BEYKENT ÜNİVERSİTESİ★FEN BİLİMLERİ ENSTİTÜSÜ

ELEKTRONİK SEÇİM MODELLERİNİN ANALİZİ VE BİR MODEL ÖNERİSİ

YÜKSEK LİSANS TEZİ

Murat ŞAHİN

Anabilim Dalı: MATEMATİK-BİLGİSAYAR

Programı: BİLGİ TEKNOLOJİLERİ

Tez Danışmanı: Yrd. Doç. Dr. Turhan KARAGÜLER

EKİM 2005

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ
YÜKSEK LİSANS TEZ SINAV TUTANAĞI

11../12../2005

Enstitümüz ***Matematik - Bilgisayar Anabilim Dalı Bilgi Teknolojileri Bilim Dalı*** yüksek lisans öğrencilerinden BT2251-006 numaralı ***Murat Şahin'in*** *"Beykent Üniversitesi Lisansüstü Eğitim - Öğretim ve Sınav Yönetmeliği"*nin ilgili maddesine göre hazırlayarak, Enstitümüze teslim ettiği ***"ELEKTRONİK SEÇİM MODELLERİNİN ANALİZİ VE BİR MODEL ÖNERİSİ"*** adlı tezi, Yönetim Kurulumuzun 12.09.2005 tarih ve 2005/11-2 sayılı toplantısında seçilen ve Enstitü binasında toplanan biz jüri üyeleri huzurunda, Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğin 27-c *maddesi gereğince* (..75..) dakika süre ile aday tarafından savunulmuş ve sonuçta adayın Tezi hakkında ***oybirliği*** ile ***Kabul*** kararı verilmiştir.

İşbu tutanak, 5 nüsha olarak hazırlanmış ve Enstitü Müdürlüğü'ne sunulmak üzere tarafımızdan düzenlenmiştir.

DANIŞMAN
YRD.DOÇ.DR.TURHAN KARAGÜLER

ÜYE
YRD.DOÇ.DR.RIZA HALUK KUL

ÜYE
YRD.DOÇ.DR.GÖKHAN SİLAHTAROĞLU

İÇİNDEKİLER

KISALTMALAR

PC : Personel Computer
CD : Compact Disc
FCO : Foreign Commonwealth Office
ATM : Automatic Teller Machine
DRE : Direct Recording Electronic Systems
PIN : Personel Idendifier Number
DOS : Denial-Of-Service
ISO : International Organization for Standardization
TCSEC : Trusted Computer System Evaluation Criteria
ITSEC : Information Technology Security Evaluation Criteria
BO2K : Back Orifice 2000
TCP/IP : Transmission Control Protocol / Internet Protocol
SSL : Secure Sockets Layer
TCPA : Trusted Computing Platform Alliance
ISP : Internet Service Provider
RSA : Rivest-Shamir-Adleman Algoritm
NIST : National Institute of Standards and Technology
NSA : National Security Agency
SHA–1 : Secure Hash Algorithm – 1
SHA : Secure Hash Algorithm
ANDOS : All Or Nothing Disclosure Of Secrets
EA : Election Authority
MIT : Massachusetts Institute of Technology
CALTECH : California Institute of Technology
VTP : Voting Technology Project
AMVA : A Modular Voting Architecture
UTF-8 : 8 bit Unicode Transformation Formats
VRDB : Central Voter Registration Database
RV : Registration Verifier
RAM : Random Access Memory
ROM : Read Only Memory
XML : Extensible Markup Language
CBC : Cipher Block Chaining
AES : Advanced Encryption Standard
JDK : Java Development Kit
MAC : Message Authentication Code
HMAC-SHA : Keyed-Hashing for Message Authentication- Secure Hash Algorithm

JVM **:** Java Virtual Machine
API **:** Aplication Programming Interface
JCE **:** Java Cryptography Extension
MacOS **:** Macintosh Operating System
JRE **:** Java Runtime Enviroment
CRL **:** Certificate Revocation Lists

ŞEKİL LİSTESİ

ÖZET

ELEKTRONİK SEÇİM MODELLERİNİN ANALİZİ VE BİR MODEL ÖNERİSİ

Murat ŞAHİN

Bu çalışmada, elektronik seçim sistemi modelleri araştırılmış olup, literatürde bilinen modellerin bir analizi yapılmıştır. Varılan sonuçlar doğrultusunda, küçük ölçekli seçimler için bir model önerilmiştir. Modelde seçimin gerçekleştirilmesinde elektronik araçlar esas alınmış olup, sistemin denetlenebilmesi için Mercuri Yöntemi kullanılmıştır.

ABSTRACT

ANALYSIS OF ELECTRONIC ELECTION MODELS AND A MODEL PROPOSAL

Murat ŞAHİN

In this study, electronic election models have been introduced and an analysis of these models has been carried out. In accordance with the attained results, a model for small-scale elections has been proposed and Mercury Method has been adapted to assure the credibility of such elections.

1. GİRİŞ

Seçimler, demokrasilerin en vazgeçilmez bileşenidirler. Elektronik seçim sistemleri, klasik kağıda dayalı seçim sistemlerinin gerçekleştirmeyi amaçladığı tüm işlevleri yazılımsal ve donanımsal elektronik araçlar kullanarak gerçekleştirmeyi amaçlayan sistemlerdir. Ancak, elektronik seçim sistemlerinin giderek yaygınlaşmaya başlaması (son zamanlarda Brezilya ve Hindistan da elektronik seçim uygulayan ülkeler arasına katılmıştır) yoğun tartışmaları da beraberinde getirmiştir. Kuşkusuz bu tartışmaların odağındaki olaylar, ABD'deki 2000 yılı başkanlık seçimlerinde yaşanan aksaklıklar ve olumsuzluklardı. Elektronik seçim sistemlerinin güvenli olup olmadığı, uygulamada olan sistemlerin açıkları ve zayıflıkları gibi konular akademik çevrelerde tartışılmaya başlandı, yeni çözüm arayışları hızlandı.

Bu çalışmanın amacı elektronik seçim sistemleri üzerine yapılan araştırmaları derleyip, incelemek ve elde ettiğimiz sonuçlarla, üzerinde yeni geliştirmeler yapılabilecek bir elektronik seçim modeli tasarlamaktır.

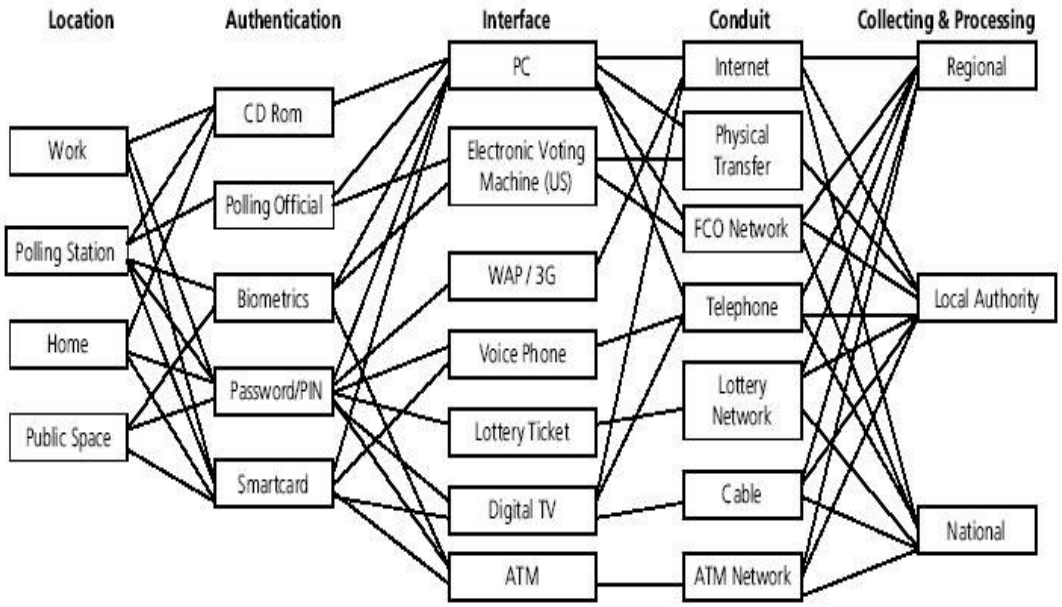
1.1. Seçimler ve Elektronik Seçim Sistemleri

Çağdaş toplumlarda yurttaşlar kendilerini yönetecek temsilcileri, seçimler yoluyla belirlerler. Bu yöntem, yönetimin ve iktidarın meşru bir zemin üzerine kurulmasını sağlamaktadır. Bununla birlikte, seçimler hayatımızda sürekli karşılaştığımız bir olgudur; üniversitelerde, meslek odalarında, sendikalarda yönetici ve temsilcilerin belirlenmesi için seçimler yapılır.

Oy kullanma hakkı olan herkesin oyunu özgür iradesiyle gizli bir biçimde kullanma hakkı vardır. Buna karşın kullanılan oyların açık sayım kuralı uygulanarak sayılması ve tasnif edilmesi gerekir. Kısaca, buna gizli oy-açık sayım ve tasnif kuralı denir.

Elektronik seçim, oy verme işleminin kağıt ve benzeri geleneksel araçlar yerine yeni elektronik teknolojiler kullanılarak gerçekleştirilmesidir. Buradaki elektronik araçlar bir oy verme makinesi, bir ev bilgisayarı, telefon, hatta dijital bir televizyon olabilir. Bu çalışmanın konusu ise, daha çok bilgisayar teknolojilerini temel alan sistemlerdir.

Aşağıdaki şekilde çeşitli elektronik seçim sistemleri gösterilmektedir.



Şekil 1.1: E-seçim uygulama seçenekleri [1]

Bir elektronik seçim sistemi, farklı biçimlerde tasarlanabilir. Bu seçenekler şunlardır;

Seçimin gerçekleştirileceği yer (Location); seçmenin oyunu kullanacağı yer, işyeri, seçim merkezi, ev, kamusal bir alan (okul gibi...).

Seçmenin kimliğinin doğrulanması (Authentication); bir CD rom aracılığı ile, bizzat seçim görevlisinin kimlik kontrolü ile, parmak izi, kan tahlili, retina taraması ve benzeri biometrik kimlik belirlenmesi yöntemleriyle yapılabilir.

Seçmenin oy verirken kullanacağı arayüzler (Interfaces); Seçmen bir kişisel bilgisayar (PC), özel olarak tasarlanmış bir oy verme makinesi, telefon, şans oyunu

kuponu, dijital TV veya otomatik para çekme makinesi benzeri araçlar kullanarak oyunu kullanabilir.

Aktarım (Conduit); seçmenin oy kullanma süresi öncesinde ve sonrasında gerekli veri iletişiminin gerçekleştirileceği ortam. Veri fiziksel olarak, internet aracılığıyla, FCO (Foreign Commonwealth Office) ağı üzerinden, telefon şebekesi üzerinden, piyango makineleri ağı üzerinden, kabloyla ya da Otomatik Para Çekme makinelerinin (ATM) kullandığı iletişim ortamı üzerinden taşınabilir.

Seçmen oyunu kullandıktan sonra oyun sayılıp tasnif edilmesi (Collecting&Processing); oyların toplanması ve tasnif edilmesi bölgesel, yerel otorite veya ulusal seviyelerde yapılabilir.

1.2. Elektronik Seçim Sistemlerinin Geçmişi

Elektronik seçimlerle ilgili ilk çalışmayı, 1 Haziran 1869'da (US Patent 90.646) "Elektronic Vote-Recorder" için bir patent alan Thomas Edison yapmıştır. Amacı, bu icadının kongre seçimlerinde kullanılmasını sağlamaktı. Ancak bu icat kongre tarafından benimsenmedi [2].

Avustralyalıların Gizli Pusula Sistemi

ABD'de 1880'lerde yaşanan birçok oy satın alma skandalından sonra bir reform gerçekleştirildi ve "Avustralya Gizli Pusulası" (Australian Secret Ballot) sistemi bir reformla uygulanmaya başlandı. Bu sistem Avustralya'nın Victoria eyaletinde ilk kez 1856 yılında kullanıldı [3]. Bu sistemde, seçim pusulalarında adaylar yer alır ve seçmen bu adaylar arasından seçimini yaparak pusulayı işaretler. Pusulalar benzersiz ardışık numaralarla basılır. Seçmen, özel bir kabinde pusulayı işaretler ve böylece kullanılan oyun gizliliği sağlanmış olur. Ancak, burada seçmen oyunu kullandıktan sonra hiçbir şekilde süreci denetleyemez; oy kaybolabilir, tahrif edilebilir veya çalınabilir. Bu sistem klasik kağıt bazlı seçim sisteminin öncülüdür.

Lever Makineleri

Lever Makineleri, seçmenin tercihlerini, üzerindeki kollar (manivela) yardımıyla yaptığı mekanik sistemlerdir.

1892'de New York'ta seçimlerde Lever Makineleri ilk kez kullanılmaya başlanmıştır. Bu sistemde arayüz, her adayla ya da pusuladaki sorularla ilgili kollardır. Burada, seçmen, uygun kolu hareket ettirerek seçimini yapar. Seçmen oyunu kullandıktan sonra makine kilitlenir ve böylece seçmenin birden fazla oy kullanması önlenmiş olur. Seçmen tüm seçimlerini yaptıktan sonra asıl büyük kolu hareket ettirir ve oyunu tamamen kullanmış olur (vote casting). Oylar, makine içindeki mekanik sayıcılar tarafından sayılır. Seçim görevlileri makinelerde kayıtlı sayıları okur ve bunların toplanmasıyla sonuçlar elde edilir. Ancak, bu sistemde oylara ait herhangi bir belge yoktur. Bu da oyların yeniden sayılmasına imkan vermez. Bu makinede kullanılmış oyların denetimi (audit trail) söz konusu değildir. Bu durum, oylarda tahrifat yapılabilmesi için açık bir yoldur. Örneğin, makineler adaylardan birisinin oyunu fazla göstermek için ayarlanabilir.

Bilgisayar Destekli Sayım Sistemleri

Bilgisayarların oy sayımında kullanılması ilk kez 1964'de Punch Card sisteminin uygulanmasıyla olmuştur. Optik tarama (optical scan) sistemi ise 1980'lerde kullanılmaya başlanmıştır. Her iki sistemde de kağıt pusulalar (ya da punch kartlar) elektronik bir okuyucuya yerleştirilir, sonra kayıt ve tasnif işlemi bilgisayar tarafından gerçekleştirilir. Bu sistemler oyların hızlı bir biçimde sayılıp tasnif edilmesini kolaylaştırır. Bu sistemlerde elle yapılan sayıma göre oyların ve sonuçların tahrif edilmesini zorlaştırmasına rağmen bu olasılığı tamamen ortadan kaldırmaz. Burada en önemli risk faktörleri, sayımı yapan donanım ve yazılım sistemlerinden kaynaklanır.

Doğrudan Kayıt Yapan Elektronik Sistemler

(DRE-Direct Recording Electronic Systems)

DRE sistemleri, tamamen bilgisayar temelli olan ilk sistemlerdir. DRE'ler ilk kez 1980'lerde kullanılmaya başlanmıştır. DRE sistemlerde arayüz, düğmelerden (buttons) ve dokunmatik ekran üzerindeki alanlardan oluşur. DRE sistemlerde, seçim alanlarına gelen seçmenler kimlik kartlarını göstererek bir PIN (Personel Idendifier Number– Kişisel Kimlik Numarası) veya smart kart alırlar. Bu kartları veya PIN'leri kullanarak DRE makinelerine giriş yaparlar. Seçmen, tercihini yaptıktan sonra DRE, seçmenin yaptığı tercihi ekrana getirir ve seçmene son bir kez kullandığı oyu değiştirme imkanı verir. Ve bunun sonucunda, DRE oyu kesin olarak kaydeder.

DRE sistemlerde seçmen gerçek seçim pusulasını görmez onun yerine sadece pusulanın elektronik bir sunumunu görür. Bugün kullanılan DRE sistemlerin çoğu, makinelerden kaynaklanabilecek hataları ortadan kaldıracak ve oyların tahrif edilmesini engelleyecek biçimde, kullanılan oyların yeniden sayılmasına olanak sağlayan özelliklere sahip değildir. Çünkü DRE'ler kullanılan her oyun ayrı ve bağımsız olarak kaydını tutmazlar. Bu, Lever makinelerindeki duruma benzer. Seçmen kullandığı oyun doğru bir şekilde kaydedilip kaydedilmediğini denetleyemez. DRE'ler yazılımdan ve donanımdan kaynaklanabilecek zayıflıklara sahiptirler.

2. ELEKTRONİK SEÇİM SİSTEMLERİNDE KARŞILAŞILAN SORUNLAR

Elektronik seçim sistemlerinin, seçim işleminin kendisine özgü koşullarından dolayı, elektronik olarak gerçekleştirilmesi birçok problemi beraberinde getirir. Elektronik olarak gerçekleştirilen bir seçimin meşru sayılabilmesi için bu problemlerin çözülmesi gerekir.

2.1. Meşru Bir Elektronik Seçimin İlkeleri

Burada kullanılan 'meşruluk' kavramından, elektronik seçim sisteminin her türlü kötü niyetli yönlendirmeye, aldatmaya ve hileye karşı sağlam olması, seçmenlerin güvenini kazanması, sistemin denetim yollarının açık olması anlaşılmalıdır.

Elektronik seçim sistemleri, uygulamada getirdiği kolaylıklarla birlikte, birçok problemi de içerisinde barındırır.

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 [3]. Özellikle DRE sistemleri üzerinde yoğunlaşmıştır. Saltman'a göre Doğruluk, Bütünlük ve Güvenlik bilgisayar temelli bir seçim sisteminin ana unsurlarıdır. Doğruluk, bir elektronik seçim sistemi için temel bir gereksinimdir, ancak bu Bütünlük ve Güvenlik olmadan tek başına bir işe yaramaz.

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

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

Güvenlik (Security): Elektronik seçim sistemine erişimin kontrol altında tutulması gerekir. Sistem, bir bütün olarak güvenli olmalıdır. Seçim sisteminin işlevlerini doğru bir şekilde yerine getirmesini engelleyecek, saptıracak, etkide bulunacak her türlü girişim engellenebilmelidir.

ABD'de 1980'lerden itibaren 50 değişik elektronik seçim sistemi uygulanmıştır Michael Ian Shamos, Electronic Voting–Evaluating the Threat adlı çalışmasında, bu elektronik seçim uygulamalarından şu sonuçları çıkarmıştır [4];

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, satın alınmasına kesinlikle imkan verilmemelidir.

4. Tüm oylar tam ve doğru bir biçimde sayılıp tasnif edilmeli ve sonuçları ilan edilmelidir.

5. Seçim sistemi, her seçimde tamamen uygulanabilir olmalıdır.

İkinci ve dördüncü maddelere karşı oluşabilecek olumsuzlukları önleyebilmek için bir denetim yolu (audit trail) olmalıdır. Ancak bu denetim yolu üçüncü kuralı kesinlikle ihlal etmemelidir.

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.

Bu konuda en kapsamlı çalışmaları yürüten Rebecca Mercuri'ye göre [5],

Seçmenin kullandığı oy ile sistem tarafından kaydedilen, iletilen ve tasnif edilen oyun aynı olduğunu tam olarak doğrulayabilmesine olanak sağlayan ve tamamen elektronik olan bir seçim sistemi yoktur. Her programcı, ekranda başka bir şeyi gösterip, aslında başka bir şeyi kaydeden ve bambaşka bir sonucu kağıda basan bir kod yazabilir. Bunların bir oylama sisteminde olmayacağı iddia edilemez ve denetleme yapılamayabilir.

