T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK – BİLGİSAYAR ANABİLİM DALI
BİLGİ TEKNOLOJİLERİ BİLİM DALI

JAVA TABANLI BİR ELEKTRONİK SEÇİM MODELİ UYGULAMASI

(Yüksek Lisans Tezi)

Tezi Hazırlayan: Murat ÖZDEMİR

İSTANBUL, 2008

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK – BİLGİSAYAR ANABİLİM DALI
BİLGİ TEKNOLOJİLERİ BİLİM DALI

JAVA TABANLI BİR ELEKTRONİK SEÇİM MODELİ UYGULAMASI

(Yüksek Lisans Tezi)

Hazırlayan:
Murat ÖZDEMİR
Öğrenci No:
050862020

Danışman: Yrd. Doç. Dr. Turhan KARAGÜLER

İSTANBUL, 2008

ABSTRACT

In recent years, fast developments on information technology systems have brought new debate over replacement of trational ballot box with the new computerized electronic system. The Electronic Election system would be particularly useful in not only speeding up counting of votes but also letting all the electorates be able to vote without having any obstacles. However, like all other new technologies, some drawbacks of electronic election system are also inevitable. This is the reason that many researchers have been working on the most critical issue of achieving safe and reliable election.

Among the well known electronic election models, the Mercuri Model suggests that there is no way that safe and secure electronic election is possible therefore any IT based system should be used together with a ballot box. In the framework of this work, the prototype of Mercuri Model is implemented by means of using Java technologies on the Turkish Election System. In order to assure the electorates about the outcome of their vote, a paper copy of the vote is also provided by the system at the final stage of voting. Further improvement regarding the election safety, an encrypted serial number is also printed on the ballot-paper.

Keywords: e-vote, electronic election, e-election, voting, Mercuri model, security, electronic voting, voting protocol

ÖZET

Son yıllarda bilişim teknolojileri alanında yaşanan gelişmeler seçimlerin geleneksel oy-pusulası-sandık sistemi yerine farklı araçlarla yapılabileceği görüşünü tartışmaya açmıştır. Elektronik oylama sistemleri özellikle oyların sayılma hızını artırarak, anında sonuç almaya ve çeşitli nedenlerle oy kullanması olanaksız vatandaşların, hiç bir etkiye maruz kalmadan, oy kullanmalarına imkan tanımaktadır. Ancak her teknolojik gelişmenin beraberinde getirmiş olduğu bir çok soru işareti ve olumsuzluk bu sistemler için de geçerli olup, tartışmalar ve çalışmalar özellikle sistemin güvenilirliğini artırmak yolunda sürmektedir.

Literatürde Mercuri Modeli diye bilinen seçim sistemi, salt elektronik seçim sistemiyle tam güvenli bir sistemin oluşturulamayacağı düşüncesiyle, mevcut sandık sistemi ile paralel kullanılacak bir elektronik seçim sistemi öngörmektedir. Yapılan bu çalışmada Mercuri modeli, Java teknolojileri kullanılarak prototip olarak gerçekleştirildi. Türkiye seçim sisteminin temel alındığı bu tezde, seçmen tarafından doğrulanmak amacıyla, tüm oyların bir kağıt bir kopyası, seçmen tarafından görülebilecek şekilde basılmaktadır. Basılan bu kağıt pusulalar ile elektronik seçimdeki oyların birbirlerini tutmaması halinde, fiziksel oyların geçerli kabul edildiği bu sistemde, elektronik oylar kadar pusula oyların da güvenliğini artırmak amacıyla, pusulaların üst kısmına özel bir algoritma ile üretilen bir seri numarası da basılmaktadır. Oyların değiştirilme, yada kaybedilmesi gibi durumların tesbiti ile oyların daha kolay sayılabilmesi amacıyla düzenlenen bu seri numaralar barkod olarak pusulaların üst kısmında yer almaktadır.

Anahtar Kelimeler: e-oy, Mercuri Modeli, elektronik seçim, güvenlik, seçim protokolü, elektronik oylama, elektronik pusula

İÇİNDEKİLER

	Sayfa
İç Kapak	i
Abstract	ii
Özet	iii
İçindekiler	iv
Şekil Listesi	vi
Kısaltmalar Listesi	vii
GİRİŞ	**1**
1. ELEKTRONİK SEÇİM SİSTEMLERİ	**3**
1.1. Elektronik Seçim Sisteminin İşleyişi	3
1.2. Elektronik Oylama Sistemlerinin İlkeleri	5
1.3. Elektronik Oylama Sistemleri	7
i) Kağıt Tabanlı (Paper-Based) Elektronik Oylama Sistemi	7
ii) DRE (Direct Recording Electronic) Sistemleri	8
1.4. Elektronik Seçim Sistemi İle Gelen Tehlikeler	10
i) Seçmen Hilesi, Ağ ve İşlevsel Şeffaflık	10
ii) Taraflılık ve İzleme Sonuçları	12
1.5. Diğer Elektronik Seçim Denemeleri	13
i) İnternet Üzerinden Oylama (Voting over Internet – VOI)	13
ii) Güvenli Elektronik Kayıt ve Oylama Deneyi	14
1.6. Elektronik Oylamanın Seçmen Üzerinde Etkisi	15
2. TÜRKİYE'DE ELEKTRONİK SEÇİM SİSTEMİ	**17**
2.1. Türkiye'de Yapılan Araştırmalar	17
2.2. Türkiye'deki Mevcut Uygulamalar	24
2.2. Değerlendirme	27
3. ELEKTROY ELEKTRONİK OYLAMA SİSTEMİ	**28**
3.1.ElektrOy Sisteminin Yazılımsal Bileşenleri	29
3.1.1.Geliştirme Birimi	29
3.1.2.Sunucu Birimi	31
3.1.2.1 Web Sunucusu – Apache Tomcat, GlassFish	31
3.1.2.2 Veritabanı Sunucusu – SQL	33
i) 'elektrOy' veritabanı	36
ii) 'ortak' veritabanı	36
iii) 'secim' veritabanı	37
3.1.3.İstemci Birimi	37

3.2. ElektrOy Seçim Sisteminde Kullanılan Donanımlar 38
3.3. ElektrOy Seçim Sisteminin Çalışma Prensibi 42

4. ELEKTROY: SEÇİMDEN-SONUÇLARA KADAR AŞAMALAR 44
4.1. İstemci Tarafı: Oy Verme 44
4.2. Seçim Kurulu Bölge Sorumlusu Tarafı: Sandık Sonuçlarını Alma 55
4.3. Seçim Memuru Tarafı: Seçmen Oluşturma, Sandık Atama İşlemleri 56
5. SONUÇ 62
KAYNAKÇA 64
ÖZGEÇMİŞ 65

ŞEKİL LİSTESİ

Şekil No.	Sayfa
Şekil 1 – Bir Pusula Örneği	4
Şekil 2 – Delikli Kart	8
Şekil 3 – DRE Oylama Sistemi	9
Şekil 4 – Seçsis Uygulama Sisteminin Altyapısı	25
Şekil 5 – NetBeans IDE 6.1	30
Şekil 6 – Tomcat Ana Ekranı	32
Şekil 7 – Tomcat Yönetim Ekranı	33
Şekil 8 – ElektrOy Sistemi Veritabanı Diagramı	35
Şekil 9 – ElektrOy'un Ülke Bazında Yayılmış Donanım Şeması	41
Şekil 10 – Elektroy Seçim Sistemi Seçmen Giriş Ekranı	45
Şekil 11 – Seçmen Sisteme Giriş Yaparken Sağ Taraftaki Tuş Takımını Kullanır	46
Şekil 12 – Sisteme Kabul Edilen Seçmene Sunulan Elektronik Pusula	47
Şekil 13 – Seçmen Tarafından Bir Parti Seçilmiş	47
Şekil 14 – Seçmen Tercihini Yaptıktan Sonra Gelen Son Uyarı	48
Şekil 15 – Oy Kullanan Seçmene Gelen Teşekkür Ekranı	49
Şekil 16 – Seçmenin Kullandığı Oyun Fiziksel Kopyası	49
Şekil 17 – Sistem Tarafından Doğrulanmayan Seçmenin Karşılaştığı Hata	51
Şekil 18 – Sistem Yalnızca Bir Kez Oy Kullanmaya İzin Vermektedir	52
Şekil 19 – Elektroy Sisteminin Akış Diagramı	53
Şekil 20 – Elektroy Sonuç Sistemi	55
Şekil 21 – Seçmen Sonuç Güvenli Oturum Açma Ekranı	56
Şekil 22 – Seçim Memuru İçin Seçmen Oluşturma ve Güncelleme Ekranı	57
Şekil 23 – Sandık Atama Modülü	58
Şekil 24 – Oy Doğrulama Modülü	60
Şekil 25 – ElektrOy Sisteminde Kullanılan Bir Barkod Okuyucusu	61

KISALTMALAR LİSTESİ

IPSEC	IPSecure
VPN	Virtual Private Network
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
SEÇSİS	Bilgisayar Destekli Merkezi Seçmen Kütüğü Sistemi
E-OY	Elektronik Oy
DRE	Direct Recording Electronic
HAVA	Help America Vote Act
VVPT	Voter Verified Paper Trail
VOI	Voting Over the Internet
FVAP	Federal Voting Assistance Program
DOD	Department of Defense
SERVE	Secure Electronic Registration and Voting Experiment
YSK	Yüksek Seçim Kurulu
SQL	Structured Query Language
MS	Microsoft Corporation
IDE	Integrated Development Environment
JSF	Java Server Faces
GPL	General Public License
VWJSF	Visual Web Java Server Faces
Java SE	Java Standard Edition
Java EE	Java Enterprise Edition
API	Application Program Interface
JDBC	Java Database Connectivity
JSP	Java Server Pages
HTTP	Hypertext Transfer Protocol
CPU	Central Processing Unit
ECC	Error Correction Code
RAID	Redundant Array of Inexpensive Disks
LAN	Local Area Network
WAN	Wide Area Network
ISDN	Integrated Services Digital Network
ADSL	Asymmetric Digital Subscriber Line
PIN	Personal Identification Number
TC	Türkiye Cumhuriyeti

GİRİŞ

Seçimler, demokrasi çatısı altında milli iradenin kendisini yönetecek kişi yada kişileri seçmesi amacıyla yapılmaktadır. Bütün seçimlerin temelinde, milli egemenlik, özgürlük ve eşitlik ilkesi yer almaktadır.

Yurttaşlar, yasal hakları çerçevesinde seçme ve seçilme hakkına sahiptirler. Bu haklar, Türkiye'de belirli mahalli idarelere yerleştirilen sandıklar ile, kağıt oy pusulaları içinden bir adayın işaretlenmesi ve bu pusulanın zarf içersine konulduktan sonra, mühürlü sandığa atılmasını kapsamaktadır. Seçim süresinin sona ermesiyle sandık sorumluları tarafından sayılan bu oylar ilçe seçim kurulu, il seçim kurulu ve yüksek seçim kuruluna aktarılıp, sonuçlar, pusulalar sayıldıkça ekrana yansıtılmaktadır. Elektronik oylama sistemleri, bu sürecin paralelelinde, aynı haklar çerçevesinde, uygulanan adımların daha güvenli ve hızlı bir şekilde yapılmasını amaç edinen bir platform olarak tasarlanmış sistemler bütünüdür.

Elektronik oylama sistemleri, delikli kartlar, optik oy tarama sistemleri, kiosk terminaller (veya bu sisteme çevrilen normal iş bilgisayarları), kağıt pusula doğrulama düzenekleri, oyların toplandığı sunucu depoları, veri-tabanları ve sunucuları merkeze aktarmayı amaçlayan güvenli bağlantı yöntemleri (IP Secure (IPSEC) – Internet gibi güvenli olmayan networkler içerisinde güvenli veri alış-verişi sağlayan bir protokol) aracıyla bağlantı imkanı sağlayan router, Virtual Private Network (VPN) sonlandırıcıları, switchler ile birlikte sisteme gelebilecek saldırıları tespit ve önlemek amacıyla kullanılan ateş duvarı (firewall), ve IDS/IPS sistemlerini içermektedir.

Türkiye'de elektronik seçim sistemi, ilk olarak 1986 yılında Hacettepe Üniversitesi'nin, 1989 yılında Yüksek Seçim Kurulu tarafından kabul edilen SEÇSİS Projesi ile başlanmıştır. Bunun yanısıra, dünyada ilk olarak 1990'lı yıllarda seçimlerde resmi olarak kullanılmaya başlanmıştır. Bu tarihten sonra başta ABD olmak üzere, Brezilya'da yapılan tüm seçimlerde bu sistemin kullanılması ile birlikte, Hindistan, Hollanda, Venezualla ile İsviçre, Kanada ve Fransa'da da geniş seçmen kitleleri ile denenmiştir.

Yapılan bu çalışma neticesinde, bütün seçim kural ve protokolleri incelenerek arkasında azami derecede güvenlik ve gizlilik bulunan sistemlerin yatırım maliyeti de göz önünde bulundurulmuştur. Bu sebeple uygulamada kullanılacak sistemlerin, düşük donanım gereksinimine sahip, lisans maliyeti gerektirmeyen, açık kaynak kodlu yazılımlardan oluşması tercih edilmektedir.

1. ELEKTRONİK SEÇİM SİSTEMLERİ

Elektronik seçim sistemleri, seçmenlerin kullandığı bilgisayar terminali ile buna bağlı bulunan yazıcıdan, oyların kaydedildiği veritabanları ve seçim programının yer aldığı sunucuyu kapsayan geniş bir sistemler bütününü tek bir başlık altında toplar.

Elektronik oylama (e-oy) ile, kullanılan tüm ekipmanlardan ziyade geliştirilmeye çalışılan sistemlerden bahsedilmektedir.

1.1. Elektronik Seçim Sisteminin İşleyişi

Seçmenin, bir bilgisayar aracılığı ile (kişisel bilgisayar gibi), bir kaç tıklama ile yasal hakları çerçevesinde ülke seçimlerine katılması ve oyunu istediği adaya vermesi mümkündür. Bu yolla, seçimi gerçekleştirmek için uygun yerler arama, okulları tertipleyip düzenleme ve saatlerce katılımcıları bekletme zorunluluğu ortadan kalkmaktadır.

Elektronik sistemlerin insan hayatını kolaylaştırdığı 21. Yüzyılda, seçim sistemleri için de bir çok çözüm önerilmiştir. Tüm bu çözümleri elektronik oylama (e-oy) başlığı altında toplamak mümkündür. Genellikle e-oy hem oylamanın elektronik olarak kaydedilmesi hem de çizelgelerle ifade edilmesi anlamına gelmektedir.

Oy sistemlerinin, elektronik ortamdaki rollerininin daha iyi anlaşılabilmesi için, öncelikle oy yönetiminin nasıl çalıştığının bilinmesi gerekmektedir. Seçimler Türkiye'de bölgesel olarak denetlenir. Bu tür merkezleşmeden uzaklaşmanın tek sebebi oyların sayılabilme kolaylığıdır.

Türkiye İstatistik Kurumundan alınan bilgilere göre, Türkiye'de kayıtlı seçmen sayısı 2007 rakamlarına göre, 42,5 milyonun üzerindedir. Bu kadar oyu koordine etmekve düzenlemek, tek bir merkezden yapılması mümkün olmayacak bir işlemdir.

Genel seçimler için, öncelikle en yakında bulunan oy kullanma merkezlerine (okul gibi) gidilir. Görevli bulunan seçim memuru, seçmenin kayıtlı olup olmadığını kontrol eder. Seçmen kayıtlı ve o seçim için daha önce oy kullanmamış ise, kendisine pusula (Şekil 1), zarf ve evet mührü verilir, oy kullanması için kapatılmış bölmelere yönlendirilir. Seçmen tercihini yaparak pusulayı katlayıp, zarfın içine koyar ve zarfını kapatarak mühürlerle kapıtılmış olan sandığa atar. Oy kullanım süresi dolduktan sonra, seçim merkezi kapanırken, seçim memuru kullanılan oyları güvenlik kontrolünde sandıkları açarak, sayar. Sayılan bu oylar kamuoyuna kademeli bir şekilde bildirilir.

Şekil 1 – Bir Pusula Örneği

Elektronik sistemlerdeki adımlar geleneksel olanlarla aynıdır. Farklılıklar ise, kağıt pusulalar yerine kapalı bölmelerde bulunan terminaller ve bunlara bağlı yazıcıların kullanılmasıdır. Seçmen, kimlik kontrolü yapıldıktan sonra, dokunmatik ekranlı bilgisayarın başına gelir. Kendisine daha önceden oluşturulmuş ve gönderilmiş olan şifresini ekranda kendisine sorulan alanlara girer ve sisteme alınır. Kendisine aday partilerin listesi getirilir ve burada seçtiği aday oy olarak sisteme işlenir. Mercuri modelinde tüm bunların yanısıra kullanıdığı oy yazıcıdan da bastırılır ve kendisine gösterilir. Bu şekilde yapılan uygulama, seçmenin aklında soru işaretleri oluşmasını engelleyerek, güvenli bir şekilde oy kullandığına ve kullandığı oyların arka planda değiştirilmediğine inanmasını sağlar.

1.2. Elektronik Oylama Sistemlerinin İlkeleri

Elektronik seçim sistemleri, uygulamada getirdiği kolaylıklarla birlikte, bir çok problemi de içerisinde barındırır. Bu problemler gerek tasarım gerekse uygulama alanında elektronik seçim uygulamalarının hatasız çalışmalarını engellemekle birlikte, bir çok tartışmaya konu olmuştur.

Roy G. Saltman Accuracy*, Integrity, and Security in Computerized Vote-Tallying* adlı çalışmasında internet üzerinden oy kullanma sistemleri hariç, hemen hemen uygulanmış tüm elektronik seçim sistemlerinin bir analizini yaparak bazı öneriler getirmiştir.[1] Özellikle Direct Recording Electronic (DRE) – Doğrudan Kayıt Elektroniği, sistemleri üzerinde yoğunlaşan Saltman'a göre Doğruluk, Bütünlük ve Güvenlik bilgisayar temelli bir seçim sisteminin ana unsurlarıdır. Doğruluk, bir elektronik seçim sistemi için temel bir gereksinimdir, ancak Bütünlük ve Güvenlik olmadan tek başına bir işe yaramayacağını savunulur.

Doğruluk: Oy sayım-hesaplama-tasnif sisteminden çıkan veriyle sisteme giren verinin mantık ve kabul edilebilirlik açısından birbirine uymasıdır.

Bütünlük: Bir elektronik seçim sisteminin kendisi için belirlenmiş işlevleri doğru ve tutarlı bir biçimde yerine getirmesidir.

Güvenlik: Elektronik seçim sistemine erişimin kontrol altında tutulması gerekir. Sistem, bir bütün olarak güvenli olmalıdır. Seçimin işlevlerini yerine getirmesini engelleyecek, saptıracak, etkide bulunacak her türlü girişim engellenebilmelidir. Seçim sisteminin hizmetlerine, alanlarına, ekipmanlarına, belgelerine ve verilerine erişimin kontrol atında tutulması gerekir.

ABD'de 1980'lerden itibaren 50 değişik elektronik seçim sistemi uygulanmıştır.

[1] Saltman, R.G, "Accuracy, Integrity, and Security in Computerized Vote-Tallying", ACM, 1988

Michael Ian Shamos, *Electronic Voting – Evaluating the Threat* adlı çalışmasında, bu elektronik seçim uygulamalarından şu sonuçları çıkarmıştır: [2]

1. Her seçmenin tercihleri ulaşılamaz bir gizlilik içinde tutulmalıdır.
2. Oy kullanma hakkı olan her seçmen sadece bir kez oy kullanabilmelidir.
3. Seçim sisteminin değiştirilerek bozulmasına ve oyların değiştirilmesine, tahrif edilmesine, satılmasına kesinlikle imkan verilmemelidir.
4. Tüm oylar tam ve doğru bir biçimde rapor edilmelidir.
5. Seçim sistemi, her seçime, (kodlarında herhangi bir değişiklik yapmadan) tamamen uygulanabilir olmalıdır.
6. İkinci ve dördüncü maddelere karşı oluşabilecek olumsuzlukları önleyebilmek için bir denetim yolu (audit trail) olmalıdır.

Birinci, ikinci ve üçüncü maddeler genelde her seçim sistemi için olmazsa olmaz koşullardır.

Shamos'a göre, dördüncü koşulun uygulanması biraz kuşkuludur. Çünkü, sayım işini gerçekleştiren işlevlerin nasıl olması gerektiği üzerinde evrensel bir görüş birliği yoktur. Seçim sonucunun doğru bir şekilde rapor edilmesi, arka planda çalışan kodlara bağlıdır. Verilen bir oyun başka bir adayın hesabına sayılıp sayılmadığı belli değildir. Mükemmellik bir seçim sistemi için aranmaması gereken bir şeydir, arandığındaysa bulunamayacağı kesindir. Doğru olan ise koşulları ihlal edebilecek olumsuzlukları, denetlenemeyen hataları değerlendirmek ve bunları engelleyip en az seviyeye indirmektir.

