MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ESTONYA ELEKTRONİK SEÇİMLERİ BİREYSEL OY DOĞRULAMA SİSTEMİ

SAVAŞ YILMAZ

YÜKSEK LİSANS TEZİ
Bilgi Güvenliği Mühendisliği Anabilim Dalı

DANIŞMAN
Prof. Dr. Ensar GÜL

EŞ-DANIŞMAN
Dr. İsa SERTKAYA

İSTANBUL, 2020

MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ESTONYA ELEKTRONİK SEÇİMLERİ BİREYSEL OY DOĞRULAMA SİSTEMİ

SAVAŞ YILMAZ

(527319010)

YÜKSEK LİSANS TEZİ
Bilgi Güvenliği Mühendisliği Anabilim Dalı

DANIŞMAN
Prof. Dr. Ensar GÜL

EŞ-DANIŞMAN
Dr. İsa SERTKAYA

İSTANBUL, 2020

Estonya Elektronik Seçimleri Bireysel Oy Doğrulama Sistemi

Bu tez Bilgi Güvenliği Mühendisliği'nde
Tezli Yüksek Lisans Programının bir koşulu olarak

Savaş YILMAZ

tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.

MARMARA
ÜNİVERSİTESİ

MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Marmara Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Öğrencisi Savaş YILMAZ'ın "**Estonya Elektronik Seçimleri Bireysel Oy Doğrulama Sistemi**" başlıklı tez çalışması, 29 Haziran 2020 tarihinde savunulmuş ve jüri üyeleri tarafından başarılı bulunmuştur.

Jüri Üyeleri

Prof. Dr. Ensar GÜL (Danışman)
İstanbul Şehir Üniversitesi .....(İMZA).....

Prof. Dr. Selim AKYOKUŞ (Üye)
İstanbul Medipol Üniversitesi .....(İMZA).....

Doç. Dr. Fatih SULAK (Üye)
Atılım Üniversitesi .....(İMZA).....

ONAY

Marmara Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ……..….. tarih ve ……... sayılı kararı ile Savaş YILMAZ'ın Bilgi Güvenliği Mühendisliği Anabilim Dalı Bilgi Güvenliği Mühendisliği Programında Yüksek Lisans derecesi alması onanmıştır.

Fen Bilimleri Enstitüsü Müdürü
Prof. Dr. Bülent EKİCİ

Yazarlık Beyanı

Ben, Savaş Yilmaz, başlığı, 'Estonya Elektronik Seçimleri Bireysel Oy Doğrulama Sistemi' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza: _____

Tarih: _____

Individual Verification of Estonian Internet Voting Scheme

Savaş Yilmaz

Abstract

Estonia has been using the Estonian Internet Voting scheme for state-wide legally binding general elections since 2005. By means of this, voters can vote not only paper-based voting by using the conventional method but also on the internet with their personal computers. This brought many advantages such as the ease of voting over the internet, the use of electronic devices in the counting processes, and its speed, but it also brought different problem spaces in terms of security. The new system must ensure vote privacy and it must be at least as safe as the conventional election system. In addition, it must not be able to prove the voting cast by other people in any way. From this point of view, the problems brought by the new system are covered with new generation technologies and developing cryptography science.

Estonia Internet Voting scheme has been developed over the time with various updates. In the 2011 election period, the individual vote verification component was added to the system as a result of developing an attack against the election system and encountering invalid vote in the central server. The individual vote verification component was added to cover the weakness, but it caused a new weakness regarding vote privacy in the system. There was a solution suggestion regarding the weakness, but unfortunately, a solution that could be used in practice was not offered. In this study, the scheme labeled as *IVXV*, which was updated later in 2016 and is currently being used, is shown to still have the same weakness and solutions that can be applied in practice is proposed in order to eliminate this weakness.

Keywords: E-voting, Estonian Internet Voting, Individual Verifiability, Privacy, Usability

Estonya Elektronik Seçimleri Bireysel Oy Doğrulama Sistemi

Savaş Yilmaz

Öz

Estonya, 2005 senesinden itibaren yasal bağlayıcılığı olan ve ülke genelinde yapılan seçimlerde elektronik seçimi kullanmaktadır. Kullanılan bu sistem ile seçmen geleneksel yöntemle kağıt tabanlı oy verme işlemini yapabildiği gibi internet üzerinden kişisel bilgisayarlarıyla oy verme işlemini de yapabilmektedir. Bu durum internet üzerinden oy vermenin kolaylığı, oy sayım süreçlerinde elektronik cihazların kullanımı, hızlı olması gibi birçok avantajı getirdi, fakat güvenlik açısından beraberinde farklı sorun uzayları da getirdi. Yeni sistemin en az geleneksel seçim sistemi kadar güvenli olması ayrıca seçmenin kullanmış olduğu oyu hiçbir şekilde başka şahıslara ıspatlayamaması ve oy gizliliğinin sağlanması gerekmektedir. Bu açılardan bakıldığında yeni sistemin getirdiği problemler, yeni nesil teknolojiler ve gelişen kriptografi bilimi ile kapatılmaktadır.

Zaman içerisinde çeşitli güncellemelerle birlikte geliştirilmekte olan bu sisteme, 2011 yılında yapılabilirliği gösterilen bir saldırı ve sistemde görülen bir aksaklık neticesinde, bireysel oy doğrulama opsiyonu eklenmiştir. Sisteme eklenen bu opsiyon bir zafiyeti kapatmak için getirildi fakat sisteme oy gizliliği ile ilgili yeni zafiyet getirdi. Gelen zafiyetle ilgili çözüm önerisi olmuş, fakat pratikte kullanılabilecek bir çözüm maalesef önerilmemiştir. Bu çalışmada, 2016 senesinden sonra güncellenmiş ve hali hazırda kullanılmakta olan IVXV yapısının aynı zafiyeti hala barındırdığı gösterilmekte, ayrıca bu zafiyetin giderilebilmesi için pratikte de uygulanabilecek çözümler önerilmektedir.

Anahtar Sözcükler: E-seçim, Estonya Internet Seçim Sistemi, Bireysel Oy Doğrulaması, Mahremiyet, Kullanılabilirlik

Teşekkür

Sağlamış oldukları destekler için ailem ve nişanlım başta olmak üzere, bana burs imkanı sağlayan kurumum TÜBİTAK'a, bu tez çalışmasına önderlik edip sağlamış olduğu destekler için sayın hocam Dr. İsa Sertkaya'ya, kritik yönlendirmeleri ve tavsiyeleri için Prof. Dr. Ensal Gül'e teşekkürlerimi sunarım.

İçindekiler

Şekil Listesi

Tablo Listesi

Kısaltmalar

EIV **E**stonia **I**nternet **V**oting (**E**stonya **İ**nternet **O**ylaması)

SSL **S**equre **S**ockets **L**ayer (**G**üvenli **G**iriş **K**atmanı)

NEC **N**ational **E**lectoral **C**ommittee (**U**lusal **S**eçim **K**omitesi)

EO **E**lection **O**rganiser (**S**eçim **O**rganizatörü)

VC **V**ote **C**ollector (**O**y **T**oplayıcı)

RC **R**egistration **S**ervice (**K**ayıt **S**unucusu)

MS **M**ixing **S**ervice (**K**arıştırma **S**unucusu)

PKI **P**ublic **K**ey **I**nfrastructure (**A**çık **A**nahtarlı **A**ltyapı)

IDE **I**ntegrated **D**evelopment **E**nvironment (**E**ntegre **G**eliştirme **O**rtamı)

SDK **S**oftware **D**evelopment **K**it (**Y**azılım **G**eliştirme **K**iti)

CA **C**ertificate **A**uthority (**S**ertifika **Y**etkilisi)

Bölüm 1

Giriş

Geçmişten beri insanlar topluluklar halinde yaşamaktalar ve bunun gereği olarak yönetici insanlara her zaman ihtiyaç olmuştur. Yöneticiler toplumdan topluma ve zamandan zamana değişik şekilde belirlenmiştir. Birçok ülkede demokrasi yoluyla yöneticiler seçilmektedir ve demokrasinin gereklerinden en önemlisi seçimlerdir. Bu yolla vatandaşlar kendisini yönetecek insanları yine kendileri seçmektedir. Bunun yanında kendisini yönetecek insanların seçilmesi haricinde toplumun bir konuda karar vermesi içinde seçimler yapılmaktadır ve referandumlar bunlara örnek verilebilir.

Günümüz geleneksel seçimlerde kağıt oy pusulası ve zarflar kullanılmaktadır. Seçim için belirli bir zaman belirlenir ve belirlenen periyot içinde seçimler tamamlanır. Seçme hakkına sahip tüm seçmenler kendileri için belirlenen adreslere giderek kendilerine verilen kağıt oy pusulalarını kullanarak kendi adayını belirler, belirlediği adayı içeren zarfı sandığa atar, seçim görevlileri seçmenin oy kullandığına dair kaydı tamamlar ve oy kullanma işlemi tamamlanmış olur. Sayım işlemi ise oylama işlemi tamamlandıktan sonra sandık görevlilerince açık olarak yapılmaktadır. Sonuç olarak geleneksel seçim sistemlerinde seçim, kağıt oy pusulası ve zarf kullanılarak gizli yapılır, ayrıca seçim sayım işlemi açık şekilde sandık görevlileri tarafından yapılır.

Geleneksel seçimleri kullanılırken bir taraftanda bilim ve teknolojinin gelişmesiyle elektronik ortamlarda seçim yapılması fikri ve pratiği yaygınlaşmaya başlamıştır. Bu yüzden, elektronik seçimlerin gelecek için popülerliğinin artacağı ve pratikte birçok ülke için uygulanacağı görülüyor ve bu durum elektronik seçim sistemini incelemek için temel motivasyon kaynağıdır. Estonya elektronik seçimleri pratiğe dökebilmiş ve 2005 senesinden

beri büyük seçimlerinde kullanmıştır. Estonyanın yıllarca bu seçimi kullanması, sisteme yapılan saldırı üzerine tecrübeler edinmesi ve buna karşın doğrulama sistemi getirmesi bu ülkenin sisteminin incelenmesi açısından motivasyon kaynağı olmuştur. Bu bağlamda tezde Estonya Elektronik Seçimleri Kişisel Oy Doğrulama Sistemi'nin sisteme getirmiş olduğu zafiyet konu alındı ve problem için çözüm önerisi yapıldı.

1.1 Elektronik Seçim

Gün geçtikçe teknolojinin ilerlemesi hız kazanmakta, bu durumun insan hayatını kolaylaştırması ve her alanda insan hayatına etki etmesi seçimlerde de kendini göstermiştir. Teknolojinin getirileri seçimlerde de etkisini göstermiştir ve elektronik seçim olarak kullanılmaya başlanmıştr. Elektronik seçim, kısaca ve basitçe elektronik aletler yardımı ile yapılan seçimlerdir ve birçok ülkede farklı modelleri kullanılmaktadır. Bazı elektronik seçim modellerinde, geleneksel seçim modeli gibi seçim merkezlerinde seçim görevlilerinin yardımı ile elektronik cihazlar kullanılarak yapılan seçimler de mevcuttur. Bu tezde uzaktan internet yolu ile ve kriptografik işlemler kullanılarak seçim güvenliği sağlanan, elektronik seçim konu alındı. Çoğu ülkede kullanılmamakta fakat kullanım oranı giderek artmaktadır. Kullanım oranı için, teknolojinin artmasının yanında güvenlik gerekliliklerinin karşılanması da önemli rol almaktadır. Elektronik seçimlerin en az geleneksel seçim gereklerini karşılayabilecek durumda olması gerekmektedir. İnternet üzerinden elektronik oylama sisteminin seçmene uzaktan oy kullanma kolaylığı verebilmesinin yanında, kullanıcıya geleneksel yöntemle oy verme hakkını da kaybettirmeyebilir, oy kullanma hakkına sahip seçmen isterse oyunu elektronik olarak internet üzerinde kullandıktan sonra kendi seçim bölgesinde fiziksel olarak geleneksel seçim yöntemiyle de oy kullanabilir, bunun yanında elektronik olarak oyunu birden fazla defa kullanabilir. Seçim otoritesinin belirleyeceği kurallara göre oyların geçerlilik durumları belirlenebilir. Örneğin, internet ortamında birden fazla kez kullanılan oy için son oyun geçerli olması ve hem internet üzerinden oylama yapılıp hem geleneksel yöntemle oylama yapıldığında geleneksel yöntemle yapılan oylamanın geçerli olması gibi.

Elektronik seçim elektronik cihazların kullanılmasıyla seçimin icra edilmesidir. Estonya'da elektronik seçimlerde oy kullanma işlemi, oy kulanma hakkına sahip seçmenin, internet üzerinden elektronik cihaz kullanarak oyunu kullanmasıdır. Elektronik seçim genelde belirli bir zaman aralığında gerçekleştirilmektedir, bu zaman aralığında internet üzerinden

seçmen oyunu kullanabilmektedir. Kullanılan oy elektronik olduğu için oyu güncellemek de seçmene verilmiş bir imkandır. Seçmen oy kullanma periyodunda oy kullandıktan sonra eğer oyunu değiştirmek isterse oyunu tekrar kullanabilmekte ve son kullandığı oy geçerli olmaktadır. Oylama işlemi elektronik ve internet üzerinden yapıldığı için mekan kısıtlaması yoktur. Oy kullanmak isteyen seçmen oy kullanma periyodu içerisinde istediği yerden oyunu kullanabilmektedir. Elektronik seçimlerde kağıt oy pusulası, sandık, mühür gibi araçlara gerek kalmaz. Seçimi yönetmek için ülkenin heryerine seçim görevlilerinin gönderilmesine gerek kalmaz, bu nedenle düşük maliyet avantajı sağlar. Elektronik cihazlar kullanıldığı için yönetmesi daha kolay bir sistemdir.

Elektronik seçimin internet üzerinden icra edilmesi geleneksel seçime göre seçmene çok fazla avantaj sunmaktadır. Oy kullanma hakkında sahip olmuş vatandaşlar düşünüldüğünde çok büyük ve çeşitli bir profil ortaya çıkmaktadır. Bu profilde seçim günü hasta olan, seçim merkezine ulaşamayacak durumda olan çok fazla insan olabiliyor. İnternet üzerinden oylama yapmak bu durumda olan ülke vatandaşlarının oylarını kullanabilmesine olanak sağlamaktadır. Bu durum seçime katılımın artmasını sağlayacaktır. Seçime katılım ne kadar önemli olduğu ve elektronik seçimin seçime katılımı artırdığı düşünüldüğünde elektronik seçimin bu konuda avantaj sağlayacağı öngörülebilir. Geleneksel seçim yöntemlerinde sayımlar seçim kurulları tarafından görevlendirilen seçim görevlileri tarafından yapılmaktadır. Seçim görevlileri seçim boyunca oylama işlemlerini takip eder ve seçim sonuçlandıktan sonra oyların sayımından sorumludur. Seçim görevlilerinin görevlendirilmesi hem insan hem de parasal kaynak gerektirmektedir. Bu kaynakların kullanımı her seçim için maliyet oluşturmaktadır, elektronik seçim ile bu maliyetler ortadan kalkmaktadır. Ayrıca elektronik seçimlerde oylama ve sayma işlemi elektronik cihazlar üzerinden yapılmaktadır, geleneksel seçimlerde ise insan eli ile sayılmaktadır, dolayısıyla elektronik seçimlerde oy sayma işlemi daha doğru, net ve hızlı sonuçlanmaktadır. Seçimlerde insanların hür iradesini kullanabilmesi demokrasinin olmazsa olmazlarındandır. Bazen seçmene başkası tarafından iradesi dışında oy kullandırma gibi olaylarla karşılaşılmaktadır. Elektronik seçimin seçmene sağladığı tekrar oy kullanma özelliği ile bu durumun önüne belli ölçüde geçilebilir. Tüm bu bahsi geçen elektronik oylamanın avantajlarının yanında dezavantajları da mevcut. İlk olarak elektronik oylama'nın kanıt bulundurma açısından geleneksel oylamadan daha zayıftır [3]. Elektronik oylamada da herbir eylem için loglama yöntemleri kullanılmaktadır ve kanıt yerine geçecek argümanlar bulunmaktadır, fakat bunun için kullanılan elektronik cihazın güvenli olması gerekir [3].

Geleneksel oylama da kullanıcının oyunu kullanduğu oy pusulası ve zarf saklanmaktadır ve herhangi problem olduğu durumlarda kanıt olarak kullanılabilmektedir. İkinci olarak sandık ile oylama cihazının direkt bağlantı kurduğu bir sistemin olduğu düşünülürse sistem çok fazla saldırıya maruz kalabilir [3].

Teknolojinin imkan vermesi ve internetin yaygınlaşması düşünüldüğünde elektronik seçimin kullanımının ancak 2000'lere denk gelmesi kaçınılmazdı. Gerçek anlamda yasal bağlayıcılığı olan elektronik seçim sistemi denemeleri 2000'li yılların başlarında gerçekleşmiştir. İlk olarak yasal bağlayıcılığı olan ve internet üzerinden oylanan seçim 2000 senesinde Almanya'da Osnarckbürg Üniversitesi'nde ve Amerikanın Arizona Eyaleti'nde gerçekleşmiştir [3], bununla beraber çeşitli organizasyon ve ülkelerde de yasal bağlayıcılığı olan ve elektronik seçim şeklinde seçimler olmuştur. Örneğin; İsviçre, Hollanda, Norveç, Avusturya Öğrenci federasyonu gibi.

1.2 Elektronik Seçim Gereksinimleri

Her sistemde olduğu gibi Elektronik Seçim Sistemleri'nde de sağlanması gereken gereklilikler vardır. Estonya Elektronik Seçimi açısından bakıldığında; Elektronik Seçim'in en az geleneksel seçim kadar güvenli olması gerekir ayrıca ve seçmenin oyunu kime kullandığını kanıtlayamamasıdır [1]. Bunun yanında Elektronik Seçim için birçok gereklilik tanımlanmıştır. Seçim güvenliğinin sağlanabilmesi, adil bir seçim ortamının sağlanabilmesi, seçmen özgürlüğünün sağlanabilmesi için seçim sisteminin bazı kriterleri sağlaması gerekir [4]. Bu bölümde maddeler halinde bu gereklilikler hakkında genel bilgiler verilecektir, detaylı bilgi için [4, 5].

1.2.1 Seçme Hakkı (Eligibility)

Ülke vatandaşlarının ülke seçimine katılım hakkının olmasıdır. İnsan hakları evrensel bildirgesinde de herkesin seçilmiş temsilciler aracılığı ile ülke yönetimi hakkına sahip olduğu belirtilmiştir [6].

1.2.2 Seçmen Mahremiyeti (Voter Privacy)

Seçimde oy kullanan seçmenin oy bilgisi bilinmemelidir ve mahremiyet seçim periyodunda korunmalı ayrıca seçimden sonra uzun müddet korunmalıdır [5].

1.2.3 Uygunluk (Eliginility)

Seçme hakkına sahip seçmenlerin seçim zamanından önce kayıt altına alınması ve bu kayıttaki seçmenlerin oy kullanabilmesi gerekir [5]. Bazı yerel seçimlerde bölgelere göre oy kullanma işlemi yapılmaktadır, bu açıdan bakıldığında da seçmenlerin bölgelere göre oy kullanma hakkı tanımlanabilir.

1.2.4 Benzersizlik (Uniqueness)

Oy kullanma hakkında sahip her seçmenin bir oy hakkı olmasıdır, fakat bu bir defa oy kullanabileceği anlamına gelmemektedir, birden fazla oy kullanılan durumda bir oy geçerli olur [5].

1.2.5 Baskı dirençliliği (Coercion Resistance)

Bir saldırgan, bir ya da daha fazla seçmene oy kullanımı hakkında veya anahtar bilgilerini verme hakkında baskı yapabilir; saldırganlar hiçbir durumda herhangi seçmenin kullandığı oy hakkında bilgi edememelidir [4].

1.2.6 Boş Oy (Null Ballot)

Oy kullanma hakkına sahip her seçmen için başlangıçta boş oy sistemde hazırlanmalıdır, seçim periyodunda seçmenin oy kullanması halinde oy doldurulmu olur, seçmenin oy kullanmaması halinde oy boş olacak şekilde; doldurulmadan, değiştirilmeden, silinemeden, geçersi kıllınamadan ve kopyalanamadan sistemde sayılmalıdır [5].

1.2.7 Uçtan Uca Doğrulama (End to End Verifiability)

Uçtan uca doğrulama ile ilgili resmi tanım olmamasıyla beraber farklı seçim sistemlerinde anlam farklılıkları olabilmektedir, tasarım gereksinimlerinin aksine performans gereksinimlerine dayalı kamu seçimlerinin tanımlamaları şu şekilde yapılıyor [7]:

Oy Pusulalarının iyi Temsil Etmesi (Presented ballots are well-formed) Oy pusulasına bakan seçmen pusula üzerindeki listeden ne anlıyosa, herkes bu pusulaya baktığında aynı anlamı çıkarmalı. Bu gereklilik önceki bölümlerde bahsedilen cast-as-intented gerekliliğini içermektedir.

Oy Formatının Doğruluğu(Cast ballots are well-formed) Kullanılan oy sadece bir oy değerinde olmalıdır, eksik ya da fazla değere sahip olmamalıdır.

Oylandığı gibi Kaydedilme(Recorded as cast) Kullanılan oy kullanıldığı gibi kayıt altına alınmalıdır.

Kaydedildiği gibi Sayılma(Tallied as recorded) Kullanılmış oylar doğru sayılmalıdır.

Tutarlılık (Consistency) Oylandığı gibi kaydedilme ile kaydedildiği gibi sayılma maddelerinin sonuçları tutarlı olmalıdır.

Her Oyun Oylandığı gibi Kaydedilme Kontrolü(Each recorded ballot is subject to the "recorded as cast" check) Kaydedilen her pusula, Oylandığı gibi Kaydedilme kontrolüne tabidir.

1.3 Estonya Elektronik Seçimleri

Teknolojik imkanların ve internetin yaygılaşmasının da elvermesiyle Estonya elektronik seçimlerinin yapısal temelini 2000'li yıllarda atmaya başlamıştır. Estonya ülkesi yasal

bağlayıcılığı olan ve ülke genelinde olan ilk elektronik seçimini 2005 senesinde yerel seçiminde gerçekleştirmiştir [3]. Devamında, sırası ile şu seçimler Estonya'da elektronik olarak internet üzerinden gerçekleştirilmiştir; Parlamento Seçimleri 2007, Avrupa Parlamentosu Seçimleri 2009, Yerel Seçimler 2009, Parlamento Seçimleri 2011, Yerel Seçimler 2013, Avrupa Parlamentosu Seçimleri 2014, Parlamento Seçimleri 2015, Yerel Seçimler 2017, Parlamento Seçimleri 2019, Avrupa Parlamentosu Seçimleri 2019 [8].

Estonya'da ülke genelinde yapılan ve yasal bağlayıcılığı olan seçimlere, internet üzerinden oylama sisteminin de eklenip kullanımasından günümüze, genel olarak internet üzerinden yapılan oylama artmıştır. Tablo 1.1'de görüldüğü üzere internet üzerinden yapılan oylamaya katılım oranı artış göstermiştir. 2005 senesinde oylamaya katılan seçmenlerden % 1.9'u internet üzerinden yapılan oyama yöntemini kullanırken bu oran son seçime kadar artmış ve 2019 senesinde yapılan Avrupa Parlamentosu Seçimleri'nde (European Parliament elections 2019) %46.7 olmuştur [2].