Elektronik seçim sistemleri seçim görevlileri tarafından gerçekleştirilen görevleri, bütünüyle göstermelik hale getirmiştir ve iki partinin (burada Demokratlar ve Cumhuriyetçiler kastediliyor) elinden bu süreci kontrol edebilme olanağını almaktadır. Her elektronik seçim süreci böylece makineleri programlayan, inşa eden ve işleten bireylere emanet edilmektedir. Bu risk, şu anda punch kartları okuyan bilgisayarlar, optik tarama sistemi, kiosk tipi uygulamalar ve internet üzerinden pusula iletilen sistemlerde vardır.

ABD'de şu an hükümlülerin ve yabancıların oy kullanması yasaktır. Ancak seçim sistemi üreten firmalar, programcılar ve yöneticiler için böyle bir kanun yoktur. Hükümlüler ve yabancılar oylama makinesi işiyle uğraşan şirketlerde çalışabilir ve hatta bu şirketlerin sahibi olabilmektedirler.

Her seçim döneminde yeni alınan donanım sistemleri kullanılırken hatalarla karşılaşılmaktadır. Satın alınan bu makinelerin güvenli olduğu ve doğru bir şekilde çalıştığı sözlerine güvenen toplumlar, seçimi etkileyecek birçok riski de göze almış olmaktadırlar. Daha da kötüsü bu sistem hataları seçimden yıllar sonra giderilmektedir ki bunun da bir anlamı kalmamaktadır.

Seçmen tarafından bizzat kontrol edilmeyen yazıcı çıktıları olmadan yürütülen bir elektronik seçim sistemi, üretici firmaların karşı iddialarına karşın bağımsız bir denetim yolu (audit trail) sağlamaz. Tüm seçimleri sistemleri, özellikle de elektronik olanları hatalara eğilimli oldukları için elle sayıma olanak vermelidirler.

Bazı elektronik seçim sistemleri, fazladan tuş basımı ve işlemler gerektirdiği için pusula oluşturma sürelerini daha uzun, sıkıcı ve karışık bir hale getirmektedir. Bu araçların kullanımı günümüzde bir okuryazarlık testi gibi görülmektedir.

Kripto sistemlerini uçtan uca gizliliği sağlayabilecek bir araç olarak düşünmemek gerekir. Kripto sistemleri, pusula üzerine kaydedilen verinin doğru kaydedilip doğru tasnif edilmesini sağlayamaz. Kriptografik sistemler, hatta en güçlü olanları bile, kırılabilir, bu yüzden de pusula içeriğini (ve olasılıkla da seçmenin kimliğini) dikkatli bir okumaya açık hale getirirler.

İnternet üzerinden oy verme (ister seçim alanından, ister uzaktan) tüm dünyadan gelebilecek DOS (Denial-of-service) saldırıları için açık yollar bırakmaktadır. Eğer bugün ABD'deki en büyük yazılım ve donanım üreticileri kendi şirketlerini tekrarlanan saldırılardan koruyabilecek yeteneklerden yoksunlarsa, internet seçim sistemleri de zayıflık açısından bu şirketlerden farklı değildir.

Uzaktan, internet erişimine dayalı sistemler ayrıca seçmenin gizliliğini ihlal etmesine ve oyların satılmasına yol açabilecek, çözümü olmayan kimlik doğrulama (authentication) problemlerine neden olurlar. Daha da ötesi internet tabanlı oy verme sistemleri, teknoloji kullanımına yatkın elit bir kesime kolaylıklar sağlarken, dijital bölünme (digital divide) yaratarak, yoksulların, yaşlıların, kırsal kesimde yaşayanların ve engelli seçmenlerin oy kullanmasını zorlaştıracaktır, bu da eşitlik ilkesini açıkça ihlal edebilecektir.

Rebecca Mercuri elektronik seçim sistemi problemlerinin tamamına yönelik çözümler bulunamayacağını, çünkü bu problemlerden bazılarının NP-complete (Non-deterministic Polynomial time)* sınıfı problemler olduğunu söylemektedir [6].

NP-Complete türü problemlerin çözümü için etkili algoritmalar bulunamaz. Traveling Salesman Problemi (Gezgin Satışçı Problemi) gibi önemli bilgisayar bilimi problemleri bu tür problemlerdendir [7].

Mercuri Yöntemi

Bu yönteme göre, seçim sistemi, bilgisayar kullanılarak yapılan seçimlerin bir yazıcı yardımıyla kağıt üzerinde yeniden üretildiği bir mekanizma içermelidir. Üretilen bu çıktı cam bir fanus içerisinde yer almalıdır. Seçmen çıktıyı kontrol ederek tercihinin doğru kaydedilip edilmediğini denetleyebilir. Eğer bir sorun varsa, seçmen seçim görevlisine başvurur ve çıktı yok edilir. Seçmene yeni bir oy hakkı verilir. Seçim sonunda resmi sonuçlar, kağıt pusulaların da sayılmasından sonra ilan edilir.

Mercuri Yöntemi, seçmenlere oylarının doğru bir biçimde kaydedilip edilmediğini kontrol etme olanağı verir. Ancak, bu uygulama sistem maliyetini arttıracaktır [8] .

Şekil 2.1: Mercuri Yöntemi [8]

Bu şekle göre,

1. Seçmen dokunmatik bir ekran yardımıyla oyunu kullanır.

2. Sistem seçmenin oyunu elektronik olarak kaydeder. Ancak kesin kayıt kağıt pusulaya yapılır. Sistem seçmenin oyunu kağıt pusulaya basar ve bir cam bölmenin arkasında gösterir.

3. Seçmen pusulaya görür ve kontrol eder. Eğer pusula seçmenin tercihlerini yansıtmıyorsa pusulanın geçersiz sayılması için seçim görevlisini çağırır ve yeniden oyunu kullanır. İşlem sorunsuzsa, makine kağıt pusulayı kutuya gönderir.

[*] Non-Deterministic Polynomial Complete: karmaşıklık teorisinde özel bazı problem türlerini tanımlamak için kullanılır. Bir NP-complete problemde, problemi çözmek için gerekli giriş parametrelerinin sayısıyla problemin karmaşıklığı arasında üssel bir ilişki vardır.

2.2. Elektronik Seçim İçin Güvenlik Kriterleri

Bir elektronik seçim sisteminin aşağıdaki kriterlere uyması gerekir [9].

i) Sistemin Bütünlüğü (System Integrity):

Bilgisayar sistemlerinin (yazılım ve donanım olarak) bozulmaya, içine sızılmaya karşı güçlü olduğunun kanıtlanması gerekir (tamperproof). Sistem, içine izinsiz sızabilecek tehditlere karşı bağışık olmalıdır. İdeal olarak, sistem üzerindeki değişiklikler seçimin aktif aşamaları boyunca engellenmiş olmalıdır. Bu, kodun, başlangıç parametrelerinin ve konfigürasyon (yapılandırma) bilgisinin bir kez sertifikalandırıldıktan(uygunluğunun onaylanması) sonra aynı (statik) kalması demektir. Uçtan uca konfigürasyon kontrolü esastır. Sistemin Trojan'lara (truva atı virüsü) karşı korunması gerekir. Oy sayımında, yeniden sayıma imkan vererek doğru sonuçların üretilebilmesi için yukarıdaki koşulların sağlanması gerekmektedir.

ii) Veri Bütünlüğü Ve Güvenirliği (Data Integrity and Reliability):

Oyların girişi ve tasnifiyle ilgili tüm verilerin, her türlü tahrifata karşı güvenli bir şekilde kaydedildiğinin kanıtlanması gerekir, oylar doğru şekilde kaydedilmelidir.

iii) Seçmenin Anonimliği Ve Gizlilik (Voter Anonymity and Confidentiality):

Seçim süreci boyunca, seçim sonuçları sistem dışı okumalara karşı korunmalıdır. Kaydedilen oylarla seçmen arasındaki bir ilişki seçim sistemi tarafından kesinlikle bilinemez olmalıdır.

iv) Operator Doğrulaması (Operator Authentication):

Bir seçimi yönetmek üzere yetkilendirilmiş herkes sisteme giriş için doğrulanmış (authenticated) olmalıdır. Bunun için sabit şifreler yeterli güvenliği sağlayamazlar. Bununla ilgili dikkat edilmesi gereken konular aşağıda sıralanmıştır:

a. Sistemin Denetlenebilirliği (System Accountability): Tüm iç işlemler seçmenin gizliliğini ihlal etmeksizin izlenmelidir (monitoring). İzleme,

oyların kaydedilmesini, tasnif edilmesini, tüm sistem programlama, seçim öncesi ve sonrası test yapılması gibi yönetsel işlemleri içermelidir.

b. Sistemin Şeffaflığı (System Disclosability): Sistem satıcıları karşı çıksalar da, sistem yazılımı, donanımı, donanım üzerindeki mikro kodlar ve her türlü elektronik devre tüm dokümanlarıyla birlikte her zaman denetlenebilmedir.

c. Sistemin Ulaşılabilirliği (System Availability): Sistem kaza sonucu veya kötü niyetli DOS saldırılarına karşı korunmuş olmadır. İstenildiği her zaman hizmet verebilir olmalıdır.

d. Sistemin Güvenirliği (System Reliabilty): Sistem geliştirimi, (tasarım, uygulama, yönetim vs) kazayla oluşmuş sistem açıkları (bug) ve amacı kötü olan kodlara karşı, bunların etkilerini en aza indirecek girişimleri yapabilecek nitelikte olmalıdır.

e. Arayüzün Kullanışlılığı (Interface Usability): Sistem yerel seçim görevlileri için kolayca kullanılabilir olmalıdır. Dışarıdan çevrimiçi olarak görevli müdahalesine gerek bırakmamalıdır (örneğin sistem satan firmanın destek görevlisi gibi). Arayüz güvenli, istem dışı veya kötü niyetli kullanıma karşı sağlam ve kullanımı kolay olmalıdır.

f. Belgeleme ve Garanti (Documentation and Assurance): Tasarım, uygulama, geliştirme pratiği, operasyonel süreçler ve test süreçleri açık bir şekilde sürekli belgelenmelidir. Belgeleme, bu süreçlerden her birine uygulanan garanti ölçülerini tanımlamalıdır. TCSEC (Trusted Computer System Evaluation Criteria) [10]'in diğer düşük seviyeli kriterleri ayrıca uygulanabilir; sisteme güvenilir yollar, güvenilir yetenek yönetimi, güvenilir iyileştirme ve güvenilir sistem dağıtımı gibi...

g. Sistem Çalışanlarının Dürüstlüğü (Personel Integrity): Elektronik seçim sisteminin geliştirme, operasyon ve yönetimle ilgili görevliler dürüst olmalıdır. Örneğin personel arasında, kumar oynayanlar ve geçmişlerinde kuşku uyandıracak suçları olanlar bulunmamalıdır.

Uzman kriptolog Bruce Schneier'e göre, ideal bir elektronik seçim sistemi şu şartları gerektirir [11]: Anonimlik (gizli oy gereği), Ölçeklenebilirlik, Hız, Denetim (audit) ve Doğruluk. Ancak genellikle ilk dört özelliğin geliştirilmesindeki aciliyet, doğruluk özelliğini ortadan kaldırmaktadır. İlk bakışta elektronik seçim sistemleri, kağıt temelli klasik sistemlerde olmayan, "oyun kutudan geri çıkartılabilmesi" özelliğiyle caziptirler ve bu sistemlerde oyun doğru bir biçimde kaydedilmesi, tasnif edilmesi ve saklanması için bilgisayara güvenilmesi gerekmektedir. Ancak bilgisayarlar ABD'deki 2000 Kasım seçimlerinde olduğu gibi, nereden kaynaklandığı belli olmayan, geri dönülemez hatalar yapabilirler. İnternet üzerinden çalışan sistemler ise, fazlasıyla güvenlik gereklerinden uzaktırlar. Schneier, teorik olarak internete dayalı bir oylama sisteminin mümkün olabileceğini, ancak bunun bilgisayarların tarihindeki ilk güvenli internet üzerinde çalışan uygulama olacağını söylemektedir. Schneir'e göre, bugün internet üzerinde çalışan hiç bir uygulama güvenli değildir.

İnternete dayalı seçim sistemlerinin ISO Common Criteria ve onun öncülleri olan TCSEC/ITSEC (Trusted Computer Security Evaluation Criteria/Information Technology Security Evaluation Criteria) standartlarına uyması gerekir [*]. Örneğin, en azından 4. Seviye Genel Kriterleri [*] (common criteria), bu tek başına yeterli olmasa da, karşılanmalıdır [12] [13].

Güvenlik sadece kendisinin en zayıf halkaları kadar güçlüdür. Kriptografik algoritmalar ne kadar güçlü olursa olsun, bu güçlü algoritmaların üzerinde çalıştırılabileceği bir internet sisteminin olması gerekir. Kişisel bilgisayarlarda yüklü olan işletim sistemlerinin açıkları birçok riski beraberinde getirmektedir; trojanlar, solucanlar ve daha birçok kullanıcı tarafından farkında olmadan bilgisayarına indirilebilecek kötü niyetli program kodları gibi.

Elektronik seçim sistemlerinde çalışan program kodları, güvenlik riskleri arasında yer alırlar. Programların derlendiği derleyicilerdeki açıklar, bu kodları güvenilmez

[*] EAL4 geliştiriciye, iyi ticari geliştirme uygulamaları bazında pozitif güvenlik mühendisliğinde kazanılan güvenceyi maksimize etme olanağı sunar. Bu uygulamalar, zorlayıcı olsa da, uzman seviyesinde bilgi, kabiliyet ve kaynak gerektirmemektedir. EAL4, daha önce geliştirilmiş bir ürüne yapılacak değişikliklerin teknolojik uyarlanması için ekonomik açıdan mümkün olan en yüksek güvenlik seviyesidir.

yapabilir. Özellikle programlama dilinin seviyesi düştükçe bu kod hatalarını yakalamak güçleşir. Ken Thompson, program kodlarından kaynaklanabilecek güvenlik risklerine dikkat çekerek kısaca şunu söylemektedir: "Bizzat kendimizin yazmadığı hiçbir koda güvenmek için bir sebebimiz yoktur" [14] .

Johns Hopkins Üniversitesi'nden 4 akademisyenin, elektronik seçim sistemi satan bir firmanın DRE sistemini analizinde çarpıcı bilgiler ortaya çıkmıştır [15]. Analiz, firmanın açıkladığı kodları temel almaktadır. Elektronik seçimlere hızla geçilmesinin getirdiği bir takım riskler vardır ve son zamanlarda yapılan çalışmalar ciddi risklerin olduğunu gözler önüne sermektedir; yazılım mühendisliğinden kaynaklanan riskler-kısaca yazılımsal riskler, e-seçim sistemlerinin tasarlanması, uygulanması esnasında içeriden gelebilecek tehditler, network altyapısından kaynaklanabilecek riskler ve denetim-kontrol problemlerinin yarattığı riskler. Güvenlikle ilgili tehditler seçmenlerin kendisinden gelebildiği gibi, "içeriden" de gelebilir; bunlar seçim görevlileri, e-seçim sisteminin geliştiricileri, DRE makinesi üzerinde çalışan işletim sisteminin geliştiricileri.

Bu sistemde riskler şunlardır; smart kartlar üzerinden yapılabilecek saldırılar (saldırılar DRE'nin düzgün çalışmasını engellemekten, her türlü seçim kurallarını ihlal eden işlemlerin gerçekleştirilmesine kadar herhangi bir amaçla yapılabilir); yazılımın geliştirildiği dilin (C++) özelliklerinden kaynaklanan sorunlar (bellek taşmaları-overflow gibi), işletim sisteminden kaynaklanabilecek saldırılar (Windows CE, yerine Linux daha güvenli bir hale getirilebilir), verinin taşınması işlemleri sırasında (internet veya zip diskler yoluyla) gerçekleşebilecek saldırılar, yazılım kurallarının tamamen uygulanmamasından kaynaklanabilecek saldırılar.

Bugünkü internet sistemi üzerinden seçim yapılabilmesinin mümkün olmadığı üzerine yapılan bir analiz de, Avi Rubin'in analizidir. Özellikle Backoffice 2000 yazılımı (www.bo2k.com) üzerinden yaptığı analiz, bize internetin güvenli bir elektronik seçim için güvenli olmadığını kanıtlarıyla ortaya koymaktadır [16]. BO2K yazılımı kullanılarak, bir bilgisayar ele geçirilebilir, içindeki veriler silinebilir, çalınabilir veya değiştirilebilir.

İnternet bazlı bir elektronik seçim için platformun gerçeğe yakın bir analiz olması için Intel işlemcili makineler, Microsoft işletim sistemleri, Microsoft veya Netscape tarayıcılar ve TCP/IP protokol kümesi olduğu varsayılmıştır. Şu anki durumuyla internet bir elektronik seçime "ev sahipliği" yapacak durumda değildir. Virüsler, insanların SSL hakkında bile yeterince bilgi sahibi olmayışı, işletim sistemlerinin yeterince güvenli olmayışı, "dijital bölünme" (digital divide)* problemi, aşılması zor ve maliyet yükseltici problemlerdir. Kullanıcı tarafında güvenli bir platformun sağlanamaması kamu seçimlerinde interneti risklerle, zayıflıklarla dolu bir alternatif yapmaktadır.

Ancak gelecek nesil PC'ler eğer donanım desteğine sahip olabilirse ki bunun bir standart olarak yaygınlaşması gerekmektedir, kullanıcı (seçmen) ile seçim sunucusu (election server) arasında güvenilir bir yol-kanal kurulabilir. Bunun yanında hiçbir kötü niyetli kodun bu iki bileşen üstünde çalışması için bir yol olmaması gerekir.

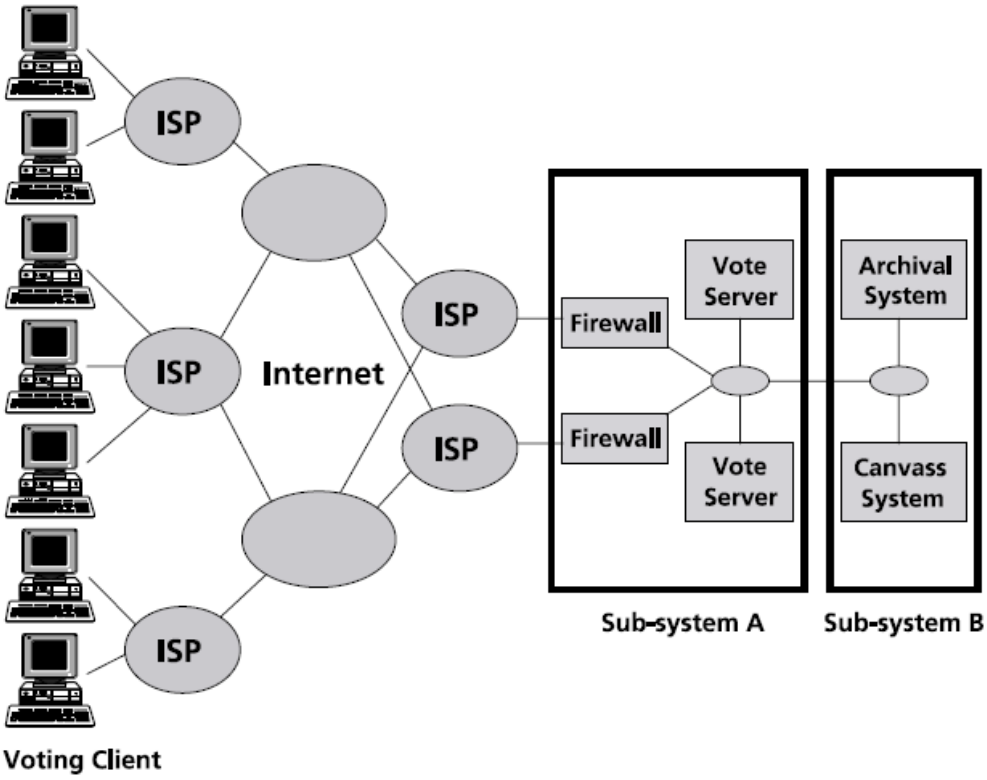
Rivest de yine aynı konu üzerine bir çalışma yapmıştır ve önemli sorun olarak "güvenli platform" üzerinde durmuştur [2]. Seçmenin bilgisayarı, işletim sistemi, kriptolama protokolü bunlar bir araya gelerek platformu oluştururlar. Ancak bunlar ciddi anlamda güvenlik riskleri barındırırlar. Kriptografik açıdan aslında çok iyi çalışan güvenli çözümler vardır, ancak burada sorun seçmen ile kriptolama (şifreleme) protokolü arasında arayüzün oluşturulmasıdır.