[2] Shamos M.I, "Electronik Voting – Evaluating the Threat", J.D., 1993

1.3. Elektronik Oylama Sistemleri

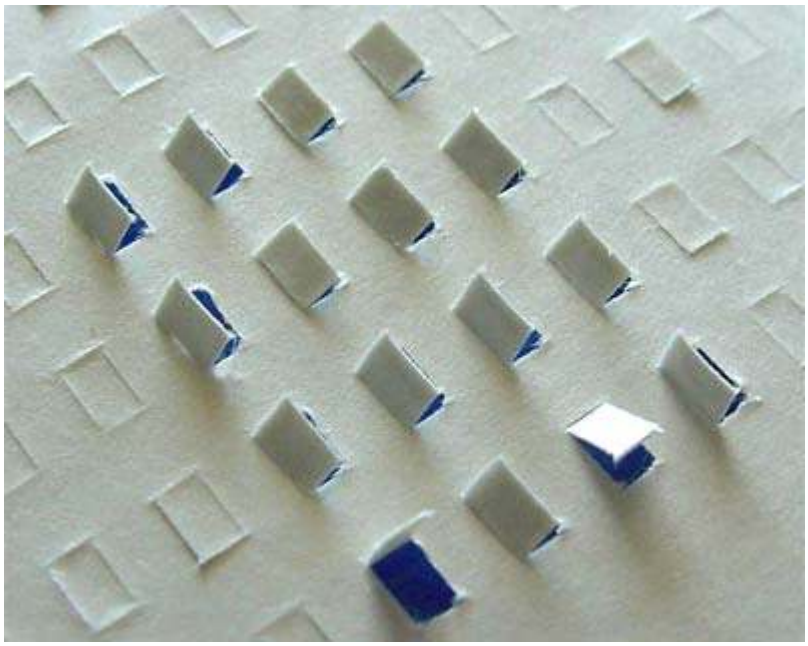
Belli başlı elektronik oylama sistemlerine örnek olarak, kağıt tabanlı oylama sistemleri ile DRE (Direct Recording Elektronic) oylama sistemleri verilebilir.

i) Kağıt Tabanlı (Paper-Based) Elektronik Oylama Sistemi

Kağıt tabanlı sistemlerde, elekronik bileşen genellikle, bir listeleme cihazıdır. Bu, oyların, el ile sayılmalarından daha hızlı olan elektronik sistemde sayılması demektir. Bir takım pusula yazdırma sistemleri DRE sistemlerine benzemektedir. Seçmenler bir dokunmatik ekran yada benzeri elektronik aygıt kullanarak tercihlerini gerçekleştirmektedirler. Seçmen oyunu kullandığında, aygıta bağlı bulunan bir yazıcıdan fiziksel bir kağıt pusula çıkmakta. Seçim memuru bu kağıt pusulayı almakta ve il merkezlerine iletmekte. Daha sonra ayrı bir elektronik aygıt da, optik olarak bu pusulaları taramakta ve sonuçları listelemektedir.

Kağıt tabanlı sistemin avantajlarından birisi de pusulanın bir parça kağıt tarafından temsil ediliyor olmasıdır. Bu somutluluk, seçmenlere oylarının sayıldığı güvenini vermektedir. Fakat, fiziksel bir pusula o oyun doğru bir biçimde sayılacağını sağlamaz. Bir çok etken oyun yanlış sayılmasına neden olabilir. Delikli karttaki (Şekil 2) delikler düzgün bir şekilde ayarlanmamış olabilir yada, tam delinmemiş olabilir, bu da sonucu yanlış yönde etkileyebilir. Örneğin 2000 seçimlerinde Florida'da bu tür olayla karşılaşılmıştı. Optik tarama kartlarında, rastgele işaretleme yada tamamlanmamış işaretlemeler, değerlendirme esnasında yanlış bir şekilde çevrilmişti. Optik tarama kartlarını işaretleyen yazıcıların tonerlerinin azalmış olması da, kartların tamamlanmamış yada okunamayacak işaretler içermesine sebep olabilmektedir. Ayrıca bir seçmen için bir yada daha fazla adayı seçmesi de mümkün olabileceğinden, bu tür seçimler değerlendirme cihazları tarafından kabul edilmemektedir.

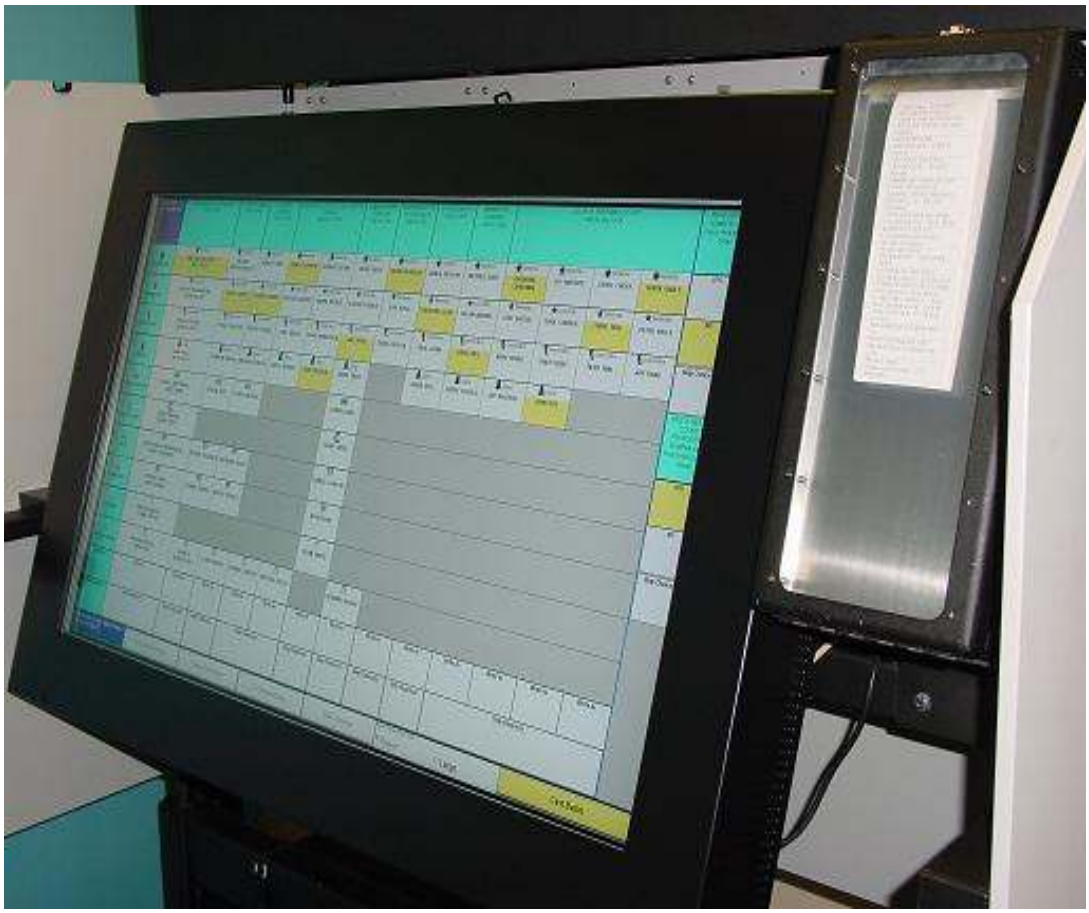
Fiziksel pusulalar değerlendirmeden önce kaybolabilir veya yok edilebilir. Ancak, kağıt pusulaları kaybetmek, elektronik kayıtları kaybetmekten çok daha zordur.



Şekil 2 – Delikli Kart

ii) DRE (Direct Recording Electronic) Sistemleri

Direct Recording Electronic System (DRE), (Şekil 3) temelinde bir bilgisayardır. Seçmenler oy pusulalarını görerek, tuşlar yada dokunmatik ekran yardımı ile seçimlerini gerçekleştirirler. Bir takım DRE sistemleri ayrıca, pusula ekrana gelmeden önce etkin olması gereken manyetik kart okuyucuları yada kartuş sistemlerini içlerinde barındırırlar. Oylar, bir cd, hafıza kartı yada başka bir hafıza biriminde saklanırlar. Seçim memurları da tıpkı kağıt tabanlı pusulalar gibi bu bellek aygıtlarını değerlendirmek için merkeze ulaştırırlar. Bazı makineler sonuçları modem üzerinden bağlantı kurarak merkeze aktarma yeteneğine sahip olmakla birlikte, veri güvenliği açısından bu sonuçlar genellikle, bellekteki asıl oylar değerlendirilene kadar resmi olmayan sonuçlar olarak kabul edilir. Birçok DRE cihazları ayrıca pusulanın çıktısını alabilmek için bir yazıcıya da sahiptir.



Şekil 3 – DRE Oylama Sistemi

Bir DRE sistemini güvenli ve inanılır olarak düşünüldüğünde, kağıt-tabanlı sisteme nazaran bir çok üstünlüklere sahiptir. Çünkü pusulalar elektronik olarak gösterildikleri için, görünümlerinde tasarım anlamında hiç bir sınırlama olmaz. Programcılar pusulaları bir çok dilde oluşturabilirler ve seçmenlerler kolaylıkla dil değişimi yapılabilir. Ayrıca görmesi zayıf olan seçmenler için büyük boyutlu pusulalar yapabilirlerken, tamamıyle göremeyen seçmenler için ise, ortak birer ses dosyaları oluşturulabilir. Seçim kurul memurları, her ihtimale karşı ne kadar pusula gereksinime sahip olmalarını tahmin etme zorunda kalmaksızın, hangi koşul olursa olsun, ona göre bir pusula biçimi oluşturulur ve ihtiyaçlar karşılanır.

Oylar bir hafıza kartında ve sayısal ortamda tutulduğu için, değerlendirme çok daha hızlı olacaktır. Taranılacak yada sayılacak hiç bir kağıt pusula olmadığından, mekanik hata riski de sıfıra indirgenecektir. Hala insani hatalar bir etken olarak kabul edilmekle birlikte, ortamda her zaman oluşabilecek bir yazılım hatası ihtimaline karşın şüpheler bulunmaktadır ki, ideal bir sistemde değerlendirme, saymaya gerek kalmayacak bir şekilde anlık olmaktadır.

1.4. Elektronik Seçim Sistemi İle Gelen Tehlikeler

Elektronik sistemlere olan güvensizliğin en büyük nedeni, sistemin bir çok hileye açık olmasına bağlanmıştır.

i) Seçmen Hilesi, Ağ ve İşlevsel Şeffaflık

Eleştirmenler DRE sistemleri hakkında bir takım endişelere dikkat çekerler. Bunlardan önemlisi seçmenin hile yapma potansiyelidir. DRE sistemlerini öneren kimseler, özel bilgilere sahip, yetenekli kimselerin sistemi kötüye kullanabileceği konusunda tartışmaktadırlar. Bu seviyede bir uzmanlıktan dolayı, çok az insan hile yapabilme yeteneğine sahiptir. DRE sistemleri ayrıca kolaylıkla erişilebilecek ortamlardan uzaktırlar. Bunun sebebi, üretildiği yada saklandığı yerlerde, yüksek güvenlik altında bulunduruldukları için, kimse erişememektedir.

Eleştirmenler, özel durumlarda (örneğin soruşturmaya uğramış bir programcı) ki bu kağıt tabanlı oy sistemine nazaran tespit etmesi daha zor bir durum olup, bu konularda endişenin haklı olduğu konusunda bir çok örnekler yaşanmıştır.

Seçim memurları ve DRE sistem üreticileri, seçmen belirsizliğini içeren bir çok etkeni göz önünde bulundurmalıdırlar. Oy kullanılmış bir pusula, kullanan oyun kime ait olduğunu göstermemelidir. Kağıt-tabanlı pusulalar yada kağıt çıktısı veren DRE sistemler her bir seçmenin tercihini gösteren fiziksel bir kayıt oluştururlar. Bu kağıt olmadığında, sağlanan tek kayıt elektronik ortamdaki olacaktır.

Kağıtsız sistemin eleştirmenleri, bir programcının pusulanın yayınlandığı kaydı değiştirebileceğini, çünkü oyların kullanan kişiye geri bağlanamayacağını, böylece oy çalmanın da tespit edilemeyeceğini vurgulamışlardır.

Sayısı onu aşkın üretici, bugün dünyanın çeşitli ülkelerinde kullanılan DRE sistemi üretmektedir. Her üretici (yada her bir geliştirme partneri) ekran, kayıt, ve değerlendirme için yazılımlar geliştirmektedir. Bir çok ülke bir seçimde birden fazla üreticinin DRE sistemlerini kullanmaktadırlar. Eleştirmenler ise, farklı sistemleri birbirine bağlamanın bir güvenlik açığı doğuracağı düşüncesindedirler. Zaten üreticiler de sistemlerinde, diğer platformlarla doğrudan çalışabilecek şekilde bir tasarım kullanmamaktadır.

Diğer önemli kaygı da şeffaflıktır. Şeffaflık, sistemin nasıl çalıştığının tam ve kesin bir şekilde açıklanmasıdır. Şeffaflığı başarmanın tek yolu da, pusulaları gösterme ve oyları seçerken kullanılan kaynak kodunun, bilgisayar bilimcileri ile paylaşmaktır. Kaynak kodu insanlar tarafından okunurken, bilgisayarlar tarafından okunamayan bir programlama dilidir – bilgisayarlar nesne kodunu okurlar. Kaynak kodlarını denetleyerek, eleştirmenler, bilgisayar bilimcilerinin, söz konusu programın istenilen işi hatasız olarak yaptığını kanıtlamasına yardımcı olduğunu savunurlar. Fakat sistem üreticilerinin kaynak kodlarının özel bilgi olduğu kanısını gütmeleri, ve başka bilgisayarlarda da izinsiz çoğaltılıp, kullanabileceği ihtimali sebebiyle kodları paylaşmakta isteksiz oldukları genel eğilimdir.

DRE sistemlerini tavsiye edenler, sistemlerini, kaynak kodları ve zayıf noktalarını açıklayarak daha güvensiz hale getirebilmektedir. Buna karşın eleştirmenler ise, kodlar dikkatlice incelenmedikce, seçmenler sistemin ilk etapda, hangi aşamada ne yaptığından haberdar olamayacağını vurgularlar. Hile, onlara göre, üreticinin kasıtlı olarak yada bir programlama hatasından dolayı, sistemin yanlış çalışması ve bunun saptanmasının mümkün olmamasıdır.

ii) Taraflılık ve İzleme Sonuçları

Taraflılık ve kötü niyetli olma, eleştirmenlerin diğer kaygılarıdır. DRE sistemleri, politik olarak tarafsız olduğu pek gözlenemeyen, özel firmalar tarafından üretilir. Eleştirmenler, seçimde özel firmaların çıkarlarına uygun bir partinin seçilmiş olabileceği kaygısını taşırlar.

Denetleme, DRE sistemlerinin kullanımında göz önünde bulundurulması gereken başka bir meseledir. Bir Amerikan kuruluşu olan Help America Vote Act (HAVA), tüm oylama sistemlerinin denetlenebilir olmasını ve yapılan ölçümün de sistemin düzgün çalıştığını kanıtlamasını gerektirdiğini iddia eder. Bu, üreticiler ile bilgisayar bilimcileri arasında süregelen bir savaştır. Seçmenlerin kimliğinin gizli tutularak yapılacak bir denetleme gerçekten çok zor bir süreçtir. Bazı uzmanlar, hem sistemin hafızasında hem de fiziksel bir kağıtta pusulaların tutulduğu, Voter Verified Paper Trail (VVPT) – Seçmen tarafından Doğrulanmış Kağıt Çıktısı'nı savunmaktadırlar. Böylece, her bir seçmen daha sonra sonuç ekranı ile fiziksel kağıdı karşılaştırarak, oyunun doğru kullanılıp, kullanılmadığını doğrulayacaktır. Bugünlerde, 27 Amerikan eyaleti yasa yada tüzüklerde belirtildiği gibi bir kağıt çıktı gereksinimi duymaktadırlar.

Bazı eleştirmenler, kağıt çıktısı olmayan DRE sistemlerinin anlaşılamaz olduğunu savunurlar. Onlara göre, bir denetim oy pusulasının ekranda gösterildiği gibi kaydedildiğini denetleyemez ise, seçimin sonucunu da doğrulayamaz. Bazıları ise kağıt çıktılarının tek başına kullanılmayacağını savunurlar.

Bir DRE sistemi, bir seçmenin tercihini ekranda göstermeli ve görünen bir hata olmadan da bellek aygıtında elektronik olarak kaydetmelidir. Onların çözümü ise, kullanılan oyların, oylama sistemleri tarafından tam ve doğru bir şekilde yakalanıp kaydedildiğini gösteren tüm simulasyonların test edilmesi sonucu verilen sertifikalara odaklanmaktır.

1.5. Diğer Elektronik Seçim Denemeleri

Başta ABD'de olmak üzere bir çok gelişmiş ülkede bu çalışmaları yürütmek amacıyla çeşitli komiteler oluşturulmuş olup farklı seçeneklerle elektronik seçim denemeleri yapılmıştır.

i) İnternet Üzerinden Oylama (Voting over Internet – VOI)

2000'de Amerika'da Federal Voting Assistance Program (FVAP), oyların internet üzerinden güvenli ve güvenilir bir şekilde kullanılabilirliği hususunda Voting Over the Internet (VOI) adında bir pilot program yönetmekteydi. Program boyut olarak mütevazi idi – 21 eyalet ve 11 ülkede 100'e yakın seçmen üzerinde 7 Kasım 2000 seçimlerinde bu sistem kullanıldı. Amerika Birleşik Devletlerindeki ilk VOI girişimindeki pusulalar devlet, eyalet ve yerel sonuçlara yansımış oldu. Seçmenlere oylarının sayıldığının garantisini vermek için, herhangi bir yanlışlık ihtimaline karşı, her bir seçmenin ayrıca geleneksel kağıt-tabanlı sistemde de oy kullanmalarına izin verildi.

FVAP, bu sistemi oyları değerlendirmek amacı ile değil, uzaktan oy kullanmak üzere tasarlamıştır. Her bir seçmen, pusulaların gösterildiği FVAP sunucularına teslim edilmesi için tasarlanan bir CD alırlar. Sistem seçmenlerden güçlü şifrelemeli Netscape Navigator 4.05 yada üstü bir browser kullanmalarını istemektedir. Department of Defense (DoD), seçmenlerin yeniden oy kullanmalarını engellemek için bir sayısal sertifikasyon programı yönetirler.

Şifrelenen pusulalar internet üzerinden FVAP sunucusuna gönderilirler. Sadece pusulanın istenilen tarafı şifrelenmemiş kalır. Sunucu kesintisiz güç kaynakları ile ve sınırlandırılmış fiziksel erişim kontrolünde bulunan bir yerde tutulur. Sistem, İki adet saldırı tespit cihazı ile, hile benzeri aktivite teşebbüslerini anlık olarak göstermiştir.

Seçmenin bulunduğu seçim bölgesinde görevli seçim memurları kendilerinde bulunan terminaller ile sunucularına erişirler. Bu sunucular da FVAP sunucularına, bağlı bulundukları bölgede kullanılan oyları teslim etmek için bağlanmaktadırlar.

Pusulalar geldiğinde, görevlinin kullanımında bulunan bilgisayar onları deşifreler ve yazıcılardan kağıt kopyalarını alırlar. Seçmenler de yazılan sonuçların birer kağıt kopyalarını alırlar. Değerlendirme için ise uygun bir yerel seçim görevlisinin bilgisayarına gönderir.

Tüm deneyimlerin bir sonucu olarak, FVAP görevlileri pilot programı bir başarı olarak tanımlamaktadırlar. Onlar, küçük bir alan üzerinde uzaktan oylamayı sıkı kontrollerle birlikte geleneksel posta yolu ile yapılan oylamaya kabul edilebilir bir alternatif olarak düşünmüşlerdir. Ayrıca, bunun 100 katılımcıdan daha azını kapsayan bir deneyim olduğunu; bunun binlerce yada milyonlarca vatandaş için internet üzerinden oy kullanmayı etkin kılan bir sistem olarak geliştirmenin çok daha fazla özen istediğini de belirttiler.[3]

ii) Güvenli Elektronik Kayıt ve Oylama Deneyi

VOI başarısından sonra, komite Department of Defense (DOD) – Amerikan Savunma Bakanlığı, tarafından kontrol edilen daha büyük bir internet-tabanlı oylama programı istedi. 2001 yılında DOD, Secure Electronic Registration and Voting Experiment (SERVE) – Güvenli Elektronik Kayıt ve Oylama Deneyi adı verilen bir sistemin tasarımına başladı. DOD, 100.000 civarında vatandaşın deneye katılacağını ve oylarının 2004 parti başkanlığı ve genel seçimlerde sayılacağını tahmin ediyorlardu. Eğer bu deneyin başarılı olduğuna kanaat getirilirse, internet oylama tüm deniz arışı askeri personel ve diğer vatandaşlara yayılacaktı.

[3] Applied Computer Security Associates (ASSAC), http://www.acsac.org/2000/presentations/Rodriguez.pdf

2004'ün başlarında DOD, bu deneyi, güvenlik kaygılarından dolayı uygulama evresinden önce iptal etti. Gerekçe olarak, seçmen kimliksizliğinin riske atılması yada hackerlerin internet üzerinden gönderilen oylara müdehale ederek alıkoymaları yada oya hile karıştırıp, değiştirme ihtimalleri açıklandı.[4] Komite, 2007'de Election Asistance Commission kurumunun uzak oylama ve kayıtlar için yeni prensiplerini belirleyeceği zaman bir kez daha deneyin denenmesini istedi.

VOI ve SERVE programları birlikte deniz aşırı seçmenlere daha kolay erişim ve uzaktan oy kullanma için tasarlanmışlardır. Yüzbinlerle ifade edilen seçmen sayısı gibi, etki sadece küçük bir miktarda sayıyı da ifade edebilmektedir. Internet-tabanlı oylar güvenlik ile ilgili şüpheleri tatmin etmek zorunda olmakla birlikte, güvenilir ve seçmen doğrulaması, pusula gösterimi, pusula kaydı ve pusula gönderimi için tekrarlanabilir olmalıdırlar.

1.6. Elektronik Oylamanın Seçmen Üzerinde Etkisi

Halkın, seçilen hükümetin, gerçekten milli irade ile iş başına geldiğini düşünmesi, seçimlere güvenmesi ile olur. Eğer halk seçimlerin adaletsiz olduğunu algılar ise, hükümetin temeli sarsılabilir. Şu anda, ABD'nin bir çok eyaletlerinde kullanımda olan en son elektronik oylama sistemleri (Electronic Data Systems'e göre bilhassa DRE sistemleri, yerel kayıtlı seçmenlerin yüzde 38'i için uygun bir oylama ekipmanı olarak hizmet vermekte) büyük çaplı inceleme ve eleştiri altındadır. Vatandaşlar, özel şirketler ve seçim memurları bu sistemleri dikkatli incelemek ve kullanıma dahil etmek için efor sarfetmektedir.