Tablo 1.1: Estonya İnternet Oylama İstatistikleri [2]

Seçimler	Katılan seçmenler arasından i-seçmenler
Avrupa Parlamentosu Seçimleri 2019	%46.7
Parlamento Seçimleri 2019	%43.8
Yerel Seçimler 2017	%31.7
Parlamento Seçimleri 2015	%30.5
Avrupa Parlamentosu Seçimleri 2014	%31.3
Yerel Seçimler 2013	%21.2
Parlamento Seçimleri 2011	%24.3
Yerel Seçimler 2009	%15.8
Avrupa Parlamentosu Seçimleri 2009	%14.7
Parlamento Seçimleri 2007	%5.5
Yerel Seçimler 2005	%1.9

Estonya, ülke genelinde yaptığı seçimlerde vatandaşlarına uzaktan elektronik olarak oy kullanma imkanı sağlayan ve dünyada bu konuda öncü olan bir ülkedir [9]. 2005 senesinden beri Estonya ülke genelinde yapılan seçimlerde oy kullanma hakkına sahip vatandaşlar oylarını uzaktan elektronik olarak kullanabilmektedir. Estonya'da seçim organizatörü tarafından düzenlenen Estonya İnternet Oylama'da (EIV) vatandaşlar kağıt tabanlı yapılan geleneksel seçimden bir müddet önce belirli bir zaman aralığında oylarını internet üzerinden kullanabilmektedir. Örneğin kağıt tabanlı yapılan geleneksel seçim gününden on gün önce internet üzerinden oylama başlar ve seçim gününden dört gün önceye kadar devam eder. EIV sisteminde oy kullanma hakkına sahip seçmenler oylarını birden fazla defa kullanabilmektedir ve seçmenin ancak son kullandığı oy geçerli olmaktadır. Bunun

yanında seçmenlere paralel oy kullanma imkanı da verilmektedir. Paralel oylama ile seçmen, internet üzerinden oy kullanabilmekte, ayrıca oy verme merkezlerine giderek kağıt tabanlı geleneksel oylama işlemini de yapabilmektedir. Bu durumda kağıt tabanlı yapılan oylama geçerli olmaktadır. Elektronik olarak internet üzerinden oylamanın gerçekleştirildiği bu sistemde oylar ikili zarf prensibi ile oluşturulmaktadır. Bu prensipte oy iç ve dış olmak üzere iki zarftan oluşmaktadır. İlk olarak iç zarf oluşturulur ki bu seçmenin seçmiş olduğu adayın bilgisini içeren zarftır. İç zarf açık anahtarlı şifreleme yöntemleri (PKI) kullanılarak oluşturulmaktadır. Daha sonra ise dış zarf oluşturulur ki bu da oy kullanan seçmenin elektronik imzasını ifade eder. Dış zarf oluşturulmada dijital imzalama yöntemleri kullanılmaktadır. Dış zarf oluşturulurken seçmen oy kullandığı cihazda dijital imzalama aracı kullanır. İç zarf olıştururken kullanılacak açık ve gizli anahtarların yönetimi ise seçim organizatörü (EO) tarafından yapılmaktadır.

Elektronik seçimlerde teknolojinin getirdiği son imkanların yanısıra kriptolojinin de getirdiği imkanlar kullanılmaktadır. Bu bilimler faydalı işler için kullanılmasına karşın zararlı ve kötü niyetli amaçlar için de kullanılagelmiştir. Şöyle ki, elektronik seçim kullanılmaya başlandı ve bu sistemlere yapılan saldırılar da kayıtlara geçti. Elektronik seçime yapılan saldırılara karşı kriptografik ve protokol tabanlı güvenlik önlemlerinin yanısıra bilgi güvenliğinin temel prensiplerinden olan güvenilirliğin de dikkate alınmasının gerekliliği bazı kötü tecrübelerle daha fazla anlaşıldı. Estonya, e-devlet sistemini benimsemesiyle bilinen bir ülke ve 2007 elektronik seçimlerinden 2 ay sonra e-devlet sistemine karşı bir DDos saldırısı yaşamıştır [10]. Ayrıca 2009'da gerçekleştirilen Avustrya Öğrenci Federasyonunun gerçekleştrdiği elektronik seçim DDos saldırısına maruz kalmıştır [3]. Bu gibi güvenlik sorunlarının yanısıra güvenilirlik sorunları da tecrübe edilmiştir. Örneğin, Norveç hem 2011 hem de 2013'de elektronik seçimlerinde implementasyon hataları meydana gelmiştir [3]. Bu hatalar hem yazılımsal hemde fiziksel kaynaklı gerçekleme hatalarından kaynaklanmaktaydı [3].

1.4 Estonya Elektronik Seçimleri Zafiyetler ve Kişisel Oy Doğrulama Sistemi

Estonya ilk olarak 2005 senesinde kullanmaya başladığı elektronik seçim sistemini, 2011 senesinde de Parlamento Seçimleri'nde kullandı, 2011 senesinde yaptığı seçimlerde Öğrenci Saldırısı (Student Attack) isimli bir saldırıya maruz kaldı. Bir öğrenci zararlı yazılımlar kullanarak oy değiştirme saldırısını ve oy bloklama saldırısını pratikte gösterdi [11]. Bu saldırı bilgi güvenliğinin temel prensiplerine uymamaktadır. Oy bloklama veya oy değiştirme seçmenin kullandığı oyu hedef almaktadır. Bu durumda seçimin sağlıklı şekilde yapılamadığı ve halkın görüşünün sandığa yansıtılamadığı sonucu ortaya çıkmaktadır ki bu durum elektronik seçimin direkt başarısız olduğu anlamına gelebilir. Bu ataktan sonra Estonya arayışa geçti [11]. Bahsi geçen ataktan dolayı yeni bir sistem getirmeleri gerekirdi.

Estonya bahsi geçen ataktan sonra girdiği yeni arayışlarda birden fazla metodu düşünmüştür. Örneğin Norveç'te kullanılan post channel sistem olan SMS sistemini kullanmak [11]. Oy veren seçmen kitlesi düşünüldüğünde profil çok geniş ve her türlü insan bulunmaktadır. Bu profil içinde telefon kullanmayan insanlara da rastlamak mümkündür. Telefon numarasını vermek istemeyen seçmen de olabilir [11]. Norveç'in kullandığı bu sistemin maliyetli ve diğer sayılan nedenlerden dolayı uygun olmadığı görülmüştür.

2011 senesinden sonra NEC tarafından doğrulama sisteminin oluşturulması istenmiştir [3]. Oluşturulan bu doğrulama sistemi, elektronik seçimi güvenlik gerekleri düşünülerek ürün haline getirilmiştir. OSCE/ODIHR tarafından NEC'e oy doğrulama yapabileceği mekanizma tavsiye edildi, ayrıca geliştirilecek oy doğrulama yapısında Popovienuc at al. tarafından tanımlanan uçtan uca performans ihtiyaçlarının tanımlandığı oylama sistemi kullanılmıştır [3]. Estonya 2011 saldırısından sonra bu gereklilikleri dikkate alarak bir oy doğrulama sistemi geliştirmiştir. Geliştirilen oy doğrulama sisteminin bahsi geçen iki gerekliliği şimdilik sağlamasının yeterli olacağını düşünmüştür. Bunlar cast-as-intended (İstenilen Niyette Oy Kullanma) ve recorded-as-cast (Oylandığı gibi Kaydedilme) gerekliliklerdir.

Cast-as-intended, oy kullanma hakkına sahip seçmene, kullanmış olduğu oyun kendi kullandığı oy şeklinde temsil edildiğini doğrulama imkanı vermektedir. Örnek vermek gerekirse oy verme hakkına sahip bir seçmen oy verme periyodunda oyunu kullanmış

olsun ve kişisel oy doğrulama sistemi ile oyunu doğrulayacak olsun. Bu seçmen eğer herhangi bir X adayına oyunu kullanmış ise seçmen oyunun X adayı şeklinde temsil edildiğini doğrulayabilmeli. Recorded-as-cast ise oy kullanma hakkına sahip seçmene kullanmış olduğu oyun merkezi sunucularda doğru bir şekilde kayıt edildiğini kontrol etme imkanı sağlanmasıdır.

EIV sistemine 2016 senesinde yapılan bir analiz neticesinde sistem ile ilgili bir zafiyet gösterilmiştir [11]. Bu analiz EIV sistemi için kullanılan EVIV yapısına yapılmıştır. Analiz, Kişisel Oy Doğrulama Uygulaması (VerApp) ile aynı akıllı cihazda çalışmakta olan başka bir uygulamanın, VerApp bilgilerine erişim riskini ön plana çıkarmıştır. Buna göre kişisel oy doğrulama aşamasının son adımlarında VerApp ekranında açık bir şekilde gösterilen seçilen aday bilgisi, aynı akıllı cihazda çalışan, gerekli izinlerin verildiği ve güvenli olduğu düşünülen başka bir uygulama tarafından elde edilebilirdi. İnternet oylama için bazı gereksinimler; seçimlerle ilgili tüm kanunlara uyması, tüm seçim ilkelerine uyması, en azından geleneksel oylama kadar güvenli olması ve seçmenin oyunu kime kullandığını kanıtlayamamasıdır [1]. Seçimin sağlaması gereken bu gerekler ve akılllı cihazlarda faaliyette olan zararlı yazılımlar düşünüldüğünde, sisteme kişisel oy doğrulama bileşeni getirilmesi, bazı zafiyetlerin önlenmesi ile ilgili olsa bile, sisteme bir açıklığı gidermek için getirilen bileşenin başka bir açıklığı getirmesi sistem güvenliği açısından risk oluşturmaktadır. Meydana gelen bu açıklık ile seçim güvenliği risk altına alınmaktadır. Yapılan analiz neticesinde çözüm olarak oy doğrulama sistemine simetrik anahtarlı şifreleme yöntemi eklenmesi önerilmiştir [11]. Buna göre simetrik anahtarlı şifreleme yönteminin de sisteme dahil olmasıyla, her aday için benzersiz bit dizileri üretilir ve bu diziler kişisel oy doğrulama için kullanılır ve VerApp uygulamasında seçilen adayın açıkça gösterilmesi yerine adayı temsil eden bit dizilerinin seçmene gösterilmesi önerilir. Önerilen bu çözümde, kişisel oy doğrulama bileşenini kullanmak isteyen seçmenden istenen, Oy Kullanma Uygulaması (VoteApp) ekranında gösterilen ve seçilen adayı temsil eden bit dizisine bakması ayrıca VerApp ekranında gösterilen tüm adaylarla ilişkili bit dizilerine bakması sonunda ise karşılaştırma yapmasıdır. VotApp'taki bit dizisi VerApp'taki hangi bit dizisi ile aynıysa, VerApp'da aynı olan bit dizisi ile ilişkili olan adayın seçilmiş olduğu anlamı çıkar.

EIV sisteminde Kişisel Oy Doğrulama bileşeni, 2013 seçimlerinden itibaren EVIV ve IVXV kod isimli yapılarda gerçeklenmektedir. Getirilen kişisel oy doğrulama sistemi ile

birlikte seçmen kullandığı oyu doğrulayabilektedir. Doğrulama sistemi kriptografik birtakım hesaplamalara dayanmaktadır. Fakat 2011 senesinden sonra getirilen bu kişisel oy doğrulama sistemi ile sistemde yeni bir zafiyet meydana gelmiştir. 2016 senesinde Muş et al. tarafından yayımlanan makalede bu zafiyet hakkında bilgi verilmiş ve yine bu makalede ilgili zafiyete çözüm önerisinde bulunulmuştur [11]. Bu makaleye göre kişisel oy doğrulama sisteminde seçmenin oyunun açık bir şekilde gösterilmesi zafiyet oluşturmaktadır. Bu zafiyet, kişisel oy doğrulama sistemini kullanan seçmenin kullandığı akıllı cihazda bulunabilecek zararlı yazılımlar tarafından kullanılabilecek durumdadır. Kişisel oy doğrulama işlemi oy kullanma sisteminden farklı olarak akıllı cihazlarda yapılmaktadır. Kişisel oy doğrulama işlemi ile oy kullanma işlemlerinin farklı işletim sistemlerinde yapılmak istenmesi güvenlik gerekçesine dayanmaktadır. Dolayısıyla kişisel oy doğrulama uygulamaları iOS, Android, Windows Phone gibi farklı işletim sistemlerinde çalışmaktadır. Akıllı cihaz kullanarak bu işletim sistemlerinden birinde kişisel oy doğrulama işleminin yapıldığı düşünüldüğünde bu işletim sistemlerinde çalıştırılan başka bir uygulama, kişisel oy doğrulama uygulamasının verilerini elde edebilir ve kullanabilir. Örneğin Android işletim sistemine sahip bir akıllı cihaz ile kişisel oy doğrulaması yapmak isteyen bir seçmen bu işlemi yapmak isterken, yine aynı işletim sisteminde çalışan bir uygulama tarafından kişisel oy doğrulama uygulamasının verileri ele geçirilebilir. Bu durum seçim güvenliğini tehlikeye atmaktadır. Akıllı cihazlarda uygulamalar açısından pek çok güvenlik önlemi alınmaktadır, fakat akıllı cihaz dünyası büyük bir dünya ve yüzde yüz güvenliğin burada sağlandığının söylenmesi zor. Akıllı cihazda kullanılan işletim sisteminin yüzde yüz güvenli olduğu düşünülse bile akıllı cihazlarda çalışan uygulamalar kendi işlerini yapabilmeleri için cihazdaki bazı verilere ulaşmak ister(örneğin harita uygulamasının cihaz konum bilgisine ulaşmak istemesi gibi) bu doğal bir süreçtir. Kişisel oy doğrulama işleminin gerçekleştiği herhangi işletim sisteminde eş zamanlı olarak çalışan herhangi bir uygulamanın, kişisel oy doğrulama uygulamasının verilerine erişme durumunda, eş zamanlı çalışan bu uygulama bu verileri kullanıp seçmenin oyunu öğrenebilir. Bu durum seçim güvenliğini tehdit etmektedir. Akıllı cihazlarda bulunan bazı verilere erişim izinleri kullanıcıya sorularak verilebilmektedir, bu böyle durumların yaşanmaması için bir önlem olarak düşünülmüş olabilir fakat oy verecek kesim düşünüldüğünde ülkenin herbir yerinden milyonlar ile ifade edilebilir. Oy verecek kitlenin çeşitli olması, her kesimden insanın olacağı anlamına gelmektedir. Bu açıdan bakıldığında seçmen bazen neye izin verdiğini tam olarak bilmemektedir. Bu da oy doğrulama sisteminin pratikte zafiyet

oluşturduğu sonucunu çıkarmaktadır. Zafiyeti kullanarak, kişisel oy doğrulama uygulaması ile aynı akıllı cihazda çalışan başka uygulama, kişisel oy doğrulama uygulamasının verilerine ulaşıp, bunu akıllı cihaz bilgilerinden kullanıcının kimliği ile birleştirip hangi seçmenin kime oy verdiği bilgisini ortaya çıkarabilir.

Zafiyet için Muş et al. çözüm önermektedir. Bu çözüm ile oy kullanma ve kişisel oy doğrulama uygulamalarında fazladan kriptografik işlemin gerçekleştirilmesi, kişisel oy doğrulama uygulamasında seçmenin seçtiği seçim adayı yerine, seçim adaylarını temsil eden bit dizilerinin görünmesi ve oy doğrulamak isteyen seçmenin bu bit dizilerini, oy kullanma uygulamasında seçtiği adayı temsil eden bit dizisi ile karşılaştırması önerilmiştir. Temel olarak önerilen çözümde işleyiş aynı olacak fakat fazladan simetrik şifreleme işin içine girecek. Kullanıcı yine ID kartı ile merkezi sunucuya giriş yapacak, daha sonra merkezi sunucudan oy kullanma uygulamasına seçim aday listesi gönderilecek. Seçmen oyunu kullanacak ve kriptografik işlemlerden sonra ilgili veri, merkezi sunuculara gönderilecek. Oyunu doğrulamak isteyen seçmen akıllı cihaza yüklediği kişisel oy doğrulama uygulamasını kullanarak oy kullanma uygulamasındaki QR kodu kişisel oy doğrulama uygulamasına okutacak. QR yoluyla ilgili verileri alan kişisel oy doğrulama uygulaması gerekli bilgileri merkezi sunuculara gönderecek. Merkezi sunucu kişisel oy doğrulama uygulamasına ilgili veriyi gönderecek. Kişisel oy doğrulama uygulaması bu veriyi kullanarak belli kriptografik işlemlerden sonra ekranda bit dizileri gösterecek.

Kişisel oy doğrulama sistemi ile gelen bu zafiyete getirilen çözüm önerisi ile, kişisel oy doğrulama uygulamasını kullanan seçmen seçimde seçtiği aday yerine seçime katılan bütün adayları temsil eden ayrı ayrı bit dizileri görecektir. Aynı zamanda seçmenin kullandığı oy kullanma uygulamasında seçmenin seçtiği adayı temsil eden bit dizisi görünecektir. Seçmenden beklenen oy kullanma uygulamasında ekranda gösterilen dizi(ler) ile kişisel oy doğrulama uygulamasında ekranda gösterilen dizileri göz ile karşılaştırmasıdır. Eğer kişisel oy doğrulama uygulamasındaki gösterilen dizilerden biri oy kullanma uygulamasındaki dizi ile eşleşiyorsa, kişisel oy doğrulama uygulamasında eşleşen bu diziye karşılık gelen adaya bakılır. Bu aday seçmenin seçtiği aday ise oy doğrulama işlemi başarı ile sonlanır. Eğer eşleşmiyorsa merkezi sunuculara alarm gönderilir.

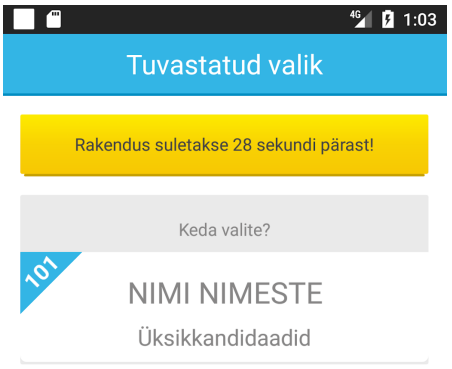
EIV seçim sistemi için hazırlanan ilk yapı EVIV kod adı ile isimlendirilmiştir ve 2005 senesinden itibaren 2015 senesine kadar kullanılmıştır. EIV sistemi yapı olarak temelde mantığı aynı olmakla beraber sistemde bazı değişiklikler ve eklemeler yapılagelmiştir.

2011 senesinde Riigikogu seçimlerinde EVIV yapısına yapılan, "Student Attack" ([12]) ismi verilen bir saldırı gösterilmiştir. Bu saldırı ile EVIV yapısını kullanarak oy vermek isteyen seçmenin bilgisayarında, uygulama giriş ve çıkış değerleri kontrol edilerek kullanılan oyun manipule edilebileceği ve bu durumun seçmenin haberi olmadan yapılabileceği gösterilmiştir. 2011 Riigikogu seçiminde 140.000 seçmen oyunu internet üzerinden kullandı ve bu kullanılan oyların %24.3'ü anlamına geliyordu [3]. Bunun neticesinde 2013 senesinden itibaren kullanılmaya başlanan VerApp bileşeni, EVIV'e eklenmiştir. Eklenen bu doğrulama bileşeni ile amaçlanan, uçtan uca doğrulama gereksinimlerinden olan cast-as-intended ve recorded-as-cast isimli gereksinimleri karşılamak olmuştur (uçtan uca doğrulama gereksinimleri hakkında daha detaylı bilgi için [7]). Bu prensipler ile EIV sisteminde oy kullanan seçmene, kullanmış olduğu oyun, doğru bir şekilde temsil edildiğini doğrulama ve doğru bir şekilde merkezi sunucularda kaydedildiğini doğrulama imkanı sağlanmıştır.

Seçmen sisteme eklenen VerApp uygulamasını kullanarak 2013 seçimlerinden itibaren, cast-as-intended doğrulaması yani kullanmış olduğu oyun doğru şekilde temsil edildiği ve recorded-as-cast doğrulaması yani kullanmış olduğu oyun merkezi sunucularda doğru bir şekilde kaydedildiği doğrulamasını yapabilmektedir. Sisteme eklenen VerApp uygulamasının oy kullanılan cihazdan farklı bir cihaza yüklenerek kullanılması, güvenlik gerekçelerinden dolayı uygun görülmüştür. Bu yüzden oy verme uygulaması VoteApp ile kişisel oy doğrulama uygulaması VerApp farklı işletim sistemi ile çalışan cihazlarda çalışmaktadır. VoteApp kişisel bilgisayarlarda kullanılırken; VerApp iOS, Android, Windows Phone gibi işletim sistemi ile çalışan akıllı cihazlarda kullanılmaktadır. VerApp kullanarak kişisel oy doğrulaması yapmak isteyen seçmene, bu uygulama ekranında kullanmış olduğu oy açıkça gösterilmektedir ve seçmen göz ile doğrulama yapmaktadır. VerApp uygulaması çıktısı Şekil 1.1 [1]'de gösterilmektedir.

EIV sisteminde temel akış benzer olmakla birlikte bazı gereklerden ve gelişmelerden dolayı sistemde değişiklikler yapılmıştır. Sistem ilk olarak EVIV yapısı ile işlevlerini yerine getirirken 2011 seçimlerinde yaşanan "Student Attack" isimli saldırı neticesinde EVIV yapısına kişisel oy doğrulama bileşeni eklenmiştir. Daha sonra denetleme mekanizması ve oylar için kayıt sunucusu eklentisi gibi yeniliklerle IVXV yapısı EIV sistemi için geliştirilmiş ve sistem bu yapı üzerinden devam etmiştir. IVXV yapısı ilk olarak 2017 senesinde

[1] Google translate kullanılarak çevrildiğinde; "Keda valite?" ve "Nimi Nimeste" sırası ile "Kimi seçiyorsun" ve "İsim Nimeste" şeklinde çevrilmektedir.



Şekil 1.1: VerApp Sonuç Ekran Görüntüsü Google Play-EH kontrollrakendus

kullanılmaya başlanmıştır. EVIV yapısında görülen kişisel doğrulama bileşeni ile gelen açıklığın IVXV sisteminde de devam ettiği görülmüştür. Bu açıklığın devam ettiği Şekil 1.1'de VerApp'nın indirileceği kaynaktan da görülmektedir.

1.5 Tezin Katkıları

Önerilen bu çözüm çalışabilir durumdadır fakat pratikte kullanılmaya çalışıldığında dezavantajlara sahiptir. Örnek olarak, kullanıcıdan karşılaştırması istenen bit dizisinin 256 bit uzunlukta (güvenlik parametresi) bir sayı olduğu düşünülürse, ayrıca seçmenin bu karşılaştırmayı göz ile yağacağı göz önüne alınırsa, bu dizinin göz ile karşılaştırma açısından büyük olmasından dolayı kişisel oy doğrulama sistemini kullanmak isteyen kullanıcı tarafından kullanımı zordur. Bu durum kişisel oy doğrulama sisteminin kullanılabilirliğini düşürmektedir. Kişisel oy doğrulama sistemini kullanacak profilin eğitimli ve büyük sayıları karşılaştırabileceği düşünülse bile bu karşlaştırma işleminin zaman alacağı ve hataya müsait olacağı aşikardır, kaldı ki kişisel sistemi herkesin kolay bir şekilde kullanabilmesi gerekir.