Bugün en yaygın kullanılan Windows ve Unix işletim sistemleri tamamıyla güvenli olmaktan oldukça uzaktır. Trojanlar ve diğer internet üzerinden bulaşan virüsler platformun güvenliğini tehdit etmektedir. Rivest, ayrıca elektronik ticaretle elektronik seçimin kesinlikle aynı kefeye konulmaması gerektiğini söylemektedir; "Çünkü elektronik ticarette satın alınan her şey için bir fiş (receipt) alınır, ancak elektronik seçimde bir fişin alınması, oyun satılabilmesi gibi olumsuzluklara yol açabilir. Elektonik ticarette satın alınan bir şey düzgün çalışmadığında bunun düzeltilebilmesi için yeterli zaman vardır, ancak elektronik seçimde zaman açısından bir sınır (deadline) söz konusudur. Elektronik ticarette yapılan işlemlerde, satış yapan

* Dijital Bölünme: Toplumun bir kısmının teknolojiye daha kolay ulaşabilmesi sonucunda, teknoloji kullanımına daha yatkın olması, diğer kısmının ise, ki bu daha çok ekonomik seviye düştükçe artan bir orandadır, teknolojiyi daha az kullanması anlamında bir bölünmeye işaret eder.

ile satın alan kişi arasındaki ilişkileri gösteren kayıtlar tutulur, ancak e-seçimde kullanılan oyun kim tarafından kullanıldığının kaydının tutulması söz konusu olamaz".

Internet Policy Institute'nin internete dayalı seçim sistemleri üzerine düzenlediği rapor ise yine birçok olumsuzluk ve riskten bahsetmektedir [17]. Aşağıda genel olarak internete dayalı sistemleri açıklayan bir şekil yer almaktadır.



Şekil 2.2: İnternet üzerinden oy kullanma sisteminin şematik gösterimi [18].

İstemciler (clients) bir veya birden fazla ISP'ye bağlanırlar. Sistemin sunucu tarafı ikiye ayrılır: alt-sistem A (Sub-system A), kriptolanmış oyları toplar; alt-sistem B (Sub-system B), oyların kriptolarını çözer, tasnif eder, depolar ve raporlar üretir (encryption-decryption) [18]. Seçim Sunucuları ile ISP'ler arasında güvenlik duvarları vardır (firewalls); bu internetten gelecek saldırılardan korunmak için gereklidir.

Rapora göre başarılı bir elektronik seçim sistemi aşağıdaki kriterleri yerine getirmelidir:

Uygunluk ve Doğrulama (Eligibility and Authentication): Sadece oy verme hakkı olanlar oy kullanmalıdır.

Teklik (Uniqueness): Her seçmen sadece bir kez oy kullanabilmelidir.

Doğruluk (Accuracy): Oylar doğru bir biçimde kaydedilmelidir.

Bütünlük (Integrity): Oylar değiştirilememeli, kopyalanamamalı ve silinememelidir.

Kontrol ve Denetim (Verifiability and Auditability): Seçim sonucunda oyların hepsinin doğru bir biçimde sayıldığı denetlenebilmeli ve seçim kayıtlarıyla kanıtlanmalıdır.

Güvenirlik (Reliability): Seçim sistemleri sağlam olmalı, oylama makinelerinden ve internet iletişiminden kaynaklanan problemlerle karşılaşılsa bile hiçbir oyun kaybolmasına imkan vermemelidir.

Gizliliğe ve Serbestliğe Dayanması (Secrecy and Non-Coercibility): Hiç kimse bir başkasının oyunu belirleyememelidir. Seçmenler kimin için oy kullandıklarını kanıtlayamamalıdır. Seçmenler oylarını satamamalı, başkasının oyunu (rahatlık olsun diye) kopyalayamamalı ve hiçbir baskı, zorlama altında kalmadan oy kullanabilmelidirler.

Esneklik (Flexibility): Seçim sistemleri farklı soru biçimleri için çeşitliliğe imkan vermelidirler (örneğin değişik dillerde pusula). Farklı platform ve teknolojilerle uyumlu olmadırlar. Engelli seçmenler için ulaşılabilir olmalıdırlar.

Kolaylık (Convenience): Sistem seçmenin fazla yetenek gerektirmeden oyunu hızlıca kullanabilmesine imkan vermelidir.

Sertifikalandırılabilirlik (Certifiability): Seçim sistemleri, gerekli ölçütleri sağladıklarına dair güvenceyi vermek için test edilebilir olmalıdırlar.

Şeffaflık (Transparency): Seçmen sistemle ilgili her türlü genel bilgiyi edinebilmeli ve seçim süreçlerini anlayabilmelidir.

Maliyetinin Düşük Olması (Cost-effectiveness): Seçim sistemlerinin maliyetleri kabul dilebilir olmalıdır.

3. ELEKTRONİK SEÇİM: ARAÇLAR VE MİMARİLER

Elektronik seçim mimarileri, seçim sistemlerinin gerekli şartları nasıl yerine getirebileceğinin açıklandığı ilkeler bütünüdür. Araçlar ise bu tasarımların uygulanabilirliği açısından her türlü yazılım ve donanım unsurlarıdır.

3.1. Kriptografik Araçlar ve Protokoller

Elektronik seçim sistemleri belirli bir protokole dayanmak zorundadır. Protokolü bir birbirine uyumlu bir kurallar bütünü olarak düşünebiliriz. Kriptografik araçlar ise bize bu protokolleri uygulayabilmek için olanak sağlarlar.

3.1.1. Kriptografik Araçlar

Kriptografik araçlar, çeşitli çevrimiçi seçim protokollerinin yapı bloklarını oluşturur. Bunların en önemlileri aşağıda açıklanmaktadır.

Dijital imzalar (Digital Signatures):

Dijital imzalar, yazılı imzaların elektronik karşılığı olarak düşünülmüşlerdir. Dijital imzalar bir dosya veya dokümana eklenerek onun imzalayan kişiye ait olduğunu reddedilmez bir şekilde belirtirler. İmzanın üç özelliği olmalıdır. İlk olarak imzalar özgün olmalıdır, yani farklı kişilerin imzaları farklı olmalıdır. İkinci olarak imzalar değiştirilebilir olmalıdır ve bir başkası, oluşturulan bir imzayı tekrar oluşturamamalıdır. Üçüncü olarak ise dijital imza doğrulanabilir olmalıdır.

Kamusal anahtar, e, özel anahtar d ve n mod olmak üzere M objesinin özel anahtarla kriptolanması aşağıdaki formülle özetlenir.

$S = M^d \bmod n$

İmzanın oluşturulması özel anahtara bağlı olduğu için kişiye özeldir.

Aşağıdaki gösterimde, kişiler kullandıkları imzanın kendilerine ait olduğunu doğrulayabilirler.

$M = S^e \bmod n = (M^d)^e \bmod n = M^{de} \bmod n = M \bmod n$.

Kör İmzalar (Blind Signatures):

Kör imza, bir dijital imza protokolü olup, imzalayan kişinin ne imzaladığının bilinmemesini istediği durumlarda kullanılır. Kör imza fikri ilk kez David Chaum tarafından ortaya atılmıştır. Chaum, RSA algoritmasını kullanarak böyle bir sistem geliştirmiştir [18]. Bir kişinin, içeriğini açıklamak istemediği bir dokümanı notere onaylatmak istemesi tipik bir kör imza uygulamasıdır. Buradaki kişi ile dokümanı arasındaki ilişki noter tarafından onaylanmaktadır. Alice ve Bob örneği aşağıda bu protokolün basitleştirilmiş şeklini göstermektedir:

Alice, M adında bir doküman alır ve bu dokümana körleştirici (blinding) faktör olarak bilinen bir rasgele değer kullanarak bir fonksiyon uygular.

Elde edilen bu dokümana körleştirilmiş (blinded) doküman denir. Bu doküman Bob tarafından imzalanır ve tekrar Alice'e gönderilir.

Alice, dokümanın orijinalini elde etmek için körleştirici faktörü kullanarak başka bir fonksiyon uygular. Fakat belge hala Bob'un imzasını taşır.

Kör imzalama sürecinde, Bob'un orijinal dokümanla Alice'in ona imzalaması için verdiği doküman arasında ilişki kuramaması sağlanmaktadır. Bu özellik çevrimiçi oy verme işlemleri sırasında çok etkilidir. Kör imza sayesinde seçmen, verdiği oyun geçerli olduğunu kanıtlayabildiği gibi aynı zamanda gözlemcinin ya da imza atan

kişinin, oyu ile kendisi arasındaki ilişkiyi kurmasını engellemiş olur. Bu daha sonra açıklanmaktadır.

Tek Yönlü Çırpı (One-Way Hashing):

Tek Yönlü Çırpı matematiksel bir fonksiyondur. H çırpı fonksiyonu, h ise M'nin H çırpı fonksiyonuna girmesiyle ortaya çıkan sonuçtur.

$h = H(M)$.

Tek Yönlü Çırpı şu özelliklere sahiptir: M'nin büyüklüğü ne olursa olsun (veya verilen aralıklar içindeki herhangi bir büyüklükte olsun), çıktının büyüklüğü h sabittir. Tersi olan H^{-1}'in hesaplanması güçtür, bu yüzden h ve H'yi bilsek bile

$H(M) = h$

şeklinde verilen herhangi bir M değerinin de bulunması güç olur. Bu projede, NIST (National Institute of Standards and Technology) ve NSA (National Security Agency) tarafından tasarlanan Güvenli Çırpı Algoritması, SHA–1 kullanılmıştır. SHA 2^{64} bit uzunluğundaki bir girdiden 160 bit uzunluğunda çıktı üretir.

Çok sayıda belgenin imzalanması hesaplama süresi bakımından fazla maliyetli bir işlem olabilir. Çırpı yöntemi genellikle dijital imzalarla bağlantılı olarak kullanılmıştır. Çünkü çırpı bazen bir objenin benzersiz (unique) parmak izi (finger print) olarak kullanılabilir ve genellikle orijinal nesnenin kendisinden daha kısa uzunluktadır. Nesne ve nesnenin imzalanmış çırpısı (hash) alıcıya gelir, alıcı objenin kendisini yeniden çırpı fonksiyonuna sokar ve "İmza Gerialımı (un-signing)" fonksiyonu uygulandıktan sonra, gelen çırpıyla kendi elde ettiği çırpıyı karşılaştırabilir.

ANDOS (ALL OR NOTHING DISCLOSURE OF SECRETS):

Bazı seçim protokollerinde, yönetici sunucuların kimlik numaralarını dağıtırken, kimlik numaralarının hangi seçmene dağıttığını bilmemesi zorunluluğu esastır. Üstelik her alıcıya sadece bir numara atanması gerekmektedir. ANDOS ise, bir veya daha fazla alıcının bulunduğu durumlarda bu soruna çözüm getirebilecek bir

protokoldür. Fakat bu protokol işlemsel olarak yoğun ve ölçeklenebilirlik açısından oy verme protokolleri için yeni sorunlara neden olmaktadır. ANDOS protokolü ilk kez Salomaa ve Santean tarafından ortaya atılmıştır. Bu protokol daha sonra elektronik seçim kâğıdında kullanılmıştır.

Eşik Şemaları (Threshold Schemes):

Gerçek hayattaki seçimlerde karşı karşıya kalınan en büyük korku, şike yada özgür ve tarafsız seçimlerin yapılmasından sorumlu olan makamların taraflı uygulamalara müsamaha edebilme ihtimalidir. Gerçek hayatta, bu sorun, yetki(otorite) ve sorumluluğun karşılıklı olarak bağımsız, birden fazla birime ayrılmasıyla çözülebilir. Bazı durumlarda, seçim sürecinin denetlenmesi amacıyla yabancı gözlemciler davet edilebilir. Eşik Kripto Sistemleri, bu sorun için kullanılan bir kriptografik çözümdür. Eşik sisteminin amacı, kamusal anahtar kriptolamasını, bir alıcılar topluluğuna paylaştırmak ve kriptolanmış bu mesajın, sadece işbirliği içerisindeki çok sayıdaki alıcılar topluluğu tarafından çözülebilecek şekilde uygulamasıdır. Çoğu eşik sistemleri iki ana protokol içermektedir:

1. Alıcıların ortaklaşa kullanabileceği özel bir anahtar yaratmak için kullanılan, bir anahtar üretme protokolü.

2. Özel anahtarı açıkça yeniden oluşturmayacak şekilde ortaklaşa kullanılabilecek bir mesajı çözecek, bir çözücü protokolü.

Homomorfik Kriptolama (Homomorphic Encryption):

Homomorfik kriptolama öyle bir kriptolama türüdür ki, iki tane kiriptolanmış sayının toplamının, o sayıların toplamının kriptolanmış şekline her zaman eşit olmasını sağlayan bir özelliğe sahiptir.

Örnek: A ve B tam sayıdır,E() kriptolama fonksiyonudur. Bu durumda homomorfik kriptolamaya göre E(A)+E(B)=E(A+B) eşitliği her zaman sağlanacaktır.

Herkes kriptolanmış sayılar grubunun toplamını hesaplayabilir ve teyit edebilir, ancak asla hangi sayıların kriptolanmış olduğunu bilemez-hesaplayamaz. Ne bu sayıların toplamını ne de bu sayıları ayrı ayrı hesaplayabilir.

MIX-NET'lerle Yapılan Anonim Haberleşme (Anonymous Communication Using MIX-NET) :

Çevrimiçi seçim protokollerinin pratik uygulamalarında, mesaj kaynağının kimliğinin gizli tutulması gerekebilir. Mix-Net, bu amaç için kullanılacak en yararlı araçtır. Mix-Net ilk defa Chaum [19] tarafından geliştirilmiştir. Bir Mix'in amacı, temel olarak gelen ve giden mesajlar arasındaki ilişkiyi gizlemektedir. Bir Mix-Net ise, çok sayıdaki bağımsız düğümden (mixes) oluşmaktadır. Her bir düğümün kendi özel ve kamusal anahtarı ile kimlik adresi bulunmaktadır. Gönderici Mixes'lerin dizilişi sayesinde hangi orijinal mesajın varış adresine varmadan önce gideceğine karar verir. Dizilişe bağlı olarak, orijinal mesaj, alıcının kamusal anahtarı ile başlayan ve ilk Mix'in kamusal anahtarı ile sonlanan bir kriptolama işleminden geçer. Her bir aşamada, bir sonraki aşamanın adresi de ayrıca orijinal mesaja eklenir. Gönderici adresi sadece Mix-Net tarafından bilinir ve alıcıya açıklanmaz. Ama bir takma ad kullanılarak alıcı, Mix-Net boyunca bu takma ad yardımıyla gönderici ile iletişim kurabilir. Mix-Net ile alıcının ve göndericinin bağlantı koparma (unlink) kabiliyetiyle ikisi dışındaki herkesin Mix dışında kalması garanti altına alınır. Çevrimiçi oy verme işlemi için tipik bir işlev, gizli oylama kutusunun elektronik sürümüdür.

3.1.2. Protokoller

Elektronik seçim protokolleri, elektronik bir seçim sisteminin sağlaması gereken ölçütleri en iyi şekilde nasıl sağlanacağının yanıtını yanıtını oluşturan kurallar bütünüdür. Elektronik seçimlerle ilgili olarak kullanılan bazı protokoller aşağıda açıklanmıştır.

Tek Seçim Otoriteli Protokoller (Protocols With Single Election Authority):

Fujioka ve arkadaşları, Kör İmzalama yöntemini kullanan bir protokol tanımlamışlardır [20]. Bu protokol, seçmen ile kullandığı oyun ilişkisini keserken, gizliliği korumaktadır. Bu protokolun işleyişiaşağıda anlatılmaktadır:

1. Seçmen oyunu hazırlar ve bunu gizli bir anahtar yardımıyla kriptolar. Kriptolanmış oyu Kör İmzalama yöntemi kullanarak işleme sokar. Elde edilen nihai oy seçmen tarafından imzalanır ve seçim merkezine gönderilir.

2. Seçim merkezi, Kör İmzalama yöntemiyle imzalanmış oyu tanımlar. Aynı zamanda bu oyu gönderen seçmenin daha önce oy gönderip göndermediği kontrol edilir. Eğer seçmenin kimliği doğrulanırsa, seçmenin kimliği veri tabanına kaydedilir. Sonra seçim merkezi bu körleştirilmiş (blinded) oyu imzalar ve seçmene geri gönderir.

3. Seçmen, seçim merkezinden aldığı bu oyu Kör İmzalama işlemi öncesi durumuna getirir. Ve seçim merkezinin imzaladığı oya ulaşır. Seçmen imzalanmış ve kriptolanmış oyu, listelenmesi için geri gönderir.

4. Seçim merkezi, tekrar aldığı bu oydaki imzanın kendisine ait olup olmadığını kontrol eder. Sonra kriptolanmış oyu kamuya açıklar. Böylece seçmen, oyunun güvenle kaydedildiğini görmüş olur.

5. Oy sayma işlemi öncesi, seçmen oyu dekripto edecek anahtarı seçim merkezine gönderir.

Seçim merkezi oyu dekripto eder ve tasnif eder.

3. ve 5. adımlarda seçmen, imzası olmadan iletişim kurmalıdır. Bunun yapılmasının amacı şudur; Eğer EA, 3. ve 5. adımlarda gönderenin kimliğini bilirse, seçmenle oyu arasındaki ilişkiyi kolaylıkla kurabilir. Bu gereksinim Mix-Net kullanılarak sağlanabilir.

Ancak bu durumun bazı sakıncaları vardır;

1. EA yine de kendi geçerli oylarını yaratarak, onlara rasgele şifre verip yayınlayarak seçimleri yapabilir.

2. Ayrıca seçmen kendi oyunun yayınlanmadığını anlarsa, şüphelerini kanıtlayamaz.

ANDOS kullanılarak yapılan benzer bir uygulama Salomaa tarafından da gerçekleştirilmiştir [21]. Bu yaklaşımda seçim yetkilisi (Election Authority) gizli,

onaylanmış numaralarla, geçerli bir liste oluşturur. Kayıt safhasında, seçmenler ANDOS kullanarak kimliklerini kanıtladıklarından sonra geçerli bir numara alırlar. Böylece EA belli bir seçmenin geçerli bir numara almış olduğunu bilir, fakat hangi numaraya sahip olduğunu bilmez. Seçmen kura çeker ve rasgele bir numara seçer. Oy, rasgele kimlik numarası ve geçerli numarayı içeren bilgi imzasız olarak EA' ya verilir. EA geçerli numaranın geçerli listeye ait olup olmadığını kontrol ederek oyun geçerliliğini onaylar. Eğer onaylama numarası gerçekten geçerliyse EA rasgele kimlik numarası ile birlikte oyu yayınlar böylece seçmen oyunun sayıldığından emin olur.

Bu protokoldeki problem bir önceki protokoldekinin aynısıdır. EA hala katılım hakkı olmayan seçmenlere onaylama numarası vermemekte güvenilir güvenilir değildir ve oyunun sayılmadığını anlayan bir seçmen, çektiği kuranın gizliliğini bozmadan bunu kanıtlayamamaktadır.