E-oylama konusunda artmakta olan tartışmalara rağmen, bir çok eleştirmen elektronik oylama sistemlerine doğru kaymanın oylama sürecinin geliştirmesi açısından kaçınılmaz olduğunun farkındadır. Çükü demokrasi, halkın adil seçimlere inanması üzerine kurulu olduğundan, bu sistemler diğer metodlara nazaran güvenli ve güvenilir olarak gösterilmelidir.

[4] Jefferson D, Rubin A.D., Simons B.,Wagner D. ," A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)", 2004

ABD'de konuya ilişkin bulunan raporlara göre, kayıp veriler, bozuk dosyalar, rüşvet alan memurlar, üreticinin parti taraftarlığı, güvenli olmayan bilgi ve diğer skandallar 2000'den bu yana sürekli bir şekilde seçim gündemlerini meşgul etmiştir. Bu raporlar halkın bu sistemlere olan güvenini sarsıcı etmenler olmakta, bu sistemi kullanan her bir ülke bur tür skandallara, yasanın gösterdiği şekilde önlemler getirmelidir. [5]

[5] EDS, http://www.eds.com

2. TÜRKİYE'DE ELEKTRONİK SEÇİM SİSTEMİ

Günümüzde, başta ABD, Hindistan ve Avrupa'nın bir çok ülkesinde geniş seçmen kitleler üzerinde uygulanmakta olan elektronik seçim sistemlerinin Türkiye'de, Yüksek Seçim Kurulu (YSK)'nın yapmış olduğu bir takım denemeler dışında rastlamak mümkün değildir. Ancak bu konuda bir çok akademik çalışmalar, uygulama öncesi, teorik konuda izlenmesi gereken polikaları belirleme amacıyla yürütülmektedir.

2.1. Türkiye'de Yapılan Araştırmalar

Türkiyede, bir çok üniversiteden, elektronik seçim, elektronik seçim ilkeleri, uygulama prosedürleri vb. konularda bir çok değerli çalışmalar sunulmuştur. Bu çalışmalara ilk örnek olarak M. Şahin'in "Elektronik Seçim Sistemlerinin Analizi ve Bir Model Önerisi" isimli çalışmasını verebiliriz.[6] Bu çalışmada bir çok elektronik seçim mimarilerin yapıları detaylı bir şekilde incelenmiş, çalışma mantığı, şekilli örneklerle anlatılmıştır. Çalışma içersinde, tüm bu mimarilerin güçlü ve zayıf yanlarına da değinilmiştir. Mimarilerin, mevcut eleştirmenler tarafından en çok takdir edilen, eleştirilen yanlarının da açıklandığı çalışmada, oyların güvenli bir şekilde saklanacağı yönünde geliştirilmeye açık bir model önerilmiştir.

Bu konuda yapılan başka bir araştırma, Yrd. Doç. Dr. M. Akın'ın "Elektronik Oy Verme Sistemlerinde Güvenlik: Deneyimler ve Türkiye İçin Öneriler"7 isimli çalışmasıdır. Akın bu çalışmasında, elektronik seçim konusunun, artık teorik bir uygulama olmadığı, bir çok ülkede kullanıldığını dile getirmektedir.

[6] Şahin, M. "Elektronik Seçim Sistemlerinin Analizi ve Bir Model Önerisi", Yüksek Lisans Tezi, Beykent Üni., 2005

[7] Akın, M. "Elektronik Oy Verme Sistemlerinde Güvenlik: Deneyimler ve Türkiye İçin Öneriler", İ.Ü. Ekonometri ve İstatistik Sayı:3 2006- 12-11

Elektronik seçim sistemleri kullanılarak kağıt oy pusulalarında görülen bir takım sakıncaların kolaylıkla giderilebileceği, fakat bu sistemlerin kendilerine özgü bir takım güvenlik sorunlarına sahip olduklarını, kullanan ülkelerde ne şekilde kullanıldığına ilişkin değerlendirmeler yapmıştır.

Yapılan tüm bu değerlendirmelerden sonra, Türkiye'de güvenli ve adil bir biçimde oy verebilmek için bir takım önerilerin de sunulduğu bu çalışmaya göre, elektronik seçim sistemlerinin kabul edilebilir bir maliyet karşılığında edinilebilmesi mümkündür.

Elektronik seçim sistemlerinin başına gelebilecek her yönlü riskler, bunlar seçmen riski, programcı riski, seçim görevlisi riski gibi. sınıflandırılmış, bunlara karşı alınan önlemler sıralanmıştır.

Akın, bir elektronik seçim sistemi oluşturulurken, bir çok başka kaynakta da belirtilen göz önünde bulundurulması gereken önerileri aşağıda sıralanmıştır:

• **Kullanım kolaylığı:** Elektronik oya kolayca geçilebilmesi için sistem hem görünüş hem de kullanılış açısından seçmenlerin alıştığı oy pusulasına benzer şekilde tasarlanmalıdır. Seçim günü kolayca kurulup kaldırılabilmeli ve sandık kurullarınca oy verme işlemi başlamadan önce kolayca test edilebilmelidir. Yıllar içinde birden fazla seçimde kullanılacağı için aygıtlar kolayca depolanabilmeli ve taşınabilmelidir.

• **Sürekli çalışma:** Sistem seçim günü oy vermenin başından sonuna kadar arızasız çalışabilmelidir. Elektrik kesilmeleri halinde de çalışmaya devam edebilmeli ve kaydedilmiş bilgileri hafızasında tutabilmelidir.

• **Kağıt Pusula Üretimi:** Kullanılacak oy verme aygıtı muhakkak bir kağıt oy pusulası üretmeli, seçmenin onayından sonra bu pusulalar el değmeden ayrıca mühürlü bir sandıkta toplanmalıdır. Bir itiraz halinde yeniden sayım için bu pusulalar kullanılabilecektir.

• **Ağ Bağlantısı:** Elektronik oy verme aygıtları hiçbir zaman bir ağ içinde yer almamalıdır. Her aygıtta seçmenlerin oyların kullanmasından sonra oluşan seçim sonucu normal seçimlerde olduğu gibi Sandık Kurulu tarafından bir tutanakla belirlenip İlçe Seçim Kurulu'na bildirilmeli, toplamlar bu şekilde alınmalıdır. Bu yolla hem her aşamada toplamların denetimi sağlanabilir hem de ağlara yapılabilecek müdahaleler sonucu seçimin sabote edilmesinin ya da sonuçların değiştirilmesinin önüne geçilebilir.

• **Güvenlik:** Oy verme aygıtları dışarıdan fiziksel ya da elektronik müdahaleye imkan vermemeli, oy verme süreci dışarıdan izlenememelidir. Her aygıt özel bir anahtarla açılabilmeli ve bu anahtarlar İlçe Seçim Kurullarında bulunmalıdır. Bu aygıtların birden fazla seçimde kullanılmaları hedeflendiği için iki seçim arasında depolanmaları için özel depolar hazırlanmalıdır. Daha az sayıda aygıt saklanması gerekeceği ve ulaşım gereksinimi daha az olacağı için depoların ilçe merkezlerinde kurulması daha uygun olacaktır. Depolardan sandık merkezlerine taşıma ve sonra tekrar depolara dönüşe kadar aygıtların bir sonraki yetkiliye devri her aşamada tutanak ile yapılmalıdır.

• **Açık Kaynak Kod:** Oy verme aygıtlarında kullanılacak yazılımların kaynak kodları seçmenlerin denetimine açık olmalıdır. Bu yolla daha önce bahsedilen "paskalya yumurtası (Paskalya yumurtası bir yazılımın içine gizlenen, kullanıcıların çoğunun hiçbir zaman farkında olmadığı, o yazılımın amacıyla ilgisiz ve sadece özel bir tuş kombinasyonuyla çalıştırılabilen bir yazılım parçasıdır.) benzeri hilelerin önüne geçilebilir.

• **Aygıt Standardı:** Kullanılacak oy verme aygıtının özellikleri bir TSE standardı ile belirlenmeli, bu standarda uygunluk iddiasında bulunan aygıtların testleri için Yüksek Seçim Kurulu'nun denetiminde olan bir teknik birim oluşturulmalıdır.

Diğer bir çalışma da, D. Çetinkaya ile, O. Çetinkaya'nın, "E-seçim Uygulamaları için Gereksinimler ve Tasarım İlkeleri [8] isimli çalışmasıdır. Bu çalışma, 'güvenilir' bir elektronik seçim protokolü için gereken şartlar ile tasarımda dikkat edilmesi gereken konular üzerinde durmaktadır. Tasarlanan bir sistemin, seçmenler tarafından güvenilir olarak nitelendirilmesi için hangi kriterlerin geçirilmesi gerektiği de açıklanan bu çalışmada, YSK'nın desteklemiş olduğu SEÇSİS projesinin özel bir yazılım firması tarafından geliştirildiği ve hakkında herhangi bir akademik döküman bulunmadığı için güvenilemeyeceği vurgulanmıştır.

Bu çalışmada ayrıca, bir sistemin, geçerli ve güvenilebilir elektronik sistem olarak tanınması için ihtiyaç duyulan bir takım gereksinimler listelenmiştir:

Temel Gereksinimler

1. *Seçmenin Gizliliği:* Seçmen ile kullandığı oy arasında bir bağlantı kurulamamasıdır. Sistem tamamen bozulsa ve saldırılara maruz kalsa bile, bütün şifreler ele geçirilse bile, hatta otoriteler anlaşıp seçimi bozmaya çalışsa bile, hiçbir kurum, kuruluş veya kişi tarafından seçmenin kullandığı oy ortaya çıkarılamamalıdır. Ayrıca seçmenin gizliliği seçim sırasında olduğu gibi, seçim sonrasında da korunmaya devam etmelidir.

2. *Seçme Hakkı:* Sadece seçmen olanların oy kullanabilmesidir. Bu özellik seçim gününden önce seçmen kütüğü kayıt otoritesine sadece kendisine kanunlarla seçme hakkı verilen kişilerin kayıt yaptırabilmesini ve seçim günü önceden kayıt olmuş seçmenlere oy kullanabilme yetkisinin verilmesini kapsar. Bu durumda seçmen olmayan kişiler oy kullanamamalıdır.

[8] Cetinkaya O, Cetinkaya D, "E-Seçim Uygulamaları için Gereksinimler ve Tasarım İlkeleri" XI. Türkiye'de İnternet Konferansı, Ankara, Aralık 2006

3. *Seçimin Dürüstlüğü:* Seçim sonuçlarının seçim bitmeden sayılamamasıdır. Seçim sürerken ve oylamalar devam ederken, oyları sayacak olan otorite de dahil olmak üzere hiçbir kurum, kuruluş, veya kişi seçim sonuçları hakkında bilgi edinememelidir. Böylece seçmenin her hangi bir şekilde yönlendirilmesi engellenmiş olur.

4. *Tek Oy:* Bir seçmenin sadece bir oyunun sayılmasıdır. Seçmen değişik nedenlerden dolayı birden fazla oy kullanabiliyorsa, sadece bir oyu geçerli olmalıdır.

5. *Oyun Zorla Kullandırılamaması:* Bütün otoriteler dahil hiçbir kurum, kuruluş veya kişi, seçmeni belli bir yönde oy kullanmaya zorlayamamalıdır. Seçmen oyunu özgür bir biçimde, hiç kimsenin etkisi altında kalmadan ve buna zorlanmadan kullanabilmelidir.

6. *Sistemin Doğruluğu:* Oyların doğru sayılmasıdır. Seçim sisteminin doğruluğunun sağlanabilmesi için;

    - Kullanılan bütün oylar sayılmalıdır,
    - Herhangi bir oy değiştirilememelidir,
    - Herhangi bir oy silinememelidir,
    - Herhangi bir oy kopyalanıp çoğaltılamamalıdır,
    - Herhangi bir oy silme, değiştirme veya kopyalama girişiminden sistem haberdar olmalıdır,
    - Bir seçmenin yalnız bir oyu sayılmalıdır ve
    - Geçersiz oylar sayılmamalıdır.

7. *Sistemin Sağlamlığı:* Kötü niyetli seçmenler, seçmen olmayan kişi ya da kuruluşlar, otoriteler ...vb sistemi ve seçimi bozamamalıdır. Seçim sisteminin sağlam olabilmesi için aşağıdakiler sağlanmalıdır:

    - Sistem saldırılara karşı korunuyor olmalıdır.

- Kriptografik teknikler sadece bugün için değil gelecek için de geçerli olmalıdır. Daha güçlü ve hızlı işlemcilerle şifreler çözülememelidir.
- Teknik altyapı sağlam olmalıdır. Uygulamaya temel teşkil eden e-seçim protokolünde, kesintisiz hatlar, anonim kanallar, ...vb. kullanıldığı varsayılıyorsa bu teknik altyapı sağlanmalıdır.
- Bellek ve iletişim gereksinimleri çok iyi hesaplanmalı ve herhangi bir yetersizliğe meydan verilmemelidir.

8. *Oyun İspat Edilememesi:* Seçmenin oyunu satamaması, nasıl oy kullandığını seçim sırasında ve seçim sonrasında ispat edememesidir. Seçmen bütün otoritelerle anlaşsa bile kullandığı oyun ne olduğunu hiç bir şekilde ispat edememelidir. Böylece oy satma ve oy satın alma gibi problemler engellenmiş olur. Oyun Zorla Kullandırılamaması gereksinimi ile ilişkili olmakla beraber ikisi farklı ihtiyaçlardır.

9. *Oy Kullanmama Hakkı:* Seçmenin oy kullanmak istemediği taktirde oy kullanmamasıdır. Bu durumda seçmen yerine bir başkası veya otoriteler oy kullanamamalıdırlar. Ayrıca seçmenin oy kullanmama hakkı olmakla birlikte, oy kullanmamaya zorlanamamalıdır ve seçme hakkı elinden alınamamalıdır.

10. *Oy Kullanmaktan Vazgeçme Hakkı:* Seçmenin oylama işlemine başladıktan sonra ve oyunu göndermeden önce herhangi bir zamanda oy kullanmaktan vazgeçebilmesidir. Bu durumda seçmen yerine bir başkası veya otoriteler oy kullanamamalıdırlar.

11. *Boş Oy Kullanma Hakkı:* Seçmenin boş oy kullanabilmesidir. Boş oylar da diğer oylar gibi silinememeli, değiştirilememeli ve kopyalanamamalıdır.

12. *Sonuçların İlan Edilmesi:* Seçim sonuçları ve gerekli bilgiler seçim sonunda basın yayın yoluyla ve İnternet aracılığıyla ilan edilir.

13. *Sistemin Geçerlenebilirliği:* Sayım sonucunun doğru olduğunun gösterilebilmesidir.

14. *Sistemin Doğrulanabilirliği*: Seçimin ve sayımın doğru şekilde yapıldığının gösterilebilmesidir.

15. *Bireysel Doğrulama:* Seçmenin oyunun sayıldığından emin olabilmesidir. Klasik kağıt oy pusulalı seçim sistemlerinde bireysel doğrulama yapılamamaktadır, ancak sistemin akışı itibariyle seçmenin sandığa oyunu bizzat atması bir çeşit bireysel doğrulama olarak kabul edilebilir

16. *Sistemin Etkinliği:* Kayıt, seçim ve sayım gibi işlemlerin tamamı etkin bir biçimde yapılmalı, bekleme süreleri en aza indirilmelidir. Klasik seçimlerle kıyaslanınca en azından oylar daha kısa sürede sayılmalıdır.

17. *Kolay Kullanım:* Seçmenin oyunu kullanabilmesi için özel yeteneklere sahip olmak zorunda olmaması ve oy kullanmak için ekstra cihaz veya ekipman kullanmamasıdır. Ayrıca kullanıcı ara yüzlerinin ve seçim ortamının ergonomik olmasına dikkat edilmelidir. Ek olarak, seçmenin oyunu kullandıktan sonra, tekrar bir şey yapmasına gerek duyulmamalıdır.

18. *Açık Yazılım:* Açık yazılım yapılmalı ve kaynak kod incelemeye açık olmalıdır. Sistemin güvenliği kaynak kod gizliliğine bağlanamaz. Sadece şifreler gizli olmalıdır ve iyi saklanmalıdır.

19. *Yedekleme ve Fiziksel Koruma:* Sistemin herhangi bir teknik arızaya karşı yedekleme ve fiziksel koruma mekanizması olmalıdır. Tek bir elektronik cihaza güvenilmemelidir. İlan panoları kullanılarak işlemler kayıt altına alınabilir.

20. *Seçimin Şeffaflığı:* Oyların ve seçmenlerin gizliliğine zarar vermeden, e-seçim sistemlerinde maksimum şeffaflık hedeflenmelidir. İlan panoları, herkes tarafından görülebilen elektronik listeler, ...vb kullanılarak seçimin herkes tarafından izlenebilmesi sağlanmalıdır. Sistemin güvenliği kullanıcılar ve otoriteler arasındaki mesajların gizliliğine bağlanamaz.

21. *Oyların Saklanması:* Oyların ve gerekli seçim bilgilerinin sayım sonrasında, elektronik ve basılı ortamda saklanmasıdır.

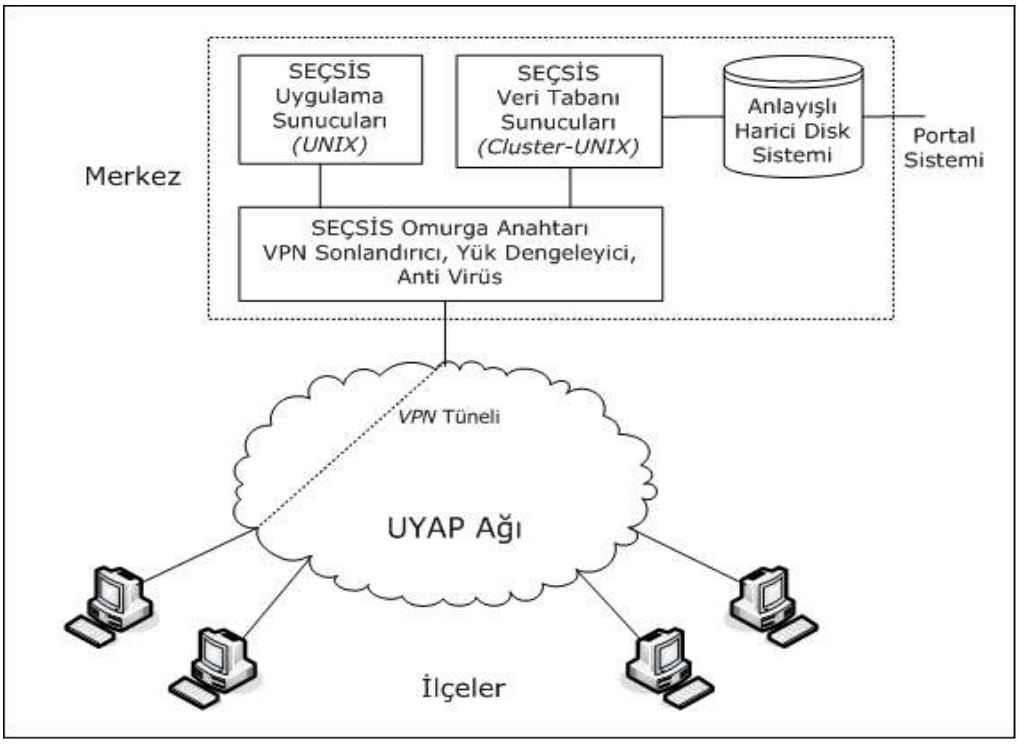
22. *Oyların Tekrar Sayılabilmesi:* Hem elektronik hem basılı ortamda saklanan oyların gerekirse yeniden sayılabilmesidir.

2.2. Türkiye'deki Mevcut Uygulamalar

Tüm Dünya'da elektronik seçim sistemlerine olan önem ve güven giderek artmaktadır. Kullanım alanları gün geçtikçe daha geniş alanı kapsamaktadır. Türkiye'de ise, Yüksek Seçim Kurulu'nun bir projesi olan SEÇSİS[9] ile denemeler yapılmıştır. Projenin tam adı, "Bilgisayar Destekli Merkezi Seçmen Kütüğü Sistemi" olup, yasal dayanağı 298 Sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanun'dur.

Türkiye'nin en büyük e-devlet projelerinden biri olan SEÇSİS Projesinin temel amacı; yasalara uygun olarak, seçmen vatandaşın eksiksiz belirlenmesi, mükerrer yazımın önlenmesi, listelerin hazırlanması, seçmenin kolay, hızlı oy vermesi, seçimin çabuk sonuçlanması, itirazların en aza indirilmesi, vatandaşlarımızın görev ve sorumluluk bilinci ile siyasal haklarını yüksek oranda kullanmasını sağlayacak düzenlemeler için gerekli bilginin; toplanması, bilgisayar ortamında doğru, güncel ve tutarlı bir bütün olarak saklanması, seçimlerde bu bilgilerin ve teknolojik olanakların kullanılarak seçim sonuçlarının ilçelerden güvenli ve hızlı bir şekilde merkeze aktaracak bir sistem olmasıdır.

[9] Yüksek Seçim Kurulu (YSK), http://www.ysk.gov.tr/ysk/index.html (Çevrimiçi 05.01.2008).