Yukarıda bahsedilen çözüm yönteminde, VerApp ekranında seçilen adayın açıkça gösterilmesi yerine, VoteApp ve VerApp ekranlarında gösterilecek bit dizilerinin seçmen tarafından karşılaştırması istenmektedir. Karşılaştırması istenen bit dizilerinin insan gözüyle karşılaştırma yapılacağı göz önüne alındığında, hataya açık bir yöntem olduğu görülmektedir, ayrıca kullanışlı değildir. EVIV yapısında, güvenliğe verilen önem kadar bu sistemin kullanışlı olmasına ve seçmenin kolay bir şekilde bu sistemi kullanabilmesine önem verilmektedir. Güvenlik açısından elektronik ve kriptografik olarak gerekli veya gereksiz bütün yöntemlerin kullanılması sistemi kullanışsız yapabilmektedir. Amaçlanan

güvenlik açısından temel gerekler sağlanırken, sistemin kullanışlı olmasını sağlamak, bunun için sistemin kullanışlı olması ve karşılanması gereken güvenlik gerekleri arasında denge gözetilmektedir. Bu denge düşünüldüğünde güvenlik için seçmenin bit dizilerini karşılaştırmasını istemek sistemi daha güvenli yaparken kullanışlılığı azaltmaktadır, bu yüzden önerilen çözüm sisteme eklenmesi için uygun değildir. Ayrıca önerilen çözümün sisteme eklenemeyeceği hakkında ayrıntılı bilgi [13] makalesinde yer almaktadır.

Açıklık olduğu düşünülen bu durumun kullanılarak seçmen oy bilgisinin ele geçirilmesi ile ilgili çalışma yapılmıştır. Bu çalışma doğrultusunda oluşturulan simülasyon ile kişisel oy doğrulama uygulamasını kullanan seçmenin oy bilgisinin başka bir uygulama tarafından ele geçirilmesi olayı gerçeklenmiştir. Bunu gerçeklemek için IVXV yapısında kullanılan ve açık kaynak kodlu VerApp indirilmiş derlenmiş ve simülasyon için kullanılabilir hale getirilmiştir. Sonrasında, aynı cihazda çalışan farklı bir uygulama kullanılarak VerApp ekran bilgisi elde edilmiştir. Bununla ilgili piyasada bulunan spyware'ler ve stalkerware'ler araştırılmıştır. Bu tür yazılımların planlı şekilde toplu kullanıldığında ve hazırlanan simülasyondakine benzer şekilde oy bilgisini ele geçirme eylemini gerçekleme amacıyla geliştirildiklerinde, seçim güvenliğinin tehlikeye düşebileceği ile ilgili açıklamalar yapılmıştır.

Zafiyetin varlığı ve neden olabileceği sonuçlarla ilgili çalışıldıktan sonra çözüm ile ilgili araştırmalar yapıldı. İlk olarak aynı cihazda çalışan farklı uygulamanın VerApp verilerini elde edememesi ile ilgili programatik olarak yapılabilecekler hakkında çalışıldı. Çalışmada VerApp'ın Android tabanlı işletim sistemi için geliştirilen versiyonu seçildi ve bu platformda yapılabilecekler üzerine çalışıldı. Çalışma neticesinde programatik olarak, VerApp uygulaması ekran verisine erişimin aynı cihazda çalışan diğer uygulamalara karşı izole edilebileceği görüldü. Spyware ve stalkerware yazılımlarının yeteneklerinin gelişmesi ve yaygınlığı düşünüldüğünde ilgili zafiyet için kriptografik çözümün önerildiği [11] incelendi. Bu önerinin güvenlik açısından işe yaradığı fakat kullanışlılık açısından eksik olduğu üzerinden yola çıkılarak önerilen bu çözümün kullanışlı olabilmesi için çalışma yapıldı. VerApp kullanan seçmenin daha kullanışlı ve rahat şekilde bu uyguamayı kullanması için çalışma yapıldı ve çözüm önerisinde bulunuldu, böylece zafiyet hem kriptografik olarak engellenmesi hem de kullanıcı dostu bir yöntem olması amaçlandı.

1.6 Organizasyon

Bölüm 1'de seçim, elektronik seçim, internet üzerinden yapılan seçim ile ilgili bilgiler verildikten sonra Estonya'nın kullanmış olduğu elektronik seçim anlatılmıştır. Sonrasında Estonya'nın kullanmış olduğu kişisel oy doğrulama sistemi incelemesi ile ilgili zafiyetten bahsedildi. Bölüm 2'de Estonya'nın kullandığı elektronik seçim sistemindeki bileşenler, roller ve tanımlar anlatıldı, devamında ise önceden kullanılan sistemden bahsedildi. Son olarak ise şimdi kullanılan yapı teknik altyapısıyla beraber anlatıldı. Bölüm 3'te Estonya'da halihazırda kullanılmakta olan kişisel oy doğrulama uygulaması için hazırlanan simülasyondan bahsedildi ve simülasyon kullanılarak zafiyetten yararlanılması ile ilgili çalışmadan bahsedildi, devamında ise kötü amaçlı yazılımlar hakkında bilgi verilip zafiyete dikkat çekildi. Bölüm 4'de bahsi geçen zafiyet hakkında çözüm önerileri anlatıldı. Son bölüm olan Bölüm 5'te tez sonucunda elde edilen sonuçlar anlatıldı.

Bölüm 2

Tanımlar

Estonya, yasal zemini olan ve ülke genelinde yapılan seçim sistemde, teknolojinin getirdiği imkanlar neticesinde internet üzerinden oylama yapma yöntemini de seçmenlerinin hizmetine sunmuştur. İlk olarak 2005 senesinde gerçekleştirilen bu sisteme elektronik seçim denilmesine rağmen internet üzerinden kullanıcılarına oylama yapmayı mümkün kıldığından Estonya İnternet Seçimi (EIV) şeklinde isimlendirilmektedir. EIV sistemi ile seçmene internet üzerinden oy kullanma imkanı sağlayan yapı EVIV şeklinde kod ile isimlendirilmiştir. Bu yapı 2005 senesinde kullanılmaya başlanmıştır, 2013 senesinde kişisel oy doğrulama mekanizması bu yapıya dahil edilmiştir. Bazı değişikliklerden sonra 2017 senesinden itibaren kullanılmaya başlanan IVXV kod isimli yapı ile EIV sistemi devam edegelmiştir. Bu bölümde EVIV, IVXV yapıları ve sisteme eklenen kişisel oy doğrulama bileşeni anlatılacaktır. Ağırlıklı olarak ise daha güncel olan IVXV üzerinde durulacaktır, ayrıca bu sistem ile ilgili ayrıntılı bilgi [1, 14] ile elde edileblir.

2.1 Estonya Elektronik Seçim Sistemi

Elektronik seçim birçok ülkede ve farklı şekillerde uygulanmaktadır. Bazı uygulama şeklinde oy vermek isteyen seçmen oy verme merkezine gidip oyunu elektronik cihaz yardımıyla kullanmaktadır. Bu şekildeki seçime de elektronik seçim adı verilmektedir ve bu hali ile kullanıcı yine oy verme merkezine kadar gitmek zorundadır. Estonya'da 2005 senesinden itibaren kullanılmaya başlanan elektronik seçimlerde ise oy kullanmak isteyen

seçmen, oyunu internet üzerinden ve istediği yerden kişisel bilgisayarı ile kullanabilmektedir. Bu yüzden Estonya'da kullanılan bu elektronik seçim yöntemine Estonya İnternet Oylama ismi de verilmektedir [1].

Elektronik seçimin ilk kullanılmaya başlandığı senelerde kişisel oy doğrulama sistemi kullanılmamaktaydı. 2011 senesinde EIV sistemine karşı bir saldırı yayımlandı [12]. Bu saldırı ile kullanılan oyların bloklanabileceği ve manipule edilebileceği gösterildi. Student attack isimli bu saldırı sonrasında Estonya, kullanılan elektronik seçime bir kişisel oy doğrulama sistemi getirmek için çalışmalara başladı. Çalışmalar sonunda kullanıcının oyunun doğru bir şekilde temsil edilmesi ve kullanılan oyun merkezi sunucuda doğru bir şekilde depolanması prensiplerini benimseyen bir doğrulama sistemi geliştirilmesine karar verildi. Bu iki prensip cast-as-intended ve recorded-as-cast şeklinde isimlendirilmektedir.

Geleneksel yöntemlerle yapılan seçimlerde seçmen oy kullanmak için oy verme merkezlerine gidip oyunu gizli bir şekilde kullanmaktadır. Oy verme merkezinde kendisine ayrılan kabinde oy kullanabilmektedir. Burada ikili zarf kullanarak oy oluşturulmaktadır. Seçmen bir dış zarf alır ve tercihini belirtmek için kullandığı pusulayı bu dış zarfın içerisine koyup oy sandığına, oluşturduğu ikili zarfı koymaktadır. EIV sisteminde de kullanıcı ikili zarf oluşturmaktadır. Bunlar dış zarf ve iç zarf şeklinde isimlendirilebilir. İlk olarak oy kullanma uygulamasında seçmen aday listesinden tercihini seçer ve bunu oy kullanma uygulamasının ürettiği bir rastgele sayıyı da işin içine katarak şifreler, şifreli bu veri iç zarf olarak tanımlanabilir. Oy kullanma uygulaması tarafından oluşturulan bu şifrelenmiş pusula seçmenin imzası ile imzalanır ve dış zarf oluşturulmuş olur. Sonra bu veri, merkezi sunuculara gönderilmektedir.

2013 senesine kadar Estonya seçimlerinde oy doğrulama sistemleri kullanılmamıştır. 2011 senesinde yayımlanan Student Attack üzerine Estonya, kişisel oy doğrulama sistemini geliştirdi ve bu sistem ilk olarak 2013 senesinde kullanılmaya başlandı. Bu sisteme göre istemci tarafında oy kullanma uygulaması ve kişisel oy doğrulama uygulaması çalışmakta. Kişisel oy doğrulama uygulaması 2013'ten itibaren kullanılmaya başlanmıştır.

Seçim işlemi tamamıyla toplamda 6 aşamadan oluşmaktadır [1]. Bu aşamalar aşağıdaki gibidir;

- **Seçim İlanı**: İlgili seçimin ilan edilmesi.

- **Adayların Kaydı**: Seçimin türüne göre eğer referandum değilse seçimde yarışacak, seçilen listelerinin kayıtlarının yapılması.
- **Seçmen Listesinin Hazırlanması**: Seçimde oy kullanma hakkına sahip adayların belirlenmesi ve bu adayların oy kullanabilecekleri bölgelerle ilişkilendirilmesi işlemleri.
- **Oylama**: Seçim Organizatörünün belirlediği tarihte oy kullanma hakkına sahip seçmenin oyunu kullanması.
- **Oy Sayımı**: Oy verme işleminin bitmesinden sonra bölgelere göre oyların sayılması.
- **Sonuçların Açıklanması**: Oy sayımından sonra sonuçların ilan edilmesi.

Yukarıda bahsi geçen oylama geleneksel oylama adımlarıdır. Elektronik oylama bu adımlardan sadece son üç aşama olan Oylama, Oy Sayımı ve Sonuçların Açıklanması aşamalarında kullanılmaktadır [1].

2.2 Estonya Elektronik Seçimi - EVIV

EIV sisteminde yapı olarak ilk EVIV benimsenmiştir, daha sonra ise oy sonuç bütünlüğü dikkate alınarak IVXV kod isimli oy doğrulama yapısı geliştirilmiştir. EVIV yapısında 2013 yılından itibaren kişisel oy doğrulama bileşeni kullanılabilmiştir. Kişisel oy doğrulama bileşeni gerçeklenirken sunucu taraflı saldırılara açık verilmemesi düşünülmüştür. Her ne kadar bilgisayarlarda zararlı yazılımlara karşı önlemler ve kriptografik önlemler alınsa da 2011 yılında açıklanan saldırı ile bilgisayarda bulunan zararlı yazılımları oy güvenliğini etkilemiştir, bu bakımdan oy verme sisteminin ve oy doğrulama sisteminin farklı cihazlarda olması uygun görülmüştür. Ayrıca oy verme sistemleri bilgisayar tabanlı sistemler olmasına karşın oy doğrulama sistemlerinin taşınabilir cihazlar üzerinden yapılmasına karar verilmiştir. Farklı sistemler kullanılması farklı işletim sistemleri ile işlem yapılmasına neden olması düşünülmüş ve böylece zararlı yazılımlara karşı önlem etkisi yapacağı düşünülmüştür. Getirilen kişisel oy doğrulama sistemi ile kullanıcı oy verme zamanı içinde herhangi zamanda yine istediği yerden oyunu kullanabilecek. Oy kullanma işlemi için bilgisayar ve internet bağlantısı gerekmekedir. NEC tarafından geliştirilen oy kullanma uygulaması kullanıcı tarafından internetten indirilebilmektedir.

Seçmen oy kullanma periyodu içindeyken internet üzerinden oy doğrulama uygulamasını indirir. İndirdiği uygulamayı kişisel bilgisayarında çalıştırdıktan sonra uygulama yardımı ile merkezi ana sunucularla SSL üzerinden iletişime geçmektedir ve oy kullanma hakkına sahip seçmen kullanıcı ID kartını kullanarak SSL bağlantısı ile merkezi sunuculara kimlik doğrulaması yapmaktadır [11]. Kimlik doğrulaması yapıldıktan sonra kullanıcıya merkezi sunucular tarafından seçim aday listesi gönderilmekte. Kullanıcı bu aday listesinden seçmek istediği adayı seçer. Seçimi oy kullanma uygulamasında yaptıktan sonra uygulama seçilen adayı merkezi sunucunun genel anahtarını kullanarak şifreler. Şifreli veri imzalanır ve saklanmak üzere merkezi sunuculara gönderilir. Oy kullandıktan sonra seçmen kişisel oy doğrulama işlemini gerçekleştirebilir. Oyunu kullanan seçmen kullanmış olduğu oyu doğrulamak için VerApp uygulamasını kullanmalı, açık kaynak olarak bu uygulama internet üzerinden paylaşılmaktadır. Oy doğrulama sistemi taşınabilir akıllı cihazlarda yapılabilmektedir. Kişisel oy doğrulama işleminin gerçekleştirilebilmesi için kamerası olan bir akıllı cihaza ve internet bağlantısına ihtiyaç vardır [11]. VerApp uygulamasını edinen seçmen oyunu doğrulamak istediğinde oy kullanma uygulamasının ürettiği QR kodunu VerApp uygulamasına okutmaktadır. VerApp uygulaması merkezi sunucularla iletişime geçer ve merkezi sunucuya QR kodu ile edindiği bazı bilgileri göndermektedir. Merkezi sunucu oy doğrulama uygulamasına şifreli ve imzalı olan veriyi ve seçim aday listesini gönderir. Bu verileri alan VerApp sistemi nihai bazı kriptografik hesaplamalar ve işlemlerden sonra seçmene kullanmış olduğu oy bilgilerini göstermektedir. Örneğin seçmen oy için A partisinden K adayını ve B partisinden L adayı için oyunu kullanmışsa kullanıcıya oy doğrulama süreçlerinin sonunda bu bilgiler gösterilmektedir. Seçmen'e bu şekilde kullandığı oyu doğrulama imkanı verilmektedir. Oy doğrulama esnasında seçmenin kullandığı oy ile VerApp uygulamasının gösterdiği oy eşleşmezse merkezi sunuculara alarm gönderilmektedir.

Estonya'nın ilk olarak 2005 senesinde seçmenlere internet üzerinden oy verme imkanı sağlayan oylama sistemi EVIV şeklinde kodlanmaktadır. EVIV seçim sistemine 2013 senesinde kişisel oy doğrulama sistemi de eklenmiş ve 2015 senesine kadar bu sistem kullanılmıştır. Bu sistem istemci ve sunucu taraflardan oluşmaktadır. İstemci tarafı oy kullanmak isteyen seçmenin oyunu kullanacağı oy kullanma uygulaması ve oyunu kullanan seçmenin, sonrasında kullanmış olduğu oyu doğrulayacağı kişisel oy doğrulama uygulaması oluşturmaktadır. Sunucu tarafında ise kendilerine göre özelleşmiş işleri yapan temel olarak şu sunucular bulunmaktadır;

- **Oy Yönlendirme Servisi (Vote Forwarding Server)**: Seçmenin oy kulanma uygulamasında ikili zarf şeklinde oy oluşturmasını sağlar, sonrasında kişisel oy doğrulama uygulaması ile seçmene oyunu doğrulama imkanı sağlar. Çevrimiçi olarak çalışan merkezi sunucudur.

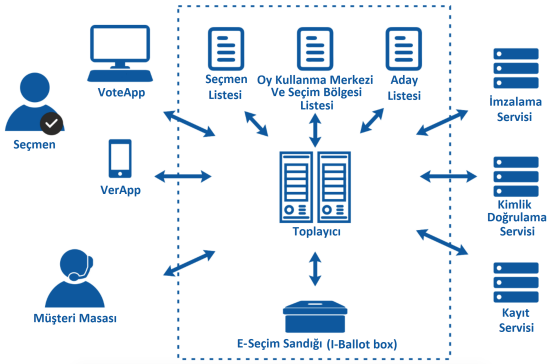
- **Oy Depolama Servisi (Vote Storage Sever)**: Seçim periyodu boyunca imzalı ve şifreli oyları saklar. Seçim sonunda sayım aşamasına geçilebilmesi için elektronik olarak birden fazla kullanılan oyları son oy geçerli olacak şekilde iptal eder. Geçersiz oyları belirler ve iptal eder. Sayım aşaması öncesi uygun olmayan oylar iptal edildikten sonra oyların imzaları alınarak anonimleştirilir ve karıştırma mekanizması kullanılarak karıştırılır. Sonuç olarak sayıma hazır anonimleştirilmiş ve karıştırılmış şifreli oylar elde edilir [11].

- **Sayım Yapan Servis (Tallier)**: Anonimleştirilmiş ve karıştırılmış şifreli oyların şifrelerini çözer ve sayma işlemini gerçekleştirir.

2.3 Estonya Elektronik Seçimi - IVXV

Sistem üzerine yeni geliştirmeler yapılarak IVXV şeklinde kodlanan seçim yapısı ile devam edilmiştir [14]. Aslında yapısal olarak EVIV ve IVXV benzerdir, sadece IVXV ile yeni özellikler getirilmiştir. Bunlardan ilki Denetleme Mekanizması ile ilgili eklentilerdir, ikinci yenilik ise Kayıt Servisi (Registration Service) isimli yeni bir rol tanımlanmış olması [14]. EVIV yapısında RSAA-OAEP kripto sistemi kullanılmaktaydı fakat esnek şifre çözme yöntemlerinini kullanmak için bu kripto sistemi, El Gamal kripto sistemi ile değiştirilmiştir [14]. Sistemin denetlenebilirliğini artırmak ve doğrulama mekanizasını geliştirmek adına eklentiler yapılmıştır, bu bölümde IVXV seçim sisteminde tanımlanan roller anlatılacak, sonrasında seçimde kullanılan uygulamalar hakkında bilgi verilecek, en sonunda ise sistemin süreçleri tanıtılacaktır. Ayrıntılı bilgi için [1, 14].

EIV sisteminde kullanılan IVXV yapısında kullanılan bazı operasyonel ve harici varlıklar Şekil 2.1 ile gösterilmektedir.



Şekil 2.1: EIV Sistemi Sunucular ve Bileşenler [1]

2.3.1 Rol Tanımları

Gelişmiş sistemlerde olduğu gibi EIV'de yapılan işler bölünmüştür ve kendi içinde özelleşmiştir, tüm sistemde bileşenler, bileşeni kullananlar ve bileşenleri yönetenler için roller vardır.

- **Seçim Organizatörü (Election Organizer)**: Elektronik seçimin düzenlenmesini sağlayan ana roldür. Seçim Organizatörü (EO) elektronik seçimi gerçeklemek için gereki olan tüm bileşenlerin görevlerini tanımlar ve gerekli rol atamalarını yapar. Seçmenin elektronik olarak oyunu internet üzerinden kullanmasını sağlayacak uygulamaları sağlar ve bu uyulamaları güvenli kanallardan seçmene ulaştırır. Ayrıca elektronik seçimin güvenli şekilde yapılması için gerekli olan kriptografik yapıtaşların oluşturulmasını sağlar. Elektronik seçimde asimetrik şifreleme yöntemi kullanılmaktadır; açık ve özel anahtar çiftlerini oluşturur. EO seçim periyodunda seçmene oy kullandırma işini Vote Collection (Oy Toplama - VC) sunucusuna yaptırır, buna ek olarak Seçim Organizatörü elektronik seçimin gerçeklenmesinde kullanılan merkezi sunuculara görevlerini yaptırmaktadır.

- **Oy Kullanacak Seçmen (Voter)**: Seçimin ilan edilmesinden sonra oy kullanma hakkında sahip olan seçmen listesi seçim bölgelerine göre belirlenir. Bu listede yer alan vatandaşlar seçmen olarak tanımlanır. Belirlenen listedeki seçmen seçim periyodu boyunca VoteApp uygulamasını kullanarak oy kullanabilir ve VerApp uygulamasını kullanarak kullandığı oyu doğrulayabilir.

- **Aday Listesi (Candidate List)**: Seçimin ilan edilmesinden sonra adayların başvuruları alınır ve bunlardan seçilme hakkına sahip olanlar için liste oluşturulur.

Elektronik seçim periyodu boyunca internet üzerinden oyunu kullanmak isteyen seçmene oy kullanma sürecinde aday listesi gönderilmektedir. Seçmen bu aday listesi üzerinden tercihini yapmaktadır.

- **Toplayıcı (Collector)**: Elektronik seçim periyodu boyunca oyunu elektronik olarak kullanmak isteyen seçmen VoteApp uygulamasını kullanarak ikili zarf şeklindeki elektronik oyunu oluşturmaktadır. Bu oyu oluşturmaya Toplayıcı yardım etmektedir. Toplayıcı, VoteApp uygulaması ile güvenli bir kanal oluşturur ve bu kanal üzerinden veri alış verişi gerçekleşir ve VoteApp ikili zarf şeklindeki oyu oluşturur. Oluşturulan bu oy yine Toplayıcı'ya gönderilir. Toplayıcı bu oyu RE'e sonrasında doğrulama işleminde kullanılmak üzere gönderir. Ayrıca Toplayıcı, VerApp uygulaması ile iletişime geçerek seçmene oyunu doğrulama imkanı sağlamaktadır.

- **İşleyici (Processor)**: İşleyici, çevrimdışı olarak çalışan bir merkezi sunucudur. Elektronik seçim sürecinde sayım işleminden önce ve oy toplama ve kaydetme işleminden sonraki süreci kapsar. Toplayıcı tarafından kendisine gelen imzalı ve şifreli oyların imza doğrulamasını yapar. RS tarafından kendisine gelen oyların zaman işareti ile Toplayıcı tarafından gelen oyların uygunluğu kontrol edilir. Hem kişisel oylarda hemde seçim sandıklarında doğrulama işlemleri İşleyici tarafından yapılır.