Bu iki kusur literatürde iyi bir biçimde ifade edilmiştir. Ancak onaylama numarası kullanan protokollerdeki başka bir sorun da; bir saldırganın EA'nın gizli listesinde tanımladığı onaylama numaralarından birini tahmin edebilme olasılığıdır. Bunun bir çözümü, onaylama numaralarının sabit olduğu sahayı genişletmektir, bu sayede böyle bir saldırının önüne geçilmiş olunur. Buna rağmen bir saldırgan, saha aralığındaki her olası numara için sahte oy göndermeye çalışırsa, bu teşebbüsü engelleyecek bir mekanizmaya ihtiyaç duyulur ki, böyle bir teşebbüs Anonimleştirici Sunucu'da büyük bir yüke sebep olur.

Anonimleştirici Sunucu, bir seçmenden sadece bir kura kabul etmek üzere yapılandırmak iyi bir çözüm olabilir. Bu, Anonimleştirici Sunucu tarafından imzalanan oyu tasdik edilmesiyle yapılabilir. Tabi ki imza, oy EA'ya varmadan önce kaldırılmalıdır.

Anonimleştirici Sunucu'ya olan güvenin yanı sıra, bu hizmet, gerçekte seçimlerin idaresinin altyapılarından birini oluşturur. Sonuçta; bu servisin en az EA'nın bağımsızlığı kadar rol oynaması gerekir. Bu tasarıma bu yüzden ikili EA tasarımı da denir. Birinci protokol, seçmenin oyunun sayılmadığını kanıtlar niteliktedir. Bu protokol, ANDOS'u kullanır ve bir önceki protokolle benzerdir. Burada ANDOS

kimlik numaralarını (Identification Numbers) ayırt etmede kullanılır. Bu protokol aşağıdaki gibi özetlenebilir:

1. I kimlik numarasıdır. Her seçmen genel bir anahtar ikilisi (k, d) üretir. Eğer v, kullanılan oy ise <I,E_k(I,v) > EA'ya yüklenir.

2. EA, <E_k(I,v)>'ı yayımlayarak aldığını bildirir.

3. Seçmen <I,d> 'ı EA'ya gönderir.

4. EA, d'yi oyu hesaplamada kullanır ve toplama ekler. EA ayrıca her youn altındaki

5. <E_k(I,v)>'lar listesini yayımlar.

6. Eğer bir sayım problemi olmuşsa, seçmen bu durumu <I,E_k(I,v),d>'ı EA'ya bildirerek iletir.

ANDOS nüfusun çok olduğu yerlerdeki sayımlarda kullanışsızdır.

Çoklu Seçim Otoriteli Protokoller (Protocols With Multiple Election Authorities):

Bütünüyle yayınlanmış birkaç protokol, yetkiyi iki ya da daha fazla bileşen arasında paylaştırmaktadır. Bir protokol, Salomaa tarafından geliştirilen iki yetki makamı kullanır. Bu protokolde, bir protokol (EA1) seçmenleri onaylama hizmetinden sorumlu iken, diğeri (EA2) onaylama numaralarındaki oyları çizelgeye geçirmek için kullanılır. Onaylama numaraları ile seçmen arasındaki bağlantı sadece EA1 tarafından bilinmektedir. EA2 sadece EA1'den gelen onaylama numaralarını kullanmaktadır. Yanlış bir sayım ya da geçerli olmayan onaylama numaraları EA1 tarafından tespit edilmektedir.

Bazı araştırmacılar, seçim düzenlemesinde yetkilerin ikiye ayrılmasının yetersiz kalacağı düşüncesine sahiptirler [22]. Bu tür protokoller tek bir kamusal anahtar kullanımını ve bu anahtara bağlı özel anahtarın eşik kripto sistemlerince paylaşılmasını sağlar. Seçmen oy pusulasını verdiği oyun geçerli olduğunu kanıtlayan bir belge ile postalar. Daha sonra bu Yönetici Sunucu'nun kamusal anahtarı ile

kriptolanır. Bu zaman içerisinde özel anahtar asla oluşturulmaz, ne zamanki Yönetici Sunucu tüm oyların kriptolarını çözer ve son sayımı yapar, o zaman özel anahtar kesin olarak kullanılır. Bu protokolün en önemli özelliği, seçimin yönetici sunucularından bağımsız olan seçmenin, kriptolama için gerekli tüm işlemleri kendisinin yapmasıdır.

Daha önceki protokoller, her ayrı oyun birbirinden ayrıldığı ve farklı yönetici sunuculara gönderildiği bölünmüş protokoller ailesinde yer almaktadırlar. Seçimlerin asıl sonucu tüm yönetici sunuculardan gelen sayımların toplamından oluşmaktadır. Bu tür protokoller, oy için iki adayla sınırlanmış ve ikiden fazla aday için kullanılamamaktadır. Bu protokoller aynı zamanda makamların birbiri arasında içi haberleşmelerinde mükemmel bir ölçeklenebilirlik sağlar.

Seçim Otoritelerinin Olmadığı Protokoller (Protocols With No Election Authorities):

Bu protokoller, herhangi bir seçim otoritesine bağlı olmayan, farklı protokollerdir. Bu protokoller, her bir seçmenin, seçimle ilgili sorumlulukları paylaştığı küçük seçim çevreleri dışında herhangi bir şekilde uygulanabilir değildir.

Çıktı Üretmeyen Protokoller:

Çıktı üretmeyen protokoller (receipt-free protocols) yaklaşımlarını kullanan protokoller, ilk protokollerden birisidir. Bu protokoller, seçmen ile seçim otoritesi arasındaki iletişimin, başkalarınca dinlenemeyen kanallarla yapılması temeline dayanır. Başkalarınca dinlenemeyen bir kanal şöyle tanımlanır: "Seçmen Vi için, başkalarınca dinlenemeyen bir kanal öyle bir fiziksel aygıttır ki, eğer yalnızca seçmen Vi, alıcı R'ye bir m iletisini yollayabilir ve başkaları bu m iletisi hakkında hiçbir şey öğrenemezler [23]."

Diğer protokoller ise, seçim otoritesi ile seçmen arasındaki iletişimin gizliliğini temin eden fiziksel bir seçim sandığı kullanır, ancak bu uygulama seçmenlerin hareketliliğini kısıtlar. Buradaki sorun, seçim otoritesinin, seçmenin kimliğini öğrenmemesi ve seçimin güvenilirliğinin sağlanabilmesi için seçmenlerin kimliklerinin tespit edilerek oyların geçerli olmasının sağlanmasıdır.

Erken dönem protokollerin pratik uygulamalarının kullanışlı olmadığı görülmüştür. Bu protokollerden birisi, dinlenemeyen kanalları kullanmadan (receipt freeness) sağlanabileceğini ileri sürmüştür [24]. Bu protokol, seçmen oylarını kriptolamak için kendi rastlantısallığını kullanan Kriptolama Kara Kutusu'nu (Encryption Black Box, EB) icat etmiştir. Bu protokolde ne seçmen ne de seçim otoritesi, Kriptolama Kara Kutusu'nun rastlantısallığını bilmez. Rastlantısallık bir gerekliliktir çünkü, rakiplerin seçmen oylarının hangi tarafa verildiğini bilmemeleri zorunludur. Ayrıca, seçmen rastlantısallığın farkında olmadığı için, seçim otoritesinin oyların geçerliliği konusunda kanıt sahibi olması sağlanır. Bu husus, sıfır bilgili kanıtları (zero knowledge proofs) yöntemiyle sağlanır. Bu protokol ayrıca, seçim otoritesi ile iletişim kurarken seçmeni korumak için gerçek seçim sandıklarını kullanır. Fiziksel ayrım yoktur. Bu yüzden seçime karşı olanlarla işbirliği yapan bir seçmen bu protokolün işleyişini aksatabilir. Ancak daha öncede bahsedildiği gibi, seçimin çıktı fişinden bağımsız olması ve seçmenlerin hareketliliği (receipt freeness ve mobility) gibi beklentiler aynı zamanda karşılanamaz. Buna rağmen bu protokol seçmeni zorlanmaktan koruyacaktır, çünkü kriptolamanın doğruluğu sıfır bilgi kanıtı kullanılarak yapılmaktadır.

3.2. Elektronik Seçim Mimarileri

Burada anlatılan mimariler, bir problem olarak elektronik seçim konusuna bazı yaklaşımlar getirmektedirler.

3.2.1. MIT/Caltech Projesi

MIT ve Caltech üniversiteleri tarafından birlikte yürütülen bu projenin adı Voting Technology Project'tir (VTP).

Bir seçimde kullanılan oylar, fiziksel bir biçim taşımalıdır. Oyların, elektronik sistemlere (veri tabanı üzerine) kaydedilmesi yeterli değildir. Her oy bir nesne üzerine kaydedilir. Bu nesneye 'Frog' denir.

Kağıt pusulalar son zamanlarda optik tarayıcı sistemlerle entegre olmuştur ve bu durum, bilginin daha kalıcı hale gelmesi, güvenliğin artması ve hızlı bir sayım olanağının sağlanması gibi önemli ilerlemelere yol açmıştır. Ancak kağıt pusula sisteminde önemli sınırlamalar vardır. Sürekli büyüyen ve genişleyen bir toplumda, bir çok dil konuşulması ve bunun farklı pusulalar gerektirmesi, kağıt pusulaların seçimlerde kullanılmasını giderek daha zor hale sokmaktadır. Kağıt pusula yeterince güvenli değildir, üzerindeki bilgiler çıkmaz ve silinmez değildir. Örneğin görme engelli bir seçmenin yardım olmaksızın oy kullanabilmesi neredeyse imkânsızdır. Ayrıca, oy kullanma işleminin sonunda, hiçbir seçmen verdiği oyun sayıldığından emin olamamaktadır.

VTP'nin amacı, bu sınırlamaları ortadan kaldırmaktır. Örneğin, seçmenin kullandığı oyun sayılıp sayılmadığını kontrol edebilmesi, bir takım kriptografik araçlar kullanılarak sağlanabilir. Teknolojiye yabancı olan insanların bile kolayca oyunu kullanabilmesi mümkün olacaktır. Önerilen sistemde görme engelli seçmenlerin oylarını hiçbir yardım almadan kolayca kullanabilmesi mümkündür. İnsanlar seçmen kayıt sisteminden kaynaklanan sınırlamalar nedeniyle sadece belirtilen yerlerde oylarını kullanmak zorunda kalmayacaklardır. Uzaktan oy kullanma hiçbir güvenlik açığına meydan vermeden sağlanabilecektir. Elektronik ortam bu sorunların çözümü için doğal bir ortam gibi görünmektedir. Ancak, şu anki uygulamalar bunları sağlamaktan oldukça uzaktır. Amaç, bu sorunu elektronik olarak çözerken, hem bu makinelerin kullanımını kolaylaştırmak hem de güvenlik sorununu çözmektir.

Seçimlerin açık ve gizli olması gereken yanları vardır. Bu noktada gizliliğin sağlanması en önemli problemlerden birisidir. Bugün hala seçmenin oy kullanmaya yetkili olup olmadığını kontrol etmek ve aynı zamanda da onun gizliliğini korumak için en doğru yöntemin bulunması gerekmektedir.

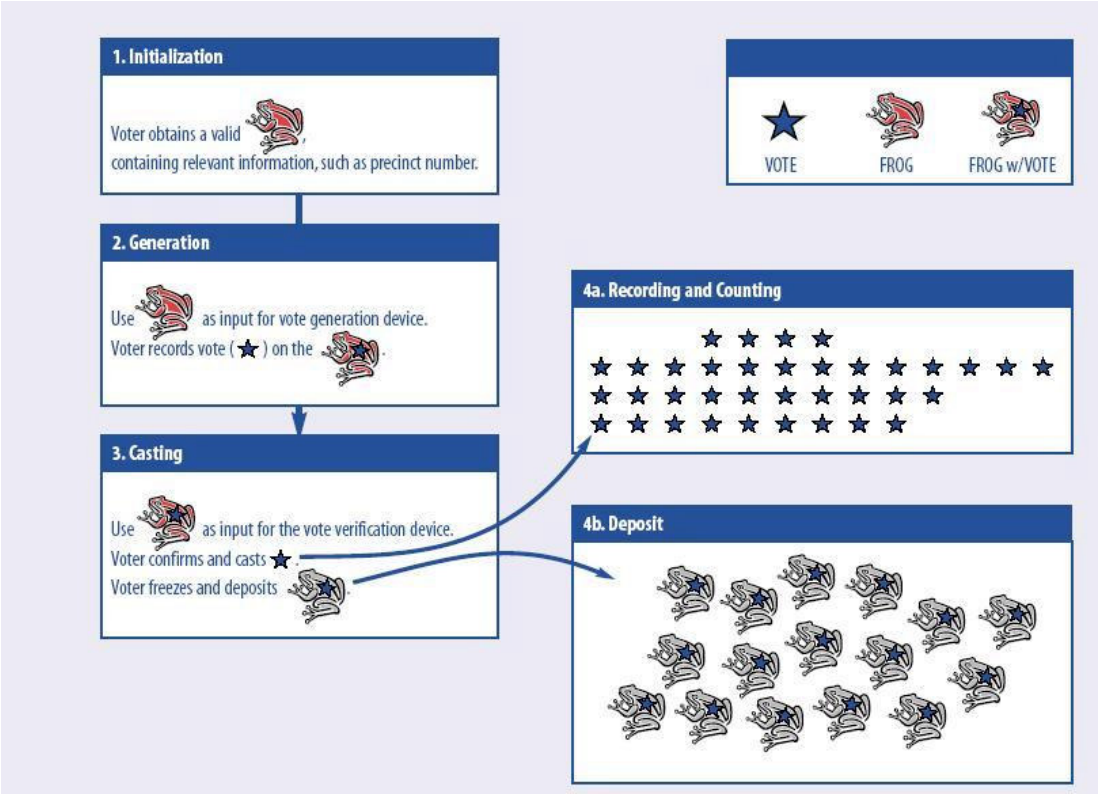
3.2.1.1. Frog Mimarisi

Bu mimari, A Modular Voting Architecture (AMVA) olarak adlandırılır. Bundan sonra kısaca AMWA olarak anılacaktır.

AMVA'da oylar Frog denilen fiziksel parçalara kaydedilir. Frog kayıt cihazının fiziksel şekli hakkında bir bilgi verilmediğini belirtmek için özel olarak seçilmiş bir terimdir. Frog, bu durumda, kağıt, mekanik cihazlar, bilgisayar ekranı ve ses kaydediciler olabilir. Frog, bir pusuladan daha fazla şey anlamına gelir, kullanılmış oylara ait bilginin dışında başka bilgileri de içerir. Bu bilgiler pusulayı imzalayan görevlinin kim olduğu, seçim bölgesi, pusulanın şekli gibi bilgilerdir. Bir Frog fiziksel bir nesne olmak zorundadır. Çünkü Frog denetim yolunu (audit trail) sağlamak zorundadır.

Frog, kartvizit boyutlarında, içinde sabit bir hafızası olan küçük bir kart olarak düşünülebilir. Frog yazılabilir-okunabilir bir hafıza, 'lock' veya muhafaza (freze) – burada kastedilen Frog'a bilgiler kaydedildikten sonra hiçbir şekilde bu bilgilerin değiştirilemez olmasıdır- gibi özellikler sağlar. Frog içinde bir işlemci bulunan bir smart kart değildir, sadece basit (dumb) bir hafıza kartıdır. Frog, elektronik veya dijital değildir. Frog'lar seçim sonrasında denetim (audit trail) için seçim sonrasında kullanılabilirler. Frog'un veri formatı düz metin formatındadır. Veri, UTF-8 karakter setiyle depolanır. Format seçimin lokalini, bölgesini, Frog'u başlatan resmi görevlinin kimliğini (ID) , pusula stilini, dili ve adaylar için gerekli parametreleri gösteren bir başlık içerir. Formatın gövdesi ise seçmenin yaptığı tercihleri gösterir. Gövde bölümü hem insan hem de makine tarafından okunabilirdir. Seçmen, oy yayınlama makinesi yardımıyla herhangi bir eksiklik olmadan yaptığı tercihleri görebilir.

Frog'ların, kullanıldıktan sonra kilitlenmemeleri gerekir (locking). Bu Frog'un bir kere kullanıldıktan sonra, üzerindeki datanın değiştirilmesini engeller.



Şekil 3.1: MIT Frog Mimarisi [19].

Şekil 3.1'deki aşamalar aşağıda açıklanmıştır;

1. Başlatma (Intialization): Seçmen geçerli bir Frog edinir.

2. Üretim (Generation): Seçmen Frog'u oy üretme (vote generation) makinesi için bir girdi olarak kullanır ve tercihlerini Frog'un üzerine kaydeder.

3. Oy Yayınlama (Casting): Seçmen Frog'u oy yayınlama (vote casting) makinesine girdi olarak kullanır. Oyunu kontrol eder ve kullanır. Seçmen Frog her türlü değiştirilme girişimine karşı kilitlenir ve depolanır.

4.a. Kaydetme ve Sayım (Recording and Counting): Frog'lar kaydedilir ve sayılır.

4.b. Depolama (Deposit): Frog'lar kaydetme ve sayım işleminden sonra saklanır.

Sistemlerin çoğu 2.,3. ve 4. adımları birleştirirler, bu ise hem güvenlik hem de tasarım açısından istenmeyen sonuçlara yol açar. Güvenlik tam olarak sağlanamaz, çünkü tek bir kompleks makine için gerekli olan güvenlik şartlarını sağlamak daha zor olmaktadır. Pusula tasarımı, makinenin tümünün sertifikalandırılması nedeniyle

olumsuz olarak etkilenmektedir. Oysa pusulaların ve kullanıcı arayüzlerinin tasarımının, diğer parçalara bağlı olmadan aşama aşama geliştirilmesi gerekmektedir. Aynı zamanda, oy kullanma makinelerinin güvenliği ve oy sayma mekanizmalarının güvenirliği için güçlü, sağlam standartlar gerekmektedir.

Sistemin tüm parçalarını tek bir kutuya koymak, en uygun pusula tasarımını yaratmak ve yüksek seviyede güvenlik ortamı yaratmak için gerekli yeteneği sınırlandırır. AMWA optik tarama (optical scaning) ve DRE elektronik sistemlerin güçlü olan yanlarının ne olduğunu görmemizi sağlar. Optik tarama sisteminin, bugünün baskın seçim teknolojisi olmasıyla birlikte, bu sistem de kendine has problemleri beraberinde getirir; yüksek pusula basım maliyetleri, kullanıcı arayüzlerinin esnek olamaması ve tarayıcı hataları. Optik tarama sisteminin en iyi özelliği, pusulanın seçmen tarafında bizzat doldurulması ve kendi oyunun doğru kaydedildiğini denetleyebilmesidir (audit trail). Elektronik DRE sistemlerde baskı maliyetleri söz konusu değildir ve aynı zamanda esnek kullanıcı arayüzleri sunarlar. Adayların pusula üzerindeki yerini değiştirmek, birden çok dili desteklemek gibi problemler düşünüldüğünde bazı elektronik seçim sistemlerinin daha baskın teknolojiler olduğu görülür. Hatta bazı elektronik seçim donanımlarının maliyetlerinin hızla düştüğü görülmektedir. 5000 dolarlık bir makine bugün 500 dolar olabilmektedir. Bununla birlikte elektronik seçim sistemlerinin çoğu karmaşıktır ve karmaşıklık bir elektronik seçim sisteminde güvenliği azaltıcı en önemli etkendir. Bu sistemlerin çoğu yazılım tabanlıdır ki, yazılımları güvenlik açıksız (bug-free), sağlam bir hale getirmek zordur.

Bu sistem oy üretimini (vote generating), oy yayınlanmasından (vote casting) ayırarak ve seçmenin oyunu bir işlemden diğerine bir Frog üzerinden taşımasını sağlayarak, güvenlikle ilgili birçok meseleyi çözmektedir:

1) Seçmenin pusuladaki tercihini fiziksel bir nesne üzerine (Frog) kaydetmesi seçmenin kullandığı oyu denetleyebilmesi imkânı sağlar ve seçmen denetimin (audit trail) öznesi olur.