Şekil 4 – Seçsis Uygulama Sisteminin Altyapısı

SEÇSİS Projesi ile birlikte sağlanan yararlar aşağıdaki gibi özetlenmelidir:

1. Seçmenler T.C Kimlik Numarası ile kayıt altında tutularak mükerrer oy kullanımı önlenmiştir.

2. Yasa değiştiği takdirde oy kullanımındaki parmak boyama işlemi ortadan kalkacaktır.

3. Vatandaşlar nerede ve hangi sandıkta oy kullanabileceklerini Internet üzerinden takip edebilmektedir.

4. Sandık Seçmen Listeleri, Muhtarlık Bölgesi Askı Listeleri, Seçmen Bilgi Kağıtları çok hızlı bir şekilde ilçe seçim kurullarınca alınabilmektedir.

5. Birleşik oy pusulası dışında hiçbir form matbaada bastırılmamaktadır.

6. Seçmenler oy verecekleri sandıklara, belirlenen kriterlere göre çok hızlı bir şekilde dağıtılabilmektedir.

7. Seçim sonuçları 733 ilçe seçim kurulundaki istemci bilgisayarlardan girilerek bilgiler anında merkezde toplandığı için seçim sonuçları çok hızlı bir şekilde alınabilmiş, hazırlanan görsel bir ekranda il seçim kurullarında, adetsel ve oransal olarak TV ve basın kuruluşları ile kamuoyuna duyurulmuştur.

8. Her türlü işlemin geriye yönelik kaydı tutulmuştur.

9. Matbaa ve nakliye masrafları azaltılmıştır.

10. Siyasi partilere seçmen listeleri, ilçelere göre sandık sayıları hızlı bir şekilde manyetik ortamda (merkezden) verilmiştir.

11. T.C Kimlik Numarasına bağlı olarak seçmenin ve adayların kimlik bilgileri MERNİS-KPS sisteminden çevrim-içi temin edildiği için, seçmenin kimlik bilgilerinin veri girişi yapılmayarak, bu yolla oluşabilecek olası hatalar önlenmiştir.

12. T.C Kimlik Numarasından veya seçmenin adı, soyadı, baba adı ile doğum yılı gibi bilgiler yazılarak yedi değişik seçenekle, seçmen sorgulama yapılabilmektedir.

13. Seçimlerde oy kullanmayan seçmenler, sandık başı görevlileri gibi yardımcı listeler hızlı bir şekilde alınabilmektedir.

14. Ayrıca seçimde çalışanlar için SEÇSİS Projesi kapsamında ücret ve yevmiye adedi oto-kontrollü harcama listeleri alınabilmektedir.

15. İlçe Seçim Kurullarındaki taşra personeli, kurulan iç e-posta ile çok hızlı bir şekilde, hem Merkezle hem de kendi aralarında bilgi alışverişinde bulunabilmekte, genelgeler, uygulama yazılımının kullanımı ile ilgili açıklayıcı belgeler, ek masrafsız gönderilmektedir.

Sonuç olarak, SEÇSİS Projesinde şeffaf ve etkin bir kamu yönetimi oluşturmaya özen gösterilmiş, seçim iş süreçleri kısaltılarak verimlilik sağlanmış, vatandaşlarımızı kamu ve özel kuruluşları, siyasi partilerimizi doğru ve hızlı bilgilendiren bir e-devlet projesi başarı ile tamamlanmıştır.[10]

2.3. Değerlendirme

Literatürdeki başlıca çalışmalar ile elektronik seçim protokollerinin analizi neticesinde tez kapsamında bir uygulama geliştirilmiştir. Bu çalışma, Java teknolojileri ile yazılmış olan, bir elektronik seçim projesidir. Temelinde, Mercuri yöntemi esas alınan Proje sadece tanımlanan istemciler tarafından erişilen bir sunucu üzerine konulan bir web uygulama sunucusu üzerinde güvenli bir şekilde çalışmaktadır. Klavye ve fare gibi girdi birimleri tamamıyle kaldırılmış ve dokunmatik ekran üzerinden T.C. Kimlik numarası ve seçmene verilecek bir PIN kodu ile sisteme, dokunmatik ekran aracılığı ile giriş imkanı veren bir sistem geliştirilmiştir.

Sistemde bugüne kadar yaşanılan e-seçim sorunları göz önünde bulundurulmuştur. Seçmenin gizliliğinin son derece önemli bir bilgi olarak tutulduğu bu sistemde, elektronik olarak oluşturulan pusulululalar, görünüş bakımından geleneksel pusulalaları aratmayacak şekilde tasarlanmış olup, Mercuri yöntemine ilave bir yanı ise, basılan kağıt oy pusulalarına sistem tarafından üretilen bir güvenlik kodunun basılmasıdır. Bu kod, fiziksel oyların güvenliğini artırmak amacıyla eklenmiştir.

[10] Yüksek Seçim Kurulu, "Bilgisayar Destekli Merkezi Seçmen Kütüğü Sistemi" (SEÇSİS) Projesi, www.ysk.gov.tr (Çevrimiçi 07.03.2008)

3. ELEKTROY ELEKTRONİK OYLAMA SİSTEMİ

Elektronik seçim modellerinin her birinin, kendine özgü bir takım eksi ve artı yanlarının söz konusu olması, bir kısmının Türkiye seçim sistemine uygun olmayışı ve ergonomik bir şekilde tasarlanmamış olması, o sistemlerin ülkemiz seçimlerinde rahatlıkla kullanılmasını olanaksız hale getirmektedir. Bu nedenle yapılan araştırmanın neticesinde, temelinde Mercuri modeli bulunan bir sistem geliştirilmiş olup, ülkemiz seçim kurallarına göre bir takım iyileştirilmelere tabi tutulmuştur.

Bu çalışmada yapılan uygulamanın (kısaca Elektroy olarak anılacaktır)seçmen bölümünün tasarım aşamasında daha önce oy kullanan kişilerin mevcut sistem üzerinde yorumları ve eleştirileri göz önünde bulundurulmuş, beklentileri sorulmuş ve tüm cevaplar derlenerek, bir elektronik sistemde nelerin olması gerektiği belirlenmiştir.

Sistemin yönetici kısmı ise, seçim görevlilerine ekstra bir bilgisayar kullanma yeteneği gerektirmeyen, gayet açık ve basit bir şekilde olması gerektiği üzerinde durulmuş, örnek çalışmanın bu kısmının şeklini bu kriterler belirlemiştir.

Sistem için gerekli olan yazılım ve donanım maliyetlerinin de önemi üzerinde durulduğu bu uygulamada, platform bağımsız, güvenli ve klasik bilgisayar donanımları ile çalışabilecek şekilde tasarlanmış bu şekilde elektronik ve programsal maliyet asgari düzeyde tutulmuştur. Örneğin, platform bağımsız çalışan Java ile yazılmış, başta Solaris olmak üzere, Ubuntu Linux, Pardus ve Fedora Core 8 gibi linux türevleri üzerinde bir çok denemeler gerçekleştirilmiştir. ElektrOy sisteminde önemi büyük olan veritabanları da, yaygın ve kolaylıkla bir çok güçlü veritabanı sistemine geçirilebilen Structured Query Language (SQL) dili kullanılarak tasarlanmış, Microsoft SQL Server, Postgre SQL ve MySQL gibi bilenen güçlü sunucularda çalıştırılmıştır.

Microsoft SQL Sunucusu'nun "Express Edition" adı dışındaki ürünleri ücretsiz olmadığından tercih için söz konusu olmamıştır. Bunun yerine ücretsiz ve güvenli bu ürünler tercih edilerek ekstra program maliyetinden kaçınılmıştır.

Kolay adaptasyon, kolay uygulanabilirlik ve değiştirilebilir yapıya sahip olan ElektrOy, tamamıyle transparan yapısı sayesinde, sistemin içinde neler döndürüldüğünün kolaylıkla anlaşıldığı, portatif bir web uygulamasından ibaret olduğu için, istemci ve sunucu tarafında geleneksel programlar vasıtasıyla bağlanmaya izin vermektedir. Böylece, sistem içersinde programlama açısından bir yanlış işleyiş, yada yazılım hileleri kolaylıkla tespit edilebilecektir. Diğer ülkelerde yapılan elektronik seçim sistemlerinin büyük sorunlarından biri de güvenilemez olmalarıdır. Güvenilemezlik: insanların programın içersinde neler olduğunu bilememesi anlamına gelmektedir. Bu tür uygulamaların genelde gerek sunucu, gerekse istemci tarafı ayrı ayrı kodlanarak, özel bir arayüz ile yazılmaları gerektiğinden, seçim sistemleri uzmanı ve eleştirmenler, program içinde olup bitenleri kolaylıkla anlayamamaktadırlar. Saydamlık adı verilen bu tür uygulama biçimi, bu sistemler için 'tarafsızlığın' önemli bir göstergesi niteliğindedir.

3.1.ElektrOy Sisteminin Yazılımsal Bileşenleri

Sistemin bileşenlerini, geliştirme, sunucu ve istemci birimi olmak üzere üç ana birim altında toplamak mümkündür. Geliştirme biriminde, sistemin tasarlandığı program araçları, sunucu biriminde sistemin çalıştırıldığı sunucu sistemi, istemci biriminde ise, sisteme bağlanacak istemci bilgisayarların içerikleri hakkında detaylar verilmiştir.

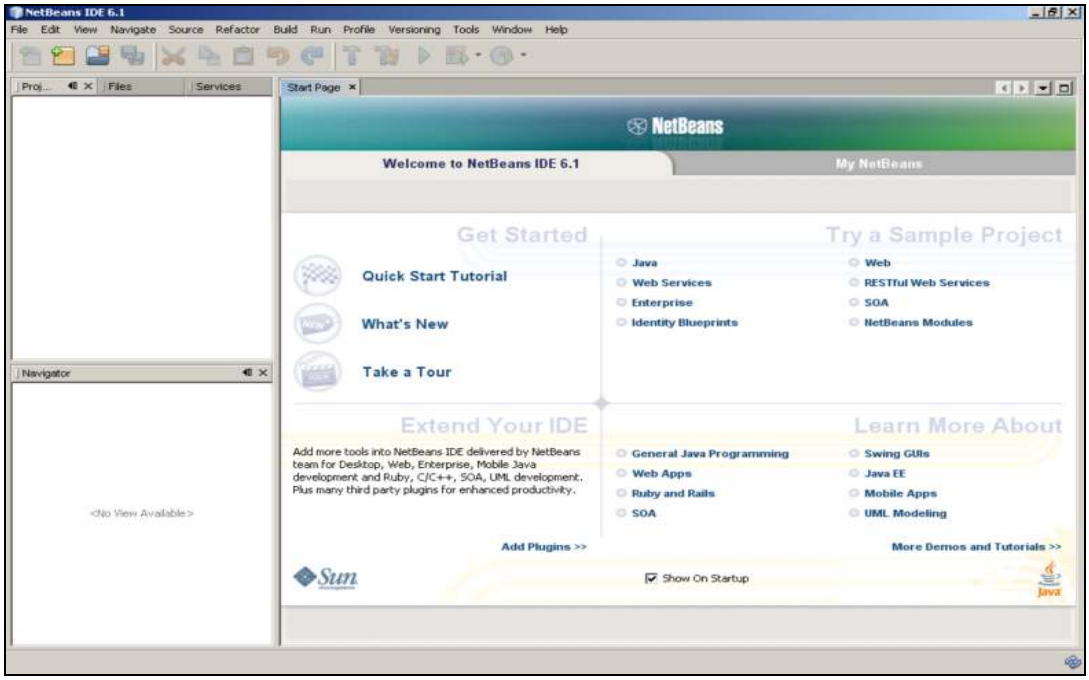
3.1.1.Geliştirme Birimi

Geliştirme, sistemin oluşum aşamasında kullanılan yazılım ve araçların içerilmiş olduğu birimdir. Sistem, bir çok program gibi, bir programlama dilinde yazılmış ve bu dili kullanan bir geliştirme aracı olan NetBeans (Integrated Development Environment – IDE) kullanılarak tasarlanmıştır.

Sistemin dili Java'dır ve görsel web uygulama platformu olan Java Server Faces (JSF) kullanılmıştır. Java, Sun Microsystems tarafından geliştirilmeye başlanmış açık kodu, nesneye yönelik, platform bağımsız, yüksek performanslı, çok işlevli, yüksek seviye, adım adım işletilen bir dildir. [11] Programa dili olarak Java'nın tercih edilmesinde en büyük etken, Java'nın platform bağımsız olarak çalışmasıdır. 13 Kasım 2006'dan itibaren General Public License (GPL) lisansıyla açık kod olan Java'nın ilk sürümü 1995'te çıkmıştı.

ElektrOy tasarlanınken, yapılanların büyük bir kısmı NetBeans 6.1 üzerinde geçmiştir.

NetBeans , yazılım geliştiriciler için, ücretsiz, açık-kaynak kodlu, sürekli yenilenen bir IDE'dir. Java, C/C++, ve Ruby dili kullanılarak Profesyonel masaüstü, kurumsal, web ve mobil uygulamalar oluşturmak için tüm araçları içerinde barındırır. Windows, Linux, MacOS ve Solaris üzerinde, kolay kurulan, sağlam çalışan ve kullanımı kolay bir IDE'dir (Şekil 5). [12]



Şekil 5 – NetBeans IDE 6.1

[11] Wikipedia, http://tr.wikipedia.org/wiki/Java_(programlama_dili)
[12] Netbeans, http://www.netbeans.org

Görsel web uygulamalarının çalıştırılabilmesi için Visual Web Java Server Faces (JSF) platformu kullanılmıştır. Java Server Faces, butonlar, yazı kutuları, tercih kutuları vb. daha bir çok görsel web nesnelerinin, sürükle bırak yöntemi ile grafiksel olarak kullanılarak sayfalara eklenmesini kolaylaştıran bir platformdur.

Yapılan tüm görsel ayarlamalar ile nesnelerin tümü .Jsf dosyasında tutulmakta ve standard Java diliyle yazılan her türlü kodlar da ikinci bir dosya olan .java dosyalarında tutulur. Böylece bir dosya, örneğin giris dosyası, aslında, biri nesneler ile görsel ayarların olduğu 'giris.jsp', diğeri kodların bulunduğu 'giris.java'. Netbeans üzerinde çalışırken her ikisini de doğrudan düzenlemek mümkün olmaktadır.

VWJSF platformunu NetBeans içerisinde kullanabilmek için Java Standard Edition platformu (Java SE) ile birlikte Java Enterprise Edition (JavaEE) gerekmektedir.

Program yazılırken, SQL bağlantısına erişebilmek için gerekli bir Application Program Interface (API) olan Java Database Connectivity (JDBC) ile programın çalışacağı web sunucusunun da ayrıca NetBeans içerisine tanıtılması gerekmektedir.

3.1.2.Sunucu Birimi

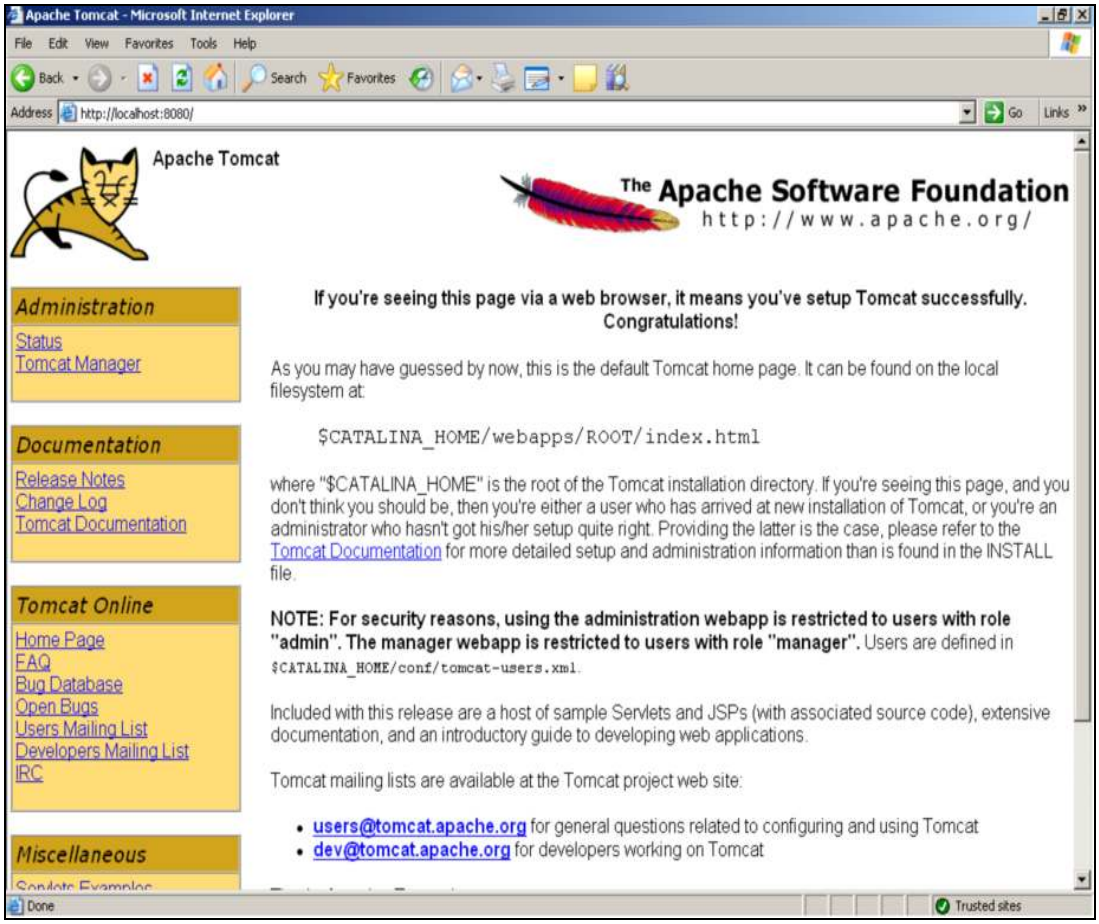
Web uygulamaları, temelinde sunucu ve istemci bileşenlerinden oluşan, istemcinin, sunucu tarafından dinlenen bir porta genellikle 80, uygun bir istemci tarafından bağlanılarak veri alış verişi sağlanan uygulamalardır. ElektrOy sisteminin çalışabilmesi için JSF uyumlu bir web sunucusuna ihtiyaç duyulmaktadır.

3.1.2.1 Web Sunucusu – Apache Tomcat, GlassFish

Çalışma kapsamında Apache firması tarafından geliştirilmiş özgür lisansa sahip Tomcat ile Sun Application Server (ayrıca GlassFish olarak da bilinir) kullanılmıştır.

Tomcat, temelinde Java Servlet bulunan, JSF ve Java Server Pages (JSP) uygulamalarını çalıştırırken, Java kodlarının da çalışması için sadec bir Java Hypertext Transfer Protocol (HTTP – www siteleri için internet üzerinde kullanılan protokol olarak da bilinir) web sunucu ortamı sağlamaktır (Şekil 6). [13]

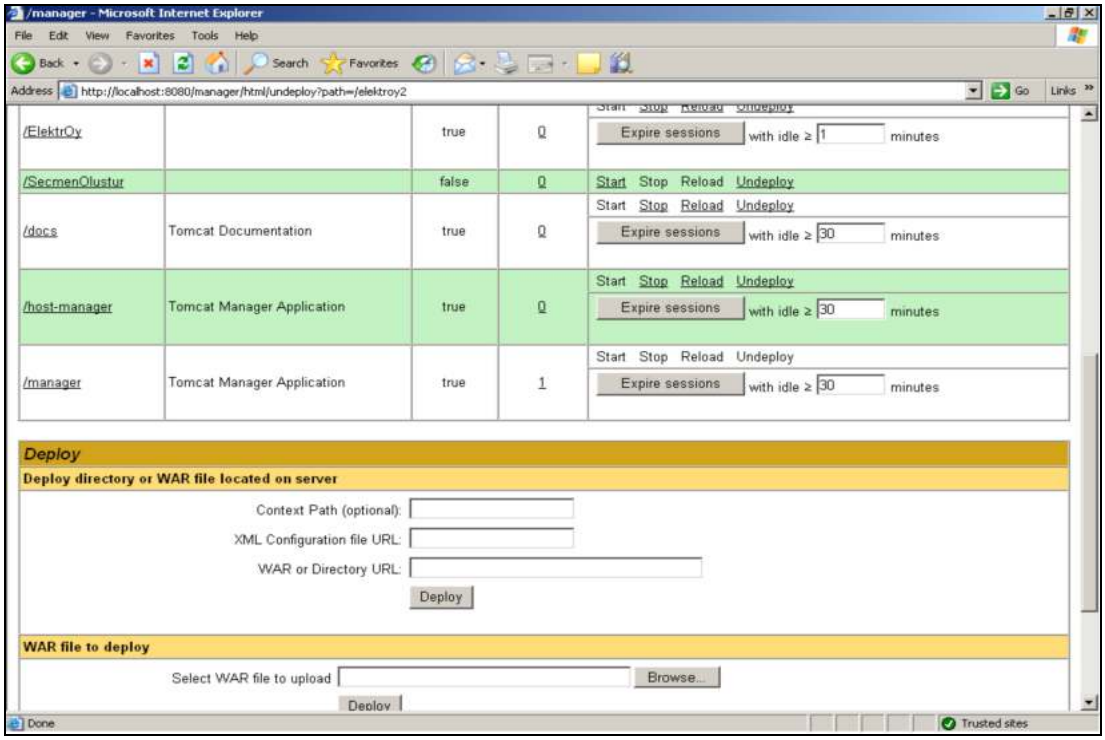
Glassfish, Sun Microsystems tarafından, Java EE platformu için geliştirilmiş bir uygulama sunucusudur. Bilinen en son versiyonu Sun Java System Application Server 9.x'tir. İçerisinde Apache Tomcat'tan türetilmiş bir bileşeni servletleri çalıştırmak maksadıyla kullanılmaktadır. GlassFish açık kaynak kodlu bir üründür ve ücretsiz olarak edinilebilir. [14]



Şekil 6 – Tomcat Ana Ekranı

[13] Brittain J., Darwin I. F., "Tomcat: The Definitive Guide", 2003
[14] Java Web Sitesi, https://glassfish.dev.java.net/

Tomcat üzerine uygulama eklemek iki yoldan yapılır. Birincisi ve kolay olanı Netbeans üzerinden kodları ve tasarımı bitirdikten sonra uygulamayı çalıştırmak, ikincisi Tomcat Manager kullanarak. Eğer sistemde halen tasarlanılan bir uygulama yoksa, başka bir ifadeyle bitirilmiş bir uygulama ise, Tomcat Manager kullanmak daha doğru bir tercihtir. Şekil 7 'de Tomcat Manager verilmiştir.