  Elektronik seçim sürecinde oy kullanma hakkına sahip seçmen hem internet üzerinden oyunu birden fazla defa kullanabilmekte hemde oy verme merkezlerine gidip oyunu kullanabilmektedir. Elektronik seçimin bu özelliği seçmene karşı uygulanabilecek zorlama ve tehdit olaylarını ortadan kaldırmaya yönelik koruma sağlayabilir. Kötü niyetliler tarafında bir seçmen seçimde bir adaya oy vermeye zorlanabilir. Bu durumda seçmenin oyunu kullandıktan sonra tekrar oy kullanması, zorlanarak kullandığı oyun iptal edilmesine neden olur, böylece zorlama olaylarına birnevi önlem olmaktadır. Sonuç olarak seçmen tarafından oy iki şekilde tekrar edebilir. Tekrar edilen bu oylar İşleyici tarafından belirlenmektedir.

  İşleyici, kendisine gelen oyların doğrulamasını yaptıktan sonra oy listesinde bir seçmen tarafından kullanılmış birden fazla oyları saptar. Belirlenen bu oylardan tarihi eski olanlar iptal edilir, yani bir seçmen elektronik seçim sürecinde internet üzerinde birden fazla oy kullandıysa bu oylardan en son olanı geçerli olacak şekilde öncekiler iptal edilir.

Seçmenin hem internet üzerinden oylama yapması hemde oy verme merkezine gidip orada oy kullanması durumunda İşleyici internet üzerinden oy kullanma uygulaması ile kullanılan oyu iptal eder. Böylelikle oy verme merkezinde kullanılan oy geçerli olur.

Tekrar eden oyların kaldırılmasından sonra oyların anonimleştirilmesi işlemi yapılır. İşleyici tarafından oylardaki imzalar kaldırılır ve böylece oyların sahipleri belirsizleşir. Bu işlemden sonra oyların karıştırılması işlemi vardır. Oyların karıştırılması İşleyici'de yapılacağı gibi ayrı bir bileşen tarafından da yapılabilir. Ayrı bileşenle yapılacaksa bunu Mixer Service (Karıştırıcı Sunucusu) gerçeklemektedir.

- **Sayma ve Sonuçlama (Tallier)**: İşleyici tarafından anonimleştirilmiş ve karıştırılmış oylar Tallier'a gelir. Tallier rolünü EO gerçekleştirmektedir. Aldığı şifreli oyları önce açmaktadır. Açma işlemini gerçekleştirebilmesi için özel anahtar'lara sahiptir. Özel anahtarları kullanarak kendisine gelen şifreli oyları çözer. Akabinde açık oyların sayımını gerçekleştirir.

- **Denetçi (Auditor)**: Her bileşen kendine ait özel işini yapar ve diğer bileşene bir sonraki yapılacak iş için veriler gönderir. Dolayısıyla bileşenler arasında veri akışları olmaktadır. Bileşenler arasında taşınan bu verilerin tamamlığı ve bütünlüğünü kontrol eden rol Denetçi rolüdür.

- **Müşteri Masası (Client Desk)**: Seçim esnasında birçok problemle karşılaşılabilir. Elektronik seçimde seçmenin sorun yaşaması durumunda muhatabı Müşteri Masası'dır. Toplayıcı tarafından alınan verilerle seçmene yardımcı olunur. Süreçte istenen yardımlar ve çözümlerini kendi veritabanına kaydeder.

- **Tanımlama Servisi (Identification Service)**: Gerekli görülen durumlarda seçmeni tanımlamak için kullanılan sevistir.

- **Seçmen Listesi oluşturan ve Güncelleyen Servis (Compiler and Updater of the List Voter)**: Bu servis Seçmen listesini derler ve gerekli olan durumlarda (listenin oylama döneminde değişmesi) liste güncellenir [11].

- **Kayıt Sunucusu (Registration Service - RS)**: Kayıt Sunucusu rolü IVXV kodlu EIV sistemine yeni eklenen bir roldür. Toplama Sunucusu ile beraber çalışmaktadır. Toplama Sunucusu, VoteApp kullanan seçmenden oyunu aldıktan sonra ilgili oyu RS'ye göndermektedir. RS kendisine gelen her oyu onaylar ve sonra herbir oya

zaman damgası iliştirir. Ayrıca VerApp'ı kullanan seçmen oyunu kullandıktan sonra bu uygulama ile RS'de oyunun doğru şekilde kayıtlı olduğunu Toplama Sunucusu üzerinden doğrulayabilmektedir.

Oylama işlemleri bittikten sonra RS kaydetmiş olduğu tüm oyları ve seçim sandık listelerini İşleyici Servis'e göndermektedir. İşleyici ise RS'den aldığı veriler ile Toplama Sunucusu'ndan adığı verileri karşılaştırır. Sonunda herbir oy için ve seçim sandığı için doğrulama işlemi yapılır.

2.3.2 Kullanılan Uygulamalar

Bir önceki bölümde EIV sistemi IVXV yapısında tanımlanmış olan rollerden bahsedilmişti. Bu roller kişiler ya da elektronik cihazlar şeklinde tanımlanmıştır. Sistemi bir bütün olarak düşündüğümüzde roller var ve bu rolleri gerçekleyen insanlar ve elektronik cihazlar. Bu bölümde sistemde kullanılan cihazlar ve uygulamalar anlatılacaktır.

Temel olarak uygulama ya da cihazlar iki şekilde sınıflandırılabilir ve bu uygulamalardan bazıları çevrimiçi bazıları ise çevrimdışı olarak çalışmaktadır. İlk olarak istemci tarafındaki uygulama ve cihazlar, ikinci olarak sunucu tarafındaki uygulama ve cihazlar şeklinde sınıflandırma yapılabilir.

İstemci tarafta çalışan VoteApp uygulaması ile VerApp uygulaması oy kullanan seçmen tarafından kullanılmaktadır ve her iki uygulama da çevrimiçi olarak kullanılmaktadır. İki cihazda da zararlı yazılımın bulunması ve eşzamanlı olarak çalıştırılması durumunda zafiyet doğacağından dolayı bu iki uygulamanın farklı işletim sistemlerinde kullanılması uygun görülmüştür. Bu sebeple VoteApp; Windows, Mac, Linux gibi bilgisayar işletim sistemlerinde kullanılacak şekilde geliştirilmiş ve VerApp ise Android, IOS gibi akıllı cihaz işletim sistemlerinde kullanılacak şekilde geliştirilmiştir.

IVXV yapısında kullanılan bazı uygulamalar:

- **Oy Kullanma Uygulaması** (VoteApp): VoteApp seçmen tarafından seçim zamanında, kendi bilgisayarında, internet üzerinden oy kullanmasını sağlayan, çevrimiçi olarak çalışan ve bu yolla merkezi sunuculara bağlanan uygulamadır. Bu uygulama EO tarafından kendi sitesinden yayımlanmaktadır ve güvenli bir kanal ile

güvenli bir şekilde seçmen bilgisayarına indirilmesi için gerekli yapı EO tarafından sağlanır. VoteApp sistemde iki bileşen ile etkileşime girerek oy verme sürecine katkı sağlar. Bunlardan birincisi Toplama Servis'idir.VoteApp, merkezi sunucu olan Toplama Servisi ile güvenli kanal kurar ve bu kanal üzerinden Toplama Servisi'nin yardımı ile ikili zarf şeklindeki oyu oluşturur. İkinci olarak kişisel oy doğrulama uygulaması ile dolaylı yoldan etkileşime girmektedir. VoteApp, kişisel oy doğrulama süreci için kullanılması gereken verileri QR şeklinde yayımlar, QR kodu kişisel oy doğrulama uygulaması tarafından kullanılarak doğrulama süreçleri gerçekleştirilir.

- **Kişisel Oy Doğrulama Uygulaması** (VerApp): VerApp, seçmene kullanmış olduğu oyun merkezi sunuculara tam bir şekilde ve bütünlüğünün bozulmadan ulaştığını ayrıca merkezi sunucularda doğru bir şekilde kaydedildiğini doğrulama imkanı sağlayan bir uygulamadır. VerApp, çevrimiçi kullanılan bir uygulamadır ve istemci tarafı uygulamasıdır. VerApp'ı kullanabilmek için kamerası olan ve internet bağlantısı olan bir akıllı cihaza ihtiyaç vardır. Oy verme ve kişisel oy doğrulama aşamalarında zararlı yazılımın hem VoteApp'da hem de VerApp'da aynı anda çalışarak zararlı faaliyette bulunmasını engellemek amacıyla bu iki uygulamanın farklı platformlarda çalışması uygun görülmüştür, bu nedenle VoteApp ve VerApp farklı işletim sistemlerinde çalışmaktadır. VerApp'ı kullanmak isteyen seçmen oyunu kullandıktan sonra ilgili uygulama mağazasından uygulamayı edinebilmektedir. VerApp süreçlerinde iki uygulama ile iletişime geçmektedir. Birincisi VoteApp, ikincisi ise Toplama Servisi'dir. VoteApp ile seçmen oyunu kullandıktan sonra uygulama bir QR kodu oluşturmaktadır. Bu kod VerApp tarafından kamera yardımıyla okutulur ve devamında Toplama Servisi ile bir iletişim kanalı oluşturulur. Bu kanal yardımı ile Toplama Sunucu'su ve VerApp arasında veri alışverişi olur. VerApp kendisine gelen verileri birtakım kriptografik işlemlerden geçirdikten sonra seçmenin kullanmış olduğu oyu veya oyları ekranında seçmene göstermektedir. Kişisel Oy Doğrulama işlemi, VoteApp ile oyun kullanılması ve Toplama Sunucusu'na oy ulaştıktan sonra, belirli bir süre ve belirli sayıda yapılabilmektedir.

- **Anahtar Uygulaması (Key Application)**: EO'nun ana aracıdır. Anahtar yönetimi, seçim ana şartlarının yerine getirilmesinde önemlidir ve oylamanın gizliliği ve doğruluğu seçmenin bağımsızlığı gibi konularda en önemli rolleri üstlenir. Seçimde kullanılan her oy için genel anahtar ve özel anahtar'ları üretir.

Seçmen VoteApp yardımıyla ikili zarf şeklinde bir oy oluşturmaktadır. İkili zarf iki aşamada oluşmaktadır. Birinci aşaması şifreleme ikinci aşama ise imzalamadır. Şifreleme işlemi için asimetrik şifreleme yöntemi kullanılmaktadır ve Anahtar Uygulaması tarafından üretilen genel anahtar kullanılarak şifreleme işlemi yapılır. Anahtar uygulaması tarafından üretilen özel anahtarlar ise şifre çözme işlemi için kullanılmaktadır. Seçim sonucu açıklandıktan sonra özel anahtarlar imha edilmektedir.

Anahtar çiftinin oluşturması ve özel anahtar kullanımı birkaç paydaş tarafından gerçekleştirilmektedir. Paydaşların belirlenmesi belirlenen kurallar dahilinde yapılmaktadır.

- **Toplama Sunucusu (Collection Service)**: Merkezi bir sunucu olan Toplama Sunucusu çevrimiçi çalışan ve seçmene şifreli oy oluşturma imkanı sağlayan bir sunucudur. VoteApp, Toplama Sunucu'su ile internet üzerinden bir kanal oluşturmaktadır. Bu kanal üzerinden VoteApp'a oy oluşturabilmesi içn gerekli veriler gönderilir. Bu sayede VoteApp ikili zarf şeklindeki oyunu oluşturur. Kişisel Oy Doğrulama işlemi de Toplama Sunucusu kullanılarak yapılmaktadır. VerApp, Toplama Sunucusu ile internet üzerinden bir kanal oluşturur ve bu kanal üzerinden Toplama Sunucusu'ndan alınan veriler doğrultusunda, VerApp doğrulama işlemini gerçekleştirmektedir. Ayrıca Toplama Sunucusu kendisine gelen oyları kayıt için Kayıt Sunucusu'na göndermektedir, gönderilen bu oylar daha sonra İşleyici Sunucusu'nda doğrulama işlemi için kullanılacaktır. Toplama Sunucusu oylama süreci sona erdiğinde kendisine gelen oyları imzalayarak İşleyici Sunucusu'na teslim eder.

- **İşleyici Uygulaması (Processing Application / I-Ballot Box Processor (IBBP))**: İşleyici rolünü gerçekleştirmek için kullanılan ve çevrimdışı olarak çalışan sunucudur. Kayıt Sunucusundan ve Toplama Sunucusundan kendisine gelen oylar için karşılaştırma yaparak doğrulama işlemi gerçekleştirir. Elektronik oylama sürecinde kullanılan oylara bakarak bir seçmenin birden fazla kullandığı oylar tespit edilir ve bunlar arasında eski oylar iptal edilerek seçmenin kullandığı en son oyun geçerli olması sağlanır. Ayrıca paralel oylama durumunda, yani bir seçmenin hem

elektronik ortamda hemde oy kullanma merkezinde oy kullanma durumunda, elektronik oyu iptal edilir, böylece geleneksel yöntemlerle oy kullanma merkezinde kullanılan oy geçerli olur. Daha sonra elektronik oyların imzaları alınarak bu oyların anonimleştirilmesi sağlanır. Bu noktada oyların artık kime ait olduğu belirsizdir. Son olarak eğer Karıştırma Sunucusu kullanılıyorsa ilgili oylar Karıştırma Sunucusu'na gönderilir, kullanılmıyorsa karıştırma işlemi yapılır ve oylar şifre çözme işlemi ve kalan diğer işlemler için ilgili sunucuya gönderilir.

- **Karıştırma Sunucusu (Mixing Application / Mixing Server (MS))**: IBBP tarafından anonimleştirilen oylar bir sonraki işlemde karıştırılırlar. Bu karıştırma işlemi IBBP tarafından yapılacağı gibi farklı bir bileşen olan MS tarafından da yapılabilir. IVXV yapısında ayrı bir sunucu olarak MS kullanılıyorsa, oy verme süreci sonunda oylar IBBP'ta işlemlerden geçtikten sonra karıştırılması için MS'a gönderilir.

- **Denetleme (Data Audits)**: IVXV yapısında süreçler arasında veri akışları olmaktadır. Bu süreçler arasındaki karşılıklı giriş ve çıkış verilerinin uyumluluğu kontrol edilir. Ayrıca süreçler arasında dijital olarak imzalanmış verilerin bütünlüğü ve gerçekliği kontrol edilir [1].

2.3.3 Estonya İnternet Seçimi - EIV

Bu bölümde IVXV yapısı anlatılacaktır ve notasyon [14] ile aynı şekilde kullanılmıştır. Bu yapıda temel olarak 3 kriptografik uygulama vardır, güvenlik parametresi λ olmak üzere bunlar şu şekildedir:

- Kriptografik özet alma fonksiyonu, $\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^{O(\lambda)}$
- Dijital imzalama , $\mathsf{Sig} = (\mathcal{G}_{\mathsf{sig}}, \mathcal{S}_{\mathsf{sig}}, \mathcal{V}_{\mathsf{sig}})$ buradaki parametreler şu şekilde açıklanabilir:
  - Kullanıcı imzası üretme $(\mathsf{sk}_{\mathsf{sig}}, \mathsf{pk}_{\mathsf{sig}}) \leftarrow \mathcal{G}_{\mathsf{sig}}(\mathsf{pp}_{\mathsf{sig}})$ şeklinde olur, burada $\mathsf{pp}_{\mathsf{sig}}$ genel parametresi ile kullanıcı özel ve genel anahtar çifti oluşturulmaktadır.
  - Kullanıcı $\mathsf{sk}_{\mathsf{sig}}$ özel anahtarı ile m mesajını imzalar, $\sigma \leftarrow \mathcal{S}_{\mathsf{sig}}(\mathsf{sk}_{\mathsf{sig}}, m)$.
  - Kullanıcı imzası σ, m mesajı ve kullanıcı imzası için üretilen genel anahtar $\mathsf{pk}_{\mathsf{sig}}$ kullanılarak imza doğrulanmaya çalışılır. Burada $b = 1$ durumu imza

ile doğrulamanın yapılabildiği, $b = 0$ ise imza ile doğrulamanın yapılamadığı anlamına gelir.

- Açık anahtarlı şifreleme yöntemi kullanılır, $\mathsf{Pec} = (\mathcal{G}_{\mathsf{pec}}, \mathcal{E}_{\mathsf{pec}}, \mathcal{D}_{\mathsf{pec}})$. Buradaki parametreler şöyledir:
  - $\mathsf{pp}_{\mathsf{pec}}$ genel parametresi kullanılarak kullanıcı için özel ve genel anahtar çifti üretilir, $(\mathsf{sk}_{\mathsf{pec}}, \mathsf{pk}_{\mathsf{pec}}) \leftarrow \mathcal{G}_{\mathsf{pec}}(\mathsf{pp}_{\mathsf{pec}})$.
  - Kullanıcı genel anahtarı $\mathsf{pk}_{\mathsf{pec}}$ kullanılarak açık metin m şifrelenir, bunun için $\mathcal{E}_{\mathsf{pec}}$ şifreleme operasyonu ile şifreli mesaj c oluşturulur, $c \leftarrow \mathcal{E}_{\mathsf{pec}}(\mathsf{pk}_{\mathsf{pec}}, m)$.
  - Kullanıcı özel anahtarı $\mathsf{sk}_{\mathsf{pec}}$ kullanılarak şifreli metin c'nin şifresi çözülür, bunun için $\mathcal{D}_{\mathsf{pec}}$ şifre çözme operasyonu ile m açık metin oluşturulur, $m \leftarrow \mathcal{D}_{\mathsf{pec}}(\mathsf{sk}_{\mathsf{pec}}, m)$.

Doğrulama işlemleri için kullanılan sistemde , Açık Anahtarlı Altyapı kullanılmaktadır (PKI) ve bu yapı sertifika otoritesi (CA) tarafından sertifikalandırılmaktadır, ayrıca oy kullanma hakkında sahip tüm seçmenler için ayrı ayrı özel-genel anahtar çifti ve bunların CA tarafından sertifikalandırılması işlemi yapılmaktadır. Seçmenin özel-açık imza anahtar çifti $(\mathsf{sk}_{\mathsf{sig}}^{\mathsf{CA}}, \mathsf{pk}_{\mathsf{sig}}^{\mathsf{CA}})$ şeklinde, ilgili sertifika ise $\mathsf{Cert}_{\mathsf{CA}}$ şeklinde ifade edilmektedir.

Benzersiz tanımlayıcıya sahip oy kullanma hakkına sahip herbir seçmen ($\mathsf{v} \in \mathsf{V}$), CA tarafından onaylanmış birer anahtar çiftine sahiptirler.

$$\forall \mathsf{v} \in \mathsf{V},\ (\mathsf{sk}_{\mathsf{sig}}^{\mathsf{v}}, \mathsf{pk}_{\mathsf{sig}}^{\mathsf{v}}) \leftarrow \mathcal{G}_{\mathsf{sig}}, \mathsf{Cert}_{\mathsf{v}} = \mathcal{S}_{\mathsf{sig}}(\mathsf{sk}_{\mathsf{sig}}^{\mathsf{CA}}, (\mathsf{v}, \mathsf{pk}_{\mathsf{sig}}^{\mathsf{v}}))$$

CA, bit dizisi b ve $\mathsf{Cert}_{\mathsf{v}}$ için Zaman Damgası Servisi'ni (TMS) sağlamaktadır.

Yukarıda bahsedilen notasyonla aynı şekilde ifade edilen ve Kayıt Servisi (RS) için sağlanmış olan özel-genel anahtar çifti $(\mathsf{sk}_{\mathsf{sig}}^{\mathsf{RS}}, \mathsf{pk}_{\mathsf{sig}}^{\mathsf{RS}})$ ve ilgili sertifika $\mathsf{Cert}_{\mathsf{RS}}$ oluşturulmuştur.

- **Ön Oylama Fazı**: EO seçim planında işletilecek roller için çeşitli görevlendirmeler yapar, ayrıca seçim sonuçlarının hesaplanması adına işlemler yapacaktır. Seçim bölgelerine göre oy kullanma hakkına sahip olacak seçmen listeleri hazırlanır, yine seçim bölgeleri dikkate alınarak aday listeleri belirlenir. Seçime katılan aday listesi C ile ifade edilir ve kaç tane aday yarıştığı bilgisi ise ℓ ile ifade edilmektedir. Ayrıca

EO, IVXV'de kullanılacak ve PKI yapısına göre düzenlenecek özel-genel anahtar çiftlerini üretir.

$$(\mathsf{sk}_{\mathsf{pec}}, \mathsf{pk}_{\mathsf{pec}}) \leftarrow \mathcal{G}_{\mathsf{pec}}$$

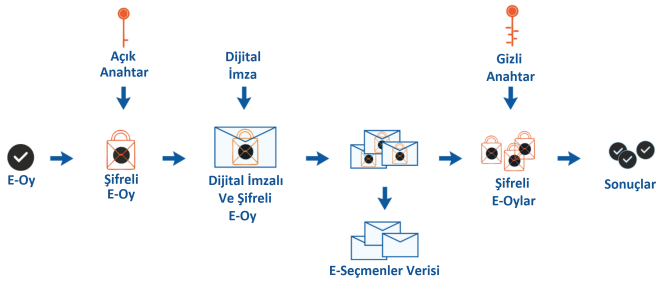
EO, diğer rolleri atamanın yanında kendisi oy sayma sürecini işletme rolünü (Tallier) gerçekleştirir ve bunun için gerekli olan özel anahtarı saklar. Özel anahatar kullanılarak şifre çözme işlemi yapılmakta ve oy sayımı yapılmaktadır.

IVXV yapısında kullanılan VC, IBBP, RS ve kullanılacaksa eğer MS gibi bağımsız merkezi sunucuların yetkilendirilmesi ve rol dağılımları EO tarafından yapılır.

Açık anahtar $\mathsf{pk}_{\mathsf{pec}}$ kullanımı aktif edilir ve anahtar çiftleri için gerekli sertifikalandırılmalar yapılır.

EO tarafından oy kullanma uygulaması olan VotApp ve kişisel oy doğrulama uygulaması olan VerApp seçmenler için güvenli yollardan sağlanır. Ayrıca VerApp, EO haricindeki organizasyonlar tarafından da seçmen kullanımına sunulabilmektedir.

- **Oy Verme Fazı**: Oy Verme Fazı'nda, oy verme hakkına sahip seçmen ($v \in V$), kişisel bilgisayarında VoteApp kullanarak, uygulamaya gelen aday listesinden $\mathsf{c_v} \in \mathsf{C}$ bir aday seçer ve ikili zarf usulü şifreli ve imzalı oy oluşturur. Oluşturulan bu oy merkezi sunucuya VoteApp marifeti ile gönderilir. İkili zarf yöntemi ile şifreli imzalı oy Şekil 2.2 ile gösterilmektedir. Ayrıca Oy Verme Fazı Şekil 2.3 ile gösterilmektedir.



Şekil 2.2: Estonya İnternet Oylama İkili Zarf Yapısı [1]

Estonya İnternet Oylama adımlarını şu şekilde özetleyebiliriz:

C_1. İkili zarf yapısı oluşturmak için ilk adım olan ve $\mathsf{ballot}_{\mathsf{c,r}}$ şeklinde ifade edilen iç zarfı oluşturma işlemi yapılır. Şifreleme işleminde kullanılacak rastgele sayı üretilir, $\mathsf{r_v} \in \{0,1\}^{O(\lambda)}$. Sonrasında ise seçmenin seçtiği aday bu rastgele sayı

da hesaba katılarak şifreleme işlemi yapılır. Şifreleme için PKI yapısındaki genel anahtar kullanılır. $\mathsf{ballot}_{\mathsf{c,r}} \leftarrow \mathcal{E}_{\mathsf{pec}}(\mathsf{pk}_{\mathsf{pec}}, (\mathsf{c}_{\mathsf{v}}, \mathsf{r}_{\mathsf{v}}))$.