2) Oy giriş (vote entry) makinesi oy kullanma (vote casting) makinesinden farklı sertifikasyon standartlarına sahip olabilir. Oy giriş makinesinde grafik yoğun yazılımların çalışması normaldir ve bunların sertifikasyonunu sağlamak zordur. Daha

hayati olan oy kullanma makinelerinde sertifikasyonun (uygunluk belgesi) sağlanması ise daha basit ve kolaydır.

3) Farklı üretici firmalar oy giriş ve oy kullanma makineleri üretebilirler. (Frog'lar için kayıt formatları ve arayüzler standardize edilebilir ve bu kamuya açılabilir.) Başka bir firmanın aynı bileşeniyle herhangi bir bileşenin değiştirebilme imkânının olması üretici firmayla yaşanabilecek sorunların çözümünü kolaylaştırır.

Frog'lar bir kağıt parçası veya bir hafıza kartı olabilir. Bu, optik tarayıcı pusulalarından ve kağıda basılı klasik pusulalardan daha ucuza mal olur. Boş bir hafıza kartının maliyeti 0,20 dolardan daha azdır. Sonuç olarak VTP, elektronik ortamların Frog için en uygun ortamlar olduğunu düşünmektedir.

Frog'un Çalışma Aşamaları

Kısaca, bir Frog'la seçim aşağıdaki gibi çalışır:

1. Bir seçmen oy kullanma alanına oy kullanmak için vardığında kendi kimliğini doğrulamak için resmi görevliye kimlik kartını gösterir (authentication). Resmi görevli boş bir Frog'u alır ve onu oy kullanmaya hazır hale getirir (initializaion), ve seçmene verir. Bunun alternatifi seçmenin Frog'la birlikle seçim alanına gelmesidir.

2. Seçmen Frog'u makinedeki uygun yere (vote-capture) yerleştirir ve kendi tercihlerini Frog'un üzerine işler.

3. Daha sonra seçmen Frog'u makineden (vote-capture eqiupment) çıkartır ve oyunu kullanır (vote casting). Seçmenin Frog'u seçimin denetiminin sağlanması için alıkonulur.

2. ve 3. aşamalar kesinlikle gizli (özel) olmalıdır ve hiçbir şekilde gözlemlenememelidir.

Frog'un Başlatılması (Frog Initialization)

Bir Frog'un başlatılması demek Frog'un üzerine yetkili seçim görevlisinin kimliğinin kaydedilmesi demektir. Bunu klasik kağıt pusula sistemindeki pusulanın resmi

mühürlerle mühürlenerek seçim için onaylanmasına benzetebiliriz. Ayrıca bu başlatılma işlemi seçimin ve seçim bölgesinin hangisi olduğunu da belirler. Burada, Frog üzerinde adaylar, adayların bağlı olduğu parti, seçimin adı, kullanılan dil v.b. gibi bilgiler kaydedilmiştir. Seçmenin kimliği kesinlikle hiçbir şekilde Frog üzerine kaydedilmez.

Mesela seçim görevlisinin elinde Frog'ları başlatmak için küçük bir cihaz olduğu düşünülebilir. Bu cihazı kullanabilmek için her seçim görevlisinin benzersiz bir anahtarı (key) olmalıdır.

Oy Üretimi (Vote Generation)

Seçmen başlatılmış bir Frog'u Oy Giriş-Vote Entry donanımına yerleştirdiğinde, makine uygun oy pusulasını sunar ve seçmenin pusulaya tercihlerini işlemesine imkan verir. Seçmene oy kullanma işleminin tüm aşamalarında geri beslenim (feedback) verilir; böylece seçmen eğer isterse, kolayca tercihlerini değiştirebilme imkanına kavuşmuş olur. Kağıt bazlı bir sistemde, Frog taranabilir bir kağıt olabilir; kağıdı işaretlemek, oy üretim aşamasına tekabül eder.

Bir elektronik sistemde ise, üretim aşaması (vote generation) elektronik paneldeki veya bir PC'deki bir oturumdan oluşur. Seçmen tercihlerini son kez gözden geçirip yaptığında, oylamayı bitiren düğmeye basar (vote-entry finished button) ve böylece seçmenin tercihleri Frog üzerine işlenir. Frog'u makineden çıkarır ve Frog, oy kullanımına hazır hale gelir.

Oyun Yayınlanması (Vote Casting)

Seçmen, Frog'u oy üretme cihazından alarak oyu yayınlama cihazına yerleştirilir.

Oy yayınlama cihazı aşağıdaki sıraya göre çalışır:

1. Seçimin başlangıcında oy yayınlama donanımı, her biri ayrı bir smartkartta olan bir veya daha fazla kriptografik imza anahtarları kullanılarak başlatılır.

2. Cihazın Frog okuma (Frog reader) bölümüne Frog yerleştirilir.

3. Cihaz Frog üzerindeki tüm veriyi okur ve hiçbir değişiklik yapmadan ekranında gösterir.

4. Seçmen cihaz üzerindeki 'Oyu Yayınla' ve 'Oyu Yayınlama' şeklinde iki butondan birisine basar. Eğer ekranda gösterilen verilerin doğru olduğunu onaylarsa 'Oyu Yayınla' butonuna, aksi durumda ise 'Oyu Yayınlama' butonuna basar.

5. Eğer seçmen 'Oyu Yayınlama' butonuna bastıysa, Frog cihazdan çıkar (ejected). Seçmen Frog'u yeniden tercihleriyle doldurmak için oy üretme cihazını kullanabilir.

6. Eğer seçmen Oyu Yayınla' butonuna bastıysa aşağıdaki aşamalar uygulanır;

   i) Bir veya daha fazla kriptografik imza Frog'un üzerindeki verinin sonuna eklenir.

   ii) Frog üzerindeki verinin hiçbir şekilde değiştirilememesi için dondurulur (frozen)

   iii) Frog dondurulmuş Froglar'ın bulunduğu kutuya atılır.

   iv) Frog üzerindeki tüm verilerin elektronik bir kopyası standart bir seri port üzerinden oy depolama birimlerine gönderilir. Seçim gününün sonunda kriptografik anahtarlar oy yayınlama donanımından çıkarılır ve cihazın fişi çekilir.

Oyun Kaydedilmesi (Vote Recording)

Seçim sona erdiğinde oy kullanma donanımı (vote casting equipment) başlangıç verisi (initialization) ve dijital imzayı (digital signature) da içeren oyların elektronik kopyalarını kayıt sistemine gönderir. Her oy yayınlama donanımı seçim görevlilileri tarafından kaydedilen imzalanmış ve gönderilmiş oyların sayısını gösterir. Frog başlatma makineleri (Frog initialization machines) ayrıca başlatmış oldukları Frog'ların sayısını da gösterirler.

Kayıt sistemi tüm oyları ve ilgili sayıları kamuoyunca ulaşılabilir olmasını sağlar. Örneğin oylar web üzerinden yayınlanabilir. Herkes sayıların tutarlılığını kontrol edebilir, oylardaki dijital imzaları doğrulayabilir ve kimin kazandığını görmek için toplamlara ekleyebilir. Evrensel olarak doğrulanabilirlik (universal verifiability) hem güvenliği hem de sisteme olan güveni güçlendirir.

3.2.1.2. Oy Kullanma Makinesinin İşlevleri

Oy Kullanma makinesi Frog'un geçirdiği aşamalar boyunca bazı işlevleri yerine getirir. Bunlar aşağıda açıklanmıştır.

Oyun Doğrulaması (Vote Verification): Frog okunur (taranır, elektronik olarak okunur veya Frog'un formuna uygun bir okuma yapılır) ve tercihleri seçmene gösterilir (displaying). Seçmene yapmış olduğu tercihleri onaylayıp onaylamadığı sorulur. Eğer seçmenin cevabı olumsuzsa, seçmenin Frog'u tekrar seçmene değiştirilmeksizin verilir ve seçmenin oy giriş istasyonuna (vote-entry aşamasına) dönüşü sağlanır, böylece seçmen tercihlerini tekrar istediği şekilde yapar.

Oyun İmzalanması (Vote Signing): Frog dijital olarak imzalanır (burada dijital olarak imzalanan aslında seçmenin Oy Yayınlama (Vote-Casting) donanımıyla yayınladığı Frog'un üzerindeki tercihleridir). Oyun imzalanması işini kotaran donanım için gerekli olan dijital imza anahtarı benzersiz bir anahtardır (unique) ve sadece bu makine için geçerlidir. Bu imza makinenin kimliğini ve oyun bu makineden kullanıldığını belirleyen bir özelliğe sahiptir. Farklı makineler farklı anahtarlar kullanırlar. Bu dijital imza hiçbir şekilde ve kesinlikle seçmenin kimliğini belirleme işlevine sahip değildir (bir seçimde oy ile seçmen arasında bir ilişki kurulamaz).

Oyun Kopyalanması (Vote Copying): Donanım, imzalanmış oyun dijital bir kopyasını çıkarır. Bu kopya daha sonra kayıt sistemiyle iletişim kuracaktır.

Oyun Mühürlenmesi (Vote Sealing): Frog pusulada herhangi bir değişiklik yapılmaması için mühürlenmiştir yada dondurulmuştur diyebiliriz. Frog, herhangi bir yazıma karşı bir sigortanın atmasıyla tepki verir. Kağıt bazlı bir mühürleme daha zordur ve ihmal edilmek zorunda kalınabilir, ancak pusulayı ince tabakalara ayırmak aynı amacı gerçekleştirebilir.

Frog Depolama (Frog Capture): Kullanılan oyların saklanması ve denetim araçları için bütün Frog'lar depolanır.

3.2.2. Grup 2 Mimarisi

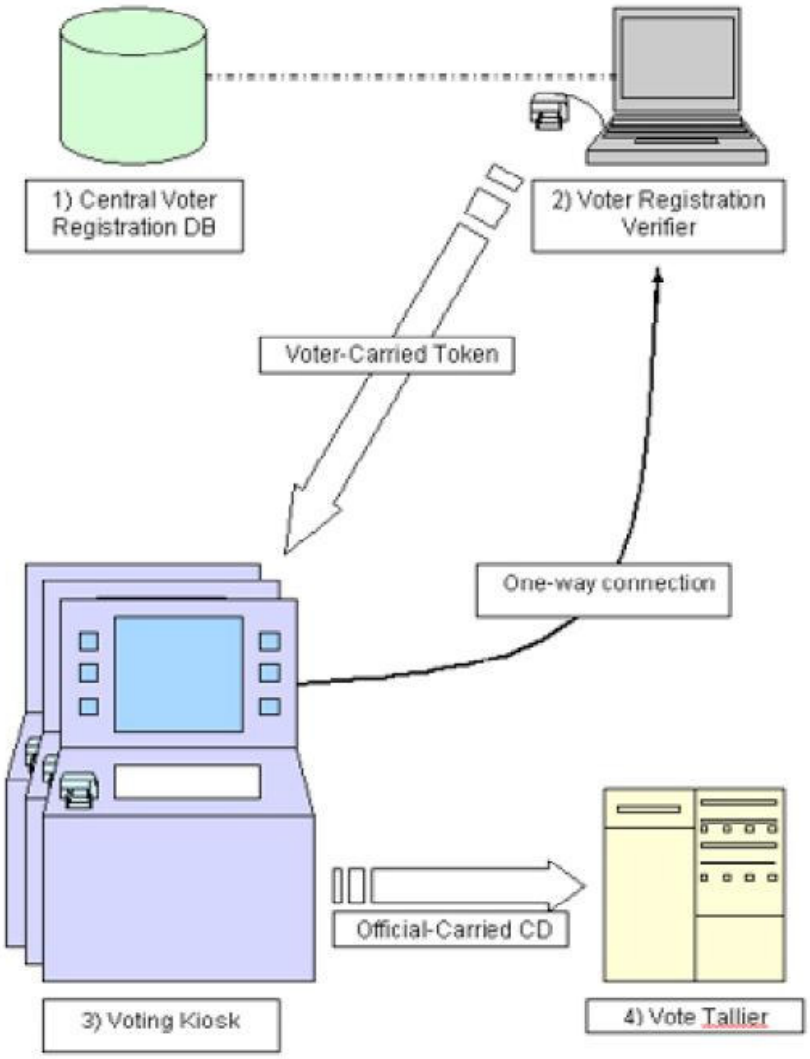
Bu mimari, Amerika Birleşik Devletleri'ndeki John Hopkins Üniversitesi'ndeki bir grup öğretim üyesi ve araştırmacının Maryland eyaleti için tasarladıkları sistemden ortaya çıkmıştır [25].

Bu mimari için ön şartlar şunlardır:

1. Seçimler bir günden daha fazla sürebilir.
2. Sistem sadece eyalet çapında veya daha küçük ölçekte kullanılabilir.
3. Tüm seçim görevlileri sistem hakkında eğitilmelidirler.
4. Tüm donanımların güvenli olduğu kanıtlanmıştır. Donanımlardan oluşan örnek bir grup seçim öncesi ve sonrası kontrol testlerinden geçirilmiştir.
5. Tüm donanımlar seçimler arasında yeniden kurulabilir ve yükseltim yapılabilir özelliktedir.
6. Tüm donanımların taşınmasında, yerleştirilmesinde ve kullanılmasında güvenliğin sağlandığı varsayılır.

3.2.2.1. Sistem Bileşenleri

Aşağıdaki şekilde sistemin bileşenleri ve işleyişi bir şekille gösterilmektedir.



Şekil 3.2: Grup 2 Mimarisi [26]

Merkezi Seçmen Kayıt Veritabanı (Central Voter Registration Database-VRDB)

VRDB eyalet çapında bir seçmen kayıt veritabanıdır. Bu veritabanında seçmenlerin adı, soyadı, adresi, telefon numarası, seçmen numarası, seçim bölgesi numarası gibi bilgiler yer alır.

Kayıt Doğrulayıcısı (Registration Verifier (RV))

Tüm RV'ler(Kayıt Doğrulayıcısı) VRDB'nin bir kopyasını bulundururlar ve bunu dekripto edecek bir smartkarta sahiptirler. RV, oy kullanma hakkı olan seçmenleri bu kopyayı kullanarak doğrular.

Öncelikle seçmen, seçimi başlatmaya yarayan bir flag ve yazıcı çıktısıyla (token) yetkilendirilir. Bu token benzersiz bir numara (unique number), pusula numarası, zaman pulu (time stamp), seçim bölgesi numarası, RV numarası ve hem insan hem de makine tarafından okunabilen barkod şeklinde RV dijital imzası içerir.

Seçmen başarılı bir biçimde oyunu kullandıktan sonra, Seçim kiosku seçmenin oturumunu kapatmak için bir paket gönderir (voted packet). Böylece RV her seçmenin ve oturumun kayıt bilgisine sahip olur.

Seçim Kiosku

Seçim Kiosku seçim işleminin gerçekleştiği yerdir. Seçmen, oy verme işlemine başlamak için token'ı yuvaya yerleştirir. Kiosk, seçmen oyunu başarılı bir biçimde kullanana kadar bu token'ı içerde tutar. Kiosk, token'ı içeri aldıktan sonra, üzerindeki bilgileri kontrol ettikten sonra token'ın geçerli olup olmadığına bakar.

Pusula belirleyicisi (identifier), seçmen ana bölgesinin seçmen bölge kimliği, ülke, posta kodu ve parti ilişkisine göre doğru olarak seçilmesini olanaklı kılan bir tanımlayıcıdır. Bölge için hazırlanmış tüm seçim pusulaları her kioskta, bir ROM'a (Sadece Okunabilir Bellek) önceden yüklenir. Bu her yeni seçmenin yeni bir pusulayla işlem yapabilmesini sağlar. Pusulalar, kendilerine özgü yardım formatlarıyla XML formatında kodlanırlar. Doğru pusulaya erişildikten sonra, seçmene pusulayı doğrulamasını veya kioskun yardım dokümanını kullanmasını

belirten bir seçim ekranı sunulur. Eğer pusula yanlış olarak listelendiyse, kiosk bir seçim görevlisinin seçmene yardımcı olması sağlamak üzere uyarı sinyali verir. Eğer doğru pusula listelendiyse, seçmen oy verme işlemine başlayabilir. Eğer seçmen kioskun yardım dokümanını kullanmayı tercih ederse seçim işleminin detaylarını anlatan yardım ekranlarıyla karşılaşır.

Oylama işlemi süresince seçmen, seçim görevlisinden yardım isteyebilir ve seçim işleminde zaman sınırlaması yoktur. Seçmen her ofis için bir aday seçer ve yaptığı seçimleri görebilir. Seçim işlemi tamamlandıktan sonra, bir doğrulama ve özet sayfası görüntülenir. Bu aşamada seçmen oylarını dikkatlice gözden geçirmelidir. Eğer seçmenin yapması gereken değişiklikler varsa bunları yapar. Seçmen doğrulama-özet sayfasını tamamen tercihlerine uygun olarak görüntüledikten sonra "Kabul" tuşuna basar. Bu seçim doğrulama-özet sayfasının çıktısının alınmasını sağlar. Bu aşamada seçmen görsel olarak doğru adayları seçip seçmediğini bir kez daha inceleyerek gözden geçirebilir. Bu aşamada seçmenin pusulayı değiştirme hakkı vardır. Eğer seçmen yanlış oy kullandıysa, bu pusulanın kullanılmayacağını belirtmek için alınan çıktıya alt başlık olarak 'Reddedildi' ibaresi eklenir ve kullanıcı yeniden pusulayı değiştirmek üzere ekranda doğrulama-özet sayfasını görür. Fakat seçmen bu aşamada doğru karar verdiğini düşünürse çıktı olarak alınan pusulanın alt başlığına 'Kabul Edildi' ibaresi eklenerek çıktı alınır. Çıktı olarak alınan pusula ayrıca zaman, kiosk ve alan bilgisini içerir.

Seçim kiosku pusulayı kriptolamak için CBC modunda AES kullanan 128-bit oturum anahtarı kullanır. Bu oturum anahtarı daha sonra RSA kullanılarak oy tasnifleyicisinin kamusal anahtarıyla (public key) kriptolanır.

Son olarak tüm paket dijital olarak oylama kioskunun özel anahtarıyla işaretlenir. Artık geçerli oy, pusulanın CD'ye yazılmasıyla hafızadan atılmıştır. Bu donanım dağılımı tüm kiosk pusulalarının kaybedilmesi riskinin ortadan kaldırılması için gereklidir. Ayrıca, donanım dağılımı, çıkarılabilir disklerle oy tasnifinde yardımcı olur.

Çıktı olarak alınan pusula 'Kabul Edildi' alt başlığıyla işaretlendikten sonra, seçmen token'ı aynı alt başlıkla işaretlenir. Seçmen token'ın üstüne başlık yazıldıktan sonra,

token'ın geçersiz hale gelir ve bu seçim kioskunun yuvasından ayrılmasını sağlar. Seçmen token'ı artık seçmenin seçim zamanı, yer ve kiosk bilgisini içeren fiziksel bir fiş (receipt) durumundadır. Bu fiş seçmenin yeniden pusulaya erişmesine kesinlikle olanak vermez.