Şekil 7 – Tomcat Yönetim Ekranı

3.1.2.2 Veritabanı Sunucusu – SQL

SQL , İngilizce "Structured Query Language" kelimelerinin baş harflerinden oluşan, Türkçesi Yapısal Sorgulama Dili anlamına gelen bir veritabanı dilidir. SQL, herhangi bir veri tabanı ortamında kullanılan bir alt dildir ve yalnızca veri tabanı üzerinde işlem yapılabilir. SQL'e özgü cümleler aracılığı ile veri tabanına kayıt eklenebilir, değiştirilebilir yada silinebilir ve ayrıca bu kayıtlardan gerekli sorgular yardımıyla listeler oluşturmak mümkündür. [15]

[15] http://tr.wikipedia.org/wiki/SQL

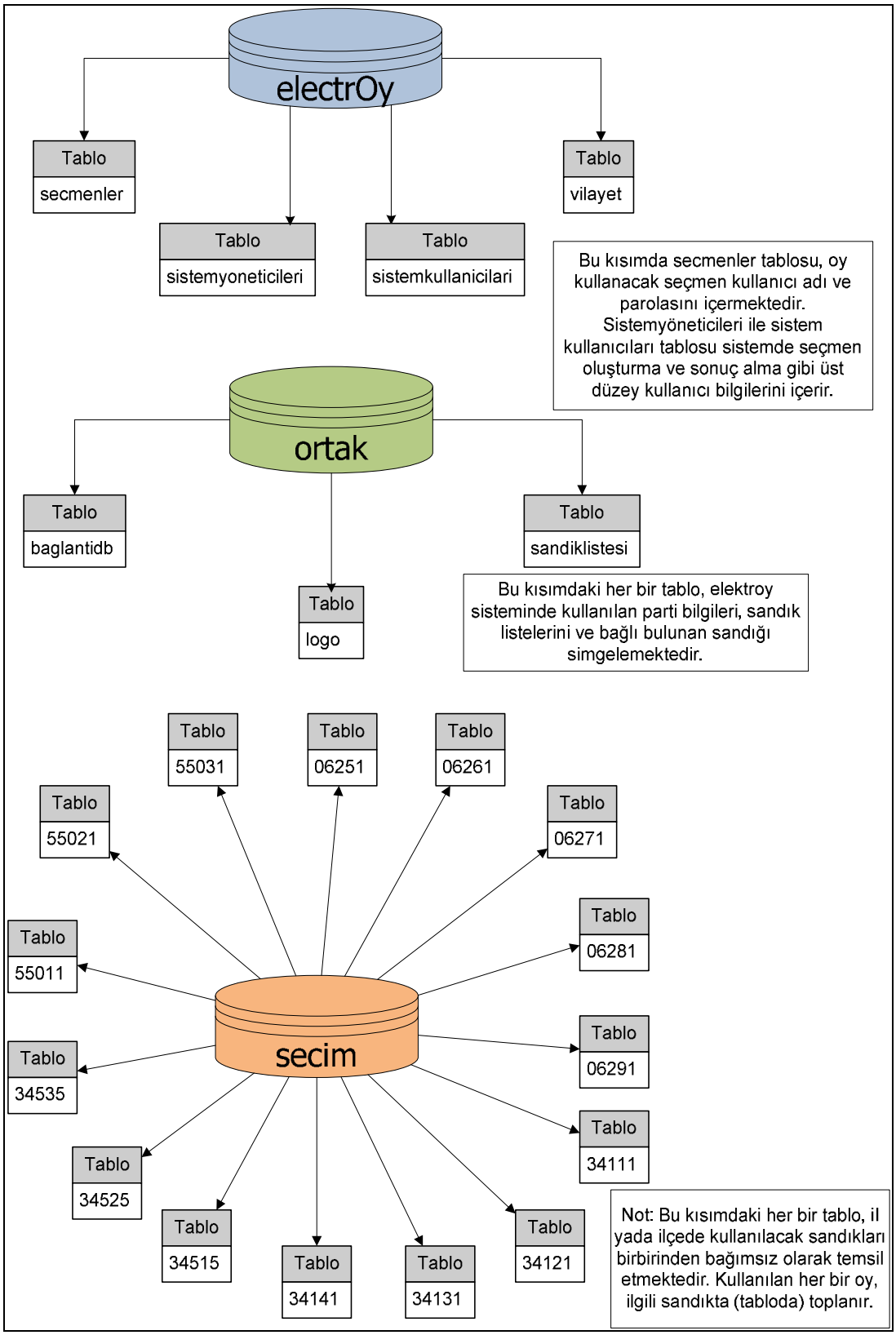
SQL teknolojisi üzerinde Microsoft firması tarafından üretilen sunucu yazılımı Microsoft SQL Server (MSSQL)'dir ve veritabanlarının oluşturulması ve yönetilmesini sağlar. Microsoft tarafından belirli bir lisans ücreti karşılığında edinilebilen bu sistemin ücretsiz bir versiyonu ElektrOy'un prototipinde kullanılmıştır.

4GB'lık veritabanı limiti ile 1Gb bellek kullanımı vb. bir kaç kısıtlama ile satılan bu versiyon" MS SQL Express Edition" ve "MSSQL Express Edition with Advanced Services" adıyla dağıtılmaktadır. Sistemde kullanılan modeli, MSSQL Express Advanced Services'dir. Geliştirilmiş yönetim arayüzü bulunan bu sistem, standart express versiyona göre, kolay yönetibilen grafiksel arayüze sahip bir yönetim konsolu (SQL Server Management Studio Express), tam metin sorgulama ile SQL Server Raporlama Servisi gibi bir çok araç ile birlikte geldiği için tercih edilmiştir. Normal sistemlere göre 64 bitlik sunucuları desteklemeyen bu ücretsiz versiyonlar, geniş verilerin tutulacağı büyük uygulamalar için uygun olmadıklarından, denemeler Postgre SQL ile MySQL üzerinde de gerçekleştirilmiş ve sorunsuz bir şekilde çalıştığı sonucuna varılmıştır.

PostgreSQL ile MySQL'de açık kaynak kodlu birer yazılım olmakta ve limit sorunu olmaksızın geniş alana yayılmış her türlü sistemde kolaylıkla kullanılabilen, sürekli yenilenen ve bir çok işletim sisteminde çalışabilen gelişmiş veritabanı sistemleridir.

Veritabanı konusunda, elektrOy için, anında yedekleme (replication) sistemi düşünülmüştür. Bu sistem, her bir yerel il seçim müdürlüğünde bulundurulan veritabanlarının anlık bir kopyaları da merkezde tutulmakta ve her iki veritabanı da merkezden kontrol edilmektedir. Bu sistemle, bağlantıda yaşanılan herhangi bir sorun durumunda, kesintiye sebep vermeksizin her türlü bilgilerinin işlenerek, daha sonra merkezde bulunan sunucuya aktarılması böylece veri kaybı ve sistemin durma probleminin en aza indirgenmesi amaçlanmıştır.

ElektrOy sisteminde üç ayrı veritabanı tutulmaktadır. Tüm bu veritabanları ve içerdiği tablolar, Şekil 8'de verilmiştir.



Şekil 8 – ElektrOy Sistemi Veritabanı Diagramı

i) ‘elektrOy’ Veritabanı

Bu veri tabanı, yalnızca merkezde bulunan, sisteme dahil tüm geçerli seçmenlerin TC kimlik numaraları ile parolalarının şifrelenmiş halde depolandığı seçmenler tablosunu içermektedir. Bu tabloda, oy kullanan seçmenleri belirleyebilmek için bir durum alanı vardır ve oy kullandıklarında bu alana işaret konulur.

Seçmenlerin dışında, sistem yöneticileri (genelde sistem sonuçlarını açıklamakla görevli kişi yada kişiler) ile, sistem kullanıcıları (seçim kurumunda bulunan, bir takım seçmen şifre oluşturma vb. işlemleri yapmakla yükümlü sistem memurları) ve bunların sisteme giriş esnasında girdikleri parolalar barındıran tablolar bulunur.

Tüm bu tabloların yanı sıra, sandıkları vilayetlere atamada kullanılan ve ülkenin tüm vilayetlerinin listesinin bulunduğu Vilayet isimli tablo da sistem tarafından kullanılmaktadır.

ii) ‘ortak’ Veritabanı

İl merkezlerine yerleştirilecek her bir sunucu sisteminde olması zorunlu sistem tarafından kullanılan bir veritabanıdır. Elektronik pusulaların oluşturulmasında kullanılan, aday parti bilgileri ile sandık listeleri gibi bir takım bilgiler bu veritabanından edinilir.

Elektroy sistemine, hangi sandığa bağlı bulunduğu bilgisini veren ‘baglantidb’ veritabanı ile, pusula oluşturulurken gerekli olan partilerin isimleri ile logolarının yollarının yer aldığı ‘logo’ veritabanı en çok kullanılan veritabanı olmaktadır.

Web uygulaması tarafından birden daha fazla sandığa bağlanılması gerektiği özel durumlarda diğer sandıkların da listelerinin bulunduğu sandiklistesi, prototipde kullanılmamış, fakat sistemde düşünülmüştür.

iii) ‘secim’ Veritabanı

Seçim veritabanı, seçimin sonunda sayılan oyların tutulduğu, diğer bir anlatımla, sandıkların birer tablo olarak tasarlandığı, kullanılan her bir oyun sandığın bağlı bulunduğu tabloya rastgele yazılacak şekilde tasarlanan bir veritabanıdır. Hem il merkezlerinde, hem de genel merkezde birer kopyası sürekli senkronize halinde çalıştırılmak zorunda olan bu veritabanı, diğer veri tabanları gibi iyice korunmalıdır.

Veritabanı içersinde, her bir sandığın ait olduğu ilin trafik kodu başında olmak üzere, üç haneli bir numaradan oluşmaktadır. Örneğin Samsun ilimizin Asarcık ilçesine bağlı bir sandık 55948 gibi bir numarayla ifade edilir. Bu seri numara, basılacak olan her bir oyun üzerinde bulunan bir numaradır ve oy sayımlarında da, sayılan oyun hangi sandığa ait olduğunu belirleyen bir bilgidir.

3.1.3.İstemci Birimi

Sistemin, seçmenler tarafından kullanılan cihazlar tarafından bağlantı kurulması için, güvenli ve kullanışlı bir istemci tarafının da tasarlanması gerekmektedir.

Genelde elektronik seçim sisteminde, sistem üretciler tarafından ayrıca yazılan istemci programları, karşılaştıkları bir çok eleştiri yüzünden tercih edilmesi riskli bir yaklaşım olarak düşünülmüştür. Böylece standart bir istemci olan internet tarayıcıları (Internet Browser) kullanılmıştır.

Elektroy sisteminde bir çok gelişmeleri içerisinde barındıran, son derece güvenilir, hızlı ve ayrım gözetmeksizin bir çok platforma kolaylıkla yüklenilen Mozilla tarafından geliştirilmiş Firefox isimli tarayıcı kullanılmıştır.

Açık kaynak kodlu olduğundan geliştirilmeye açık olan bu tarayıcıyı, seçmen bilgisayarlarını sade tutmak için kiosk modu adı verilen bir modda çalıştırmak gerekmektedir. Böylece seçmen tarafına herhangi bir adres çubuğu, menü düğmeleri vs. gözükmeyecek, seçmenin yalnızca oy pusulasına adapte olması sağlanmış olacaktır.

Firefox'u kiosk moduna çalıştırmak için, yine Mozilla sitesinden ücretsiz edinebilen Real Kiosk eklentisine ihtiyaç duyulmaktadır. K. Heiaaro tarafından yazılan bu eklenti, tarayıcıyı tam ekran olarak başlatır, bütün menü, toolbar, klavye komutları ile sağ tuş menülerini devre dışı bırakarak tam bir kiosk ortamı oluşturmayı hedefler.

Windowsla gelen Internet Explorer ve diğer bir çok tarayıcıların da bir kiosk çalışma modları bulunmaktadır. Fakat ElektrOy sistemi, seçmenin kullandığı oyu, çıkarken görüp onaylaması için kağıda da basacağı için, kullanıcı onayı gerektirmeyen bir yazdır komutu çalıştırmaktadır. JavaScript kullanılarak gönderilen bu komut, çalıştırılmadan önce mutlaka kullanıcıdan onay almak zorunda olduğundan, kiosk uygulamalarının bir çoğunda, en azından ElektrOy uygulamasında böyle bir soru seçmene sorulamayacağından iptal edilmesi gerekmekdir. Firefox dışında hiç bir uygulamada bu kadar detaylı ayar gerçekleşemediğinden tercih sebebi olmuştur. Firefox içine eklenen iki satırlık bir konfigurasyon parametresi ile, istemci bilgisayarına bağlı varsayılan yazıcı, artık doğrudan yazdırılabilen yazıcı konumundadır. Diğer firmaların kendi istemcilerini yazmalarının bir diğer nedeni de, ihtiyaçlarına göre tasarlama şanslarına sahip olduklarından, istedikleri gibi yönetebilmeleridir.

3.2. ElektrOy Seçim Sisteminde Kullanılan Donanımlar

Her bir yazılım, belli bir donanım üzerinde çalışmaktadır. Sistemlerin fiziksel bir parçası olan donanım, bilgisayar sistemlerinin elle tutulan parçalarına genelde verilen isimdir.

Sunucu ve istemci kısmı için ayrı ayrı gerekli olan donanım parçaları, ihtiyaca yönelik olarak standart, yükseltmeye hazır bir şekilde tasarlanarak seçilmelidir. İstemci bilgisayarlarını, seçim dışında günlük kamu işlerinde kullanılabilen bilgisayarlar üzerinde ufak bir kaç ayar ile elde etmek ve hiç bir veri kaybı olmaksızın eski halinde geri döndürmek kolay bir şekilde yapılabilir. Böylece istemci tarafı için yeni bilgisayar yatırım maliyeti mümkün olduğunca düşecektir.

Sunucu bilgisayarları, 7/24 kesintisiz ve sıfır hata ile çalışmaları zorunlu sistemlerdir. Bu nedenle güçlü bir soğutma sistemine ve geniş kasalara sahiptirler. Bu sistemlerde ayrıca, paralel işlem yapmaya yönelik geliştirilen Xeon tipi özel işlemciler (CPU) kullanılırken, bellek olarak da yüksek kapasiteli Error Correction Code (ECC) hata toleranslı bellekleri ile, RAID 5, RAID 10 vb. Redundant Array of Inexpensive Disks adı verilen ve birden fazla diskin, sanki bir diskmiş gibi çalışmasını ve verilerin o diskler arasında paylaştırılarak ve kopyalanarak yazılmasını sağlayan böylece performanslı ve hata toleranslı olan disk sistemi tercih edilmelidir. Sunucunun gücü, seçim sisteminin gereksinim oranına göre değiştirileceğinden, verimlilik açısından önem arz etmektedir. Bu sebeple, sunucu seçiminden önce, uygulanacak hedef kitlenin boyutları ön araştırma olarak analiz edilmelidir.

İstemci bilgisayarları ise, sunucu bilgisayarlarının aksine, sıradan düşük kapasiteli bilgisayarlar bile olabilmektedir. Fakat dikkat edilmesi gereken önemli bir unsur, bu sistemlere bir dokunmatik ekran takılmasıdır. Seçmenler oylarını klavye, fare gibi standart bir giriş birimi yerine, parmaklarını kullanarak sözkonusu partinin üstüne basarak kullandıklarından, ekranların dokunmatik ekran olarak tercih edilmeleri gerekmektedir. Normal bir ekranında, önüne özel bir cam yerleştirilerek dokunmatik hale dönüştürülebildiği için, maliyet sınırlarını çok fazla zorlamayacak olan bu yaklaşım, istemci bilgisayarlarında klavye ve fareleri kaldırılmasına izin vererek güvenli bir hale getirmektedir.

İstemci bilgisayarları yada, sunucu bilgisayarlarına yada ağa doğrudan bağlı olarak kurulan bir yazıcı ile elektronik oyların fiziksel bir kopyaları yazdırılacak ve mühürlü sandığa atılacaktır. Bu aşamada seçmen kullandığı oyu, sandığa atılmadan önce de kapalı bir alandan görebilecektir. Yazıcının yanısıra, bütün bunları yapan elektro-mekanik bir sistem de, yine elektroy sistemi içersinde söz konusu olabilecek bir donanımdır.

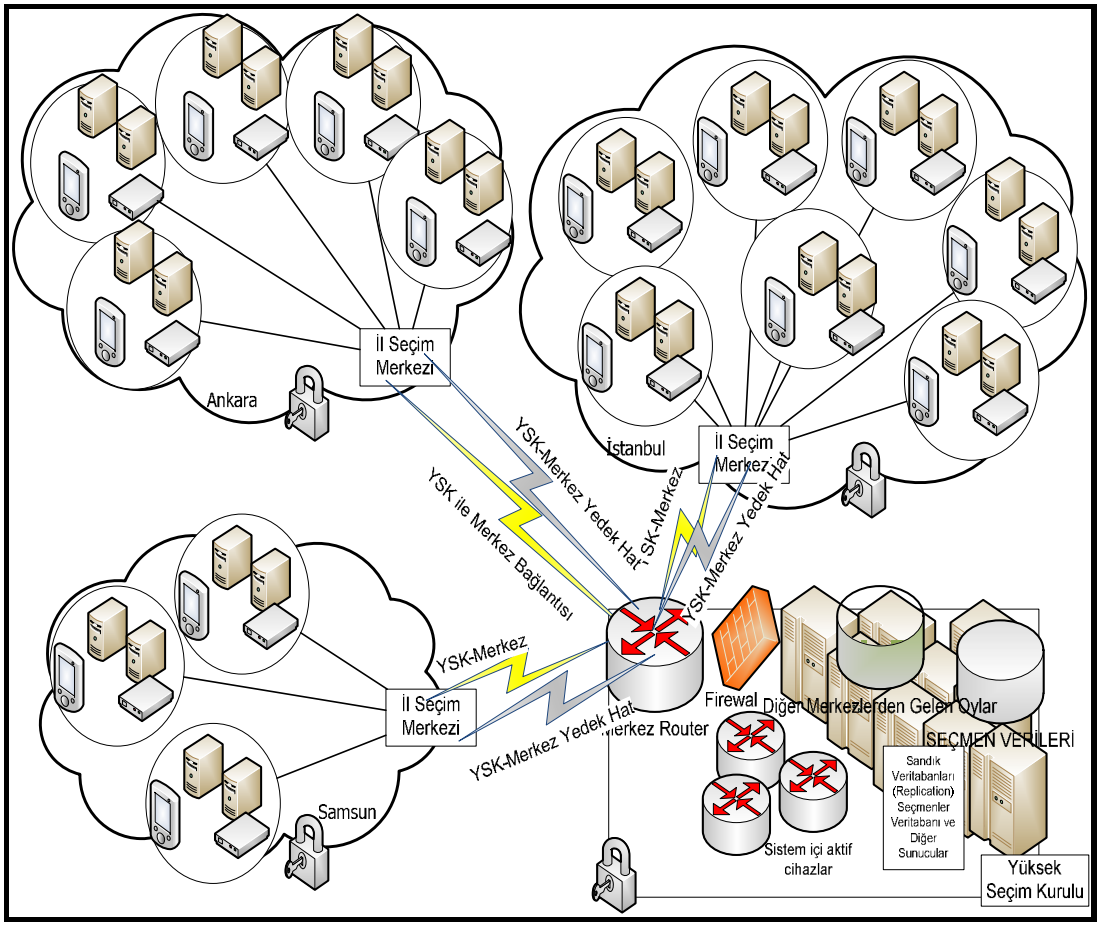
Sunucu ve istemci dışında, sistemde önemli bir yeri olan, fakat her alanda kullanıldığı için bu çalışmaya özel olmayan diğer bir donanım da ağ yapısı ve güvenlik mekanizmalarıdır.

Ağ yapıları, istemci makinelerini sunuculara yada yazıcılara bağlayacak yerel ağ (Local Area Network – LAN) olabileceği gibi uzaktaki sunucuya bağlantı imkanı veren bir geniş alan networkü (Wide Area Network – WAN) olabilmektedir.

LAN bağlantı tipleri, genelde aynı bina içerisinde bulunan sistemleri birbirine bağlarken kullanıldığı ve 100 metreyi geçmeyen uzaklıklar söz konusu olduğu için, basit bir kablo ve switch adı verilen bir ekipman aracılığı ile gerçekleştirilebilirken, bir WAN yapısı ulaştırmak nispeten daha fazla ekipman ve aylık bir maliyet gerektirmektedir. Kullanılabilecek Wan metodları, yüksek hızlı telefon hatları imkanı üzerine kurulu Integrated Services Digital Network (ISDN), hızlı paket anahtarlamalı bir teknoloji kullanarak düşük maliyetli bir bağlantı imkanı veren Frame Relay, mevcut evdeki telefon hatları üzerinden çalıştırılabilen Asymmetric Digital Subscriber Line (ADSL), noktadan noktaya doğrudan bir kablo gibi çalışan kiralık hatlar vb. bir çok teknik, telekom altyapısı altında sunulmuştur. Bunların yanısıra standart bir internet bağlantısı üzerinden güvenli bir şekilde bağlantıya izin verilen Virtual Private Network (VPN) teknolojisi kullanılarak, güvensiz internet üzerine kurulan bir tünel içerinden şifreli veri aktararak güvenlik etkin çözümler sunmak mümkündür. Sistem ayrıca tüm yerel ağ ve uzak ağ bağlantıların IP Secure (IPSEC) ile her bir veriyi şifreleyerek network üzerinde gönderme/alma işlemi gerçekleştirmektedir. Böylelikle, gerek sunucu, gerekse istemciye, dışarıdan hiç bir makine bağlanamayacaktır.