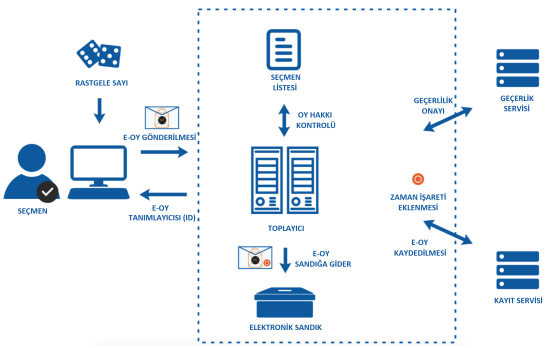
C_2. İkili zarf yapısı oluşturmak için ikinci adım olan dış zarfı oluşturma işlemi yapılır. Burada şifrelenmiş oy seçmen özel anahtarı kullanılarak imza işlemi yapılır, $\sigma_{\mathsf{v}} \leftarrow \mathcal{S}_{\mathsf{sig}}(\mathsf{sk}^{\mathsf{v}}_{\mathsf{sig}}, \mathsf{ballot}_{\mathsf{c,r}})$. Sonuç olarak şifreli imzalı ikili zarf prensibinde oy oluşturulmuş olur, $\mathsf{vote}_{\mathsf{v}} \leftarrow (\mathsf{ballot}_{\mathsf{c,r}}, \sigma_{\mathsf{v}})$.

C_3. $(\mathsf{v}, \mathsf{Cert}_{\mathsf{v}}, \mathsf{vote}_{\mathsf{v}})$ verileri merkezi sunucu olan VC'ye çevrimiçi olarak gönderilir.

C_4. VC ise cevap olarak oy için benzersiz tanımlayıcı ($\mathsf{vote}_{\mathsf{id}}$) ve RS sunucusunun onayını ($\mathsf{reg}_{\mathsf{vote}_{\mathsf{id}}}$) cevap olarak döner.

C_5. VoteApp dijital olarak imzalanmış $\mathsf{reg}_{\mathsf{vote}_{\mathsf{id}}}$ verisini $\mathcal{H}(\mathsf{vote}_{\mathsf{v}})$ ile doğrular.

C_6. Benzersiz tanımlayıcı olan $\mathsf{vote}_{\mathsf{id}}$ bilgisi ile rastgele üretilen r_{v} değeri bilgisi VoteApp tarafından oylama yapıldıktan sonra kullanılmak için QR kod formuna dönüştürülür. Oluşturulan bu QR kodu oylama işlemi tamamlandıktan sonra VerApp tarafından kullanılarak kişisel oy doğrulama işlemi için kullanılır.



Şekil 2.3: Oy Verme Fazı [1]

- **Oy Depolama Fazı**: Seçmen tarafından VoteApp kullanılarak internet üzerinden oy kullanma işlemi gerçekleştikten sonra merkezi sunucularda ilgili bu oyu kaydetme ve oyu doğrulama süreçleri çalışır. Bu işlemler, VC ve RS merkezi sunucuları ile gerçekleştirilmektedir. Bu sürecin adımlarını şu şekilde sıralayabiliriz:

S_1. VC tarafından $\mathsf{vote}_{\mathsf{v}}$ için seçmen (v) ve onun imzası (σ_{v}) doğrulanır.

S_2. İlgili oy için oyun temsil edilmesi adına VC tarafından benzersiz tanımlı olarak $\mathsf{vote}_{\mathsf{id}}$ oluşturulur.

S_3. $\mathcal{H}(\mathsf{ballot}_{\mathsf{c,r}})$'ın $\mathsf{Cert}_{\mathsf{v}}$ ile zaman olarak ($\mathsf{Cert}_{\mathsf{v}}$) doğrulanabilmesi için VC zaman işareti ($\mathsf{ts}_{\mathsf{vote}_{\mathsf{id}}}$) elde eder, $\mathsf{ts}_{\mathsf{vote}_{\mathsf{id}}} = \mathcal{S}_{\mathsf{sig}}(\mathsf{sk}^{\mathsf{TMS}}_{\mathsf{sig}}, (\mathsf{Cert}_{\mathsf{v}}, \mathcal{H}(\mathsf{ballot}_{\mathsf{c,r}}), \mathsf{utc}_{\mathsf{vote}_{\mathsf{id}}}))$.

S_4. VC tarafından oyun kaydedilmesi için RS'ye kayıt isteği gönderilir, $\mathsf{req}_{\mathsf{vote_{id}}} = \mathcal{S}_{\mathsf{sig}}(\mathsf{sk}^{\mathsf{VC}}_{\mathsf{sig}}, (\mathsf{vote_{id}}, \mathcal{H}(\mathsf{vote_v})))$.

S_5. RS tarafından $\mathsf{req}_{\mathsf{vote_{id}}}$ kayıt isteği doğrulanır, daha sonra VC'ye imzalı onay gönderilir, $\mathsf{reg}_{\mathsf{vote_{id}}} = \mathcal{S}_{\mathsf{sig}}(\mathsf{sk}^{\mathsf{RS}}_{\mathsf{sig}}, \mathcal{H}(\mathsf{req}_{\mathsf{vote_{id}}}))$.

S_6. VC merkezi sunucudan oy kullanma uygulaması olan VoteApp'a, oy için oluşturulan benzersiz tanımlayıcı $\mathsf{vote_{id}}$ ve RC tarafından oluşturulan kayıt onayı $\mathsf{reg}_{\mathsf{vote_{id}}}$ gönderilir.

Oy kullanma hakkına sahip herhangi seçmen elektronik olarak birden fazla defa oy kullanabilmektedir. Kullanılan oylardan en sonuncusu geçerli olur fakat kullanmış olduğu oyların hepsi kaydedilir, Oy Depolama Fazı süreçlerinden geçer. Herhangi oy kullanma hakkına sahip seçmenin başarılı şekilde kullandığı bir oydan sonra VC ve RC merkezi sunucularında oy ile ilgili şu bilgiler tutulur:

- VC tarafından depolanan veriler

$$\mathsf{stored}_{\mathsf{vote_{id}}} = (\mathsf{v}, \mathsf{Cert_v}, \mathsf{vote_v}, \mathsf{vote_{id}}, \mathsf{ts}_{\mathsf{vote_{id}}}, \mathsf{reg}_{\mathsf{vote_{id}}}),$$

- RC tarafından depolanan veriler

$$\mathsf{registered}_{\mathsf{vote_{id}}} = (\mathsf{req}_{\mathsf{vote_{id}}}, \mathsf{reg}_{\mathsf{vote_{id}}}).$$

- **Kişisel Oy Doğrulama Fazı**: Oy kullanan seçmen bu işlemden sonra kullanmış olduğu oyun doğru bir şekilde temsil edildiği ve doğru bir şekilde merkezi sunucularda kayıt edildiğini VerApp kullanarak doğrular. Kişisel oy doğrulama adımları şu şekilde sıralanabilmektedir:

V_1. VoteApp tarafından oluşturulan ve oy benzersiz tanımlayıcısı $\mathsf{vote_{id}}$ ile oy kullanma esnasında oluşturulan rastgele sayı $\mathsf{r_v}$ bilgilerini barındıran QR kodu VerApp tarafından kamera yardımı ile elde edilir.

V_2. VerApp, VC ile TLS tabanlı güvenli kanal oluşturur. Bu kanaldan benzersiz tanımlayıcı olan $\mathsf{vote_{id}}$ VC sunucusuna gönderilir.

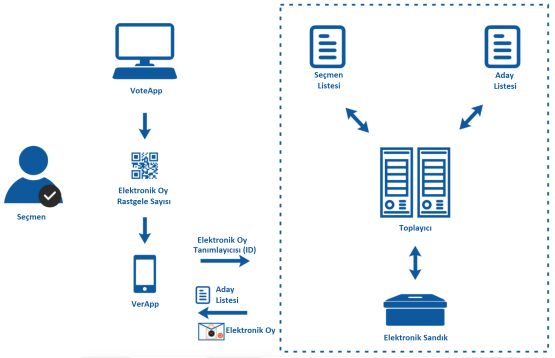
V_3. VC tarafından cevap olarak, şifreli imzalı oy $\mathsf{vote_v}$ ve oyun kayıt onayı $\mathsf{reg}_{\mathsf{vote_{id}}}$ gönderilir. Bilinmeyen bir $\mathsf{vote_{id}}$ için veya kişisel oy doğrulama için müsade edilen zaman dolmuş ise hata dönülür.

V_4. VerApp tarafından $\mathsf{vote}_{\mathsf{id}}$ ve $\mathsf{reg}_{\mathsf{vote}_{\mathsf{id}}}$ doğrulanır. Daha sonra seçmenin seçmiş olduğu aday uygulama ekranında seçmene gösterilir.

V_5. VerApp kendisine gelen seçim aday listesi C ve QR kodundan elde ettiği rastgele sayı olan $\mathsf{r_v}$'yi kullanarak tüm aday listesi için şifreleme işlemi yapar, $\mathsf{c}' \in \mathsf{C}$.

$$\mathcal{E}_{\mathsf{pec}}(\mathsf{pk}_{\mathsf{pec}}, (\mathsf{c}', \mathsf{r_v})) = \mathsf{ballot}_{\mathsf{c,r}} \, .$$

V_6. Herbir aday için şifeleme işlemi ve karşılaştırma işlemi tamamlandıktan sonra c' olan seçmenin kullanmış olduğu oy veya hata mesajı VerApp ekranında seçmene gösterilir.



Şekil 2.4: Kişisel Oy Doğrulama Fazı [1]

Yukarıda bahsedilen IVXV fazlarından Kişisel Oy Doğrulama Fazı Şekil 2.4 ile gösterilmektedir. Kişisel Oy Doğrulama Fazı'ndan sonraki fazlar için detaylı anlatım burada yapılmayacaktır. Bu fazlar için [14] kaynağından detaylı bilgi elde edilebilir.

Bölüm 3

Analiz

Oy kullanma hakkına sahip seçmene internet üzerinden oy kullanma imkanı sağlayan EIV sistemi, elektronik ortamlarda yapılan ve güvenlik gerektiren diğer sistemler gibi çok fazla gerekliliklere sahiptir. Bu gerekliliklerin başında güvenlik ve kullanılabilirlik gelmektedir. Seçim için seçim gerekliliklerinden hepsinin sağlanması zordur [7, 15]. Kriptografik altyapının sağlanırken, gizlilik ve doğrulanabilirlik ile kullanıabilirlik arasındaki denge gözetilmelidir [16]. Güvenlik gerekliliklerini sağlamak adına kullanıcı dostu olmayan bir sistem geliştirmek sistemin kullanılmamasına neden olacaktır, bu yüzden sağlanması gereken gerekliliklerin belirlenmesi ve bu gerekliliklerin kullanıcı dostu bir sistemle karşılanması gerekmektedir.

EIV sisteminde seçim için gerçekleştirilecek operasyonlar özelliklerine göre bölünmüş ve farklı otoriteler arasında paylaştırılmıştır, böylece sistem içinde güven otoriteler arasında paylaştırılmıştır. Seçmenin oy kullanabileceği kişisel bilgisayarları da bu bileşenlerden birini oluşturmaktadır ve güvenli olduğu varsayılmaktaydı. 2011 senesinde EIV'ye karşı "Student Attack" saldırısının gösterilmesi ve merkezi sunucularda geçersiz oy ile karşılaşma gibi durumların oluşması, sistemin gözden geçirilmesi gerekliliğini göstermiştir. Yaşanan bu olaylardan sonra sisteme Kişisel Oy Doğrulama bileşeni eklenmiştir ve 2013 senesinden itibaren kullanılmaya başlanmıştır. Doğrulama için getirilen bileşen, oy kullanma uygulamasının çalıştığı cihazdan farklı bir cihazda çalışmak üzere tasarlanmıştır ve sisteme eklenen yeni cihaz ile saldırı yüzeyi artmıştır. Bu bölümde, ilk olarak sisteme eklenen Kişisel Oy Doğrulama bileşeni ve bu bileşenle meydana gelen yeni zafiyet ile ilgili bilgi verlecektir. Sonrasında, VerApp uygulaması ile aynı Android cihazda çalışan farklı

bir uygulamanın, VerApp'ı kullanan seçmenin oy bilgisini elde etmesi gösterilecetir. Son olarak bahsedilen zafiyeti kullanabilecek zararlı yazılımlar ile ilgili bilgiler paylaşılacaktır.

3.1 Kişisel Oy Doğrulama Bileşeni ve Bununla Gelen Zafiyet

EIV sisteminde, VerApp uygulaması akıllı cihazlarda kullanılmaktadır. EIV sisteminde, VoteApp ile kullanıcıya elektronik seçim periyodunda konum sınırlaması olmaksızın oy verebilme imkanı sağlandığı gibi VerApp ile seçim periyodunda konum sınırlaması vermeden oyunu doğrulayabilme imkanı sağlanmaktadır. Böylelikle kullanıcı yani oy verme hakkına sahip seçmen kişisel oy doğrulama işlemini seçim süreci boyunca istediği yerde yapabilme özgürlüğüne kavuşmaktadır. Bu kolaylık elektronik seçimin seçmene getirdiği avantajlardan biridir, bununla seçmene oyunu doğrulayabilme imkanı verilmektedir ve güvenlik gereklerinin sağlanması açısından fayda sağlamaktadır. Fakat, sistem güvenlik gereklerinin sağlanması için eklenen yeni bileşen ya da özelliklerin farklı zafiyetler doğurmaması gerekir ve EIV sisteminin en az kağıt bazlı geleneksel yöntemlerle yapılan seçimler kadar güvenli olması gerekir.

VerApp uygulamasını kullanarak, kullanmış olduğu oyu doğrulamak isteyen seçmen VoteApp uygulamasının ürettiği QR kodu kullanarak doğrulama işlemini gerçekleştirebilmektedir. VoteApp uygulamasının çıktısı olan QR kodu VerApp uygulamasının girdisi olacaktır. Kişisel Oy doğrulama işlemi için oy kullanma hakkına sahip seçmenin, elektronik seçim periyodu içinde VoteApp ile oy verme işlemini gerçekleştirmesi gerekir. Kişisel oy doğrulama işlemi, oy kullanma işlemi yapıldıktan sonra otoritenin belirlediği zaman içinde ve yine otoritenn belirlediği sayıda yapılabilmektedir. Kişisel oy doğrulama için seçmen VoteApp çıktısı olan QR kodunu VerApp uygulamasına okutur. Kişisel oy doğrulama işleminin yapılacağı akıllı cihaz kamerası marifetiyle VerApp uygulaması, giriş olarak aldığı bu QR kodunu önce anlamlandırır ve sonra elde ettiği verilerden gerekli olanları merkezi sunucuya gönderir. Sonrasında oy doğrulama yapılacak uygulamaya sunucu tarafından doğrulama için kullanılacak veriler gelir. VerApp bu verileri kullanarak seçmene kendi oyuna ait bilgiyi ekranda göstermektedir. Oy doğrulama işlemleri sırasında kriptografik işlemler kullanılmaktdır ve güvenliğin sağlandığı düşünülmektedir fakat seçmene tüm bu işlemlerin sonucunda kullandığı oy bilgisi açık bir şekilde gösterilmekte

ve bu durum seçim güvenliği açısından zafiyet doğurmaktadır. VerApp uygulamasının kullanıldığı akıllı cihazlarda kullanıcının haberi olmadan çalışan zararlı yazılımlar olabilir. Kriptografik olarak ve yazılım kabiliyetleri kullanılarak bu tür yazılımların tam anlamıyla engellendiği varsayılsa dahi kullanıcıdan cihaz erişimleri ile ilgili izinler alındıktan sonra herhangi bir uygulama yine izin alınan erişimleri kullanarak kullanıcı bilgisi dışında zararlı faaliyetler yürütebilir. Seçim sisteminde kullanılan oy doğrulama uygulamasının çalıştığı cihazda eş zamanlı çalışan diğer uygulamalar için de bu durum geçerli olabilir. Ayrıca seçim sisteminde oy kullanacak kitleyi düşündüğümüzde ülke vatandaşlarından geniş bir profil ortaya çıkmaktadır ve bahsi geçen bu kitledeki tüm kişi profillerinin kendi cihazı ve cihazındaki uygulamaları bilinçli kontrol etmesini, ayrıca hakkında bilgili ve uzman olduğunu düşünmek yanlıştır.

Gizli oylama prensibi açısından zafiyet bulunması seçim güvenliği açısından tehdit oluşturmaktadır. Seçmenlerin oylarının açığa çıkması seçim gidişatını bozabilir, kişisel çıkarlar için kullanılabilir, daha önemlisi demokrasi açısından birçok zafiyet doğurabilir. Bu tehditler düşünüldüğünde ve oy doğrulama işlemi süreci sonunda seçmen oyunun açık bir şekilde gösterilmesi düşünüldüğünde bu zafiyetin üzerine gitmek için motivasyon ortaya çıkmıştır.

3.2 VerApp Simülasyonu ve Zafiyetin Kullanılması

EIV için çeşitli platformlarda açık kaynak kodlu projeler geliştirmiş ve bunlar yayımlamıştır. VerApp için geliştirilen projelere iOS tabanlı oy doğrulama, Android tabanlı oy doğrulama ve Windows telefonlar için oy doğrulama projeleri örnek verilebilir. Analiz için kullanım yaygınlığı ve ilerde kullanım potansiyeli de dikkate alınarak android tabanlı oy doğrulama sistemi incelendi.

Geliştirilen oy doğrulama sistemleri açık kaynak kodludur ve kodlar Github [1] internet sayfalarında paylaşılmaktadır. Android tabanlı doğrulama bileşeni kodu da bu platformda paylaşılmıştır. Analiz için IVXV yapısında kullanılan VerApp projelerinden Android tabanlı geliştirilen ivotingverification projesi kullanıldı. Github'ta açık kaynak kodlu olarak paylaşılan bu proje indirildi ve Android tabanlı cihazlar için geliştirme olanağı sağlayan Android Studio IDE'sinde derlendi.

[1] Github Web Sayfası: https://github.com/vvk-ehk/

Temel olarak amaçlanan bahsi geçen zafiyeti Android tabanlı sistemde gerçeklemek oldu ve oy doğrulamada bu açıklığı ortaya çıkarmak için bir simülasyon sistemi kurmak gerekti. Hedeflenenin sadece bahsi geçen zafiyetin ortaya çıkarılması olduğu için VerApp kullanımı sırasında, seçilen aday bilgisinin aynı cihazda çalışan başka bir uygulama tarafından elde edilmesi üzerine gidildi. Simülasyon modelinde VerApp karşısında gerçek bir seçim sistemi bulunmadığından VerApp modifiye edilerek uygulama üzerinde seçilen listesi hazırlandı.

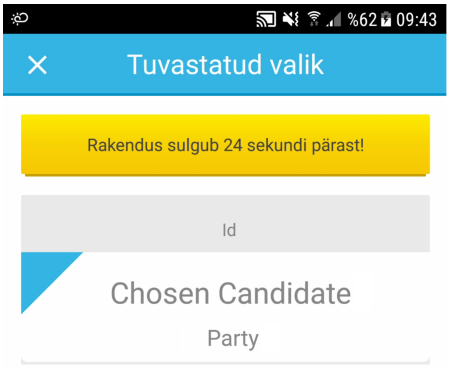
Simülasyon için ilk olarak IVXV yapısında kullanılan Android tabanlı oy doğrulama sistemi üzerinde çalışıldı. Bu uygulama Android tabanlı geliştirilen bir yazılım olmasından dolayı Android Studio IDE'si kullanılarak analiz edilmiştir. Analiz işlemini gerçekleştirmek için Android uygulama geliştirme üzerine çalışmalar yapıldı. Edinilen yetkinlikler de kullanılarak Android tabanlı VerApp uygulaması analiz edilmiştir. Simülasyonda hedeflenen, kişisel oy doğrulama uygulamasının son aşamalarından olan seçilen listesinin ekranda gösterildiği anda, cihazda çalışan başka bir uygulamanın cihaz ekran görüntüsünü almasını sağlamak olmuştur. Bunu sağlamak için cihazda ekran görüntüsü alan başa bir uygulama üzerinde çalışılmıştır. Araştırmalar sonunda, kullanıcıya istediği zaman aralıklarında cihaz ekranında ne gösterildiyse kaydetmesini sağlayan Ekran Görüntüsü Kaydet (Screenshot Capture and Recorder) (SCAR) isimli ve 3.0.9 versiyonlu uygulama Google Play Store'dan tespit ve temin edildi.

IVXV yapısında kişisel oy doğrulama için kullanılan ivotingverification isimli uygulama (VerApp) temel olarak MainActivity, QRScannerActivity, VoteDownloadActivity ve BruteForceActivity gibi aktivitelerden oluşmaktadır. Android cihazda VerApp başlatıldığında, seçmenden ilerleme talimatı alındıktan sonra uygulamada QR okuma işlemi başlatılmaktadır. Okunması istenen QR ise VoteApp uygulamasının ürettiği QR kodudur. Kod okutulduktan sonra anlamlandırılıyor, veriler elde ediliyor ve sonra merkezi seçim sunucusuna gönderiliyor. Daha sonra merkezi sunucu, seçmenin seçtiği seçilenin verisini ve kriptografik işlemlerde kullanılacak veriyi VerApp'a gönderiyor. VerApp bu verileri bazı kriptografik işlemlerden geçiriyor ve seçmenin seçtiği adayları açık olarak elde ediyor. Son aşamada ise VerApp elde ettiği kullanıcı tarafından seçilen listesini açık metin şeklinde ekranında gösteriyor.

Simülasyonu gerçeklemek için yukarıda bahsedilen seçim sunucuları kullanılmayacağından ve hedeflenenin sadece ekranda açık şekilde gösterilecek seçilen listesinin başka bir

uygulama tarafından ekran görüntüsü alma yöntemi kullanılarak elde edilmesi olduğundan, VerApp'ın bazı işlemleri atlayıp sadece seçmene doğrulaması için gösterdiği seçilen listesini göstermesi sağlandı.

VerApp işleminin bu şekilde simüle edilebilir hale getirilmesinden sonra SCAR uygulaması VerApp ile aynı cihazda çalıştırıldı. SCAR uygulaması başlatıldığı ve sonlandırıldığı zaman aralığındaki cihaz ekranında gösterilen tüm içerikleri kaydetme özelliğine sahiptir. Bu uygulama başlatıldığında kullanıcıdan erişim izni almakta. Erişim izni alması VerApp uygulamasının güvenliği açısından Android'in sağladığı güzel bir özellik, fakat önceden de bahsedildiği gibi kişisel oy doğrulama uygulamasını kullanan kitle düşünüldüğünde, kullanıcının diğer uygulamalara cihaz kaynaklarına erişim izni vermeden oy doğrulama uygulamasını kullanacağı varsayımı güvenlik açısından zafiyet doğuracak bir yaklaşımdır. Bu yüzden ekran görüntüsü alan uygulamaya kaynak erişimi izni verildi başlatıldı ve sonrasında simülasyon için hazırlanan VerApp uygulaması çalıştırıldı. VerApp yukarıda bahsedildiği şekilde aşamalardan geçirildi ve nihai olarak cihazı kullanan seçmenin seçmiş olduğu adayı/adayları ekranda görüntüledi. Daha sonra ekran görüntüsü alan uygulamanın ekran görüntülerini kaydettiği ve gizli olan seçilen aday bilgisini elde edebildiği gözlemlendi. Şekil 3.1'da ekran görüntüsü alan uygulamanın (SCAR) elde ettiği veri gösterilmektedir, bu verideki bilgi VerApp uygulamasına ait seçilen aday bilgisidir.



