulut bilişimin kullanıcılarına veri akışı, depolama ve esnek zamanda veriye erişme gibi özellikler sunması, şirketlerin dijital platformlara yönelmesine yol açmıştır. Bulut bilişime olan talebin giderek artması bulut bilişim güvenlik risk faktörünü de ortaya çıkarmıştır. Kullanıcıların sahip olduğu veriye yasa dışı erişim sağlanması ve/veya istenilmeyen herhangi bir durumda yetki sahibi olmayan başka kimsenin erişim sağlaması bulut bilişim kullanımını zayıflatmaktadır. Bu durum veya durumlara karşı bulut hizmeti sunan şirketler güçlü önemler almaktadır. Bulutta yer alan verilere karşı herhangi bir saldırı veya tehdit durumuna karşı bulut hizmeti sunan şirketler tedbirler alsa da kullanıcılara da büyük rol düşmektedir. Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Ofisi [23] bilgi ve iletişim güvenliği rehberinde, bulut bilişim kullanıcıları için genel güvenlik tedbirleri belirlemiştir. Belirlenen 14 tedbir, bu çalışmada 5 uzman tarafından değerlendirilerek çok kriterli karar verme yöntemlerinden AHS ve BAHS yöntemleri ile önceliklendirilmiştir.

Uygulama kapsamında, AHS ve BAHS kriter öncelik değerlerinin sıralaması incelendiğinde benzer bir sıralama elde edildiği görülmüştür. Uygulama sonucunda elde edilen 14 tedbirin öncelik sırası, bulut hizmeti kullanımı, bulut ortamı güvenliği, erişim yetkilerinin yönetiminin sağlanması, veri iletimi güvenliği, sanal makineye ait disk bölgelerinin imhası, güvenli veri depolama politikasının uygulanması, bulut ortamı işlem kayıtlarının tutulması, iş sürekliliğinin sağlanması, hizmet kapsamı ile rol ve sorumlulukların belirlenmesi, kaynakların izole edilmesi, kaynakların fiziksel olarak izole edilmesi, sanal makineye ait belleklerin imhası, imajların imha edilmesi, hizmetin sonlandırılması hususları şeklindedir. Bu sıralamaya göre bulut bilişim güvenliği çerçevesinde kullanıcılar, bulut hizmeti kullanımı, bulut ortamı güvenliği, erişim yetkilerinin yönetiminin sağlanması ve veri iletimi güvenliği tedbirlerini öncelikle belirlemelidirler. Bu ilk 4 tedbir dikkate alındıktan sonra geri kalan bulut hizmetlerinde diğer tedbirler dâhil edilerek bulut hizmet seçiminde bulut bilişim güvenliği seçiminde kolaylık sağlanacağı görülmektedir.

Karar vericiler, güvenlik tedbirlerinin öncelik değerlerini belirleyerek bulut hizmet seçimini yaptıklarında, sahip oldukları tüm verileri düşük maliyette, kolay erişim ve esnek kullanım zamanın yanında güvenlik ve gizlilik riskini de en az seviyede tutarak ileride oluşabilecek sorunları minimum seviyede tutacaktır. Aksi takdirde, dijital

ortamda erişim kolaylığı, daha az maliyet ve süreç gibi etkenleri kullanırken veri gizliliği ve güvenliğinin en az seviyede dikkat edilmesi şirket verileri ve gizliliği için problem teşkil edecektir.

Bu çalışmada, şirketler bulut hizmet seçiminde bulut bilişim güvenliklerinin belirlenmesi ve seçim aşamasındaki etki düzeylerinin belirlenmesi için nasıl bir yol izlemesi gerektiğini görebileceklerdir. Bu sayede, dijital dönüşüm ofisinin belirlediği tedbirler doğrultusunda tedbirlerin profesyonel bir bakış yardımıyla bulut hizmet seçiminde gizlilik ve güvenliğe üst düzey önem vererek daha güvenilir bir seçim yapma kolaylığı elde edeceklerdir.