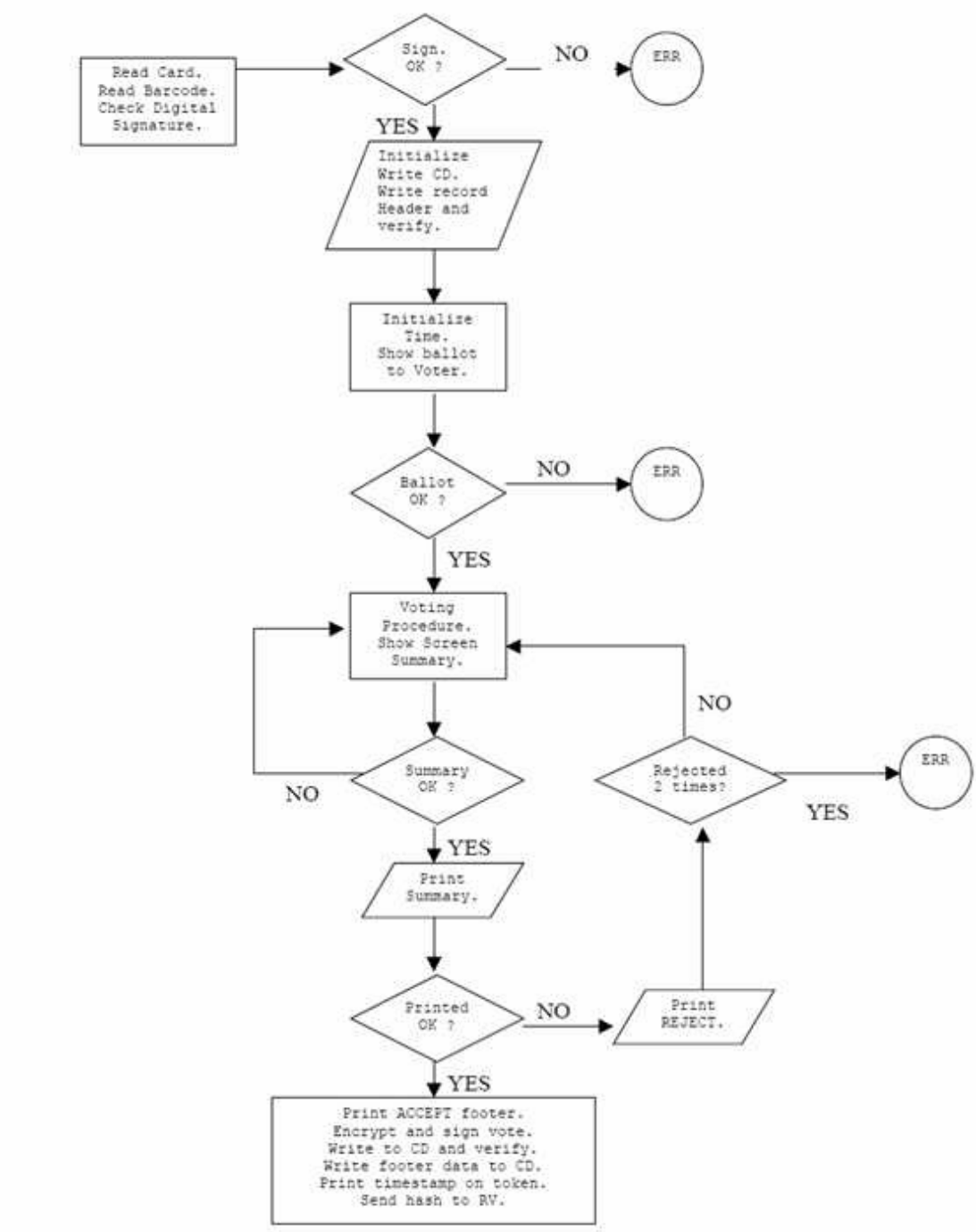
Başlık token* denilen bir parçaya yazılırken, önemli adımlardan biri oylama kiosku içinde gerçekleşir. Kiosk, seçmenin oylama işlemini doğru şekilde tamamladığını belirten aynı başlığı tek yol (one-way) network bağlantısı üzerinden VR(Seçmen Kayıt Veritabanı)'ye gönderir. Bu adım VR'deki seçmen oturumunu kapatır. Bu adım, daha çok oturum, pusula ve oy kullanma işlemlerini gerçekleştiren seçmenlerin sayısının belirlenmesini sağlar. Tek yönlü (one-way) bağlantı, VR'nin seçmen, seçim kiosku veya sayım pusulasıyla ilgili bilgileri sızdırmamasını garanti altına alır.

Seçim alanı kapandıktan sonra, kiosk pusula CD'sini dijital olarak imzalar ve kalan boşluğu veri doğruluğunu sağlamak için özgün bir sırayla doldurur.

Oy Tasnifleyicisi

Bir eyalette bulunan her şehirde bir oy tasnif merkezi konumlandırılmıştır. Seçim gününün sonunda, pusula CD'leri oylama kiosklarından alınarak güvenilir bir seçim görevlisine teslim edilirler. Seçim görevlisi, resmi oy sayımı için pusula CD'sini merkezdeki ofise götürür. Sayım (tasnif) işleminden önce Pusula CD'sinin güvenilir ve izin verilen bir kiosktan geldiği doğrulanmalıdır.

* Token : Kağıt, metal yada plastikten yapılmış jeton .



Şekil 3.3: Kiosk Veri Akış Diyagramı [26]

3.2.2.2. Değerlendirmeler

Bu mimarinin tasarım grubu projeyi sonlandırırken kullanılabilirlik, verimlilik, yazılı fişlerden bağımsız olma, doğrulanabilirlik, gizlilik, güvenlik, maliyet, ağda kullanılan cihazlar ve tek başına kullanılan cihazlar, hard disk ve ROM kullanılması gibi konuları değerlendirmiştir.

Bu elektronik seçim sisteminin başarılı olabilmesi için, seçimle ilgili temel işlevlerin yürütülmesiyle birlikte, kullanımının da kolay olması gerekir. Eğer önerilen oy kullanım şekli seçmenlerin daha önce kullandıklarından çok farklıysa, bu caydırıcı olabilir ve seçmenlerin oy vermekten çekinmeleri sonucunu doğurabilir. Bu göz önünde bulundurularak proje grubu en az sistemin verimliliği kadar kullanılabilirliği üzerinde de durmuştur. Bu sistemin verimsiz olması olarak algılanmamalıdır, fakat bazı görünümler sistemin daha verimli çalışacağı şekilde uygulanabilir. Özel bir tasarım seçilmesinin sebebi bunun oylama işleminde olumlu bir etkide bulunabilecek olmasıdır. Örnek olarak, seçilen pusula taslağı her bir aday veya partinin ayrı bir ekranda görünmesini gerektirir. Programcının bakış açısına göre, tüm adayların tek bir ekranda görüntülenmesi daha etkili gibi görünse de, bu seçmenin kafasının karışmasına ve pusula seçimlerinde hatalar yapmasına sebep olabilir. Ayrıca seçmenin pusulasını bir kağıt çıktısında görmesine izin verilmesi ve kabul, ret ifadelerinin burada görüntülenmesi sisteme fazladan işler yükleyen gereksiz aşamalar olarak görülebilir, fakat böyle bir yöntem izlenmesinin çeşitli sebepleri vardır. Böyle bir yardım sadece pusula sayımlarının doğruluğunu kesinleştirmekle kalmaz, ayrıca seçmenin kendi seçimlerinin makine tarafından doğru kaydedildiğini görmesini sağlayarak sisteme güveninin artmasını sağlar.

Karşılaşılan bir diğer problem ise seçmene herhangi bir çıktı vermeden, seçmenin, kullandığı oyun doğru bir biçimde sayıldığını kontrol edebilmesidir. Bu ikisi arasında seçim yapmaya çalışırken, amaç seçmenin kullandığı oyun sayıldığını kesin olarak bilmesini sağlamaya çalışmaktır. Bununla birlikte, bu şekilde çalışan güvenli bir sistemin düzenlenmesi mümkündür, fakat oldukça zordur, bunun için çıktı vermeden seçmenin doğrulamayı yapabilmesi düşüncesinin sistemde uygulanması üzerine odaklanılmıştır. Sistemin seçmene seçim işlemini tamamlandıktan sonra bir seçmen fiş (receipt) vermesinin, seçimle ilgili yapılacak usulsüzlüklere olanak sağlayıp sağlamayacağı, üzerinde durulması gereken bir noktadır.

Bütün sistem tamamen tasarlandıktan sonra, böylesi bir sistemin gerçekte uygulanmasının oldukça pahalı olduğu fark edilmiştir. Kiosklar, dizüstü bilgisayarlar, yazıcılar, kağıt kriptolama araçları ve kullanılan seçim tekniklerinin geliştirilmesi için oldukça yüksek miktarda para gerekmektedir.

Bir ağ bağlantısı olmadan tek tek bilgisayarlarla çalışılması böyle bir tasarım için çok olumsuz bir özelliktir. Önceden yüklü veritabanlarına sahip olan makineler gerektirmeyen bir ağ bağlantısının kullanılması verimliliği artırır. Bununla birlikte ağ olmadan makineler kullanılması istenmesinin temel sebebi kullanılabilirliktir. Maryland'de 1600'den fazla seçim bölgesi bulunmaktadır ve günde binlerce sorgu yapmak için bir merkezi veritabanında her bir seçim bölgesinde fazladan 4 kiosk bulunması pratik bir çözüm değildir. Seçim süresince verinin mümkün olduğu kadar yerel olarak depolanması daha verimli bir çözümdür.

Maliyetler gerçekten sorun olmaya başladığından beri bu token'ların tekrar kullanımı üzerinde durulmaya başlanmıştır. Bu ise doğru bir şekilde yapılamazsa büyük bir karmaşaya neden olur. Ayrıca doğru olarak yapılsa bile verinin dışarı sızması riski büyüktür. Bu yüzden bir fişin (receipt) kullanılması olumlu bir sonuç doğurmuştur. MIT bildirisi tüm token'ları kullanıldıktan sonra elde tutulmasını önerir, fakat pratikte bunun uygulanması çok güçtür [24]. Sadece okunabilir hard diskler kullanılması mümkün olmakla birlikte, bunlardan binlerce yaratılması maliyet açısından etkili bir yöntem değildir.

3.2.3. E-Vox Mimarisi

Mark A. Herschberg, MIT'de yaptığı bir çalışma sonucunda bu mimariyi geliştirmiştir. Amaç World Wide Web teknolojisi üzerinden kriptografik araçları kullanarak elektronik bir seçim sisteminin uygulanmasıdır. [26]

Fiziksel Sistemlerle İlgili Varsayımlar

Aşağıdaki varsayımlar E-vox'un çalışacağı bir ağ için gereklidirler.

1. İletişim kanalları TCP/ IP gibi düşük düzey veri doğrulaması sağlarlar.

2. Sunucularda JDK 1.1 veya daha üstü vardır

3. Host makineler de Java 1.1 (veya üst versiyonunu) destekler ve (imzalı) appletlerin çoklu hostlara bağlanmasına izin verir.

4. Host makinelerinin açık bir şekilde üzerinde gerçekleştirilen işlemleri kaydetmeyecek kadar güvenilir olmaları gerekir.

3.2.3.1. E-Vox'un Protokolü

E-Vox, Fujioka ve arkadaşlarının "A Practical Secret Voting Scheme for Large Scale Elections" adlı çalışmalarını kendisine temel almaktadır [21]. Çalışma gizli oy sistemine dayalı bir seçim işleminin matematiksel altyapısını açıklar. Bununla birlikte tam bir uygulama için pek çok detayın ucu açık bırakılmıştır.

Fujioka ve arkadaşlarının protokolü Yönetici Sunucu, Sayıcı Sunucu ve Seçmen'den (istemci) oluşur. Çoğu elektronik seçim protokolünde olduğu gibi bu protokol de bir anonim kanal kullanılmasını gerektirir. Seçmen kimliğini doğru şekilde belirttikten sonra Yönetici Sunucu işlenmiş ve körleştirilmiş pusulayı seçmene verir. Daha sonra, seçmen oy kullanabilecekler listesinden çıkarılır. Protokolün sonunda, Yönetici Sunucu işlenen körleştirilmiş pusulaları listeler ve bu pusulalar imzalanarak seçmenlere verilir. Seçmen bu imzayı Sayıcı Sunucu için, oy kullanabileceğini ispatlamak üzere kullanır. Oy, Sayıcı Sunucu'ya anonim bir kanal üzerinden yollanır. Sayıcı Sunucu'nun pusulaları seçmenden aldığı anda eşleştirmesi mümkün değildir. Buna rağmen Sayıcı Sunucu, Yönetici Sunucu'nun imzasını taşıdıkları için oyları sayar. Oy gerçekte iki parça olarak gönderilir. İlk olarak Yönetici Sunucu tarafından işlenen pusula anonim olarak Sayıcı Sunucu'dan geçer. Sayıcı Sunucu oyun geçerli olduğunu bildiği sürece bu durum işleme şemasını bozmaz. Protokolün sonunda işlenen pusulanın bir listesi, Yönetici Sunucu'nun imzası ve işlemeyi geriye almak için kullanılan anahtarlar açık olarak gönderilir.

Fujioka'nın sisteminde de listelenen detaylar aşağıdaki gibidir.

1. Seçmen adayını seçer ve pusulayı işler.

2. İşlenen pusula körleştirilir (blinding) edilir ve seçmen tarafından imzalanır sonra Yönetici Sunucu'ya gönderilir.

3. Yönetici Sunucu seçmenin oy verip veremeyeceğini ve körleştirilmiş (blinded) oyun doğruluğunu kontrol eder. İmza geçerliyse, Yönetici Sunucu işlenen körleştirilmiş pusulayı imzalar, imzalı pusulayı geri gönderir ve işlemin günlüğünü oluşturur.

4. Kullanıcı pusulayı körleştirilmişliğini ortadan kaldırır (unblind) ve blinding özellikleri nedeniyle geçerli ve işlenmiş olup olmadığını anlamak için Yönetici Sunucu'nun imzasını doğrular.

5. İşlenen pusulalar, artık Yönetici Sunucu tarafından imzalanmıştır, ve indeks numarasıyla birlikte yayınlanan Sayıcı Sunucu'ya anonim bir kanal üzerinden gönderilirler.

6. Tüm işlenen oylar içeriye gönderildikten sonra, seçmenler oylarının listelenip listelenmediğini ve tüm oyların geçerli imzalara sahip olup olmadığını teyit ederler.

7. Herkes, Sayıcı Sunucu'nun yayınladığı listede girişlerini onaylama fırsatı bulduktan sonra, her bir seçmen işlenen oyun indeksi üzerinden işlemi tersine çeviren anahtarları gönderirler. İletişim yine anonim bir kanal üzerinden yürütülür.

3.2.3.2. Fujioka Sisteminin Analizi ve Eleştirisi

E-Vox Sistemini geliştirenler Fujioka Sistemi'nde yeterince açıklanmamış dört konu olduğunu ileri sürmüşlerdir.

1. Belgeleme (Doğruluğunu Kanıtlama): Açıkça belirtilmemesine rağmen belgeleme, dijital bir imzalama kullanarak Yönetici Sunucu tarafından oy veren kişinin belgelemesi gerektiği zaman istenir.

2. İletişim: Hiçbir haberleşme konusu dikkate alınmamıştır. Buna mesajın alı konması, gönderim süresince verilerin karışmasının önlenmesi ve anonim kanalın kendisi de dahildir.

3. Anahtarlar: Sunucular arasındaki anahtarların dağıtımı açıklanmamıştır.

4. Hatalar: Alındı fişlerinin (receipt) ve sunucu kütüklerinin nasıl kullanılacağından bahsedilmesine rağmen, bunun için biçimsel bir yöntem tanımlanmamıştır.

Doğrulama (Authentication)

Seçmenin kimliğinin teşhisi için iki seçenek düşünülmüştür. Bunlardan biri kamusal anahtar sistemi diğeri de kripto sistemidir. Birinci seçenek (kamusal anahtar sistemi) iki sebepten dolayı tercih edilmemiştir. Birinci sebep, en yüksek önceliğin kullanım kolaylığına verilmesidir. Şifreler, dışarıdan biri için bile alışılmış ve kabul edilmiş bir kavramdır. Kamusal anahtarlar ise daha az alışılmış ve çok kafa karıştırıcı bir olgudur. Aynı zamanda kamusal anahtarların imzalanma işlemi için yüzlerce bitin dizilişi gerekmektedir. İkinci sebep ise kamusal anahtar sisteminin önceden kullanıcıda bulunması ya da anahtarlar güvenli bir ortamda dağıtılması zorunludur. Anahtarların dağıtılması işlemi genellikle seçmenin kayıt işlemi sırasında anahtarlarını almasına karşılık gelir. Ki bu, seçmenin hafızada tutulması zor sayıları hatırlamasını ya da bazı güvenli elektronik iletim sınıflarına sahip olmasını gerektirir. Teknik olmayan kullanıcı açısından olaya yaklaşıldığında, şifrelerin hatırlanması ve kullanılması daha kolaydır. Fakat sistem çok modüler bir sistemse, geçici olmak kaydıyla kamusal anahtarları kullanarak sisteme, belgeleme alt sistemi yerleştirilmedilir.

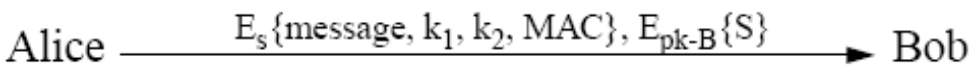
İletişim (Communication)

Fujioka ve arkadaşları tarafından önerilen protokolde, basit haberleşmeler (isimsiz bir kanal gerektirmeyen türde olanlar) pasif bir saldırgandan korunmayı sağlayan yeterli kriptografik bir korumaya sahiptir. Adı geçen pasif saldırgandan kasıt, gönderilen mesajı görebilen ama mesaj üzerinde değişiklik yapamayan kimselerdir. Gerçekte haberleşmeler çok daha karmaşıktır ve çoğu kötü niyetli kişiler tarafından izlenmekte ve kesilmektedir. Bu sayılanlar herhangi biri haberleşmede gerçekleşebilir. Gizlice dinlenmeye ek olarak, haberleşme kanalı gürültülü olabilir, bunun sonucunda mesajın tümü ya da bir kısmı bozulabilir ya da kaybolabilir veya mesajların bir kısmı ya da tümü başka bir mesajla karışabilir. Bu tür istenmeyen

etkilere karşı koymak için, haberleşen iki taraf (örneğin Seçmen ve Yönetici Sunucu) arasında güvenli iletişimi sağlama amacıyla aşağıdaki protokol kullanılmalıdır.

1. Güvenli Kanallar (Secure Channels)

Alice'in, mesaj gönderecek kişi, rasgele sayı üreticine; alıcı kişi olan Bob'un da kamusal anahtarına gereksinimi vardır. Alice Bob ile iletişimi kurmuş olsun(TCP soketi açılır.)



Şekil 3.4: Güvenli Mesaj Aktarımıs

E-Vox tüm haberleşmeyi kriptolamak amacıyla Bruce Schneier tarafından geliştirilen bir blok kriptolayıcı olan Blowfish* kullanmaktadır. Şekil 7'de Alice S adında bir oturum anahtarı (Blowfish anahtarı) oluşturur. Oluşturulan bir rasgele bayt (byte) dizisidir. Alice bunun yanı sıra doldurma (padding) amacıyla k1 ve k2 adında iki rasgele byte dizisi daha üretir. Bu byte dizileri (mesajla berber gönderilir) daha sonra MAC (Mesaj doğrulama kodu) oluşturmak amacıyla kullanılır. Mac bir HMAC-SHA olup bu dizilerin karıştırılmasıyla oluşturulur. Amacı ise gönderim süresince bitlerin doğruluğundan emin olmaktır. Mesaj (padding anahtarları) ve MAC daha sonra Blowfish kullanarak kriptolanır. İlk başta oluşturulan Blowfish anahtarı ise alıcının kamusal anahtarı ile kriptolanır. Daha sonra bunların tümü sırasıyla (önce kriptolanan mesaj ve MAC daha sonra kriptolanan Blowfish anahtarı gönderilir) Bob'a gönderilir. Bob gönderinin ikinci kısmını çözerek Blowfish anahtarını elde eder. Bu anahtarı mesaj ve dolgu (padding) anahtarlarını almak için kullanır. Aynı zamanda Bob mesajı ve anahtarları karıştırarak iletişimin doğruluğunu onaylayabilir. Rasgele bir anahtar düzenli bir karıştırma için yeterlidir.