Şekil 3.1: SCAR Tarafından Elde Edilen VerApp Bilgisi

3.3 Zararlı Yazılımlar ve VerApp Zafiyeti

Bir önceki bölümde anlatıldığı şekilde simülasyon ortamında, VerApp ile aynı cihazda çalışan başka bir uygulama kullanılarak VerApp bilgilerine ulaşım sağlanmıştı. Simülasyonda ekran görüntüsü bilgisini almak için zararlı yazılım alanında özelleşmiş ve işletim

sisteminden ekran görüntüsü bilgisini illegal yollarla alma konusunda kabiliyetli bir uygulama kullanılmadı, aksine sadece kullanıcıdan gerekli izinleri aldıktan sonra ekran görüntüsü kaydı alan herhangi bir uygulama ile bilgiler elde edildi. Alanında özelleşmiş bir zararlı yazılım kullanılmadan, sadece ekran görüntüsü alan bir uygulama ile VerApp ekran görüntüsü verisinin elde edilebildiği düşünüldüğünde, akıllı cihazlarda spyware, stalkerware, spouseware türünden yazılımlar kullanılması durumunda seçmenin kullandığı oy bilgisinin açığa çıkması zafiyeti olduğu görülmektedir.

Spyware yazılımlarını detaylandırmak gerekirse, kullanıcının bilgisi ile veya bilgisi dahilinde olmadan cihazına kurulan ve akıllı cihaz aracılığı ile bilgi toplamaya çalışan casus yazılımlardır. Bu tür yazılımlar akıllı cihazın sistematik bir zayıflığından yararlanarak veya kullanıcı tarafından akıllı cihazın yanlış kullanımı, uygulamanın yanlış kullanımı gibi durumlardan yararlanarak faaliyet sürdürür. Spyware; yenilik ve eğlence (örn: Walkinwat (Android), Ikee (iOS), NMPlugin (Symbian OS)), kullanıcının özel bilgilerini toplama ve satma (örn: Droid Dream Light (Android), Privacy.A (iOS), SPIsSaga (Symbian OS)), kullanıcı kimlik bilgilerini çalmak (örn: Ikee.B (iOS), InSprit (Symbian OS)), özel tarifeli çağrılar ya da SMS mesajları (örn: Fake Player (Android), Flocker (Symbian OS)), SMS spam'ı (örn: Geinimi (Android), Shurufa (Symbian OS)), web sayfası sıralaması manipülasyonu (örn: Hong Tou Tou (Android)) gibi amaçlar için kullanılabilmektedir [17]. Spyware'ler çok geniş amaçlı kullanılmaktadırlar ve ayrıca farklı şekillerde kullanılabilmektedirler bu yüzden farklı sınıflandırmalara ihtiyaç duyulmuştur, stalkerware'de bunlardan biridir. Stalkerware için net bir tanımlama bulunmamasına rağmen yasal casus olarak da ifade edilebilmektedir [18]. Bu yazılımlar ticari amaçlı veya kötü amaçlı olarak kullanılabilirler. Stalkerware'ler çocuk bakımı veya gözetimi, akraba bakımı veya gözetimi, meslektaş gözetimi gibi konularda kullanılabildiğinden yasal zemine oturmuş halde kullanılabilmekteler [19]. Çocuğu akıllı cihaz kullanan ebeveynler, internet ya da cihazın çeşitli zararlarından çocuklarını korumak, çocuklarının akıllı cihazlarını kontrollü bir şekilde kullanmasını sağlamak için bu hizmeti veren stalkerware uygulamaları kullanabilir ve bu uygulamaya gerekli izinleri verebilir. Bir işyerinde personeli takip etmek için bu tür stalkerware'ler kullanılabilir. Örneklere bakıldığında stalkerware'lerin kullanım alanları anlaşılabilir. Yukarıdaki örneklerden de anlaşılacağı gibi bu tür yazılımlar bazı yasal ihtiyaçları karşılayabilmektedir, fakat bu yazılımların sahip oldukları olanaklar onlara başka türülü kullanılma imkanı da vermektedir. Stalkerware kötü amaçlı olarak kullanılırsa eğer, kullanıcının özel bilgilerini farklı amaçlar için elde

edip kullanabilir. Ayıca, yazılım mağazaları istatistiklerine bakıldığında şu şekilde bilgiler elde edilmiştir; casus yazılımların %28'i sadece Android'de kullanım için, uygulamaların geri kalanı ise hem Android hem de iOS için kullanılabilir; iOS uygulamalarının %52'si cihaza veya herhangi bir uygulama kurulumuna fiziksel erişim gerektirmez, bunun yerine iCloud kimlik bilgilerine ihtiyaç duyar; uygulamaların %41'i tam takvim erişimine sahiptir; uygulamaların %79'u sosyal medya sızıntısını desteklemştir; uygulamaların %82'si kullanıcının tarayıcı alışkanlıklarını gözetlemek için işlevsellik sağlar; uygulamaların % 82'si cihazda depolanan dosyalara erişim sağlar ve uygulamaların %50'si uzaktan kontrol yeteneği sağlar [20].

Yukarıda bahsedildiği üzere spyware ve stalkerware gibi yazılımların akıllı cihazlardaki etkinliği kullanıcılar açısından risk oluşturmaktadır. VerApp için yapılan simülasyon ve bu simülasyonda bir uygulamanın VerApp ekran görüntüsü bilgisine ulaşmasının yanında, yaygın olarak kullanılan spyware ve stalkerware yazılımları dikkate alındığında ve bu yazılımların akıllı cihazlarda yaygınlığı düşünüldüğünde, bu yazılımların seçime yönelik sistemli bir şekilde kullanılması durumunda, seçmenlerin kullandığı VerApp uygulamasının verileri elde edilebilir ve bu durum seçim güvenliği açısından risk oluşturmaktadır.

EIV sistemi, oy kullanmak için, VoteApp uygulamasının kullanıldığı kişisel bilgisayarın güvenli olduğunu varsaymaktadır. Bunun yanında kişisel oy doğrulaması için VerApp uygulamasının kullanılacağı akıllı cihazın da güvenli kabul edilmesi, güvenlik varsayımları düşünüldüğünde tutarlı görünebilir. Ayrıca, sistem, güvenlik gereklerini ve kullanılabilirlik gereklerini dengede tutarak tasarlandığından tutarlı görülebilir, fakat akıllı cihazlardaki kullanım artışı daha çok saldırganın dikkatini çekmektedir [21, 22], bu yüzden zafiyeti önlemek için getirilen kişisel oy doğrulama bileşeninin yeni bir açıklığa neden olmaması gerekir.

Bölüm 4

İyileştirme Onerileri

Önceki bölümlerde EIV sisteminde güvenlik gerekçesi ile sisteme eklenen kişisel oy doğrulama bileşeninin yeni bir açıklık getirdiğinden bahsedildi, ayrıca bu durum geliştirilen bir simülasyon ile gösterildi. Bu doğrultuda uygun çözümler hakkında çalışmalar yapıldı. Bu bölümde yapılan bu çalışmalar anlatılacaktır. Çözüm olarak iki yöntem üzerinde durulmuştur. Birincisi VerApp uygulamasını modifiye etmek, ikincisi ise [11]'de önerilen çözüm önerisini geliştirerek sisteme eklenen kişisel oy doğrulama sürecini seçmen açısından daha kullanıcı dostu hale getirmek. İlk yöntem programatik olarak VerApp uygulamasında yapılacak geliştirme hakkındadır. Bu geliştirme, kişisel oy doğrulama süreci boyunca oy doğrulamanın yapıldığı cihazda VerApp uygulaması haricinde çalışan başka uygulamaların ekran görüntüsü almasını engellemeye yönelik olmuştur. Diğer yöntem için kriptografik çözüm önerisinde bulunan [11] incelendi ve önerilen bu çözümün eksik noktası olan kullanıcı dostu olmaması sorunu için çeşitli algoritmalar düşünüldü geliştirme yapıldı ve bu konuda çözüm önerilerinde bulunuldu.

4.1 Ekran Görüntüsü Almayı Engelleme

IVXV yapısında oy kullanan seçmenler VerApp uygulamasını kullanarak kişisel oy doğrulama işlemini gerçekleştirmektedir. Önceki bölümlerde bahsedildiği gibi ekran görüntüsü alma ile ilgili zafiyet VerApp uygulaması üzerinden olmaktadır. Bu uygulama istemci taraflı çalışan bir uygulamadır ve VoteApp uygulamasının çalıştığı işletim sisteminden farklı bir işletim sisteminde çalışması güvenlik gerekçelerinden dolayı uygun görülmüştür.

VerApp akıllı cihazlarda kullanılabilmektedir, bu yüzden akıllı cihazlarda ekran görüntüsü alma operasyonları üzerine çalışıldı. Temel olarak amaçlanan akıllı cihazlarda çalışan bir uygulamaya ait ekran görüntüsü verilerinin aynı cihazda çalışan başka bir uygulama tarafından elde edilmesini engellemek olmuştur. Bunu gerçekleyebilmek için VerApp uygulamasını çalıştırmak ve bu uygulama üzerinden bunu gerçeklemek uygun görülmüştür. VerApp akıllı cihazarda çalışmaktadır ve akıllı cihazlar üzerinde de iOS, Android ve Windows Phone gibi farklı işletim sistemleri için çalışması gerekmektedir, bu yüzden farklı işletim sistemleri için geliştirilen ve IVXV'de kullanılan VerApp uygulamaları mevcuttur. Bu uygulamalar Github [1] internet sitesi sayfasında yayımlanmaktadır. Bu versiyonlar üzerinde çalışıldı ve Android işletim sistemi için geliştirilen VerApp (ivotingverification) uygulaması seçildi.

Akıllı cihazda çalışan bir uygulamanın ekran görüntüsü verisini, aynı akıllı cihazda çalışan başka bir uygulamadan koruması için çeşitli yollar vardır [23]. Örneğin, iOS işletim sistemi kullanan akıllı cihazlarda ekran görüntüsü koruma ile ilgili önlem build zamanlı alınmak yerine kullanıcının ekran görüntüsü alma zamanında alma üzerinedir. Fakat, Screen-ShieeldKit gibi üçüncü parti SDK'lar kullanılabilmektedir [23]. Diğer bir yandan Android işletim sistemi Honeycomb (ver. 3.0) versiyonundan itibaren build zamanında ekran görüntüsü almayı bloklama ile ilgili mekanizma sunmuştur. Yapılan araştırmalar neticesinde , Android cihazda geliştirilen uygulamada, ekran görüntüsünün korunmasının istendiği ilgili kod bölümüne

```
WindowManager.LayoutParams.FLAG_SECURE
```

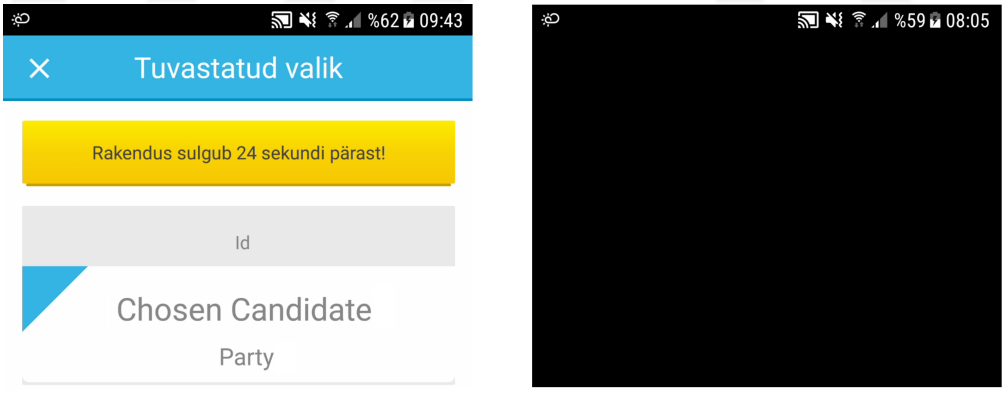
kod satırı eklenerek ekran görüntüsü verisini koruma işlemi yapılabileceği görülmüştür. Bu yöntem kullanılarak VerApp uygulamasının çalıştığı cihazda çalışan diğer uygulamaların, VerApp uygulaması ekran görüntüsü verisine ulaşması engellenebilir.

FLAG_SECURE bir window bayrağıdır ve pencere (window) içeriğini korumak için kullanılır, aynı cihazda kullanılan başka uygulamalarca ekran görüntüsü verisinin korunmasını sağlayabilir. Bu bayrak kullanılarak ekran görüntüsü verisine ulaşmak isteyen uygulamalara ayrıca kontrollü bir şekilde engel olunabilmektedir. Örneğin bu bayrak (flag) kullanılarak ekran görüntüsü eylemi için içerik göstermeme, bilgilendirici hata mesajı gösterme, alternatif bir içerik akışı seçme veya farklı bir strateji seçilebilir [24].

[1] Github Web Sayfası: https://github.com/vvk-ehk/

Android geliştirme ortamının bu flag ile sağlamış olduğu imkanın IVXV ortamında kullanılabileceğini görmek için çalışma yapıldı. Bunun için, Github'tan indirilen Android işletim sistemi için geliştirilmiş VerApp uygulaması Android Studio ortamında derlendi, çalıştırıldı. Uygulama IVXV sistemi ile çalışmaktadır, bu yüzden seçim zamanında merkezi sunucu ile ve VoteApp ile veri alışverişi yapması gerekmektedir. Bunu sağlayabilmek için kendi ortamıma indirdiğim VerApp uygulamasında geliştirmeler yapıldı. Bu geliştirme sonucunda uygulama, karşısında sunucu ve VoteApp olmadan da aldığı herhangi bir QR kodu ile belirlenmiş olan seçilen aday listesini ekranında göstermektedir.

Uygulama bu şekilde derlendikten sonra bahsedilen güvenlikle ilgili flag BruteForceActivity içerisindeki onCreate metodu içerisine yerleştirilmiştir. Seçilen aday listesi BruteForceActivity'de gösterildiğinden flag'i uygulamanın bu modülüne koymak uygun görülmüştür. VerApp bu şekilde hazırlandıktan sonra bu uygulama ile aynı cihazda çalışacak ve uygulamanın ekran görüntüsü verisini alacak uygulama (SCAR) akıllı cihazda çalışır hale getirildi. Bu şekilde simülasyon hazırlandıktan sonra VerApp uygulamasının ekran görüntüsü verisinin SCAR tarafından alınamadığı görüldü. Simüasyonunda güvenlik bayrağının kullanılması ve kullanılmaması durumunda SCAR'ın elde etmiş olduğu ekran görüntüsü Şekil 4.1 ile gösterilmektedir.



Şekil 4.1: Güvenlik bayrağı kullanılmadan öncesi ve sonrası

4.2 Oy Oluşturma ve Kişisel Oy Doğrulama İşlemerinde İyileştirme

Şimdiye kadar akıllı cihazda çalışan VerApp uygulaması ekran görüntüsü bilgisi alma sorunu için programatik olarak yapılabilecek çözümden bahsettik, fakat bu yöntem kök

(root) cihazlarda çalışan uygulamalar için işe yaramayabilir. Programatik yönteme karşı, root akıllı cihazlardaki geliştiriciye sunulan esneklikler ve geliştirme olanakları kullanılarak VerApp ekran görüntüsü bilgisi alma işleminin yapılabilme imkanı vardır. Bu yüzden ekran görüntüsü bilgisi alma problemi ile ilgili ikinci bir yöntem incelenmiştir. Oylama sürecinde, oy depolama sürecinde ve kişisel oy doğrulama sürecinde değişikliğe gidilen kriptografik çözüm incelenmiştir [11]. Bu yöntemle EIV sistemine eklenen VerApp uygulamasından kaynaklanan yeni bir açıklık kriptografik yöntemler kullanılarak giderilmiştir ve EIV sisteminde VerApp ile ilgili olan, ekran görüntüsü verisine ulaşma durumu programatik olarak gerçekleştirilebilse bile elde edilen bu veri anlamlı olmayacaktır. Sonuç olarak bu ikinci yöntem kullanıldığı durumda VerApp bileşeninin saldırıya uğrayıp ekran görüntüsü bilgisi elde edilse bile bu veri bir anlam ifade etmeyecek, çünkü seçilen adayların açıkça gösterilmesi yerine anlamsız bit dizileri elde edilmiş olacak. Eklenmesi önerilen bu yöntemde Bölüm 2 deki IVXV için geçerli olan notasyonlar kullanılmıştır.

Önerilen çözümde seçim sisteminde seçim sisteminin ilan edilip oylamadan önceki süreçlerde bir değişiklik yapılmayacak, IVXV ile aynı olacaktır. $(\mathcal{H}, \mathsf{Sig}, \mathsf{Pec})$ gibi kriptografik yapılar aynı şekilde olacaktır. Bumlara ek olarak simetrik anahtar şifreleme yöntemi $(\mathsf{Sec} = (\mathcal{E}_{\mathsf{sec}}, \mathcal{D}_{\mathsf{sec}}))$ IVXV sistemine dahil edilecektir. Buna göre:

- $c \leftarrow \mathcal{E}_{\mathsf{sec}}(\mathsf{sk}_{\mathsf{sec}}, m)$. Burada $\mathsf{sk}_{\mathsf{sec}}$ simetrik şifrelemede kullanılacak anahtardır ve şifrelenmek istenen veri m dir. Şifreleme sonucunda şifrelenmiş veri olan c elde edilmektedir.

- $m \leftarrow \mathcal{D}_{\mathsf{sec}}(\mathsf{sk}_{\mathsf{sec}}, c)$. Burada $\mathsf{sk}_{\mathsf{sec}}$ simetrik şifre çözmede kullanılacak anahtardır ve şifresi çözülmek istenen veri c'dir. Şifre çözme sonucunda açık veri olan m elde edilmektedir.

IVXV sisteminde kişisel oy doğrulamasındaki zafiyeti önlemek için önerilen bu çözüm seçim sisteminin üç fazında değişiklik gerektirecektir. Bunlardan ilki seçmenin VoteAppile oy kullandığu süreç olan oylama süreci, ikincisi kullanılan oyun merkezi sunuculara ulaştıktan sonra depolanması sırasında, yani oy depolama işleminde yapılacak değişiklik, sonuncusu ise VerApp uygulaması kullanılarak kişisel oy doğrulama sürecinde yapılacak değişikliktir.

- **Oylama Fazı**: Oy verme hakkına sahip seçmenin kişisel bilgisayarında indirdiği VoteApp uygulamasını kullanarak oylama işlemini internet üzerinden gerçekleştirdiği fazdır. Bu fazda VoteApp kullanılarak ikili zarf prensibindeki oy oluşturulur. VC tarafından seçmen listesi VoteApp uygulamasına gelir, gelen listeden seçmen seçimini yaptıktan sonra seçilen aday bilgisi VoteApp yardımı ile şifrelenir ve böylece iç zarf oluşturulmuş olur. Şifreli veri bir imza aracı yardımı ile seçmen imzasıyla imzalanır, bu aşamadan sonra dış zarf oluşturma işlemi de tamamlanmış olur ve böylece ikili zarf hazır hale gelir. Bu şekilde şifreli ve imzalı oy tekrar merkezi sunucu olan VC'e gönderilir, oy kullanma işlemi tamamlanmış olur. VoteApp oy kullanma işlemi tamamlanmasının ardından kişisel oy doğrulaması adımında kullanılmak üzere bir QR kodu üretir, bu kod VerApp tarafından kullanılacaktır.

  Özetle seçme hakkına sahip seçmen $v \in V$, seçmek istediği adayı $\mathsf{c_v} \in \mathsf{C}$ VoteApp kullanarak seçer ve ikili zarf halindeki oy oluşturulmuş olur. IVXV sistemi için önerilen oy verme fazı adımları şu şekilde sıralanmaktadır:

  C_1. VoteApp rastgele $\mathsf{r_v}, \mathsf{q_v}$ değerlerini seçer. $\mathsf{r_v}, \mathsf{q_v} \in \{0,1\}^{O(\lambda)}$.

  C_2. İç zarf oluşturmak için açık anahtar kullanılarak şifreleme işlemi yapılır. $\mathsf{ballot_{c,r}} \leftarrow \mathcal{E}_{\mathsf{pec}}(\mathsf{pk_{pec}}, (\mathsf{c_v}, \mathsf{r_v}))$.

  C_3. Bir önceki adımda oluşturulan iç zarf seçmenin kişisel imzası kullanılarak imzalanır ve dış zarf oluşturulur. İmzalama için seçmenin özel imza anahtarı kullanılır. $\sigma_\mathsf{v} \leftarrow \mathcal{S}_{\mathsf{sig}}(\mathsf{sk^v_{sig}}, \mathsf{ballot_{c,r}})$, $\mathsf{vote_v} \leftarrow (\mathsf{ballot_{c,r}}, \sigma_\mathsf{v})$. Burada $\mathsf{vote_v}$ şifrelenmiş ve imzalanmış ikili zarf şeklindeki oy'dur.

  C_4. $(\mathsf{v}, \mathsf{Cert_v}, \mathsf{vote_v}, \mathsf{q_v})$ VoteApp tarafından VC merkezi sunucusuna gönderilir.

  C_5. VC tarafından VoteApp uyglamasında, $\mathsf{vote_{id}}$ benzersiz tanımlayıcısını ve RS onayı olan $\mathsf{reg_{vote_{id}}}$'i gönderir. $\mathsf{vote_{id}}$, seçmenin kullanmış olduğu oy'un temsil edilmesi için diğer oylar ile benzersizdir. Bir seçmen birden fazla oy kullanabilir, böyle bir durumda kullanılan her oy için ayrı ayrı $\mathsf{vote_{id}}$ ve $\mathsf{reg_{vote_{id}}}$ üretilir.

C_6. VoteApp $\mathcal{H}(\mathsf{vote_v})$'a göre dijital olarak imzalanmış $\mathsf{reg_{vote_{id}}}$'i doğrular.

C_7. VoteApp tarafından QR kodu oluşturulur. Bu kod $\mathsf{vote_{id}}$ ve $\mathsf{r_v}$ değerlerinin bilgisini içerir. Kişisel oy doğrulama fazında bu kod kullanılacaktır, yani kod VerApp tarafından okutulup doğrulama sürecinde işleme sokulacak. Ayrıca $\mathsf{q_v}$ değeri VoteApp uygulamasında kalacak ve daha sonra kişisel oy doğrulama fazında kullanılacak. Kişisel oy doğrulama fazında seçilen adayı doğrulamak için VoteApp ekranında $\mathsf{q_v}$ değeri gösterilecek, VerApp uygulama ekranında ise aday listesi ile ilişkili $\mathsf{q_i}$ değerleri gösterilecek ve sonunda bu sayıların karşılaştırması işlemi seçmenden beklenecek.