Her bir merkeze konulan, yönlendirici (router), ateş duvarı (firewall) cihazları da elektrOy sistemini güvenli kılan yardımcı ağ donanım bileşenleridir ve olmazsa olmaz aygıtlardır.

ElektrOy sisteminin bütün bir yapı mimarisi Şekil 9'da detaylı bir şekilde verilmiştir.



Şekil 9 – ElektrOy'un Ülke Bazında Yayılmış Donanım Şeması

Verilen şekilde, sağ alttaki dikdörtgen alan, Yüksek Seçim Kurulu (YSK)'nu temsil etmektedir. Bu alandaki tüm sunucular her türlü güvenlik ve diğer kontrollerden geçirilmiş, yük dengelemesi yapılmış (load balancing) yüksek derecede erişilebilir sunuculardan ibarettir.

Her bir il, bulut olarak temsil edilen uzak lokasyonları göstermektedir ve YSK'ya biri asıl diğeri yedek olmak üzere iki şekilde bağlanmıştır. Bulutların içerisinde bulunan ufak daireler ise, her bir ilçeyi ifade etmektedir. Her bir ilçedeki sandıklar bağlı bulunduğu ile bağlıdır. Önemli yönetim görevleri YSK tarafından üstlenildiği için, bakım maliyetleri olmayan bu sunucularda, herhangi bir sorun olması durumunda, geçici olarak merkezdeki sunucular kullanılabileceği şekilde replikasyon yöntemi ile veriler işlenmektedir.

Bütün bu sistemler, elektrOy elektronik oylama sisteminin düzgün ve güvenilir bir şekilde çalışabilmesi, vatandaşların rahat bir ortamda, herhangi bir gerilim söz konusu olmaksızın, kendi iradelerini azami derecede kullanarak, içlerinin rahat bir şekilde oy kullandıklarına kanaat etmesi amacıyla tasarlanmıştır. Vatandaş dışında seçim memurlarının da ekstra özel bilgi ve beceriye ihtiyaçları olmaksızın kolaylıkla kullanabilecekleri bu sistemlerde temel prensip, doğruluk ve güvenirlilik üzerine kurulduğundan, sistemin transparan bir şekilde tasarlanması son derece önemlidir.

3.3. ElektrOy Seçim Sisteminin Çalışma Prensibi

Sistem, kullanılan oyların fiziksel kağıtlarla da ayrıca temsil edilmesini temel amaç edinen Mercuri yöntemini baz alarak tasarlanmış olup, ilave olarak güvenlik sağlamak amacıyla bir takım iyileştirmelerle güvenilir bir seçim sistemi olacak şekilde düşünülmüştür.

1. **İstemci ve Sunucu Bilgisayarlarının Güvenliği** – ElektrOy sisteminde sunucu yalnızca IPSEC teknolojisi kullanarak belirlenen bağlantıları kabul etmekte, istemciler de belirlenen ayarlar yardımıyla yalnızca o sunuculara bağlanabilmekte, hiç bir şekilde bağlantı kabul etmemektedirler. Böylece elektronik seçim bölgesine, seçmenlerin bilgileri dışında herhangi bir atak başarılı olamayacaktır.
2. **Kolay adaptasyon** – ElektrOy seçim sistemleri, herhangi bir seçim döneminde yapılan aday değişikliği aşamasında, herhangi bir kod değişimine gerek kalmadan, yetkili memurlar tarafından adaptasyonu kolaylıkla gerçekleştirilecek şekilde tasarlanmıştır.
3. **Uygulama kolaylığı** – Elektronik olarak tasarlanan oyların şekli, boyutu kolaylıkla tasarlanmakta, oy kullanacak kişi bunların üzerine bir kere basarak istediği oyu kullanabilecektir. Bir bankomat cihazı kullanmaktan bile daha basit bu sistemle, yapılması gerekenler tanıtım broşürlerinde yer alan ufak bir broşür ile kolaylıkla anlatılacaktır.

4. **Transparanlık** – Sistemin bir çok parçası standart yazılımlardan oluşturulduğu için, kodlar belli başlı ve açık olarak tasarlanacağından sistemin hangi aşamada ne yaptığı belli olacak, eleştirmen ile seçmenlerin aklında soru işareti kalmayacaktır.
5. **Kağıt pusula** – Sistemde her bir elektronik oyun yanı sıra basılacak kağıt pusula, istemci bilgisayarından seçtiği oyun aynısını kağıtta görecek olan seçmenin içini rahatlatırken, akıllara arkada neler dönüyor gibi bir soru getirmeyecektir.
6. **Ekstra güvenlik** – Basılan kağıt pusulalara bir kimlik atayarak, sandıklara yapılabilecek olası saldırılarda, hangi oyun tahrip edildiği belirlenebilecektir. Bunun sebebi, elektronik sistemlerde elektronik oylardan daha çok kağıt oylara güvenilmesidir. Bu yüzden herhangi bir anlaşmazlık ve itirazlarda, kağıt pusulaların sayım sonucu resmi olarak kabul edilmekte. Tüm elektronik sistemin güvenliğini sağladıktan sonra, fiziksel pusulaların güvenliğini düşünmemek büyük bir risk oluşturur ve yapılan tüm çalışmaları geçersiz kılacağından, bu fiziksel kağıtların üst kısmına, sandık no ve parti bilgisinin yer aldığı bir seri numara yada kimlik numarası oluşturulur. Bu kimlik numarası ile, oyun sıra numarası, hangi sandığa ait olduğu ve hangi parti için kullanılmış olduğu, tespit edilebilecektir. Birilerinin oyu çoğaltması, oyu değiştirmesi vb. hileli durumlarda hemen bilgi veren bu doğrulama sistemi, yazılımsal yapılan tüm güvenlik geliştirmelerine karşılık, donanımsal olarak da alınan önlem olarak düşünülmelidir.

4. ELEKTROY: SEÇİMDEN-SONUÇLARA KADAR AŞAMALAR

Elektronik seçimlerde üç adet fiziksel donanım sözkonusudur. Bunlardan birincisi istemci ve bağlı bulunduğu yazıcı, ikincisi sunucu, üçüncüsü de istemcileri sunucuya bağlayan ağ yapısıdır.

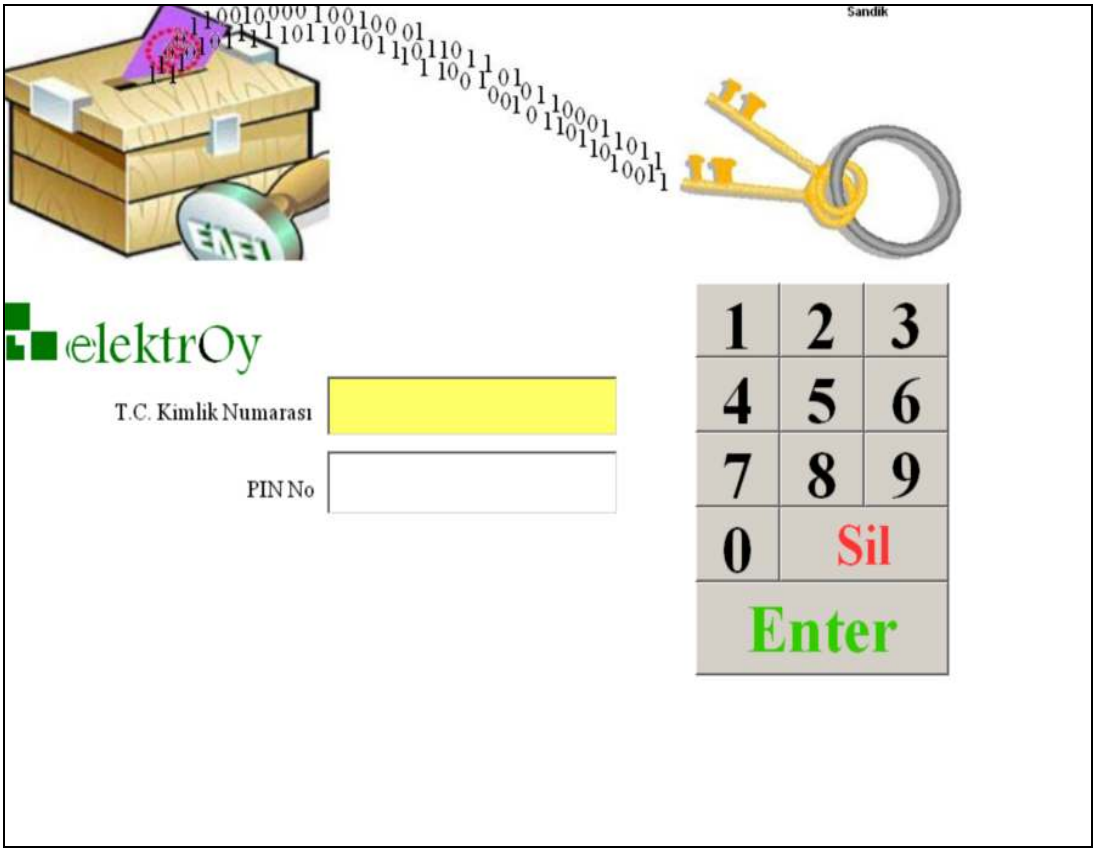
İstemci bilgisayarları ve bunlara bağlı bulunan yazıcılar, seçmen tarafında kullanılan cihazlardır ve seçim esnasında, sunucuya bağlanarak, gerekli bilgileri sunucudan çeker ve kullanılan pusulanın yazıcıdan çıkarılmasını sağlar.

Sunucu bilgisayarları, seçim sisteminde kullanılan web sunucu, veritabanı sunucusu gibi birimleri içerisinde barındırarak, seçmen bilgisayarının isteklerine yanıt verir.

Ağ yapısı ise, sandıkların, oy kullanılan yere olan uzaklığına göre değişiklik gösterir. Sunucu, güvenlik nedeni ile yalnızca izin verdiği istemci ile bağlantı kurmaktadır. Güvenlik amacıyla, IPSecure (IPSEC) tünelleme kullanılan bu sistemde amaç, tüm verilerin şifrelenerek gönderilmesi dolayısıyla, paketlerin yakalanmasının engellenmesi, sunucuya, önceden belirlenen istemcilerden başka hiç bir cihaz bağlanamayacak, böylece gelebilecek saldırı riski en aza indirgenecektir.

4.1. İstemci Tarafı: Oy Verme

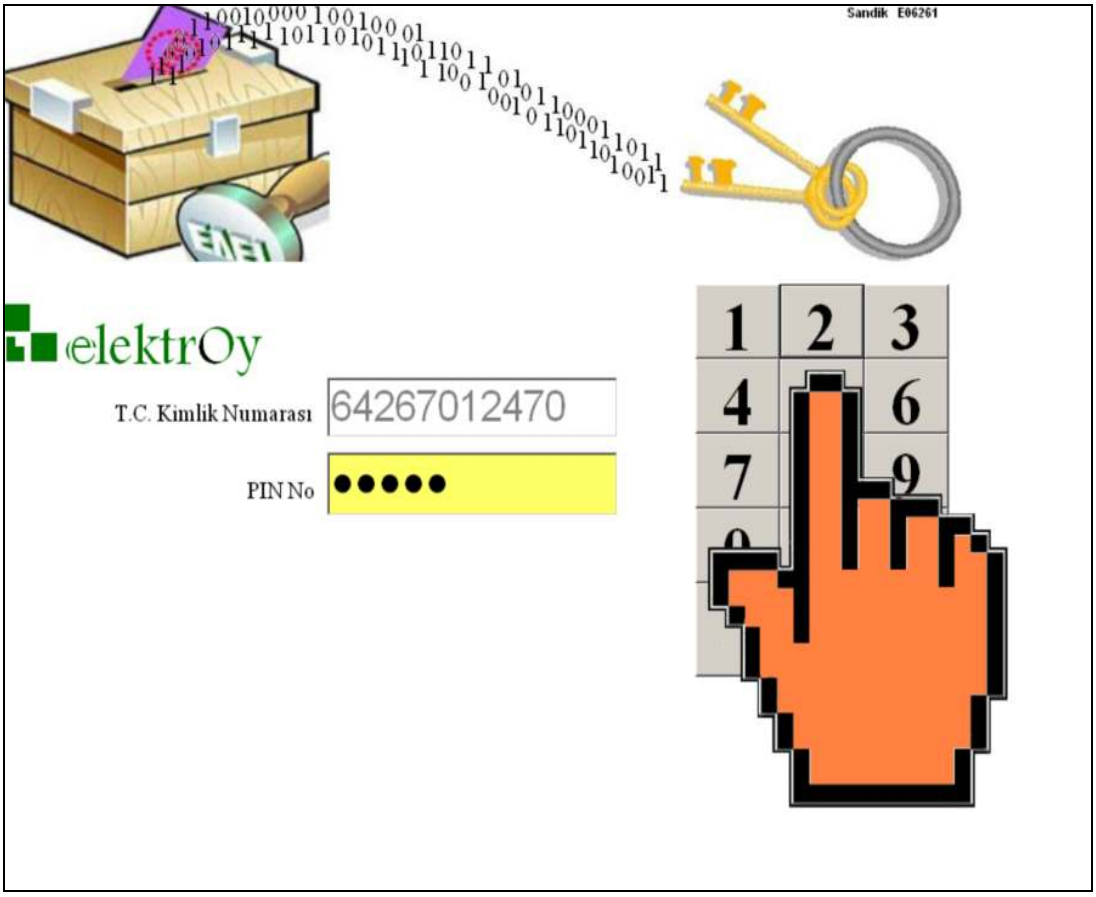
İstemciler, klavye ve faresi olmayan, yalnızca ekrana sahip olan ve kasası ve bağlı bulunduğu yazıcı da dahil olmak üzere her türlü fiziksel müdehalelerden uzakta tutulmalıdır. Seçim memuru gerekli kimlik kontrolü de yaptıktan sonra, oy kullanma kabinine girmesine izin verdiği seçmen Şekil 10'deki gibi bir ekranla karşılaşır.



Şekil 10 – Elektroy Seçim Sistemi Seçmen Giriş Ekranı

İstemci bilgisayarında klavye ve fare bulunmadığından, yukarıdaki gibi bir tuş takımı vardır ve kullanıcı dokunmatik ekran vasıtasıyla, tuşlara parmağı ile temas ederek, sisteme girişini gerçekleştirecektir (Şekil 11).

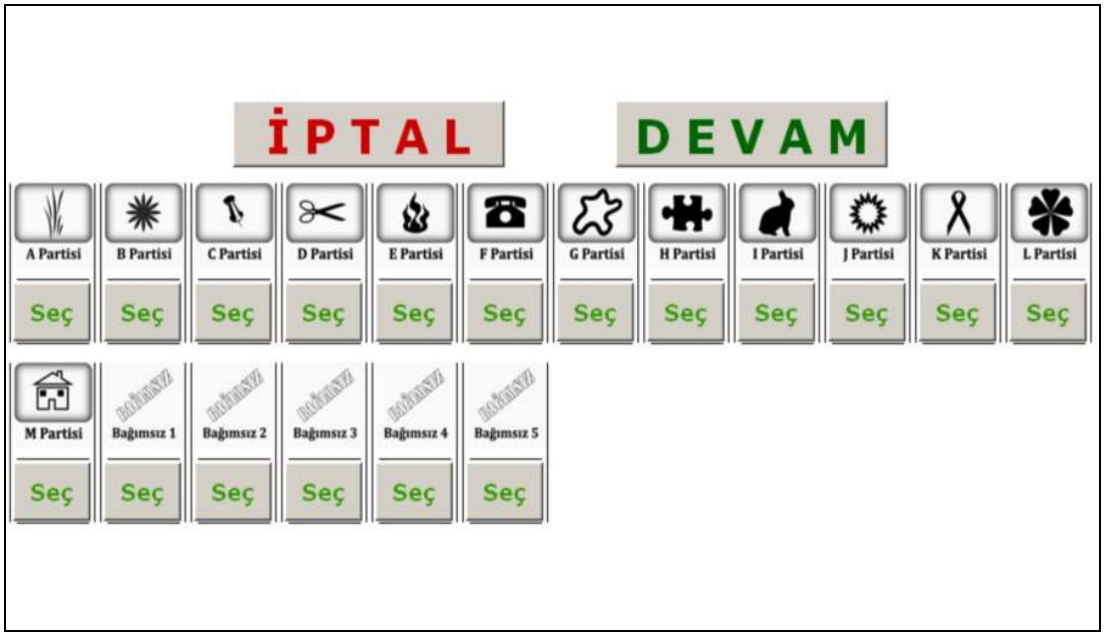
Klavye ve fare, kioskların güvenliğini sağlamak amacıyla sistemden çıkarılmış, yerine dokunmatik ekranlar konulmuştur. Bu ekranlar sayesinde yurttaşlar ekstra bir bilgisayar bilgisine gerek kalmaksızın, sıradan bir bankamatik makinelerini kullanmaktan çok daha zor olmayan bu sistemde kolaylıkla oy kullanabileceklerdir.



Şekil 11 – Seçmen Sisteme Giriş Yaparken Sağ Taraftaki Tuş Takımını Kullanır

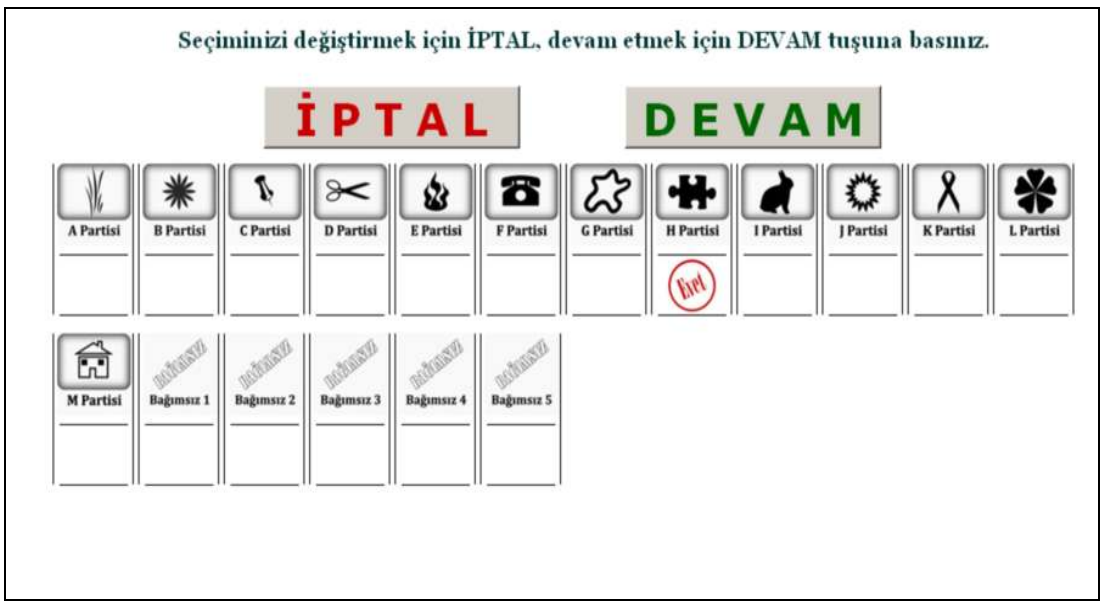
Seçmen TC Kimlik numarası ile kendisine verilen PIN kodunu ilgili alana girerek sisteme giriş yapar. Sistem ise, seçmenin girdiği bilgilerin geçerli olup olmadığını kontrol eder. PINler şifrelenerek veritabanına kaydedildiği ve networkten de şifrelenerek geçireleceği için ekstra bir güvenlikten bahsetmek sözkonusudur. Sunuculara güvenli bir şekilde bağlandıktan ve diğer kontrollerden de geçildikten sonra, geçerli seçmenler sisteme dahil olmaktadır.

Sisteme dahil olan her bir seçmen, oy kullanabilmesi için elektronik pusula (Şekil 12) ile karşılaşır.



Şekil 12 – Sisteme Kabul Edilen Seçmene Sunulan Elektronik Pusula

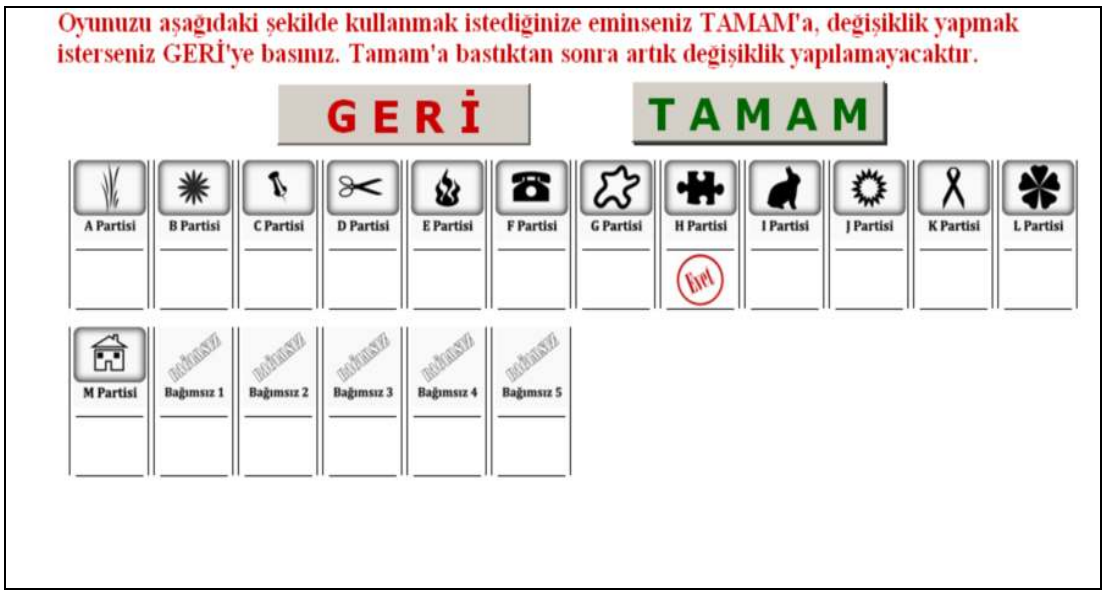
Seçmen gelen pusulada, seçmek istediği partinin altında bulunan Seç düğmesine bir kez dokunur. Diğer Seç butonları silinir ve seçmene Şekil 13'te verilen ekran gelir.