Gizlice dinlenme olayından korunma, Blowfish algoritması kullanılarak sağlanmıştır. TCP katmanı gürültüye ve nadiren gerçekleşen paket kaybına karşı korunma sağlar.

* Blowfish : Bruce Schneier tarafından geliştirilmiş, 64 bitle 448 bit arasında değişen büyüklükteki anahtar bloklarını kullanan bir blok şifreleyicidir.

MAC ise, mesaj paketlerinin, fark edilmeden gerçekleşen kısmi yer değiştirmelerini veya kayıplarını engeller. Güvenli ya da değil haberleşmelerimizde alınan ve gönderilen kodlar zaman-aşımı fonksiyonları kullanmamızı gerektirir. Sonuç olarak, bu protokol toplam mesaj yer değiştirmelerini yakalayamaz. Tekrarlanan ataklar (örneğin oyların toplandığı kutuyu doldurmaya yönelik) etkisizdir. Yönetici Sunucu bir imza için seçmen başına bir oy kabul edebilir.

Eğer seçmenden Yönetici Sunucu'ya gelen oy ya da talep tekrarlanırsa, Yönetici Sunucu bu oyu kabul etmez ve yetkili kişiye bunu bildirir. Tekrarlanan tüm mesajlar sunucu tarafından Sayıcı Sunucu'ya iletilir. Fakat Sayıcı Sunucu, tekrarlanan hiçbir oyu kaydetmez, böylece oyun yeniden sayılma işlemi başarısız olur. Bu tür saldırılar, kriptografi kullanılarak başarısız kılınırken, yine de istenilen bir durum değildir. Tekrarlanan mesajlar zaman, bant genişliği ve hesaplayıcı güç kullanımının israfına yol açar. Daha genel saldırılara karşılık vermek ve sistemdeki mesajları kısıtlamak için Kara Liste Tutma Yöntemi (blacklisting methode) uygulanabilir.

2. Anonim Kanallar (Anonymous Channels)

Fujioka ve arkadaşlarının sisteminde belirtilmeyen en önemli konulardan birisi de anonim kanallardır. Mesajlar bu kanallar içinden taşınması gerekmektedir. Bu kanalların optimize edilmesini sağlayacak varsayımlara ihtiyaç vardır. Bu varsayımlar;

1. Her seçmenin tek oy hakkı vardır.

2. Bilgi akışı tek yönlü olmalıdır, böylece gönderenin adresi hakkında hiçbir bilgi mesaj gönderilmesine gerek yoktur.

3. Mesajların tümü yaklaşık olarak aynı büyüklükte olmalıdır.

4. Tüm mesajlar sabit ve kısa bir zaman aralığında gönderilmelidir.

5. Mesajların alınabilmeleri için sadece teslim tarihine gereksinimleri vardır. Bunun dışında, kronolojik sıralamaya ya da benzeri sıralama gereksinimlerine gerek yoktur.

Bu düşünceyle, anonim kanal, güvenli iletişimin sağlanması için tek bir sunucu kullanır. Özellikle, seçmen ile Yönetici Sunucu arasındaki güvenli bağlantıyı, seçmen ile Sayıcı Sunucu arasındaki güvenli bağlantıdan yalıtmak gerekmektedir. Seçmen tek bir nesneyi alır ve bunu oy ile beraber kriptolar, aynı zamanda Blowfish oturum anahtarını kullanarak çırpı (hash) anahtarlarını ve MAC'i oluşturur. Daha sonra seçmen, Sayıcı Sunucu'nun kamusal anahtarı ile oturum anahtarını kriptolar. Kriptolanmış bu iki parça Yönetici Sunucu'ya güvenli haberleşme ortamı içerisinde mesaj olarak gönderilir.

Oy kullanma süresi sonuna kadar olmak kaydıyla Yönetici Sunucu güvenli bir ortam içerisinde oyları kabul eder. Daha sonra Yönetici Sunucu nereden gönderildikleri hakkında hiçbir bilgi olmaksızın bu oyları saklar. Oy kullanma işlemi süresinden çok kısa bir zaman sonra sunucu bu oyları karıştırır ve Sayıcı Sunucu'ya iletir.

Sonuç olarak, mesajların seçmenden Yönetici Sunucu'ya gönderimi ile Yönetici Sunucu'dan Sayıcı Sunucu'ya gönderimi sırasında hiçbir zaman analizi yapılamaz.

3. Serileştirme (Serialization)

Tüm nesneler haberleşme kanallarından seri olarak (byte dizileri şeklinde) iletilir. Hiçbir nesne, dizi haline getirilmez. Nesnenin yapısı (içindeki veri ile birlikte) özel sınır baytları (byte) kullanılarak kaydedilir. Böylece nesne kolayca gönderilebilir ve kanalın bitiminde tekrar eski haline getirilebilir.

Anahtar Dağıtımı (Key Distribution)

Anahtar dağıtımı kriptografide karşılaşılan yaygın bir sorundur. Sorulması gereken soru siyasi partiler bu anahtarları seçmenlere nasıl ulaştıracaktır? Seçmen gönderilen anahtarın geçerli olduğundan nasıl emin olacaktır? Ve gönderim esnasında herhangi birinin anahtarı değiştirmesi nasıl engellenecektir? Bunun için uygulanacak çözüm özellikle bu amaç için tasarlanmış güvenli bir kanal kullanmaktır.

E-Vox paketine bir RSA anahtar üretici eklenmiştir. Seçim başlamadan önce her sunucu kendi anahtar çiftini yaratmalıdır. Bu anahtar takımları durum uygun olursa sunucular arasında karşılıklı olarak iletilebilir. Başlangıçta, tüm sunucular kendisininki de olmak üzere tüm anahtarlara sahip olacaktır. Önceden sunucular

tarafından hazırlanmış güvenli bir kanal aracılığıyla karşılıklı olarak iletilir. Başlangıçta bozulmuş bir sunucunun dağıttığı geçersiz anahtarlar derhal seçim merkezlerince belirlenmelidir.

Hata Bulma ve Yanıtlama (Error Detection and Response)

Fujioka ve arkadaşlarının çalışmasında açıklanmış işlem, protokolde gerçekleşmiş herhangi bir hile ya da yasa dışılığın gerçekleşmesine olanak vermektedir. Örneğin ikinci etap sonrası Sayıcı Sunucu, Yönetici Sunucu'nun tasdik ettiği sayıdan daha fazla oy sayabilir, ki bu sayı, oylar sayılmadan ve açılmadan önce bilinir.

E-Vox'un yaptığı bu değişikliklerde, bu tür hatalar seçim sonuçlanana kadar belirlenemez. Aynı zamanda bu değişiklikler ile seçmenin, özel bir çalışma-istasyonundan oy kullandığını varsayılırsa, hatayı tanımlamasına gayret edilmesini ve eğer hata varsa en uygun bir bilirkişiye bildirmesini önermektedir. Applet ve Sunucu kodları farklı türdeki hataları tanımlama ve otomatik olarak bu hataları analiz eden Yönetici Sunucu'ya hataları gönderme yeteneğine sahiptir. Sunucular da aynı zamanda şüpheli olduğundan, kendi hatalarını tutabilmektedir. Yönetici Sunucu'nun kendisi de sonuçta diğer kişiler tarafından gözetlenebilmektedir. Seçim süresince ve seçim sonuçlandıktan sonra şikayetlere en uygun yanıtları vermek zorundadırlar. Örneğin, seçmenlerin yarısı Yönetici Sunucu geçersiz bir imza aldıklarını iddia ettiklerinde hemen o sunucunun kapatılmasını ve hakkında araştırma yapılmasını isteyebilirler. Diğer tarafta binlerce seçmen Yönetici Sunucu'ların ikna edici bir sebep göstermeksizin bağlantılarını reddettiğini iddia ederse, gürültülü haberleşmeyi suçlu olarak gösterebilir ve bu sorunu önemsememeyi seçebilir.

3.2.3.3. E-Vox

E-Vox'u geliştirenler Fujioka ve arkadaşlarının geliştirdiği protokolü revize etmişler ve kendi sistemlerini oluşturmuşlardır.

Bu protokolün adımları sırasıyla aşağıda verilmiştir.

1. Seçmen kendi adayını seçer ve aday oy pusulasına HMAC-SHA kullanarak işlenir.

2. Sonra işaretlenmiş oy pusulası seçmen tarafından körleştirici faktör kullanılarak körleştirilir ve güvenli bir haberleşme ortamı içerisinde ismi ve şifresini de pusulaya ekleyerek Yönetici Sunucu'ya gönderilir.

3. Yönetici Sunucu seçmenin oy kullanma hakkının olup olmadığını ve ile şifresinin doğruluğunu kontrol eder. Yönetici Sunucu daha sonra körleştirilmiş ve işaretlenmiş pusulayı imzalar. Daha sonra imzalanmış pusulayı seçmene geri gönderir (Seçim süresinin bitiminden sonra yet. Yönetici Sunucu seçmenin isimlerini, körleştirilmiş pusulalarını ve imzalarını halka açıklar).

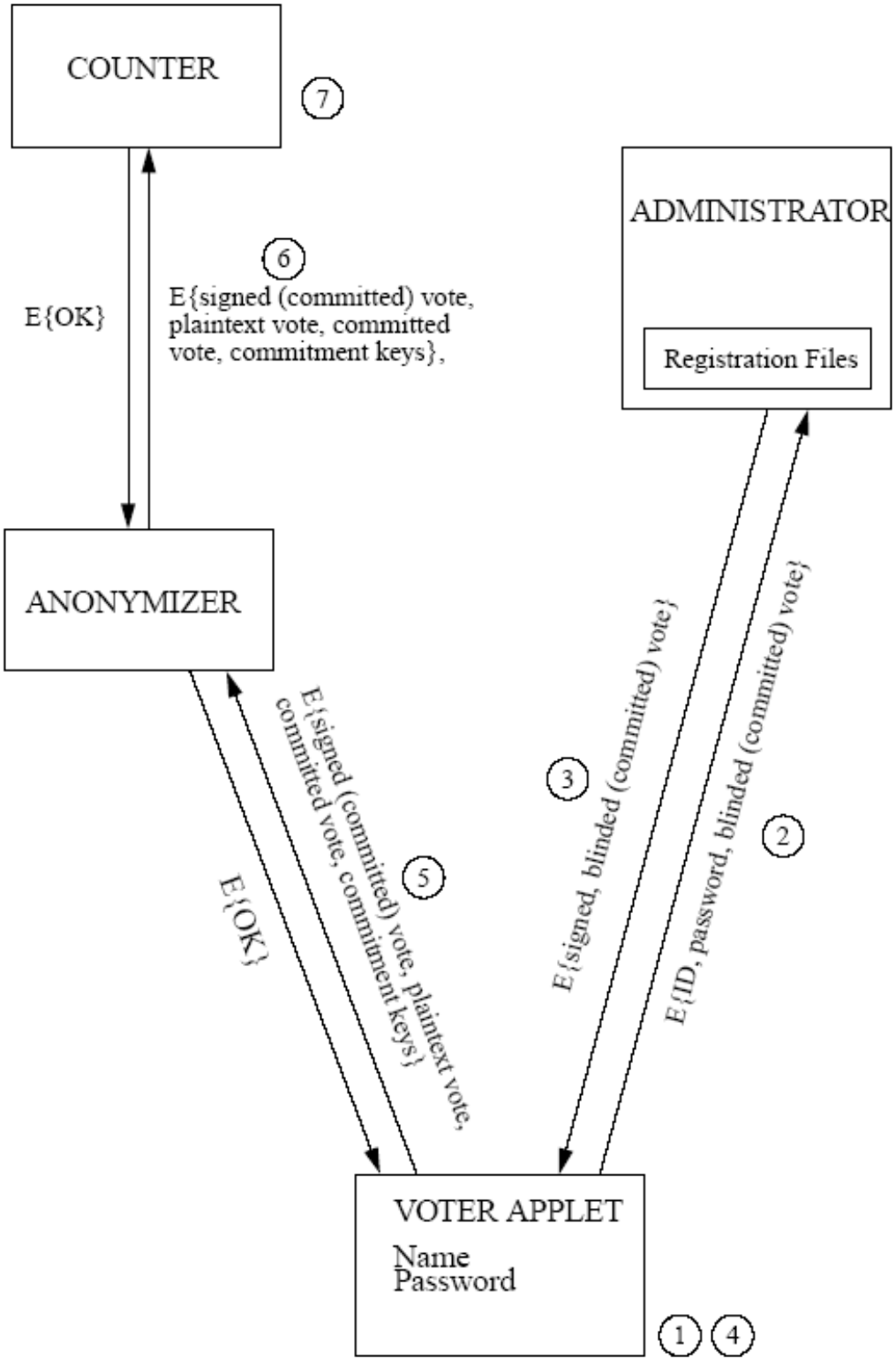
4. Seçmen, Yönetici Sunucu'nun imzasını doğrular ve pusulayı tekrar eski haline getirir.

5. Yönetici Sunucu tarafından imzalanmış pusulayla imzalanmamış pusulayı, basit metin formatı (plaintext) ve bağlantı anahtarlarını iki katmanlı güvenlik kanalından Anonimleştirici Sunucu'ya gönderir.

6. Tüm oylar isimsiz sunucu tarafından alındıktan sonra karışık bir şekilde sıralanır ve Sayıcı Sunucu'ya gönderilir.

7. Sayıcı Sunucu, Yönetici Sunucu'nun imzalarını doğrular ve oyları sayar. Bunun sonrasında Sayıcı Sunucu halka oy pusulalarını, bağlantı anahtarlarını ve imzalanmış oyu sunar.

Aşağıdaki şekilde E-Vox'un işleyişini gösteren bir şekil yer almaktadır.



Şekil 3.5: E-Vox Akış Diagramı [27]

Seçmen, adayını seçer ve bir oy nesnesi hazırlar, bu oy nesnesi adayının yer aldığı oy pusulasını içerir. Bu oy pusulası sonra bir çırpı (hash) fonksiyonu kullanılarak gönderilir. Özel olarak, iki anahtar gerektiren HMAC-SHA kullanılır. Bu çırpı işlemi, imzalama gerektiren, sabit boyutlarda daha küçük mesajlar oluşturur.

Çırpı işlemi daha sonra körleştirilir ve imzalanması için Yönetici Sunucu'ya gönderilir. Yönetici Sunucu seçmenin oy kullanma hakkı ile şifresinin doğruluğunu kontrol eder ve daha önce oy kullanıp kullanmadığına bakar. Eğer seçmenin oy kullanmasına engel olacak bir durum görülmezse, makam körleştirilmiş oy pusulasını imzalayarak seçmene geri gönderir. Seçim tamamlandıktan Yönetici Sunucu seçmenin adını, körleştirmiş olduğu oy pusulasını ve üzerindeki kendi imzasını kamuya açıklar. Seçmen imzalanmış oyu aldıktan sonra makamın imzasını doğrular. Ve işaretlenmiş pusuladan körleştirmeyi kaldırır (Yani körleştirme öncesi duruma getirir). Seçmen daha sonra basit metin formatındaki oyunu, anahtarlar kullanarak hazırladığı oyunu ve imzalanmış işlenmiş oyunu Anonimleştirici Sunucu'ya gönderir. Bu görüldüğü gibi bit fazlalığıdır çünkü basit metin ve anahtarlar, işlenmiş ve imzalanmış oy ile karşılaştırmak üzere işlenmiş oyu oluşturmak için kullanılır. Fakat bu fazlalık, fazladan kontrol, güvenilir olmayan insanlar ve hatalara karşı bir avantaj sağlar.

Anonimleştirici Sunucu da, Sayıcı Sunucu da cevap gönderebilir. Normal koşullar altında ikisi de 'tamam' mesajı gönderebilir. Eğer bazı olumsuzluklarla karşılaşılırsa, bir sunucu gönderene uyarı bilgisi gönderebilir. Bu yanıt protokol tarafından gerekli değildir bu yüzden de protokol listesinde açıkça belirtilmemiştir. Fakat yanıtlamalar güvenlik kontrolü için faydalıdırlar. Yanıt, gönderenin seçtiği oturum anahtarı ile kriptolanır. Daha önce ifade edildiği gibi oturum anahtarı gönderim esnasında alıcının kamusal anahtarı ile kriptolanır. Ve sadece, doğru bir şekilde kriptolanmış yanıtı oluşturmak isteyen seçilmiş alıcı bu mesajı çözebilir.

Anonimleştirici Sunucu her oyu, kaynağı hakkında hiçbir bilgi kaydetmeksizin, farklı bir dosya içinde saklar. Seçim süresi sona erdikten sonra Anonimleştirici Sunucu karışık bir sırada, güvenilir bir kanaldan Sayıcı Sunucu'ya gönderir. Alt katmandaki güvenli iletişim kanalı devrede olduğu için oylar hala Sayıcı Sunucu'nun kamusal anahtarı ile kriptolanmıştır. Tüm oyların Sayıcı Sunucu'ya gönderimi

tamamlandıktan sonra Anonimleştirici Sunucu gönderilenlerin bir listesini yayınlar. Oylar Sayıcı Sunucu'ya gönderilirken bu yayınlanan liste anonimliği sağlama adına aynı rasgele sıralamayı kullanır.

Sayıcı Sunucu ilk önce tekrarlanan oyları kaldırır. Tekrarlanan oylardan kasıt tüm bitleri aynı olan oturum anahtarları ve mesajı aynı olan oylardır. Bunu yaptıktan sonra Sayıcı Sunucu, Yönetici Sunucu'nun imzalarını doğrular ve işlenmiş ve imzalanmış oyları, işleme için kullanılan anahtarları, basit metin fomatında (plaintext) oy pusulalarını listeler. Seçim süresi bitince bu liste halka açıklanır. Herkes imzaların doğruluğunu onaylar ve bir sunucu tarafından fazladan oy eklenmezse sayım işlemi doğru şekilde yapılmış olur.

4. BİR ELEKTRONİK SEÇİM MODELİ ÖNERİSİ

Bu model, elektronik seçimler için bir prototip olarak tasarlanmıştır. Modelin amacı, bir seçimin sağlaması gereken asgari ölçütleri karşılamak, güvenlikle ilgili problemleri denetlenebilir seviyelere indirmektir.

4.1. Giriş

Seçim probleminin, önceki bölümlerde anlatıldığı gibi son derece karmaşık bir yapısı vardır. Siyasi bir konu olması nedeniyle de, içinde herkesin kuşku duyabileceği özellikler içerir.

Bu modelde elektronik seçim probleminin karmaşıklığını, Rebecca Mercuri'nin akademik olarak ifade ettiği ölçütleri temel alarak, kendi seçim modelimizde aşmayı öngörmekteyiz [5] [6] [8].

Bu modelde bazı varsayımları kabul etmemiz gerekmektedir. Bunlar;

1. Tüm seçmenler okur-yazar ve bilgisayar kullanabilirdir (computer literacy).

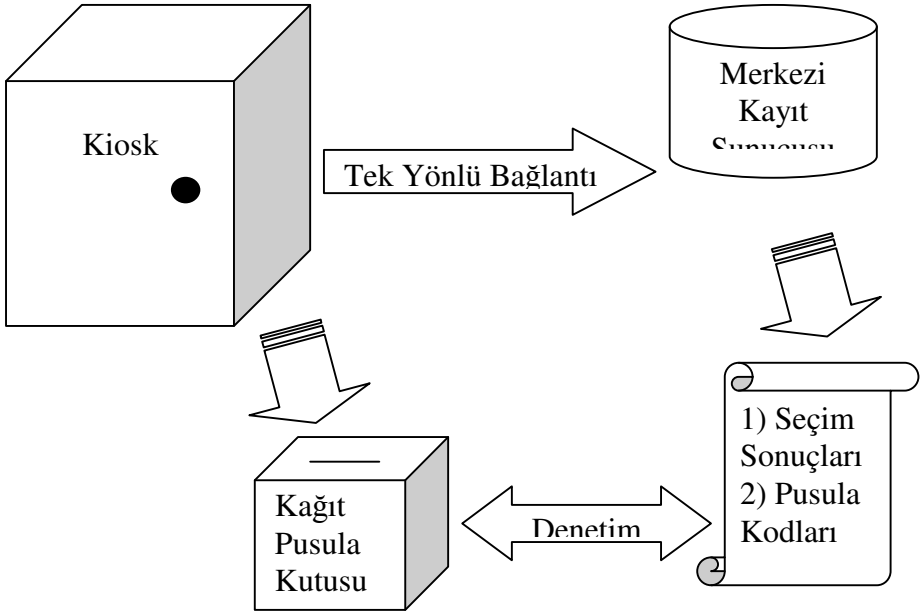
2. Tüm seçmenler görme ve işitme duyularına sahiptirler.