- **Oy Depolama Fazı**: Bu fazda VC oy depolama işlemi için oyun doğrulanmasında ihtiyaç duyar ve oyu kaydeder. VC bu fazda VoteApp tarafından kendisine gelen oyu doğrular kaydeder ve RS'da depolanmasını sağlar, önerilen sistemde bunun için gerçekleştirilecek adımlar şu şekilde sıralanabilir:

S_1. VC kendisine VoterApp tarafından gelen ve v ile σ_v değerlerini içermekte olan $\mathsf{vote_v}$ değerini kullanarak seçim hakkı kazanmış seçmen v, σ_v'yı doğrular.

S_2. VC tarafından oyların temsil edilmesi amacıyla oyu ifade eden ve benzersiz olan $\mathsf{vote_{id}}$ değerini üretir.

S_3. VC TMS'den time-mark elde eder,
$\mathsf{ts_{vote_{id}}} = \mathcal{S}_{\mathsf{sig}}(\mathsf{sk}^{\mathsf{TMS}}_{\mathsf{sig}}, (\mathsf{Cert_v}, \mathcal{H}(\mathsf{ballot_{c,r}}), \mathsf{utc_{vote_{id}}}))$, böylece $\mathcal{H}(\mathsf{ballot_{c,r}})$ verisinin $\mathsf{utc_{vote_{id}}}$ zamanına göre $\mathsf{Cert_v}$'ın geçerli olduğu tarihte var olduğu gösterilmiş olur.

S_4. VC tarafından RS'ye kayıt isteği gönderilir. Bu istek şu şekildedir,
$\mathsf{req_{vote_{id}}} = \mathcal{S}_{\mathsf{sig}}(\mathsf{sk}^{\mathsf{VC}}_{\mathsf{sig}}, (\mathsf{vote_{id}}, \mathcal{H}(\mathsf{vote_v})))$.

S_5. İsteği alan RS tarafından $\mathsf{req_{vote_{id}}}$ doğrulanır ve VC'ye yanıt olarak onay gönderilir, $\mathsf{reg_{vote_{id}}} = \mathcal{S}_{\mathsf{sig}}(\mathsf{sk}^{\mathsf{RS}}_{\mathsf{sig}}, \mathcal{H}(\mathsf{req_{vote_{id}}}))$.

S_6. VC tarafından VoteApp uygulamasına $\mathsf{vote_{id}}$ ve RS onayı olan $reg_{vote_{id}}$ gönderilir.

EIV'nin gereklerinden olan seçme hakkında sahip adayın internet üzerinden oyunu birden fazla defa kullanabilmesi gerekliliğinden dolayı seçen internet ortamında EIV seçim periyodunda birden fazla defa oy kullanabilmektedir. Bu şekilde bir seçmen birden fazla oy kullandığında oy depolama fazında kullanılan her oy için ayrı ayrı süreçler işletilir.

Oy depolama fazı merkezi sunucular olan VC ve RS tarafından gerçekleştirilen süreçlerdir ve oy depolama fazı yürütüldükten sonra herbir oy için VC ve RS de bulunan veriler şu şekildedir:

– VC stores

$$\mathsf{stored_{vote_{id}}} = (\mathsf{v}, \mathsf{Cert_v}, \mathsf{vote_v}, \mathsf{vote_{id}}, \mathsf{q_v}, \mathsf{ts_{vote_{id}}}, \mathsf{reg_{vote_{id}}}),$$

– RS stores

$$\mathsf{registered_{vote_{id}}} = (\mathsf{req_{vote_{id}}}, \mathsf{reg_{vote_{id}}}).$$

- **Kişisel Oy Doğrulama Fazı**: Oy kullanma ve oy depolama fazlarından sonra kişisel oy doğrulama fazı gerçekleşmektedir. Kişisel oy doğrulama fazı için VerApp uygulaması kullanılmaktadır. Oy kullanan seçmenlerin kullanmış oldukları oyu doğrulaması opsiyoneldir, isteyen seçmen bu işlemi yapmaktadır. Oy kullanma hakkında sahip seçmen oy kullandıktan sonra oy kullanmış olduğu cihazdan yani VoteApp uygulamasının çaıştığı cihazdan farklı bir cihazda VerApp uygulamasını kullanarak oy doğrulamasını kullanır. VerApp uygulamasının çalıştığı cihaz akıllı cihaz olmalıdır ve ayrıca internet bağlantısı olmaı ve QR okumak için kameraya sahip olmalıdır.

  Kişisel Oy Doğrulama Faz'ında seçmene uçtan uca doğrulama prensiplerinden cast-as-intended ve recorded-as-cast imkanları sağlanmış olur. Önerilen sistemde kişisel oy doğrulama adımları şu şekilde sıralanmaktadır:

  V_1. VerApp uygulaması VoteApp uygulaması tarafından QR kodu şeklinde gösterilen veriyi kamerasına okutur. QR kodu kullanılarak VerApp uygulamasının

elde ettiği veri içinde $\mathsf{vote_{id}}$ ve $\mathsf{r_v}$ bulunmaktadır.

V_2. VerApp merkezi sunucu olan VC ile iletişime geçer. İkisi arasında kurulan bu kanalın güvenli olabilmesi için TLS kullanılır. Kurulan bu güvenli kanal yardımı ile VerApp $\mathsf{vote_{id}}$ veisini VC sunucusuna gönderir.

V_3. VC $\mathsf{vote_{id}}$'ye karşılık gelen $(\mathsf{C}, c_{\mathsf{q_v}})$ verilerini VerApp'a gönderir. Burada (C ilgili seçim bölgesindeki tüm aday listesini temsil etmektedir ve $c_{\mathsf{q_v}}$) şu şekilde hesaplanır:

$$c_{\mathsf{q_v}} \leftarrow \mathcal{E}_{\mathsf{sec}}(\mathcal{H}(\mathsf{ballot_{c,r}}), \mathsf{q_v}).$$

VC'ye gelen $\mathsf{vote_{id}}$'nin bir karşılığı olmaması durumunda veya zaman uyumluluğu ile ilgili bir sorun olduğunda hata dönülmektedir.

V_4. VerApp ℓ kadar adaydan oluşan (C'yi , $c_{\mathsf{q_v}}$)'yi ve VoteApp'dan alınmış olan ve rastgele üretilmiş $\mathsf{r_v}$ değerini kullanarak $\mathsf{Q} = \{\mathsf{q}_1, \mathsf{q}_2, \ldots, \mathsf{q}_\ell\}$ şeklinde $\mathsf{q_i}$) değerleri hesaplar. Herbir $\mathsf{q_i}$) değeri C listesinde ki adaylar için tek tek hesaplanmıştır, $\mathsf{c}_i \in \mathsf{C}$.

- $\mathsf{ballot_{c}}_{i,\mathsf{r}} \leftarrow \mathcal{E}_{\mathsf{pec}}(\mathsf{pk_{pec}}, (\mathsf{c_i}, \mathsf{r_v}))$,
- $\mathsf{q}_i \leftarrow \mathcal{D}_{\mathsf{sec}}(\mathcal{H}(\mathsf{ballot_{c}}_{i,\mathsf{r}}), \mathsf{c_{q_v}})$.

V_5. VerApp ekranında bir önceki adımda hesaplanan Q listesi gösterilir. Bu listedeki herbir eleman C listesindeki bir adayla birebir karşılıklı ilişkilidir.

V_6. Bu adımda seçmen karşısında iki ekran vardır, birincisi bir önceki adımda VerApp ekranında gösterilen ve herbir elemanı bir adayla birebir olarak ilişkili Q listesi, ikincisi ise VoteApp ekranında gösterilen ve seçmenin seçmiş olduğu adayı temsil eden $\mathsf{q_v}$ değeridir. Seçmenden bu adımda beklenen VerApp ekranındaki Q listesindeki herbir $\mathsf{q_i}$ değeri ile VoteApp ekranında gösterilen $\mathsf{q_v}$ değerini karşılaştırmasıdır. Sonuç olarak, $\mathsf{q_v}$ değerine karşılık gelen $\mathsf{q_i}$ bulunur ve bu durum $\mathsf{q_i}$'ye denk gelen adayın seçmen tarafından seçildiği anlamına gelir.

Yukarıda tanıtılmış olan yöntem [11] ile önerilmiş yöntemdir. Bu yöntem ile VerApp uygulamasında seçilen aday açıkça gösterilmemektedir bunun yerine λ-bit güvenlik parametresine sahip $\mathsf{q_i}$ değerleri gösterilmektedir ve bu değerier ile VoteApp uygulamasında

gösterilen $\mathsf{q_v}$ değerinin karşılaştırılması istenmektedir. Güvenlik parametresi olan λ-bit uzunlukta verileri karşılaştırmak seçmenler tarafından gözle yapılacak bir karşılaştırmadır ve kullanışlı olmadığı düşünülmektedir. Örneğin q değerlerinin uzunluğunun 256 bit olduğu bir senaryoda kullanıcıdan gözle bu büyüklükte bir sayıyı karşılaştırmasını istemek sistemi kullanılabilir yapmaktan çıkarmaktadır. Ayrıca önerilen bu çözümüm kullanıcı dostu bir çözüm olmamasından kaynaklı kullanılamayacağı [13] tarafından gösterilmiştir.

EIV sistemine eklenen ve IVXV yapısında kullanılan doğrulama bileşeninden kaynaklanan ve bu bileşenin (VerApp) ekranında seçilen adayın açıkça gösterilmesinden doğan zafiyet, teoride önerilen bu çözüm ile ortadan kalkmaktadır fakat dezavantajı kullanıcı dostu olmaması ve dolayısıyla sistem üzerinde kullanılırlığının olmamasıdır. Uygulanan seçim sisteminde güvenlik gereklerinin yerine getirilmesi kadar bu sistemin kullanışlı olabilmesi, yani seçmen tarafından zorlanmadan rahat bir şekilde kullanılabilmesi gerekmektedir. Bu durum göz önüne alındığında kriptografik olarak getirilen bu çözüm önerisi kullanışlı değildir. Seçmenden gözle karşılaşılaştırma yapması istenmektedir ve karşılaştırma yapması istenen sayılar insan eliyle yapılması oldukça zordur. Bu yüzden bu sistemin bahsedilen güvenlik açığını çözdüğü de düşünülerek nasıl kullanıcı dostu bir şekilde gerçeklenebileceği üzerinde düşünülmüştür.

Seçme hakkına sahip seçmen oy kullandıktan sonra VerApp kullanarak kişisel oy doğrulama işlemi yapmak istediğinde seçmen için doğrulama sürecinde VoteApp ve VerApp ekranlarında q değerleri gösterilmektedir. Bu değerlerin uzunluğu λ-bit olmaktadır ve bu güvenlik parametresi değişkenlik göstermekle beraber kullanıcıların gözle karşılaştırma yapabilmeleri için büyük bir değerdir. Ayrıca bu oy doğrulaması yapmak isteyen seçmenden karşılaştırma yapmak istediği değer sadece iki tane değildir, tam olarak istenen VoteApp ekranında gösterilen $\mathsf{q_v}$ değerinin VerApp ekranında gösterilen ve herbiri birebir olarak aday listesindeki adaylara karşılık gelen $\mathsf{q_i}$ değerleri ile tek tek karşılaştırması istenmektedir. Bu sürecin seçmen tarafından gerçekleştirilebileceği düşünülse bile bu oldukça zahmetli, zaman alan ve oldukça hataya açık bir süreç olacaktır.

4.2.1 Kullanılabilirlik

Bölüm 4.2'de bahsedilen ve gerektiği kadar kullanıcı dostu olmayan yönteme, pratikte kullanılabilir olması için getirilecek çözüm önerileri üzerinde çalışmalar yapılmıştır. Buna

göre kişisel oy doğrulama sürecinin doğrulama adımında yine λ-bit uzunluktaki güvenlik parametrelerinin kullanıldığı q değerlerinin kullanılması uygun görüldü, fakat kullanıcının q değerleri yerine bu değerleri temsil edebilecekleri ve kolay ayırt edilebilecek yöntemler üzerinde duruldu. Karşılaşturma için kullanılan q değerinin yerine onları temsil edecek varlıkların bazı gereklilikleri karşılaması gerekmekte olduğu düşünüldü. Örneğin temsil edecek varlık uzayı en az λ-bit uzunluktaki q değeri kadar ve birbirinden farklı eleman içermelidir, böylece λ-bit uzunluktaki olası herbir q değeri, bu değeri temsil edecek varlık (şekil, resim, foto, pixmap vs.) uzayındaki farklı bir elemana karşılık gelmesi sağlanabilecek. Yani λ-bit uzunluktaki olası herbir q değeri için farklı bir şekil oluşabilecek. Bir diğer gereklilik ise q değerini temsil edecek şeyin farklı örnekleri mümkün olduğunca birbirinden gözle ayırt edilmesidir.

Bu anlatılanlardan yola çıkılarak farklı yöntemler üzerinde duruldu. Bunlardan bir tanesi, q değerini temsil edecek şeyin fotograf ya da resimlerin olması düşünüldü. Bu yöntemle λ-bit uzunluktaki olası herbir q değeri için bir fotograf ya da resim olacak ve q değeri yerine bu fotograf ya da resim gösterilecek. Bu yöntem için seçilecek fotograf ya da resimlerin mümkün olduğunca birbirinden ayırt edilmesinin mümkün olması sağlanacak. Fakat λ-bit uzunluktaki olası herbir q değeri göz önüne alındığında λ-bit uzunluğuna göre ihtiyaç duyulan fotograf ya da resim sayısı artmaktadır.

Örnek vermek gerekirse, λ değeri 256 olduğunu düşünürsek ihtiyaç duyulan fotograf ya da resim sayısı karşılamak çok zor. Karşılansa bile bunu uygulamaların kullanıldığı cihazlara indirmek şuanki teknoloji ile mümkün değil, kaldı ki akıllı cihazların tümü bu veriyi depolayabilecek kapasiteye sahip olması halinde bile bu verileri işlemek olanaksız olacaktır. Düşünülen diğer bir yöntem ise λ-bit uzunluktaki q değerinin bir algoritmadan geçirilip grafik halinde seçmene gösterilmesi yaklaşımı, fakat bu yöntemde de oluşacak grafiklerin birbirinden ayırt edilmesi ile ilgili sorunlarla karşılaşıldı.

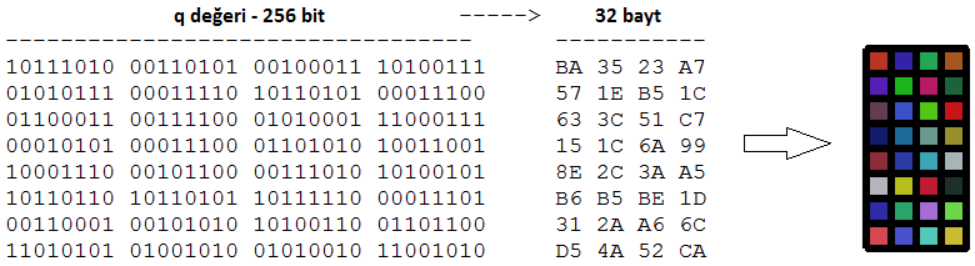
Yukarıda bahsedilen olası yöntemlerle beraber pixmap yöntemine benzer bir yöntemin, ilgili problemin çözümü için uygun olabileceği düşünüldü. Bu yönteme göre λ-bit uzunluktaki q değeri önce parçalanarak daha küçük yapılara ayrılacak. Sonrasında ise herbir yapı kendi içinde görselleştirilecek. Parçalama sonucu meydana gelen herbir veri için bir kare çizme ve bu karenin içini de bir renk ile doldurmak uygun görüldü. Herbir kare için renk değerinin belirlenmesi işlemi ise q değeri parçalara ayrıldıktan sonra oluşan verilerin bir algoritmadan geçirilmesiyle sağlanacak. Bu işlemler tamamlandıktan sonra

herbir kare parçasının bir araya gelmesiyle ortaya bir şekil çıkacak. Ortaya çıkan bu şekil q değerini benzersiz olarak temsil edecek. Bu yöntem kullanıldığında VoteApp ekranında q değeri yerine bunu temsil eden şekil gösterilecek, VerApp ekranında ise $\mathsf{q_i}$ değerleri yerine bu değerleri temsil eden şekiller listelenecek. Seçmen ise çıkan bu şekilleri kullanarak karşılaştırma işlemini yapıp kişisel oy doğrulama işlemini tamamlayacak.

Seçmenin karşılaştırması istenen q değerlerinin görselleştirme işlemini daha detaylı anlatabilmek için örneklendirmek gerekirse, güvenlik parametsesi λ 256-bit uzunluğunda olduğunu varsayalım. Bu durumda görselleştirilmek istenen herbir q verisi 256-bit uzunluğunda olacaktır. Uygulanacak ilk adım q verisini küçük parçalara ayırıp herbir parçayı ekranda kare biçiminde çizme işlemidir. Görselleştirilecek q verisinin 32 parçaya bölüneceğini düşünürsek herbir parça 8-bit (1 bayt) değerinde sayılardan oluşacaktır ve q değerinin görselleştirilmesi için 32 adet kare çizilmelidir. Parçalama sonucu elde edilen 32 adet 1 baytlık sayılar ise bir algoritmadan geçirilecek ve çizilen 32 adet kare için 32 adet RGB (Red Blue Green) değeri oluşturacak. Algoritma sonucunda meydana gelen 32 adet RGB değeri ise herbir karenin içini doldurmak için kullanılacaktır. İşlemler tamamlandıktan sonra q verisinin görselleştirme işlemi tamamlanmış olacaktır.

RGB renklendirmede renk tanımlamak için 3 veriye ihtiyaç duyulur. Yukarıdaki verilen örnekte herbir kare için bir RGB değeri gerekmektedir. Bu değerler için parçalanan ve 1 bayt uzunlukta olan sayılar kullanılmaktadır. Örnek için, q değeri görselleştirmesinde q değerinin parçalara ayrılmış hali bahsedilen algoritmadan geçirildiği ve ilk kare için 3 adet 1 baytlık parça seçildiği düşünülürse ilk karenin renklendirilmesinde kullanılacak 3 adet RGB değeri bu bayt'lardır. Bu şekilde q veri görselleştirme işlemi Python Programlama Dili'nde gerçeklenmiştir. Karelerin boyanması işlemi için QT kütüphanesi kullanılmıştır. QT kütüphanesinde ise QColor sınıfından faydalanmıştır. Bu sınıf RGB, HSV (Hue, Saturation and value), CMYK (Cyan, Magenta, Yellow and Black) tabanlı renklendirme olanakları sağlamaktadır [25]. Python Programlama Dili'nde QT kütüphanesi kullanılarak 256-bit güvenlik parametserine sahip olan q verisinin görselleştirme işlemi Şekil 4.2 ile gösterilmektedir.

Yukarıda verilen örnek üzerinden gidip, detaylı açıklama yapacak olursak, Şekil 4.2 ile gösterilen q değeri için güvenlik parametresi olan λ değeri 256-bit olmakta. Şekilde de sol tarafta q değerinin bit gösterimi yer almıştır ve bu şekilde gösterim için ikilik tabanda 256 sayı kullanılmıştır. Bu 256-bit uzunluğundaki sayı 8 parçaya bölünmüş ve böylece



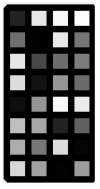
Şekil 4.2: q değerinin görselleştirilmesi

32 tane 8 bit (1 bayt) sayı elde edilmiştir. Bu parçalardan herbiri 1 bayt olmakta ve her bayt gösterimi için iki adet onaltılık sistemde (hexadecimal) sayı kullanılmaktadır. Örnek vermek gerekirse 8 bit olan, 32 adet parçalardan bir tanesi ikilik sistemde 10111010 olduğunu düşünürsek, bu sayı iki adet hexadecimak sayı ile ifade edilebilmektedir. Yani 10111010 sayısı 1011-1010 şeklinde ikiye bölünür ve BA şeklinde ifade edilir. Sırayla 1011 sayısı hexadecimal B'ye denk gelmektedir, 1010 sayısı ise hexadecimal sistemde A'ya denk gelmektedir. Bu şekilde 32 adet parça ikişer hexadecimal sayı ile ifade edilmiştir. Şekil 4.2'de ilk olarak ikilik sistemde gösterilen q değeri yukarıda bahsedilen şekilde 32 adet parçaya ayrılmıştır ve her parça iki hexadecimal sayıya çevrilmiştir. Şekilde ikilik sistemde olan değerin 32 parçaya ayrıldıktan sonraki hali gösterilmektedir.

Dönüştürme işlemi yapıldıktan sonra 32 adet her parça için birer kare çizdirilmiştir. Kareler yanyana gelecek şekilde ve 8x4 matris oluşturulmuştur. Şekil 4.2'de 32 adet her parça için çizdirilen kareler şeklin en sağ tarafında gösterilmektedir. Her 32 adet parça için çizilen karelerin bir araya geldiklerinde oluşturduğu şekil q değerinin temsil edildiği şekildir.

Kare çizme işlemi tamamlandıktan sonra herbir q değerini birbirinden farklılaştıracak olan kareleri boyama işlemine sıra geldiğinde, her bir kare için 3 parametresi olan RGB değerlerinin belirlenmesi üzerinde çalışılmıştır. İlk olarak düşünülen, bayt olarak gösterilen herbir 32 parçanın da 8x4 şeklinde matris haline getirilmesi ve 32 parça için çizilen 8x4 şeklindeki karelerle eşleştirilmesi ve herbir karenin, eşleştiği bayt değeri kullanılarak renklendirilmesi oldu. Yani Şekil 4.2 üzerinden anlatılacak olursa bayt şeklindeki gösterimde BA bayt değeri kullanılarak kare matristeki 1x1 karesinin renklendirilmesi düşünülmüştür. Renklendirme işlemi için ilgili karenin RGB değerinin 3 parametresinin de BA değeri olması düşünülmüştür, fakat böyle bir kullanımda yani RGB'nin almış olduğu 3 parametreninde aynı olması durumunda renk değeri gri tonlarında değer almaktadır. Şekil 4.3

da 32 karenin herbiri için ayrı ayrı RGB değerleri düşünüldüğünde, RGB parametreleri birbirinden farklı olan hali ve RGB değerlerinin 3 parametresinin de aynı değeri aldığı hali örnek gösterilmektedir. Bu şekilde renklendirme yapılması (RGB parametrelernin 3 değerinin de aynı olması) `q` değeri için farklı şekiller oluşturma noktasında çalışabilir ancak karşılaştırmada kullanılacağından ve aynı yöntemle boyanan diğer şekillerden ayırt edilmesi zor oacağından bu yöntem kullanılmamıştır. Bunun yerine yine `q` değeri kullanılarak, 32 karenin ayrı ayrı herbiri için RGB değerlerinin parametrelerinin 3 farklı değer alması yoluna gidilmiştir, böylece kareler renkli boyanmış olup ayırt edilme daha kolay olacaktır.