Literatürde yapılan çalışmalar incelendiğinde bulut hizmet sağlayıcı seçiminde etkili olan kriterler belirlenmiş ve çok kriterli karar verme yöntemleri kullanılarak kriterin bulut hizmet sağlayıcı seçimindeki kriter ağırlıkları tespit edilmiştir. Bulut hizmet sağlayıcı seçimi için, tespit edilen kriterlerin ağırlıkları kullanılarak bulut hizmet sağlayıcıları kendi aralarında kullanılan yöntemlere göre bir sıralama elde edilmiştir. Ele alınan bu çalışmada ise, şirketlerin bulut hizmet seçimi sürecinde dikkate alması gereken güvenlik tedbirleri önceliklendirilmiştir. Böylelikle, şirketler bulut hizmet sağlayıcı seçim aşamasında güvenlik tedbirlerine göre bir sıralama elde edip bir sonraki aşamada bulut hizmet sağlayıcı seçiminde etkili olan kriterler ile bulut hizmet sağlayıcıları değerlendirilebileceklerdir. Bundan dolayı bu çalışma, bulut hizmet seçiminde bulut bilişim güvenliğinde karşılaşılabilecek durumlara karşı alınan tedbirlerin öncelik değerlerinin elde edilmesinde hangi yöntemleri kullanacakları hakkında bir yol gösterici olma niteliğini taşımaktadır. İleri de yapılacak çalışmalarda bulut bilişim güvenliği için alınan tedbirlere bağlı olarak güvenli yedekleme, ağ erişim kontrolü, cihaz üzerindeki verinin şifrelenmesi ve açık rıza durumunda teknik yanıt süresi gibi alt tedbirler eklenerek baskınlık değerleri belirlenebilir ve örnek bir çalışmada elde edilen baskınlık değerleri bulut hizmet sağlayıcıları üzerinde değerlendirilebilir.

KAYNAKLAR (REFERENCES)

[1] Liu W., Research on Cloud Computing Security Problem and Strategy, In 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNET), 1216-1219, 2012.

[2] Khalil I.M., Khreishah, A., Azeem M., Cloud Computing Security: A Survey, Computers, 3(1), 1-35, 2014.

[3] Marston S., Li Z., Bandyopadhyay S., Zhang, J., Ghalsasi, A., Cloud Computing: the Business Perspective, Decision Support Systems. 51(1), 176-189, 2011.

[4] Afify Y.M., Moawad I.F., Badr N.L., Tolba M.F., Cloud Services Discovery and Selection: Survey and New Semantic-Based System, In Bio-Inspiring Cyber Security and Cloud Services: Trends and Innovations, 70, 449-477, 2014.

[5] Zheng Y.F., Xu J., Multiple Attribute Decision Making With Triangular Intuitionistic Fuzzy Numbers and Application to Cloud Service Provider Selection, in Proceedings of 2nd International Conference on Information Technology and Electronic Commerce, 311-315, 2014.

[6] Garg R., Naudts, B., Verbrugge S., Stiller, B., Modeling Legal and Regulative Requirements for Ranking Alternatives of Cloud-Based Services, In 2015 IEEE Eighth International Workshop on Requirements Engineering and Law (Relaw), 25-32, 2015.

[7] Khowfa W., Silasai O., The Integration of Association Rules and AHP in Cloud Service Selection, International Journal of Applied Engineering Research, 12 (24), 15814-15820, 2017.

[8] Khurana R., Bawa R.K., Quality Based Cloud Service Broker for Optimal Cloud Service Provider Selection, International Journal of Applied Engineering Research, 12 (18), 7962-7975, 2017.

[9] Al-Faifi A., Song B., Hassan, M.M., Alamri A., Gumaei A., A Hybrid Multi Criteria Decision Method for Cloud Service Selection From Smart Data, Future Generation Computer Systems, 93, 43-57, 2019.

[10] Sohaib O., Naderpour M., Hussain W., Martinez L., Cloud Computing Model Selection For E-Commerce Enterprises Using A New 2-Tuple Fuzzy Linguistic Decision-Making Method, Computers & Industrial Engineering, 132, 47-58, 2019.