Şekil 13 – Seçmen Tarafından Bir Parti Seçilmiş

Şekil 13’de verilen ekranda, eğer seçmen, yapmış olduğu seçimi değiştirmek isterse, İPTAL tuşuna basması yeterli olacaktır, böylece ekran yine Şekil 12’daki hiç bir parti seçilmemiş haline dönecektir.

Seçimini yaptıktan sonra Şekil 13’deki ekrandan kullanıcı DEVAM butonuna bastığında, aynı resimdeki ekrana çok benzeyen Şekil 14’deki gibi bir ekran ile karşılaşılır. Bu ekranda kırmızı harflerle Tamam butonuna basılması durumunda, artık bir daha değişiklik olmayacağı yönünde bir uyarı ile düğmeler değiştirilmiştir. Burada seçmen oyunu kaydetmek ve çıktısını alabilmek için TAMAM tuşuna dokunmalıdır.



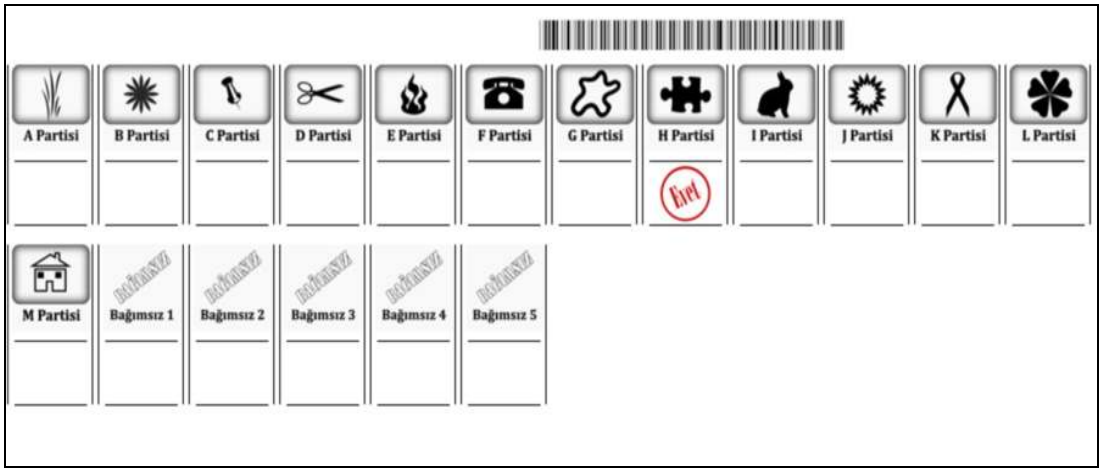
Şekil 14 – Seçmen Tercihini Yaptıktan Sonra Gelen Son Uyarı

Tercihini değiştirmek isteyen seçmen, bu aşamada GERİ tuşuna basabilir ve Şekil 12’deki, hiç bir partinin işaretlenmediği konuma dönüş yapabilir.

Seçmen herhangi bir değişiklik yapmak istemez ise yeşil harflerle yazılmış TAMAM düğmesine bir kez dokunur ve oy sisteme kaydolur. Seçmene gelecek olan ekran Şekil 15’deki gibidir ve ekran seçmenin herhangi bir şey yapmasına gerek kalmadan beş saniye sonra, bir sonraki seçmen için hazır hale gelmektedir.

Şekil 15 – Oy Kullanan Seçmene Gelen Teşekkür Ekranı

Bundan sonra sistem yazıcısından, Şekil 16'deki gibi bir kağıt çıkar. Bu kağıt seçmenin kullandığı oyun fiziksel bir kopyasıdır. Normal pusulalardan hiç bir farkı yoktur.



Şekil 16 – Seçmenin Kullandığı Oyun Fiziksel Kopyası

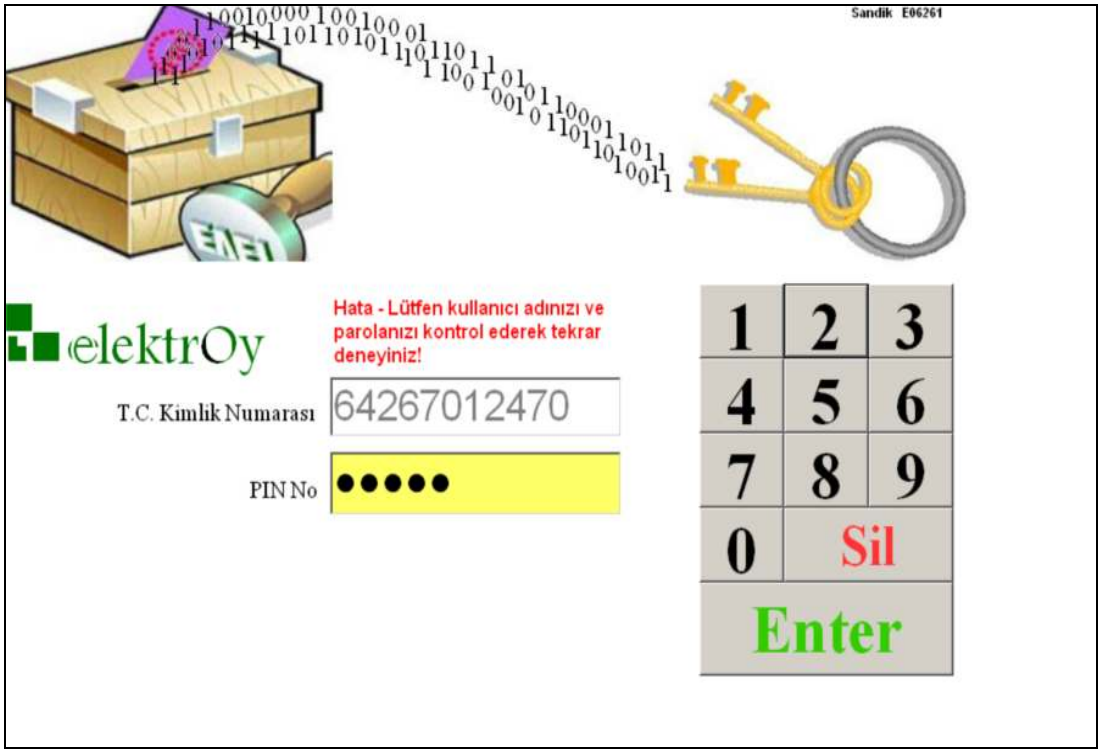
Oyların kağıda basılmış kopyaları, normal pusulaya benzer bir şekilde tasarlandığından, sıradan bir seçmen tarafından kolayca anlaşılmaktadır.

Klasik bir pusula üzerinde olduğu gibi, seçmen tarafından ekranda seçilen partiyi gösteren bu pusula örneğinde, normalinden farklı olarak bir barkod bulunmaktadır. Bu barkod, pusulanın üst tarafına yerleştirilmiştir ve içerisinde pusulanın kimlik numarası bilgisi bulunmaktadır. Bu kimlik numarası özel bir algoritma ile oluşturulmuş olup, oyun kullanıldığı yılı, oyun kullanıldığı sandığı, oyun sıra numarası ile oyun verildiği parti bilgisini içerisinde tutan özel bir sayı dizisinden oluşmaktadır. Bu sayı dizisi art arda gelmediği ve değişiklik gösterdiği için çözülemeyeceğinden, sandık üzerinden fiziksel pusulaların değiştirilmesi olanaksız hale gelmektedir.

Tez kapsamında yaptığımız çalışmada, örnek bir algoritma kullanılmış olup, geliştirilmeye açık bir şekilde tasarlanmıştır ve daha güvenli olması için geliştirilmelidir. Üzerine basılı bulunan barkodu, normal barkod makinelerinin okuyamayacağı bir şekilde tasarlamak da mümkündür. Örnekte standard bir barkod formu kullanılmış olup, sıradan bir barkod okuyucusu ile rahat okunabilmektedir. Yapılan tüm bu güvenlik geliştirmeleri, oyun o anda değiştirilmesini olanaksız hale getirmek içindir.

İlk şifre giriş ekranından sonraki tüm ekranlar, oy kullanma aşamalarını oluşturur ve seçmeni doğrulayıp, oyunu sisteme geçerli bir şekilde kaydedilmesini sağlar. Tüm bunlar TC Kimlik numarası ile kendisine verilen PIN numarasını doğru olarak bilen ve sisteme girebilen seçmenler için geçerlidir. TC Kimlik numarasını yada şifresini yanlış giren, yada unutmuş, daha önce oy kullandığı halde tekrar sisteme girmeye teşebbüs eden seçmenler sistem tarafından geçerli seçmen olarak kabul edilmez ve doğrulanamazlar. Sistem bu tür seçmenleri bilgilendirmek amacıyla bir takım hata / uyarı ekranları getirmektedir.

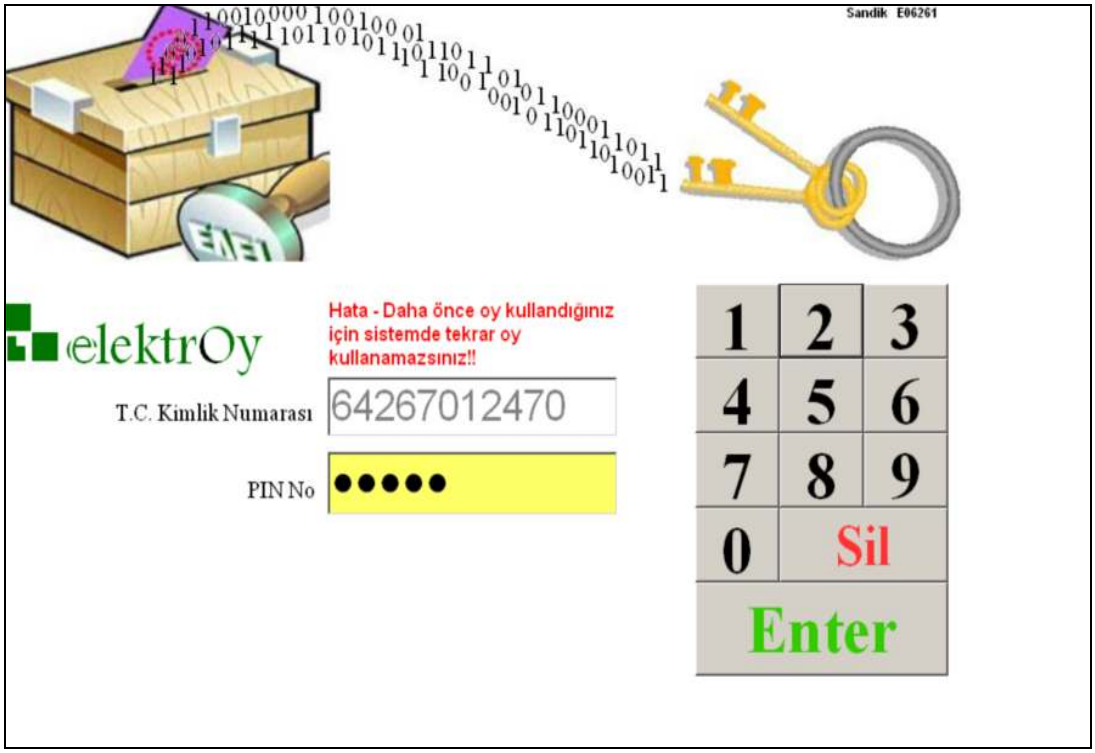
Şekil 24'de sisteme TC Kimlik numarası yada şifresini yanlış girmiş bir seçmenin karşılaştığı hata ekranı verilmiştir.



Şekil 17 – Sistem Tarafından Doğrulanmayan Seçmenin Karşılaştığı Hata

Şekil 17'de de görüldüğü gibi, hatalı TC kimlik no ve PIN no giren hiç bir kullanıcı seçim yapılan ekrana geçemeyecek ve oy kullanamayacaktır. Sistem tarafından kontrol edilen her bir TC Kimlik numarası ve PIN kodu, veri tabanında seçim öncesi oluşturulmuş bilgilerden ibarettir ve her seçim zamanında güncellenmesi gereken bilgiler arasındadır. Elektronik seçim sistemi ile birlikte bu bilgilerin içine PIN kodları da dahil olduğundan, oluşturulan yada güncellenen şifreler seçmenlere kapalı zarflarla gönderilecek yada muhtarlıklardan alınabilecektir.

Daha önce seçime katılan bir kullanıcı ise, yeniden oy kullanmak istediğinde Şekil 18'deki bir uyarıyla karşılaşacaktır.

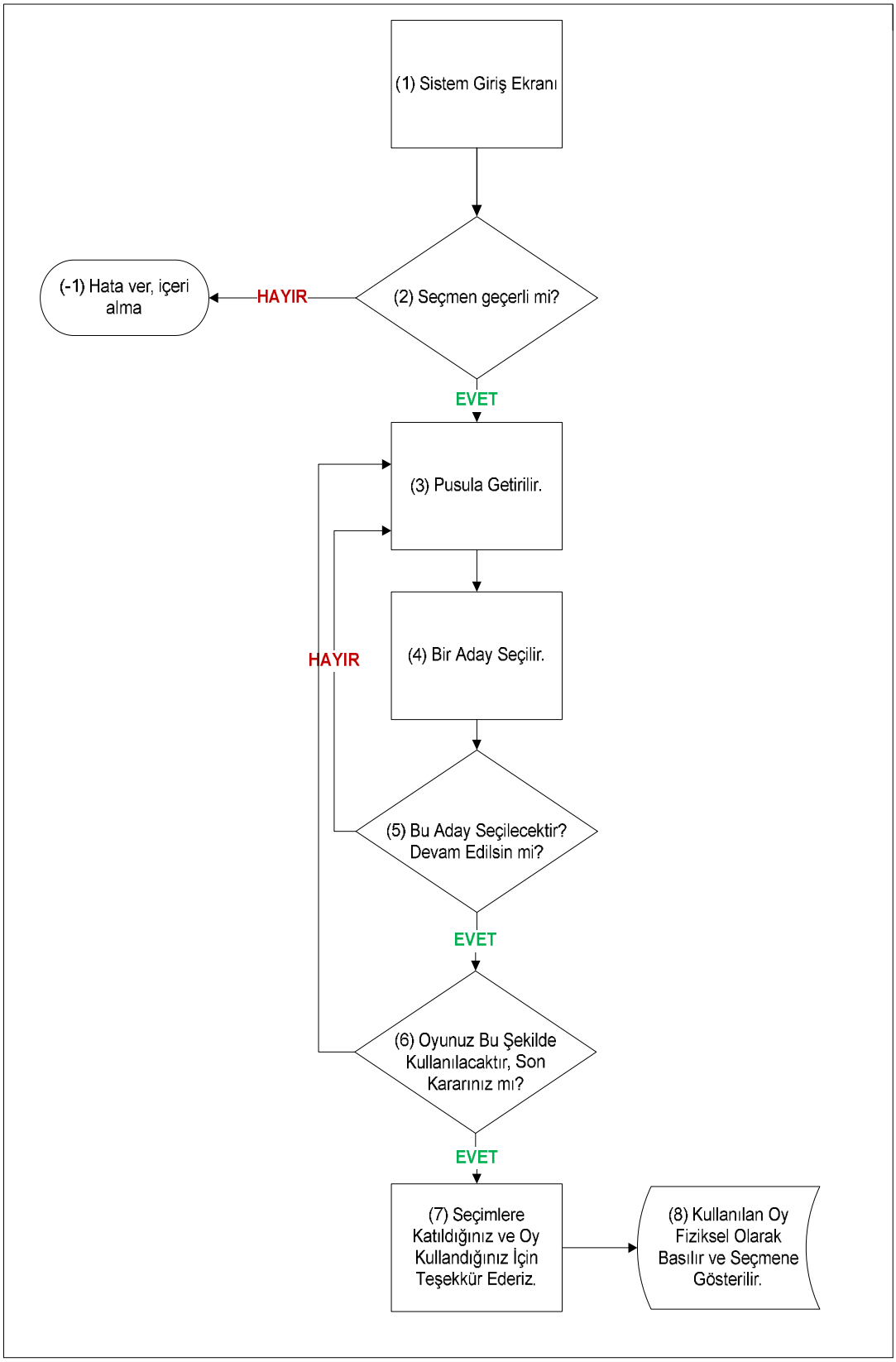


Şekil 18 – Sistem Yalnızca Bir Kez Oy Kullanmaya İzin Vermektedir

Anayasa'nın 298 sayılı kanununun 34. Maddesinde yer alan "Seçmen kütüğüne seçmen bir kez yazılır ve birden fazla oy kullanamaz." [16] ifadesine göre, her bir seçmen, sistemde yalnızca bir kez oy kullanma hakkına sahiptir. Oyunu kullanan her bir seçmen için veritabanında ilgili alanlara oyunu kullandığı bilgisi yer almaktadır. Sistem her bir girişte, söz konusu seçmen için o alanı kontrol etmeden, seçmeni içeriye dahil etmemektedir.

Seçim sistemi, içerisinde bulunan bir çok kontrol ve prosedürleri ile birlikte bütün bir platform olarak düşünülmüştür. Bu platformun tüm adımlarının bir özeti Şekil 19'da verilmiştir.

[16] Anayasa, 298 sayılı kanunun 34. maddesi



Şekil 19 – Elektroy Sisteminin Akış Diagramı

Diagramda da verildiği gibi programın seçmenlere açık olan kısmını sekiz adıma bölmek mümkündür.

1. Sistem TC Kimlik numarası ve PIN kodu sorar.

2. Kullanıcı bu bilgileri düzgün giremez ise, yada daha önce oy kullanmış ise, geçerli bir seçmen sayılamaz. Bu bilgileri düzgün giren seçmenler geçerlidir.

3. Sistem tarafından kabul edilen seçmenlere elektronik pusula getirilir.

4. Seçmen getirilen pusuladan bir aday seçer.

5. Devam tuşuna basar.

6. Emin olup, olmadığı sorulur. Sorulduktan sonra Tamam tuşuna basar.

7. Oy sisteme kaydedilir ve seçmene teşekkür ekranı 5 sn boyunca gösterilir. Bu aşamada oy kullanma işlemi tamamlanmıştır.

8. Ekrandaki oyun bir kopyası ile özel algoritma ile oluşturulan bir kimlik numarası, kağıda basılır ve seçmene gösterilir.

   Böylece seçmen, kullandığı oyun, hiç bir hileye maruz kalmadan, tam kullandığı gibi basıldığını ve sayılacağını düşünerek oradan ayrılır.

Not: Geçerli seçmen kavramı, sistem tarafından kimlik numarası ve pin kodunu doğru bir şekilde giremeyenler ile, daha önce oy kullanmış olan seçmenler ve T.C. Anayasası 298 sayılı kanunda tanımlanan,

1. Silah altında bulunan erler, onbaşılar ve kıta çavuşları (Her ne sebeple olursa olsun, izinli bulunanlar da bu hükme tabiidir.

2. Askeri öğrenciler.

3. Ceza infaz kurumlarında hükümlü olarak bulunanlar[17]. İle yine aynı yasanın, 8. maddesinde geçen, seçmen olamayanlar:

1. Kısıtlı olanlar,

2. Kamu hizmetinden yasaklı olanları [18] kapsamaktadır.

4.2. Seçim Kurulu Bölge Sorumlusu Tarafı: Sandık Sonuçlarını Alma

Seçim yasağının kalkmasının ardından, seçim kurulu bölge sorumluları, bağlı bulundukları sandıklardaki oyları saymak için veritabanlarına bağlanırlar ve sonuçları sistemden alırlar (Şekil 20).