Şekil 4.3: RGB parametrelerinin hepsinin aynı olması durumu

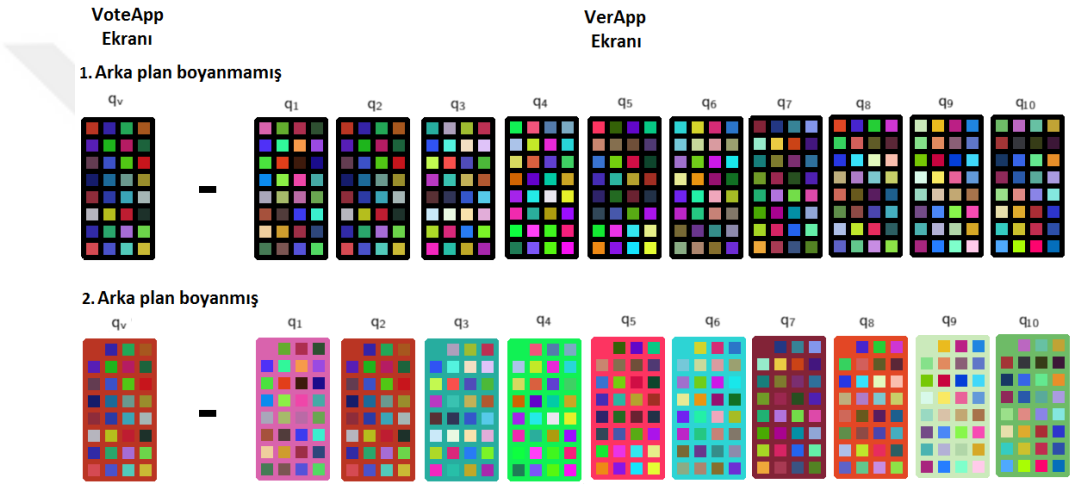
Yine Şekil 4.2 şeklinden yola çıkacak olursak, şekildeki bayt değerlerini kullanarak herbir kare için 3 adet değer elde etmemiz gerekiyor. Toplamda 96 değer üretilmesi gerekiyor. Bunun için bayt değerleri sıralandı ve üç'erli gruplandırıldı toplamda 32 adet 3'erli grup elde edildi. Her gruptaki 3 değer bir kareye denk gelecek şekilde renklendirme yapıldı. Üç'erli değer elde etmek için birinci bayt değerinden başlayarak sonrasındaki iki kare ile beraber 3 değer elde edildi ve bu ikinci bayt için ve diğer bayt'lar için de yapıldı. 31. bayt değeri için, kendisi 32. bayt ve baştan 1. bayt kullanıldı. 32. bayt için kendisi 1. bayt ve 2. bayt kullanıldı, böylelikle toplamda 32 adet 3 değer elde edildi.

Yukarıdaki algoritmayı yürüttüğümüzde Şekil 4.2'de en sağdaki q değerinin görsel halini 8x4 matris şeklinde düşünürsek, bayt değerlerini kullanarak karelerin RGB değerleri şöyle olacaktır:

- $(1, 1)$'deki ilk kare için `0xBA,0x35,0x23`,
- $(1, 2)$'deki ikinci kare için `0x35,0x23,0xA7`,
- $(1, 3)$'deki üçüncü kare için `0x23,0xA7,0x57`,

- ...
- $(8, 3)$'deki 31. kare `0x52,0xCA,0xBA`,
- $(8, 4)$'deki 32. kare `0xCA,0xBA,0x35`.

Görselleştirilen q değerlerini birbirinden ayırt etmenin daha kolay olması için ayrıca karelerin gösterildiği arka plan da renklendirilebilir. Arka plan rengi oluşturulması şeklin genel görünümüne fark katarak ayırt edilebilirliği artırmaktadır. Şekil 4.4 ile karşılaştırma yapılması istenen $\mathsf{q_v}$ değeri ve $\mathsf{q_i}$ değerlerinin nasıl bir görünüme sahip olacağı gösterilmiştir.

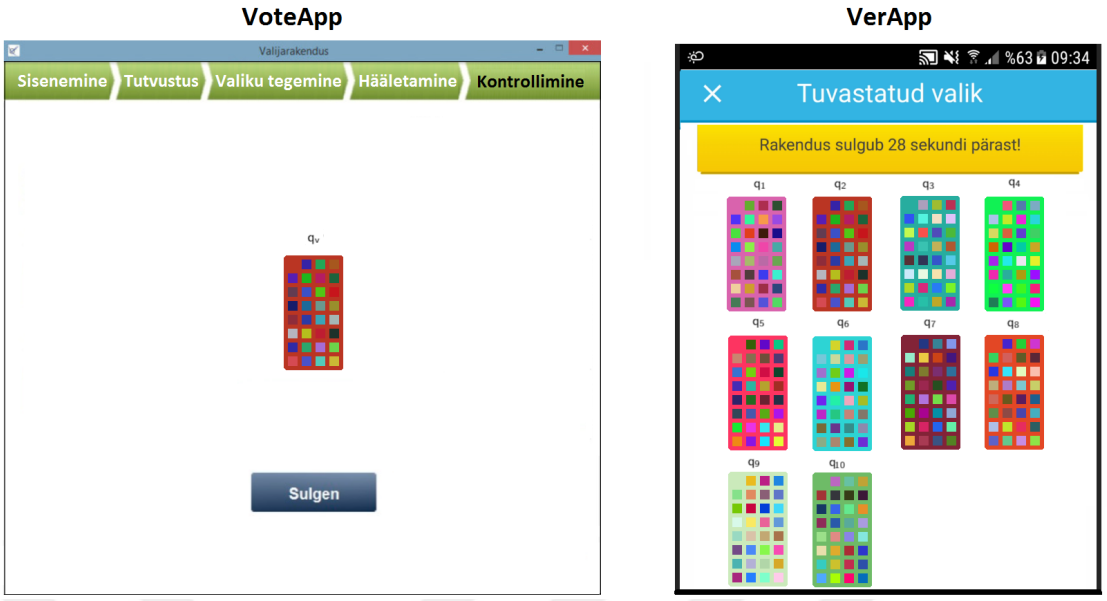


Şekil 4.4: Görsel Karşılaştırma Modeli

Kişisel oy doğrulamasının seçmen tarafından gözle doğrulama aşamasında VoterApp ekranındaki bulunan $\mathsf{q_v}$ ile VerApp ekranında bulunan $\mathsf{q_i}$ değerlerinin görselleştirme yapıldıktan sonra uygulama ekranlarında nasıl durabileceğine dair gösterim Şekil 4.5 ile örnek olabilir. Bu örnek Python Programlama dilinde Qt kütüphanesi kullanılarak oluşturulmuştur.

VerApp uygulamasının EIV sistemine getirdiği açıklıkta bu yöntemin kullanılması durumunda bir önceki yöntem olan ekran görüntüsünü programatik yollarla engelleme yöntemini kullanmaya gerek kalmayacaktır. Çünkü bu yöntem ile kişisel doğrulama bileşeninin son adımında, doğrulamak için seçilen adaylar cihaz ekranında açık şekilde gösterilmeyecek. Bunun yerine VoteApp ekranında seçilen adayı temsil eden şekil olacak ve VerApp ekranında aday listesindeki her aday için bir şekil olacak.

Seçmenden bu şekilleri karşılaştırması istenecek. Ekran görüntüsünün istenmeyen taraflarca ele geçirilmesi bir anlam ifade etmeyecektir, çünkü λ-bit güvenlik parametreli



ŞEKIL 4.5: VoteApp ve VerApp uygulamalarında şekil karşılaştırma

q_v değeri oy verme işlemi sırasında rastgele üretilmektedir. Doğrulama aşamasında ise VC tarafından VerApp'a q_v değerinin simetrik anahtarlı şifreleme kullanılarak şifreli hali gönderilir. VerApp simetrik anahtarlı şifreleme kullanarak şifre çözme işlemi yapar. Sonunda her aday için q_i değerleri oluşturulur ve bu değerler görselleştirilerek seçmenden karşılaştırma yapması istenir. Herhangi saldırganın VerApp ekranında görüntülenen q_i değerlerini ya da bunların görsel halini elde etmiş olsa dahi saldırgan q_i değerlerinden veya görsellerinden hangisinin seçilen adaya ait olduğunu bilemez.

Renk körlüğü gibi olası zorlukların aşılması açısından, mobil cihazların renk doğrulama gibi yöntemlerinin araştırılarak sistemin renk açısından optimize edilmesinin daha fazla kullanım kolayligi saglaması beklenmektedir ve bu kısım gelecek çalışma alanı olarak bırakılmıştır.

Bölüm 5

Sonuç

Elektronik cihazlar, haberleşme, kriptoloji gibi alanların gelişme göstermesi ile beraber birçok sektör hizmetlerini internet üzerinden vermeye başlamıştır. Buna seçim sistemleri de dahil olmuş ve yaygınlığı artmıştır. Estonya'da bu gelişmelerden yararlanmış ve kağıt tabanlı yapılan seçim sistemlerine eklemeler yaparak seçmenlerine internet üzerinden kişisel bilgisayarlarını kullanarak oy kullanma imkanı sağlamıştır. Böylelikle ilk defa yasal bağlayıcılığı olan ve ülke geneli yapılan EIV sistemi, Estonya 2005 seçiminde kullanılmıştır. Kullanılan bu sistem bileşenleri ve çalışma yapısı genelde aynı olmakla beraber çeşitli eklemeler ve değişikliklerle günümüze kadar farklılaşmıştır. EIV sistemi ilk olarak EVIV kod isimli yapıyla hizmet vermiş ve devamında IVXV kod isimli yapıyla hizmet vermiştir.

EIV sistemi ile oy kullanma hakkına sahip seçmen seçim periyodunda kendisine tanınan zaman aralığında internet üzerinden oy kullanabilmektedir. EIV'nin kağıt tabanlı oy kullanma sistemine getirdiği en büyük yeniliklerden biri olan internet üzerinden oylama akla güvenlikle ilgili soruları da getirmektedir. İnternet üzerinden yapılan basit bir işlem için bile güvenlik konusu önemliyken ülke seçimi gibi bir konuda güvenlik keza çok önemlidir. EIV sisteminin en az kağıt tabanlı oy kullanma sistemi kadar güvenli olması ve oy kullanan seçmenin kullanmış olduğu oyu başkalarına kanıtlayamaması gerekmektedir [1]. Bu bakımdan EIV sisteminin ilk kullanıldığı zamandan itibaren güvenlikle ilgili gerekler üzerine düşünülmüş ve sisteme eklemeler de yapılmıştır.

İlk olarak EVIV yapısıyla uygulanmaya başlayan EIV sistemine 2011 senesinde "Student Attack" adında bir saldırı gösterilmiştir [12], ayrıca 2011 seçiminde merkezi sunucuda

geçersiz oy görülmüştür. Bu gelişmelerden sonra EVIV yapısının güvenlik ile ilgili gerekleri tekrar gözden geçirilmiş, sonucunda ise seçmene kullanmış olduğu oyları doğrulama imkanı sağlayan kişisel oy doğrulama bileşeni sisteme dahil edilmiştir. Bu gelişme ile EVIV yapısına dahil edilen VerApp uygulaması ilk defa 2013 senesinde kullanılmaya başlanmıştır.

Sisteme getirilen VerApp bileşeni, seçmenin oy kullandığı bilgisayarda değil, akıllı cihazda çalışan bir uygulama olmuştur. Uçtan uca doğrulamanın gerekliliklerinden iki tanesi olan cast-as-intended ve recorded-as-cast VerApp tarafından sağlanma imkanı oluşmuştur. Böylece seçmene, kullanmış olduğu oyun doğru bir şekilde temsil edildiğini, yani gerçekten seçtiği adayın merkezi sunuculara gönderildiğini ve merkezi sunucularda oyun kullandığı şekilde kaydedildiğini doğrulama imkanı sağlanmıştır.

2016 senesinde, EIV sistemine güvenlik açığı kapatmak için getirilen ve EVIV yapısıyla kullanıma sunulan kişisel oy doğrulama bileşeninin, sisteme başka bir açıklık getirildiğine dair iddiada bulunulmuştur [11]. Buna göre EVIV yapısında kişisel oy doğrulama için kullanılan VerApp, seçmenin oy gizliliğini ihlal edecek bir açıklık getirmişti. Bu açıklık, VerApp kullanılarak kişisel oy doğrulamak isteyen seçmene doğrulama için uygulama ekranında seçtiği adayın açıkça gösterilmesi olarak tanımlanmıştır. Bu açıklığın VerApp ile aynı cihazda çalışan başka uygulamalarca elde edilebileceğine dikkat çekilmiş ve bu doğrultuda EVIV sistemine simetrik anahtarlı şifreleme eklenerek bir çözüm önerisinde bulunulmuştur. Çözümde, VerApp ekranında seçilen adayın açıkça gösterilmesi yerine, λ bit güvenlik parametreli olan ve adayları temsil eden sayıların gösterilmesi, sonunda ise bu sayıların VoteApp ile VerApp uygulama ekranlarından karşılaştırması mantığı bulunmaktadır. Böylece ekran görüntüsü elde edilse bile elde eden uygulama ya da kişilerce bu verinin bir anlamı olmayacaktır.

Geliştirilen EIV sistemi tasarlanırken güvenlik gerekliliklerinin yanında sistemin kolay kullanılabilir olması için gereklilikler de dikkate alınmıştır. Güvenlikle ilgili gereklilikler ile sistemin kolay kullanılabilirliği ile ilgili gereklilikler dengeli olması gerekmektedir, tüm güvenlik gereklerinin sağlanması sistemi kullanıcı dostu olmaktan çıkarmamalıdır. Bu doğrultuda önerilen çözümüm [11], kullanılabilirlik açısından kötü olduğu düşünülmüştür [13]. Çünkü kullanıcıdan iki uygulama üzerinden büyük sayıların karşılaştırması istenmektedir, bu durum kişisel oy doğrulama bileşenini kullanmayı zor hale getirmektedir.

İlk başta EVIV yapısı ile gerçekleştirilen EIV sistemi, bazı denetleme mekanizması eklenmesi ve Kayıt Sunucusu RS gibi eklemeyle IVXV ile gerçekleştirilmeye başlanmıştır. İlk olarak 2017 senesinde kullanılan IVXV yapısında kullanılan VerApp uygulaması başta tasarlandığı gibi kullanılmaktadır. VerApp'ın sisteme eklenmesiyle meydana gelen zafiyet hala devam etmektedir.

Akıllı cihazlar için geliştirilen spyware, stalkerware gibi yazılımlar düşünüldüğünde ve bu yazılımların yaygınlığı düşünüldüğünde, bu yazılımlardan birinin EIV sisteminde VerApp ekran görüntüsü bilgisi almak için özel geliştirilmesi ve planlı bir şekilde kullanılması seçim güvenliği için risk oluşturmaktadır. Bu durum oy gizliliğini ihlal edebileceği gibi oranların önceden bilinebilmesi halinde seçim gidişatını dahi değiştirebilecek sonuçlar doğurabilir.

Bu çalışmada, ilgili gelişmelerden yola çıkılarak, EIV sisteminde kullanılan IVXV yapısı incelenmiştir. Bu yapıda kullanılan ve seçmene kişisel oy doğrulama imkanı sağlayan VerApp için bir simülasyon ortamı hazırlanmıştır. Bunun için Estonya'nın paylaştığı EIV sisteminde kullanılan ve açık kaynak kodlu olan yazılım kullanılmıştır. Simülasyon ortamında VerApp ile aynı akıllı cihazda çalışan başka bir uygulama tarafından VerApp'a ait olan ekran görüntüsü bilgisi elde edilmiştir. Böylelikle herhangi bir akıllı cihaz uygulaması ile seçmenin seçtiği aday bilgisi elde edilerek oy gizliliği ihlali gösterilmiştir.

Hazırlanan simülasyon ile seçilen aday bilgisi elde etme işlemi tamamlandıktan sonra, problemin çözümü ile ilgili çalışmalar yapılmıştır. Bu çalışmalar sonucunda iki adet çözüm önerilmektedir. Bunlardan ilki programatik olarak VerApp ekran görüntüsü bilgisinin başka uygulamalar tarafından elde edilmesinin engellenmesi. Diğer önerilen çözüm, simetrik anahtarlı şifreleme yöntemi kullanılarak önerilen çözüm ([11]) üzerinde düşünülerek, bu yöntemin seçmen tarafından kullanılabilir olmasını sağlamak olmuştur.

İlk çözümde programatik yöntemler araştırıldı ve kullanılabilecek yöntem keşfedildi. Sonrasında kullanılabilecek yöntem, daha önce zafiyeti tekrarlamak için oluşturulan VerApp simülasyonuna eklendi. Sonuç olarak, bu geliştirilme yaptıktan sonra VerApp ile aynı cihazda çalışan ve ekran görüntüsü alan uygulama ile sistem tekrar denendi ve VerApp ekran görüntüsü bilgisinin korunduğu gözlemlendi. Bu yöntemle ekran görüntüsü alan diğer uygulama sadece siyah ekran elde edebildi. İkinci olarak simetrik anahtarlı şifreleme yöntemi kullanılarak önerilen çözüm ([11]) için daha kullanışlı bir yöntem üzerinde çalışıldı. Adayları temsil eden λ bit güvenlik parametreli q değerlerinin kullanışlı bir şekilde

görselleştirilmesi ve bu şekilde birbirlerinden rahatça ayırt edilebilmesi üzerine çalışmalar yapıldı. Çalışmalar sonucunda q değerlerinin yerine bu değerlerin, geliştirilen algoritma kullanılarak görselleştirilmesi sağlandı. Böylece, seçmen VoteApp ekranındaki seçilen adayı temsil eden görsel ile VerApp ekranında gösterilen ve tüm adayların ayrı ayrı temsil edildiği görsellerde karşılaştırma yaparak kişisel oy doğrulama süreci gerçekleşecek. Bu yöntemin kullanılmasıyla, oy kullanan seçmenin oyunu başkalarına ıspatlayamaması ([1]) gereğinin sağlanmış olacağı ve yukarıda bahsedilen risklerin ortadan kalkacağı düşünülmektedir.

Kaynaklar

[1] State Electoral Office of Estonia. General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia, 2017. https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf.

[2] State Electoral Office of Estonia. Statistics about Internet voting in Estonia, 2020. https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia.

[3] S. Heiberg and J. Willemson. Verifiable internet voting in estonia. In *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*, pages 1–8, Oct 2014. doi: 10.1109/EVOTE.2014.7001135.

[4] Latif Anıl Büyükbaskın. Blokzincir tabanlı e-seçim sistem önerilerinin güvenlik ve mahremiyet analizleri, 2019.

[5] O. Cetinkaya and D. Cetinkaya. Towards secure e-elections in Turkey: Requirements and principles. In *The Second International Conference on Availability, Reliability and Security (ARES'07)*, pages 903–907, April 2007.

[6] İnsan Hakları Evrensel Bildirgesi. İnsan Hakları Evrensel Bildirgesi, (accessed 04.2019). URL http://www.unicankara.org.tr/doc_pdf/h_rigths_turkce.pdf.

[7] S. Popoveniuc, J. Kelsey, A. Regenscheid, and P. Vora. Performance requirements for end-to-end verifiable elections. In *Proceedings of the 2010 International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections (EVT/-WOTE'10)*, pages 1–16, Berkeley, CA, USA, 2010. USENIX Association. URL https://www.usenix.org/legacy/event/evtwote10/tech/full_papers/Popoveniuc.pdf.

[8] Estonia Internet Voting Statistics, 2020, (accessed 10.02.2020). URL https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia.

[9] Priit Vinkel and Robert Krimmer. The how and why to internet voting an attempt to explain e-stonia. In Robert Krimmer, Melanie Volkamer, Jordi Barrat, Josh Benaloh, Nicole Goodman, Peter Y. A. Ryan, and Vanessa Teague, editors, *Electronic Voting*, pages 178–191, Cham, 2017. Springer International Publishing. ISBN 978-3-319-52240-1. doi: 10.1007/978-3-319-52240-1_11.

[10] Andreas Ehringfeld, Larissa Naber, Karin Kappel, Gerald Fischer, Elmar Pichl, and Thomas Grechenig. Learning from a distributed denial of service attack against a legally binding electronic election: Scenario, operational experience, legal consequences. In *In Kim Andersen, Enrico Francesconi, ke Grnlund, and Tom van Engers, editors, Electronic Government and the Information Systems Perspective, volume 6866 of Lecture Notes in Computer Science*, pages 56–67. Springer, 2011.

[11] Koksal Mus, Mehmet Sabir Kiraz, Murat Cenk, and Isa Sertkaya. Estonian voting verification mechanism revisited. arXiv preprint arXiv:1612.00668, 2016.

[12] Sven Heiberg, Peeter Laud, and Jan Willemson. The application of i-voting for estonian parliamentary elections of 2011. In Aggelos Kiayias and Helger Lipmaa, editors, *E-Voting and Identity*, pages 208–223, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. ISBN 978-3-642-32747-6.

[13] Ivo Kubjas, Tiit Pikma, and Jan Willemson. Estonian voting verification mechanism revisited again. In Robert Krimmer, Melanie Volkamer, Nadja Braun Binder, Norbert Kersting, Olivier Pereira, and Carsten Schürmann, editors, *Electronic Voting*, pages 306–317, Cham, 2017. Springer International Publishing. ISBN 978-3-319-68687-5. doi: 10.1007/978-3-319-68687-5_19.

[14] Sven Heiberg, Tarvi Martens, Priit Vinkel, and Jan Willemson. Improving the verifiability of the estonian internet voting scheme. In *International Joint Conference on Electronic Voting*, pages 92–107. Springer, 2016.

[15] J. Benaloh, R. Rivest, P. Ryan, P. Stark, V. Teague, and P. Vora. End-to-end verifiability. arXiv preprint arXiv:1504.03778, 2015.

[16] Gina Gallegos-Garcia, Vincenzo Iovino, Alfredo Rial, Peter B. Roenne, and Peter Y. A. Ryan. (universal) unconditional verifiability in e-voting without trusted parties. Cryptology ePrint Archive, Report 2016/975, 2016. https://eprint.iacr.org/2016/975.

[17] Mahinthan Chandramohan and Hee Beng Kuan Tan. Detection of mobile malware in the wild. *Computer*, 45(9):65–71, 2012.

[18] Keylogger.org Team. What is stalkerware? https://android.keylogger.org/tag/stalkerware-spouseware/. Accessed: 2020-05-05.

[19] Kaspersky IT Encyclopedia. Stalkerware, Spouseware. https://encyclopedia.kaspersky.com/glossary/stalkerware-spouseware/. Accessed: 2020-05-05.

[20] The Risks of Commercial Spyware. https://www.wandera.com/the-risks-of-commercial-spyware/. Accessed: 2020-05-05.

[21] Android Security & Privacy Team. Android Security & Privacy 2018 Year In Review. https://source.android.com/security/reports/Google_Android_Security_2018_Report_Final.pdf. Accessed: 2020-05-08.

[22] A. Arabo and B. Pranggono. Mobile malware and smart device security: Trends, challenges and solutions. In *2013 19th International Conference on Control Systems and Computer Science*, pages 526–531, 2013.

[23] Michal Miedlarz. Screenshot preventing on mobile apps. https://medium.com/nomtek/screenshot-preventing-on-mobile-apps-9e62f51643e9. Accessed: 2020-05-06.

[24] Android Developer Team. Android Developer Documentation: WindowManager.LayoutParams. https://developer.android.com/reference/android/view/WindowManager.LayoutParams. Accessed: 2020-05-05.

[25] Qt for Python Team. Qt for Python Documentation: QColor Class. https://doc.qt.io/qtforpython/PySide2/QtGui/QColor.html. Accessed: 2020-05-5.