[11] Uslu B., Eren T., Gür, Ş. Bulut Hizmet Sağlayıcı Seçiminde Etkili Olan Kriterlerin Çok Kriterli Karar Verme Yöntemleri ile Değerlendirilmesi, Yönetim Bilişim Sistemleri Dergisi, 5(1), 31-51, 2019.

[12] Uslu B., Gür Ş., Eren T., Özcan E.C., Çok Kriterli Karar Verme Yöntemleri ile Bulut Hizmet Sağlayıcı Sıralaması, Pamukkale İşletme ve Bilişim Yönetimi Dergisi, 6 (1), 20-34, 2019.

[13] Devi R., Shanmugalakshmi R., Cloud Providers Ranking and Selection Using Quantitative and Qualitative Approach, Computer Communications, 154, 370-379, 2020.
[14] Gireesha O., Somu, N., Krithivasan K., Vs S.S., Iıvıfs-Waspas: An Integrated Multi-Criteria Decision-Making Perspective for Cloud Service Provider Selection, Future Generation Computer Systems, 103, 91-110, 2020.
[15] Liu M., Shao Y., Yu, C., Yu, J., A Heterogeneous Qos-Based Cloud Service Selection Approach Using Entropy Weight and Gra-Electre III, Mathematical Problems in Engineering, 2020, 1-17, 2020.
[16] Youssef A.E., An Integrated MCDM Approach for Cloud Service Selection Based on TOPSIS and BWM, IEEE Access, 8, 71851-71865, 2020.
[17] Tiwari R. K., Kumar R., G-TOPSIS: A Cloud Service Selection Framework Using Gaussian TOPSIS for Rank Reversal Problem, Journal of Supercomputing, 2020 (108), 1-40, 2020.
[18] Uslu B., Bulut Hizmet Sağlayıcılarının Çok Kriterli Karar Verme Yöntemleri ile Değerlendirilmesi, Yüksek Lisans Tezi, Kırıkkale Üniversitesi, Fen Bilimleri Enstitüsü, Kırıkkale, 2020.
[19] Henkoğlu T., Külcü Ö., Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme, Information World/Bilgi Dünyasi, 14(1), 2013.
[20] Keskin N., Kıran, A. N., Eğdemir, F. K., Eren T., Bulut Bilişim Güvenlik Gereksinimlerine Göre Çok Ölçütlü Karar Verme Yöntemleri ile Hizmet Sağlayıcı Seçimi, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 6(1), 45-60, 2020.
[21] Şengül G., Bostan, A., Bulut Bilişimde Bilgi Güvenliği ve Standardizasyon Çalışmaları. 6. Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı, 263-267, 2013.
[22] Dijital Dönüşüm Ofisi, Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi 2020, Elektronik Ankara, Dijital Dönüşüm Ofisi, 2020.
[23] Namasudra S., Roy, P., Balusamy B., Cloud Computing: Fundamentals And Research Issues, In 2017 Second International Conference on Recent Trends And Challenges In Computational Models, 7-12, 2017.
[24] Shawish A., Salama M., Cloud Computing: Paradigms and Technologies, In Intercooperative Collective Intelligence: Techniques and Applications, 495, 39-67, 2014.
[25] Garber D., Malik, J., Fazio A., Windows Azure Hybrid Cloud, John Wiley & Sons, Indianapolis, 2013.
[26] Tripathi A., Jalil M.S., Data Access and Integrity with Authentication in Hybrid Cloud, Oriental International Journal of Innovative Engineering Research, 1 (1), 30, 2013.
[27] Godse M., Mulik S., An Approach For Selecting Software-As-Aservice (Saas) Product, In 2009 IEEE International Conference on Cloud Computing, 155-158, 2009.
[28] Adhikari M., Amgoth T., Heuristic-Based Load-Balancing Algorithm for Iaas Cloud, Future Generation Computer Systems, 81, 156-165, 2018.
[29] Yasrab R., Platform-As-A-Service (Paas): The Next Hype of Cloud Computing, Arxiv Preprint Arxiv: 1804, 10811, 2018.
[30] Sanaj M.S., Prathap P.J., Nature Inspired Chaotic Squirrel Search Algorithm (CSSA) for Multi Objective Task Scheduling in An Iaas Cloud Computing Atmosphere, Engineering Science and Technology, An International Journal, 23(4), 891-902, 2020.
[31] Uslu B., Eren, T., Gür Ş., Özcan E., Evaluation of The Difficulties in The Internet of Things (IoT) with Multi-Criteria Decision-Making, Processes, 7(3), 164, 2019.
[32] Sun C.C., A Performance Evaluation Model by Integrating Fuzzy AHP and Fuzzy TOPSIS Methods, Expert Systems with Applications, 37 (12), 7745-7754, 2010.
[33] Zhang, B., Zou Z., Liu M., Evaluation on Security System of Internet of Things Based on Fuzzy-AHP Method, In 2011 International Conference on E-Business and E-Government (ICEE), 1-5, 2011.
[34] Singla C., Kaushal S., Cloud Path Selection Using Fuzzy Analytic Hierarchy Process for Offloading in Mobile Cloud Computing, In 2015 2nd International Conference on Recent Advances in Engineering Computational Sciences, 1-5, 2015.
[35] Ahmed A.I.A., Khan S., Gani A., Ab Hamid S.H., Guizani M., Entropy-Based Fuzzy AHP Model for Trustworthy Service Provider Selection in Internet of Things, In 2018 IEEE 43rd Conference on Local Computer Networks (LCN), 606-613, 2018.
[36] Alam K.A., Ahmed R., Butt F.S., Kim S.G., Ko K.M., An Uncertainty-Aware Integrated Fuzzy AHS-WASPAS Model to Evaluate Public Cloud Computing Services, Procedia Computer Science, 130, 504-509, 2018.
[37] Ly P.T.M., Lai W.H., Hsu C.W., Shih F.Y., Fuzzy AHP Analysis of Internet of Things (IoT) in Enterprises, Technological Forecasting And Social Change, 136, 1-13, 2018.
[38] Simon J., Trojanova M., Zbihlej J., Sarosi J., Mass Customization Model in Food Industry Using Industry 4.0 Standard with Fuzzy-Based Multi-Criteria Decision Making Methodology, Advances in Mechanical Engineering, 10 (3), 1-10, 2018.