Seçim Sonuçları

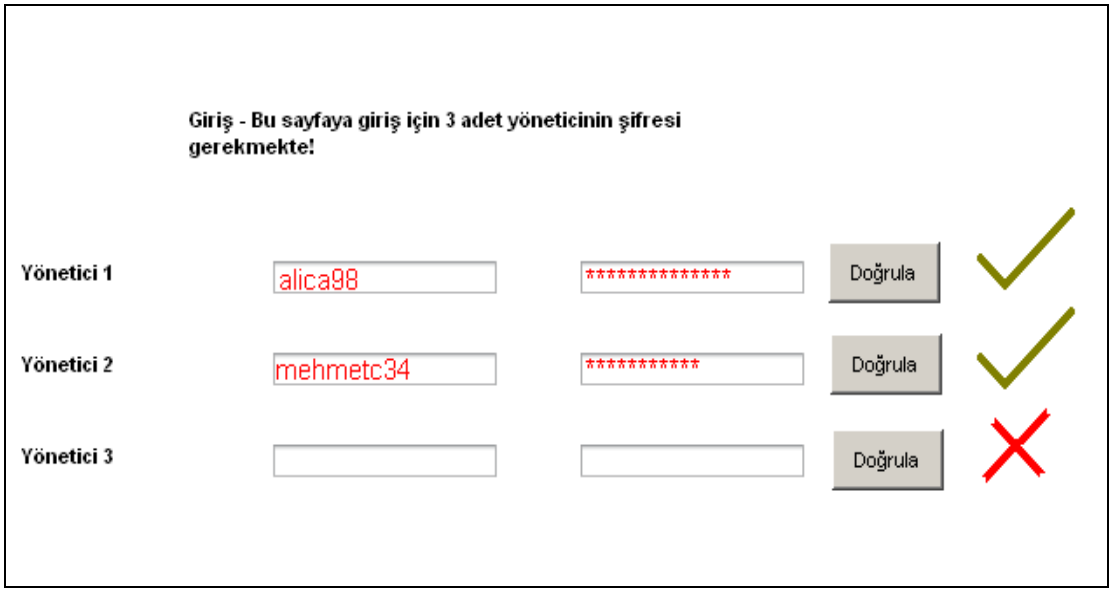
Sonuçları Getir Kayıtlı Seçmen: 20 Oy Kullanan: 15 Sayılan Oy: 15

	A Par	B Par	C Par	D Par	E Par	F Par	G Par	H Par	I Par	J Par	K Par	L Par	M Par	Bağ.1	Bağ.2	Bağ.3	Bağ.4	Bağ.5
Türkiye	1	3	1	3	0	2	0	0	1	1	0	0	1	0	0	1	1	0
İstanbul	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0
Fatih	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Şişli	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bağcılar	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Eyüp	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Kadıköy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Üsküdar	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
Adalar	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Ankara	1	3	0	3	0	1	0	0	0	1	0	0	1	0	0	1	0	0
Çankaya	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sincan	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
Çamlıdere	1	2	0	2	0	1	0	0	0	1	0	0	1	0	0	0	0	0
Elmadağ	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mamak	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Samsun	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Merkez	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Terme	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Alaçam	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Şekil 20 – Elektroy Sonuç Sistemi

[17] T.C. 1982 Anayasası, 298 sayılı kanunun 7. Maddesi
[18] T.C. 1982 Anayasası, 298 sayılı kanunun 8. Maddesi

Seçim sonuçları açıklanacağı zamanda, üç ayrı kişiye verilmiş olan oturum açma ekranı üzerinden güvenli şekilde oturum açılmasına imkan veren bu sistemde, hiç bir kullanıcı tek başına oturum açamayacak ve sonuçları görüntülemeyecektir. Bu grup oturum açma sistemi de yine bu elektroy projesi için özel olarak düşünülmüş, olası riskleri en aza indirmiştir. Üç adet yetkili kişinin oluru ile sonuçların getirilmesi hedeflendiğinden, gerekli bürokrasi ortamı oluşturulmuş olur. (Şekil 21).

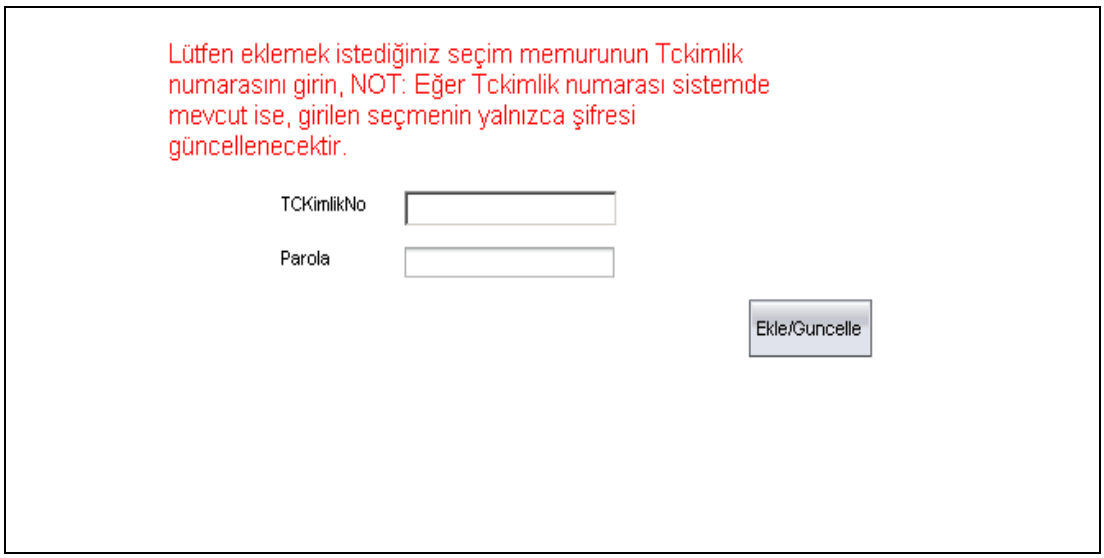


Şekil 21 – Seçmen Sonuç Güvenli Oturum Açma Ekranı

Üç adet yetkili kullanıcının birlikte girişi doğrulandıktan sonra Şekil 27'deki ekran gelecektir ve sonuçlar görüntülenmiş olacaktır.

4.3. Seçim Memuru Tarafı: Seçmen Oluşturma, Sandık Atama İşlemleri

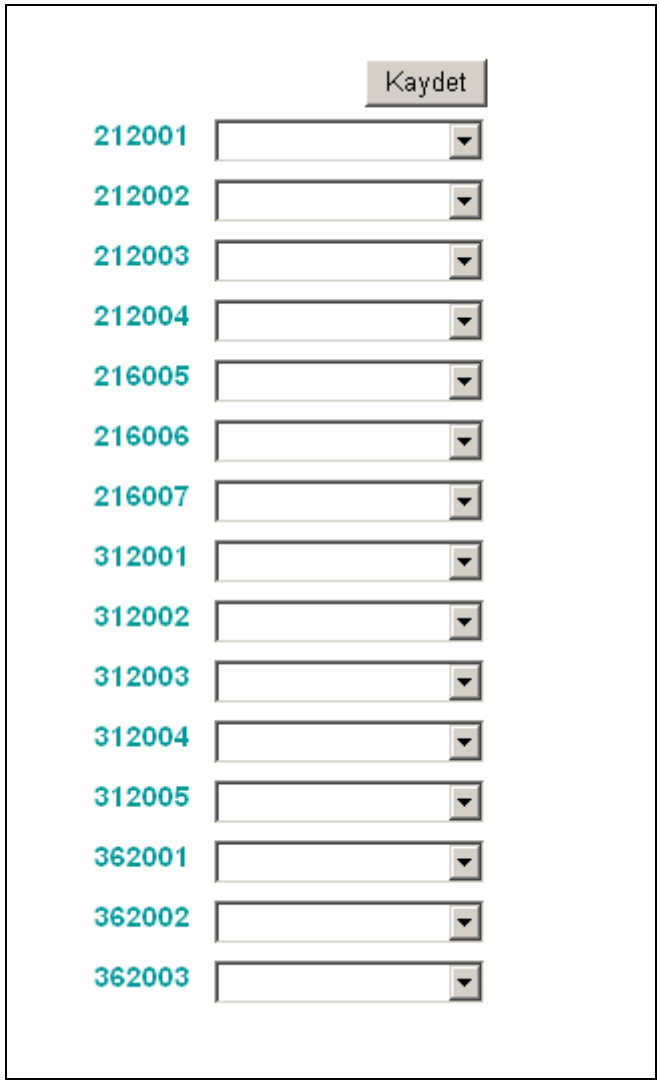
Seçmen memuru tarafından, bir kullanıcı oluşturma ve şifre belirleme/resetleme ekranı kullanılmaktadır. Memur bu ekran ile, yetkisi bulunan seçmen veri tabanına, yada istenirse, tümüne birden bağlantı kurabilir, yeni seçmen oluşturabilir, seçmen güncelleyebilir.



Şekil 22 – Seçim Memuru İçin Seçmen Oluşturma ve Güncelleme Ekranı

Şekil 22'de verilen ekranda, seçim görevlisi memuru, YSK'nin verdiği yetkiler dahilinde, istediği seçmeni buraya ekleyebilecek. Parola kısmına eğer birşey girmez ise, parola otomatik olarak oluşturulacak ve seçmenlere basılıp gönderilecek. Şifreler, şifre zarfına basıldığından basan kişi bile –istenirse, şifreyi göremeyecek, bilemeyecek. Şimdilik prototip, şifre belirleme ve görme hakkı vermektedir.

YSK, sandıkları oluştururken, hangi sandığın hangi ilçeye ait olduğunu belirlemelidir. Bir modül de, bu amaçla yazılmış olup, yetki çerçevesinde, sandıkları atama işlerinin gerçekleştiği ortam için kullanılır (Şekil 23).



Şekil 23 – Sandık Atama Modülü

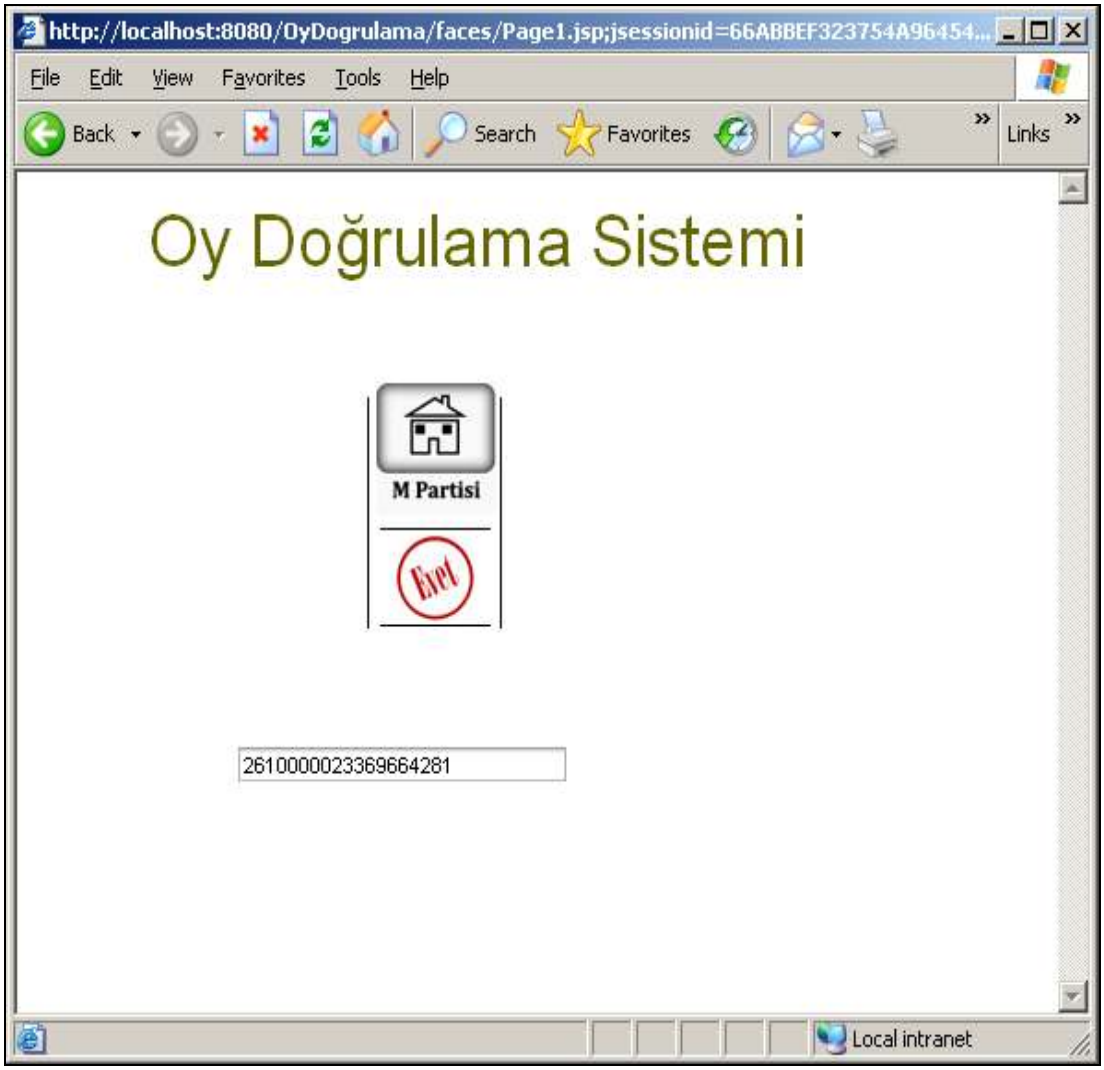
Şekil 23'de de verildiği gibi, her sandık yalnızca bir İlçeye yada ile atanabilir. Bir il yada ilçeye, birden fazla sandık atanması mümkündür. Bu atamalar bittikten sonra, bir çıktı alınır ve YSK tarafından onaylanır. Buna göre, seçim bölgelerine yerleştirilen sunucular, bağlı bulundukları veritabanlarına göre ayarlanmalıdır.

Günümüzde otomasyon uygulamalarına her alanda karşılaşmak mümkündür. E-devlet uygulaması ve günümüzde adından sıkça söz ettiren, e-fatura uygulaması bunun büyük örnekleridir. Elektronik seçim de, bu kolaylıklardan biri olabilir.

Elektronik seçimde alınan güvenlik önlemleri, onu geleneksel seçimlerden daha güvenli ve hızlı yapmaktadır. Örneğin, projede pusulaların üzerine yazılan barkodlar ve bu barkodların içinde bulunan her bir oyun farklı rakamlardan oluşan kimlik numaraları, oyların fiziksel olarak çalınmasını, kaybolmasını ve kopyalanmasını engelleyici bir unsurdur. Kaybolan oylar, veri tabanında belli olduğundan, hangi partinin, kaç oyunun kaybolduğu bilgisine ulaşmak kesinlikle mümkün olacaktır. Tüm bu yöntemler, hile ile iş yürütmek isteyenlerin önünü kesecek güvenlik önlemleridir.

Sistemde kullanılan tüm oyların elektronik çıktılarının üst kısmında bir barkod bulunmaktadır. Bu barkod sistemi, barkod okuyucuları ile okunarak, oyun değiştirilip, değiştirilmediği kontrol edilmektedir.

Oy doğrulama modülü ismini verdiğimiz bu modülde, seçim memurları, olası bir itiraz ve anlaşmazlık durumunda, bir yandan fiziksel oyları sayarken, diğer taraftan, fiziksel oyların da değiştirilme ihtimali karşısında, barkod okuyucuları ile pusulaları okutmaktadadır. Geçerli olan pusulalar bu şekilde de sayılabilirken, diğer yandan, pusulanın doğrulanması sağlanmış olur. Şekil 24'de oy doğrulama modülü verilmiştir.



Şekil 24 – Oy Doğrulama Modülü

Bu modül, oy pusulalarında bulunan imzayı barkod okuyucusu (Şekil 25) yardımıyla okutarak, oyun hangi partide, hangi sandıkta kullanıldığını sistem incelemeyi ve doğrulamayı mümkün kılmaktadır.

Şekil 25 – ElektrOy Sisteminde Kullanılan Bir Barkod Okuyucusu

Seçim memurunun fiziksel oyları saymasını kolaylaştırırken, ayrıca fiziksel oyların gerçekliğinin ve düzgünce basıldığının kontrol edilmesi amacıyla kullandığı barkod okuyucusu, istenirse yazılan barkodların özel bir barkod okuyucusu ile okunacak bir şekilde tasarlanması, güvenliği daha da artırabilmektedir. Bu barkod okuyucuları, fiziksel güvenlik için düşünülülebilen maliyeti düşük cihazlardır.

5. SONUÇ

Tez kapsamında, yürütülen çalışmalar neticesinde, elektronik sistemlerin karşı karşıya geldiği riskler araştırılmış, tüm dünyada yapılan uygulamalarda karşılaşılan sorunlar analiz edilmiştir. Tüm bu detaylı incelemelerin sonunda, sistemin yazılımsal olarak geliştirilmesinin yanısıra, fiziksel olarak da güvenliğinin en üst düzeye çıkartılması hedeflenmiştir.

İncelenen tüm çalışmaların, oyların elektronik olarak güvenliği üzerinde yoğunlaştığı görülmektedir. Geleneksel seçim sistemlerinde de olduğu gibi pusulaların güvenliği tam sağlanamamaktadır. Sandıklara konulan mühür, bu sandıklarda bulunan oyların değiştirilemeyeceği anlamına gelmemektedir.

Tüm yapılan çalışmalar neticesinde, yeni bir oylama protokolü tasarlanmış ve buna bağlı bir uygulama yazılmıştır. Elektroy adı aldında geliştirilen bu yazılımda, sistem seçmenlerin kullandığı oyları, şifrelenmiş bağlantılar kullanarak bağlandığı sunuculara iletmekte, ayrıca oyun bir kopyasını da fiziksel olan, elle tutulan bir kağıda basmaktadır. Basılan bu pusulanın üzerinde, seçmenin rahatlıkla görebileceği ve anlayabileceği şekilde dizayn edilmiş partiler ile, seçtiği partinin alt kısmında yazan bir evet yazısı bulunmaktadır. Bunların yanısıra, pusulanın üzerinde bir kimlik bilgisi bulunmaktadır. Bu kimlik bilgisi pusulanın değiştirilmediği garantisini vermek amacıyla basılmıştır. Kimlik bilgisi barkod yazı karakteri ile basılmıştır ve barkod okuyucular tarafından okunarak, pusulanın hangi tarihte kullanıldığı ve kime oy verildiğini çıkarmaktadır. Bu barkod bilgileri veri tabanında tutulmaz, yani olası herhangi bir sorun durumunda bile, oy kaybı söz konusu değildir.

Yapılan bu çalışmada, elektronik seçimde mevcut çalışmaların olumlu ve olumsuz yanları araştırılarak, oylama protokolleri incelenmiş ve geliştirilmeye çalışılmıştır.

Bir çok elektronik seçim sistemlerinin zayıf ve güçlü yanlarını detaylı bir şekilde inceleyen çalışmalardan yararlanılmış, bu çalışmaların neticesinde hibrit bir oylama protokolü oluşturulmuştur. Bu protokol, tüm seçim kurallarına uymakta, sonuçları ayrı veritabanlarında tutmakta ve fiziksel pusulaların üzerine bir kimlik numarası basmaktadır. Bu kimlik numaraları barkod yazı ile yazılmış olup, fiziksel oy saymanın yanı sıra, dijital olarak kimlik kontrolünü gerçekleştirerek, ekstra güvenlik sağlamaktadır.

KAYNAKÇA

1. Saltman, R.G, "Accuracy, Integrity, and Security in Computerized Vote-Tallying", ACM, 1988

2. Shamos M.I, "Electronik Voting – Evaluating the Threat", J.D., 1993

3. Applied Computer Security Associates (ASSAC), http://www.acsac.org/2000/presentations/Rodriguez.pdf (Çevrimiçi 03.03.2008)

4. Jefferson D, Rubin A.D., Simons B.,Wagner D. ," A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)", 2004

5. EDS, http://www.eds.com (Çevrimiçi 08.04.2008)

6. Şahin, M. "Elektronik Seçim Sistemlerinin Analizi ve Bir Model Önerisi", Yüksek Lisans Tezi, Beykent Üni., 2005

7. Akın, M. "Elektronik Oy Verme Sistemlerinde Güvenlik: Deneyimler ve Türkiye İçin Öneriler", İ.Ü. Ekonometri ve İstatistik Sayı:3 2006- 12-11

8. Cetinkaya O, Cetinkaya D,"E-Seçim Uygulamaları İçin Gereksinimler ve Tasarım İlkeleri", XI. Türkiye'de İnternet Konferansı, Aralık 2006

9. Yüksek Seçim Kurulu (YSK), http://www.ysk.gov.tr/ysk/index.html (Çevrimiçi 05.01.2008).

10. Yüksek Seçim Kurulu, "Bilgisayar Destekli Merkezi Seçmen Kütüğü Sistemi" (SEÇSİS) Projesi, www.ysk.gov.tr

11. Wikipedia, http://tr.wikipedia.org/wiki/Java_(programlama_dili) (Çevrimiçi 09.05.2008)

12. Netbeans, http://www.netbeans.org (Çevrimiçi 09.05.2008)

13. Brittain J., Darwin I. F., "Tomcat: The Definitive Guide", 2003

14. Java Web Sitesi, https://glassfish.dev.java.net/ (Çevrimiçi 09.05.2008)

15. http://tr.wikipedia.org/wiki/SQL (Çevrimiçi 13.05.2008)

16. T.C. 1982 Anayasası, 298 sayılı kanunun 34. Maddesi

17. T.C. 1982 Anayasası, 298 sayılı kanunun 7. Maddesi

18. T.C. 1982 Anayasası, 298 sayılı kanunun 8. Maddesi

ÖZGEÇMİŞ

Murat Özdemir 1984 yılında Samsun'da doğmuştur. Lisans eğitimini Anadolu Üniversitesi, İşletme Fakültesi – İşletme bölümünde almıştır. Öğrenciliği esnasında bir çok mali müşavirlik firmasına bilgi sistemleri otomasyonları hakkında seminerler veren Murat Özdemir, lisans eğitiminden sonra, Beykent Üniversitesi Matematik Bilgisayar Anabilim Dalı, Bilgi Teknolojileri Bilim Dalı'nda yüksek lisans eğitimine başlamıştır.

Uzmanlık alanlarından bir kısmı, bilgisayar sistemleri güvenliği, elektronik iletişim sistemleri, aktif network ekipmanları, embedded sunucu cihazları ve uydu internet sistemleridir. Sektörde öncü bir internet şirketinde, beş yıla yakın bir süredir teknik destek ve güvenlik uzmanı olarak çalışmakta olup, Microsoft, Cisco, Dexar gibi bir çok teknoloji firmalarının profesyonel sertifikalarına sahiptir. Firmaların IT sektöründe bulunan yetkililere zaman zaman bilgi güvenliği ve yedeklemeler konusunda seminerler veren Murat Özdemir, zaman zaman teknik eğitim veren kurumlarda eğitmenlik yapmaktadır.