3. Seçmenler kimliklerini doğrulayacak kimlik kartlarına sahiptirler ve seçim sürecine bu kimlik kartlarını göstererek katılırlar.

4. Sistemin üzerinde çalıştığı iletişim hatları güvenlidir. Kioskun, Merkezi Kayıt Sunucusu dışında hiçbir fiziksel bağlantısı yoktur.

4.2. Model

Önceki bölümlerde ifade edildiği gibi, güvenlik sorunu, bir elektronik seçim sistemi için çözüme kavuşturulması gereken konuların en önemlisidir. Bu modelde elektronik seçim alanı olarak belirli noktalara yerleştirilmiş birbirinden bağımsız çalışan seçim kioskları öngörülmüştür. Şekil 4.1'de görüldüğü gibi sistem basit olarak Kiosk ve Merkezi Kayıt Sunucusu (MKS) bileşenlerinden oluşur. Kağıtı çıktı kutusu kiosklara gömülü olarak tasarlanmıştır. MKS ile Kiosk arasında Kiosk'tan MKS'ye doğru tek yönlü bir bağlantı tanımlıdır. Bu, MKS'nin herhangi bir şekilde Kiosk üzerindeki veriye bir etkide bulunmasını önler. Sistemin internet üzerinden çalışmaması, güvenlikle ilgili tehditlerin kaynaklarını önemli ölçüde azaltmaktadır. Ancak güvenlikle ilgili tehditler sadece internet kaynaklı olmamaktadır. Bir elektronik seçim sistemi hiçbir şekilde seçimin gizliliğini ihlal edebilecek bir süreç akışına izin vermemelidir. Seçimin akışı tamamen bu gizliliği temel alarak tasarlanmalıdır.



Şekil 4.1: Sistem Bileşenleri

Seçmenin sisteme doğrulanması ile ilgili güvenlik problemleri bu modelde detaylı bir şekilde tartışılmamakla birlikte, seçmenin biyolojik özellikleri kullanılarak yapılan biyometrik kimlik doğrulama yöntemleri, bu bilgilerin başka amaçlar için kullananılabileceği göz önünde bulundurularak bu sistemde önerilmemiştir. Ayrıca bir seçim için bu maliyet yükseltici bir etken olacaktır. Önerdiğimiz model , seçmenin kimlik kartını göstermesini sisteme doğrulanması için yeterli saymaktadır.

Seçmen, kimlik kartını gösterir ve bunun karşılığında isminin bulunduğu yere imzasını atar; böylece sisteme doğrulanmış olur. Görevli, seçmen için dokunmatik bir ekrana sahip olan kiosk oturumunu başlatır. Şekil 4.2'de görüldüğü gibi seçmen kioskun bulunduğu kabine girer ve ekran üzerindeki 'Dokununuz' yazısına dokunur.

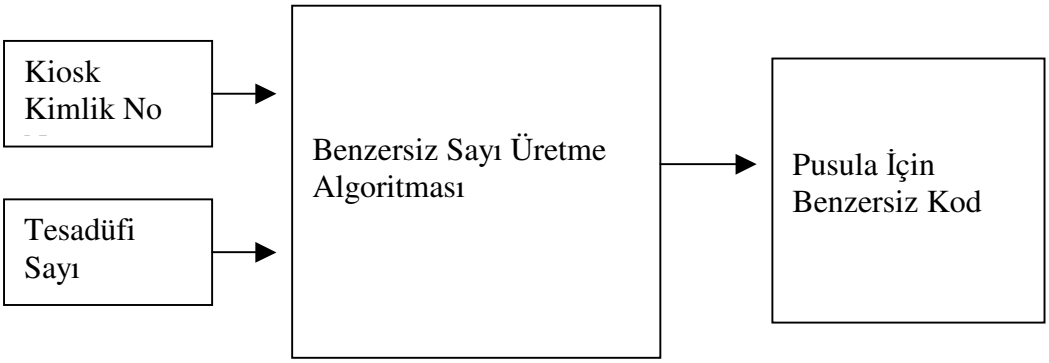
.

Şekil 4.2: Seçime başlama

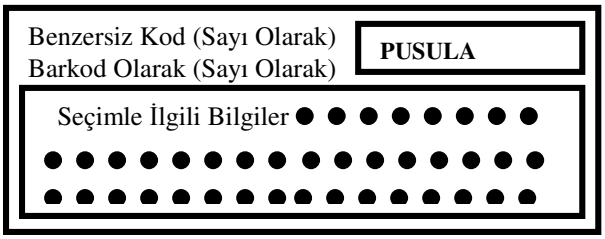
Kiosk bu işlem sonucunda Şekil 4.3'de görüldüğü gibi, seçmene, üzerine, o anda ürettiği benzersiz bir kodu bastığı, kağıt pusulayı sunar.

Şekil 4.3: Pusula Sağlanması

Kiosk her oturum için benzersiz bir koda sahip bir kağıt pusula üretmektedir. Kiosk bu kodu Şekil 4.4.'de olduğu gibi, her kioskun sahip olduğu özel kod ve tesadüfi olarak üretilmiş bir sayının birlikte girdi olarak kullanıldığı bir algoritma kullanarak hesaplar. Seçmen isterse bu kodu seçim sonucunda oyunun geçerli olarak sayılıp sayılmadığını kontrol etmek için kullanabilecektir. Bu, seçmenin pusulayı imza karşılığında seçim görevlisinden almasının yol açacağı sakıncaları ortadan kaldırmak için gereklidir.



Şekil 4.4: Benzersiz Sayı Üretimi

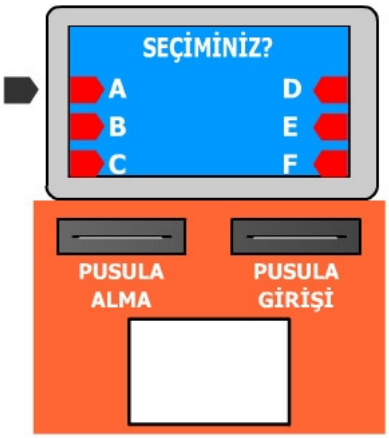


Şekil 4.5: Pusula Yapısı

Seçmen kioskun kendisine sunduğu pusulayı, kioskun 'Lütfen Pusulayı Giriş Yuvasına Yerleştiriniz' talimatı üzerine, seçmen Şekil 4.6'daki gibi pusulayı yuvaya yerleştirir.

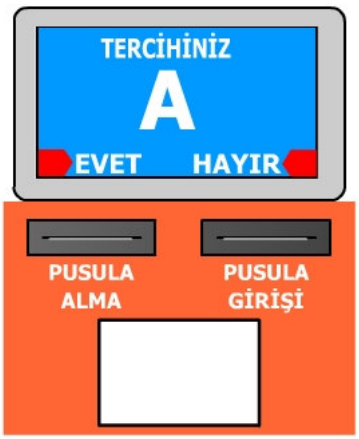
Şekil 4.6: Kioska Pusula Girişi

Kiosk üzerinde bir oturum boyunca sadece bir kağıt pusula vardır ve sadece bir seçmenin tercihleri RAM üzerinde tutulur. Kiosk güvenlik nedeniyle hiçbir bilgiyi hard disk üzerinde tutmaz. Seçmen dokunmatik bir ekran üzerinde Şekil 4.7'de görüldüğü gibi ekrandaki oklar yardımıyla tercihlerini oluşturur.



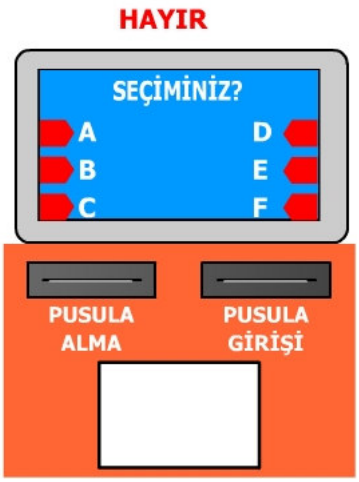
Şekil 4.7: Tercihlerin İşlenmesi

Daha sonra ekranda 'Tercihlerinizi Kontrol Edin' yazısı çıkar ve seçmenin bu yazı üzerine dokunmasıyla ikinci ekran sunulur. Bu ekranda seçmenin önceki ekranda yaptığı tercihler, kontrol etmesi amacıyla, gösterilir ve kendisine Şekil 4.8'deki gibi 'Evet' ve 'Hayır' olmak üzere iki seçenek sunulur.



Şekil 4.8: Doğrulama

Seçmen gerek görürse önceki ekrana döner ve tercihlerini düzelterek tekrar oluşturur. Seçmen ‘Hayır’ seçeneğine dokunduğunda Şekil 4.8.a’daki ekran sunulur.



Şekil 4.8.a: Tercihlerin Değiştirilmesi

Eğer seçmen tercihlerinin istediği gibi ekranda gösterildiğini görürse, ‘Evet’ yazısına dokunur. Bunun sonucunda, seçmenin tercihleri kağıt pusula üzerine basılır ve cam bir fanus içinden seçmene gösterilir. Seçmen fanustan tercihlerinin doğru bir biçimde kağıt üzerine basılıp basılmadığını kontrol ederken, ekranda ‘Pusulayı Kutuya Gönder’ ibaresi görüntülenir ve seçmene Şekil 4.8.b’deki görüldüğü gibi ‘Evet’ ve ‘Hayır’ seçenekleri sunulur.

Şekil 4.8.b: Tercihlerin Çıktıyla Doğrulanması

Seçmen eğer bir yanlışlık olduğunu fark ederse, ‘Hayır’ yazısına dokunur ve bunun sonucunda kağıt pusula iptal yazılarak ayrı bir kutuya gönderilir. RAM üzerindeki bilgiler silinir ve kiosk oturumu sonlandırır. Şekil 4.8.b.1’deki gibi ‘Oturum Kapatıldı’ ibaresi gösterilir.

Şekil 4.8.b.1: Oturumun Kapatılması

Seçmen bunu görevliye bildirir. Seçmen kiosku test kipinde çalıştırır, sonuç olumsuzsa kiosk seçim sisteminden çıkarılır. Eğer seçmen ‘Pusulayı Kutuya Gönder’ yazısına dokunursa, kağıt pusula kutuya düşer ve RAM üzerindeki pusula bilgisi tek yönlü bir bağlantıyla Merkezi Kayıt Sunucusu’na gönderilir. Sunucu, Kioskun, IP adresini ve kiosk kimlik numarasını doğrular. Gelen pusula bilgisini kayıt ettikten sonra, bu pusulanın üzerindeki benzersiz kodu da ayrı olarak kaydeder ve seçmene Şekil 4.8.b.2’deki gibi oyunun hem elektronik olarak hem de kağıt çıktısı olarak kaydedildiğini belirten bir mesaj verir. Oturum sonlanır.

Şekil 4.8.b.2: Pusula Elektronik Ve Kağıt Olarak Kaydedilir

Bu numara daha sonra seçim sonuçlarıyla birlikte geçerli oylar listesi içinde açıklanacaktır.

Tüm kiosklardan Merkezi Kayıt Sunucusu'na doğru tek yönlü bir bağlantı vardır. Seçim sonucunda Merkezi Kayıt Sunucusu seçim sonuçlarını ve geçerli olan benzersiz pusula kodlarını yayınlar. Kağıt pusulalar ise herhangi bir itiraz halinde denetim yolu (audit trail) olarak kullanılmaya hazırdır.

4.3. Sayım ve Kontroller

Merkezi Kayıt Sunucusu, seçim için ayrılan zamanın dolmasından sonra, kendisini herhangi bir kayıt işlemine karşı kilitler ve tüm kiosklardan gelebilecek kayıt isteklerini geri çevirir. Sunucu seçim sonuçlarıyla birlikte, seçmenlerin kullandıkları oyun sayılıp sayılmadığını kontrol etmelerine olanak sağlayan, sayılan oy listesini de her pusula için yaratılmış olan benzersiz numaraları yayımlar.

Seçimle ilgili herhangi bir şüphe ya da itiraz olduğunda, kağıt pusulalar her türlü denetim için ulaşılabilirdir.

5. SONUÇ VE TARTIŞMA

Önerdiğimiz model, seçmene olabildiğince tercihlerini kontrol etme hakkı vermiştir. Bu sağlanmadığında seçmen topluluğunun teknolojiyi kullanma yeteneklerine göre değişen oranda, hatalı oy kullanımı olacaktır. Sistem, seçmene kağıt pusula oluşturulduktan sonra bile, pusulayı ve oturumdaki seçim tercihlerini yok etme hakkı vermektedir. Bu, kötü niyetli seçmenlerin seçimi engellemesi gibi sorunlara yol açabilir; seçmen bu aşamada sürekli 'Hayır' seçeneğini seçebilir. Burada çözüm, seçmenlerden birisinin en son aşamadaki 'Hayır' tercihini kullanması durumunda, kioskun son derece titiz bir şekilde doğru çalışıp çalışmadığının test edilmesidir. Eğer kiosk hatalı çalışıyorsa, seçimden men edilmelidir.

Model, oyların elektronik olarak sayılmasını ve tasnif edilmesini öngörürken, herhangi bir itiraz halinde, denetim yolu olarak kağıt pusulaların saklı tutulmasını sağlamaktadır.

Günümüzde seçim ve/veya referandum oylamalarında modern teknolojiler, sanıldığından daha yaygın olarak, kullanılmaktadır. Son yıllarda elektronik seçim sistemleri üzerine yapılan araştırmalar da giderek artmaktadır. Ayrıca son dönemde bazı ülkelerde yaşanan seçim güvenilirliği tartışmaları, üniversitelerin ve akademisyenlerin bu yönde çalışmalarını yoğunlaştırmalarına neden olmuştur. Elektronik seçim konusunu çözülmesi zor karmaşık bir problem olarak tanımlayan grupların varlığının yanı sıra, özellikle çok küçük bir ilave çaba ile internet üzerinden güvenli bir şekilde gerçekleştirilebileceğini öne süren gruplar da bulunmaktadır.

Son 20–30 yılda bilgi teknolojilerinde yaşanan gelişmeler, yakın gelecekte ülke çapında genel seçimler de dahil olmak üzere, birçok konuda kamuoyu yoklamalarının daha hızlı ve etkili bir biçimde elektronik çözümler kullanılarak yapılabileceğini göstermektedir. Bu konuda herhangi bir ciddi çalışmaya rastlanmayan, seçim sonuçlarında ciddi oranda hile ve mükerrerlik tartışmalarının yaşandığı ülkemizde, bu

tez, elektronik seçim tartışmalarının ülke gündemine taşınmasına ve uzun olmayan bir süreçte gerçeklenebilmesine katkı sunması durumunda, önemli bir başlangıç hedefini gerçekleştirmiş olacaktır.

KAYNAKLAR

[1] **Dr. Lawrence Pratcheet and, on behalf of E-Voting Resarch Team: Dr. Sarah Birch, Sara Candy, Dr. N. Ben Fairweather, Prof. Simon Rogerson, Vanessa Stone, Bob Watt, Dr. Melvin Wingfield,** De Monfort University, University of Essex, BMRB International, The Implemantation of E-voting in the UK, Page 51, May 2002.

[2] **Ronald L. Rivest,** Electronic Voting, http://theory.lcs.mit.edu/~rivest/voting/

[3] **Roy G. Saltman,** Accuracy, Integrity, and Security in Computerized Vote-Tallying, 1988.

[4] CFP'93 - Electronic Voting - Evaluating the Threat by **Michael Ian Shamos**, Ph.D., J.D., 1993.

[5] Testimony by **Rebecca Mercuri,** Ph.D., 2001.

[6] **R. Mercuri,** Electronic Vote Tabulation Checks and Balances. PhD thesis,

University of Pennsylvania, Philadelphia, PA, October 2000.

[7] **Rifat Çölkesen,** Veri Yapıları ve Algoritmalar, 2002.

[8] **Rebecca Mercuri,** A Better Ballot Box?, Ph.D., IEEE Spectrum, October 2002.

[9] **Peter G. Neumann,** Security Criteria for Electronic Voting, 1993.

[10] **http://www.itsecurity.com/dictionary/tcsec.htm**

[11] **Bruce Schneier,** Voting and Technology, Crypto-Gram Newsletter, http://www.counterpane.com/crypto-gram-0012.html, December 15, 2000.

[12] **Peter Neumann, Rebecca Mercuri, and Lauren Weinstein,** Internet and Electronic Voting, The Risks Digest (Forum on Risks to the Public in Computers and Related Systems), ACM Committee on Computers and Public Policy, Volume 21, Issue 14 Tuesday 12 December 2000.

[13] **http://csrc.nist.gov/cc/**

[14] **Ken Thompson,** Reflections on Trusting Trust, 1995.

[15] **Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin,** Analysis of an Electronic Voting System, 2003.

[16] **Avi Rubin,** Security Considerations for Remote Electronic Voting over the Internet, http://avirubin.com.

[17] **Internet Policy Institute,** Report of the National Workshop on Internet Voting: Issues and Research Agenda, 2001.

[18] **David Chaum,** "Blind Signature Systems" U.S, Patent # 4,759,063, 19 Jul. 1988.

[19] **David Chaum,** Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms Communications of the ACM, 24, 84-88 .

[20] **Atsushi Fujioka, Tatsuaki Okamoto, Kazuo Ohta,** A Practical Secret Voting Scheme for Large Scale Elections, Springer-Verlag, 1992, London, UK.

[21] **Arto Salomaa,** Public Key Cryptography Springer-Verlag, 1990.

[22] **R. Cramer R Gennaro, B. Schoenmakers,** A Secure and Optimally Efficient Multi Authority Election Scheme In Advances in Cryptology - Proceedings of EUROCRYPT'97 (LNCS 1233), pages 103-118. Springer-Verlag, 1997.

[23] **Benaloh and D. Tunistra,** Receipt-Free Secret-Ballot Elections, 26th STOC,

pp. 544- 552, 1994.

[24] **www.vote.caltech.edu,** MIT/Caltech Voting Technology Project, July 2001.

[25] **Jamie Brown, Domari Dickinson, Carl Steinebach, Jeff Zhang,** E-voting System:Specification and Design Document, John Hopkins University, www.cs.jhu.edu, March 6, 2003.

[26] **Mark A. Herschberg,** Secure Electronic Voting Over the World Wide Web, Massachusetts Institute of Technology, May 27, 1997.

ÖZGEÇMİŞ

Murat Şahin, 1977, İstanbul doğumludur. Kağıthane Cengizhan Lisesi, Fen Bölümü (1994) ve İstanbul Üniversitesi, İktisat Fakültesi, İşletme Bölümü (1999) mezunudur. 2001 yılında Beykent Üniversitesi, Yabancı Diller Yüksek Okulu'nda İnglizce dil eğitimi almıştır. 2002 yılında Beykent Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Teknolojileri yüksek lisans programına başlamıştır.

Ocak 2004'ten itibaren, kurumsal kaynak planlaması uygulamaları alanında yazılım geliştirici ve danışman olarak çalışmaktadır.