[39] Li W., Peng X., Evaluation of Cloud Computing Copyright Protection Based on AHP, Mathematical Problems in Engineering, 2020.
[40] Gür Ş., Hamurcu M., Eren T., Ankara'da Monoray Projelerinin Analitik Hiyerarşi Prosesi ve 0-1 Hedef Programlama Yöntemleri İle Seçimi, Pamukkale University Journal of Engineering Sciences, 23(4), 2017.
[41] Hamurcu M., Eren T., Sürdürülebilir Kent İçi Ulaşım için Bulanık AHP Tabanlı VIKOR Yöntemi ile Proje Seçimi, In International Conference on Advanced Engineering Technologies, 21, 23, 2017.
[42] Özcan E., Gür Ş., Eren T., A Hybrid Model to Optimize The Maintenance Policies in The Hydroelectric Power Plants, Politeknik Dergisi, 2020.
[43] Eren T., Gür Ş., Ameliyathanelerin Performanslarına Etki Eden Faktörlerin Bulanık AHP ile Değerlendirmesi, Harran Üniversitesi Mühendislik Dergisi, 3(3), 197-204, 2018.
[44] Uslu B., Gür Ş., Eren T., Endüstri 4.0 Uygulaması için Stratejilerin AAS ve TOPSIS Yöntemleri ile Değerlendirilmesi, Eskişehir Teknik Üniversitesi Bilim ve Teknoloji Dergisi B-Teorik Bilimler, 7(1), 13-28, 2019.
[45] Saaty T., The Analytical Hierarchy Process, Planning, Priority Resource Allocation, RWS Publications, 1980.
[46] Uslu B., Gür Ş., Eren T., Özcan, E.C., Mobil Uygulama Seçiminde Etkili Olan Kriterlerin Belirlenmesi ve Örnek Uygulama, İstanbul İktisat Dergisi, 70(1), 113-139, 2020.
[47] Chang D.Y., Applications of the Extent Analysis Method on Fuzzy AHP, European Journal of Operational Research, 95(3), 649-655, 1996.