T.C.
BEYKENT ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI

BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

MERCURI MODELİNE DAYALI ÖRNEK ELEKTRONİK SEÇİM UYGULAMASI

Yüksek Lisans Tezi

Tezi Hazırlayan:**Haluk ALEMDAROĞLU**

İSTANBUL, 2014

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

MERCURI MODELİNE DAYALI ÖRNEK ELEKTRONİK SEÇİM UYGULAMASI

Yüksek Lisans Tezi

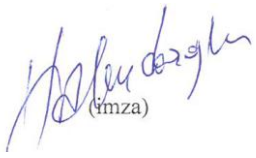
Tezi Hazırlayan:
Haluk ALEMDAROĞLU Öğrenci No:
120820012

Danışman:
Yrd. Doç. Dr. Turhan KARAGÜLER

İSTANBUL, 2014

YEMİN METNİ

Yüksek Lisans tezi olarak sunduğum " Mercuri Modeline DayalıÖrnek Elektronik Seçim Uygulaması" başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım. 04.09.2014



Aday: Haluk ALEMDAROĞLU

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZ SAVUNMA SINAVI SONUÇ TUTANAĞI

Beykent Üniversitesi
Fen Bilimleri Enstitüsü Müdürlüğü'ne,

Aşağıda tez adı belirtilen yüksek lisans öğrencisi **120820012** no'lu **Haluk ALEMDAROĞLU'nun** 04 /09 /2014 tarihinde yapılan tez savunma sınavı[1] sonucunda 45 dakika süreyle sunduğu ve savunduğu tezi hakkında[2] **oybirliğiyle kabul** kararı verilmiştir.

Bilgilerinize saygılarımızla arz ederiz.

Anabilim Dalı : Bilgisayar Mühendisliği
Programı : Bilgisayar Mühendisliği
Proje Konusu[3] : Mercuri Modeline Dayalı Örnek Elektronik Seçim Uygulaması

Tez Sınav Jürisi	Öğretim Üyesi	İmza
Danışman	: Yrd. Doç. Dr. Turhan KARAGÜLER	
Üye	: Yrd. Doç. Dr. Ediz ŞAYKOL	
Üye	: Yrd. Doç. Dr. Rıza Haluk KUL	

---

[1] Jüri üyeleri söz konusu tezin kendilerine teslim edildiği tarihten itibaren en geç bir ay içinde toplanarak öğrenciyi tez savunma sınavına alır. Belirlenen günde yapılamayan jüri toplantısı, katılanların hazırladığı bir tutanakla enstitü yönetimine bildirilir. Bu durumda jüri en geç onbeş gün içinde toplanarak adayı tez savunma sınavına alır. Tez savunma sınav süresi en az 45 dakikadır. Yüksek lisans tez savunma sınavı, tez çalışmasının sunulması ve bunu izleyen soru-yanıt bölümlerinden oluşur ve dinleyiciye açıktır. (Beykent Lisansüstü eğitim ve Öğretim Yönetmeliği-Madde30-3)

[2]Tez sınavının tamamlanmasından sonra jüri, tez hakkında "kabul", "düzeltme" veya "red" kararı verir. Jüri başkanı, jüri üyelerince imzalanmış sınav tutanağını, tez sınavını izleyen üç gün içinde ilgili enstitü yönetimine teslim eder. Tezi başarısız bulunan öğrencinin Enstitü ile ilişiği kesilir. Tezi hakkında düzeltme kararı verilen öğrenci en geç üç ay içinde gerekli düzeltmeleri yaparak ve yönetmelikte belirtilen usullere uygun olarak tezini aynı jüri önünde yeniden savunur. Bu savunma sınavında da tezi kabul edilmeyen öğrencinin enstitü ile ilişiği kesilir.(Beykent Lisansüstü eğitim ve Öğretim Yönetmeliği-Madde30-4)

[3]İlerideoğabilecekaksaklıklarınengellenmesiiçintezinbaşlığınınyazılmasıgerekmektedir.

Adı ve Soyadı : Haluk Alemdaroğlu

Danışmanı : Yrd. Doç. Dr. Turhan Karagüler

Türü ve Tarihi : Yüksek Lisans, 2014

Alanı : Bilgisayar Mühendisliği

Anahtar Kelimeler : Seçim Yöntemleri, Seçim Sistemleri, Türkiye' de Seçimler, Elektronik Seçim Sistemi, Elektronik Oy Verme, E-seçim, DRE Sistemler, IP Tabanlı Elektronik Seçim, Mercuri Model

ÖZET

MERCURI MODELİNE DAYALI ÖRNEK ELEKTRONİK SEÇİM UYGULAMASI

Yapılan bu çalışmadaelektronik seçim sistemlerinin en güvenilir örneklerinden biri olan Mercuri Modeline dayalı, IP tabanlı elektronik seçim sisteminin analizinin yapılması amaçlanmıştır. Mercuri modelinin güvenilir olmasının nedeni, hiçbir elektronik veya dijital seçim uygulamasının tam güvenlikli olarak gerçeklenemeyeceğini varsaymasıdır. Bu nedenle model, elektronik ve bilişim araçlarını seçim süresinceher aşamada kullanmasına karşın son noktada seçmenin tercihini gösteren oy pusulasını da üretebilme ve saklayabilme esasını benimser. Uygulanabilirliği ve pratikliği de dikkate alacak şekilde, modelin uygulaması olarak üniversite rektör seçimleri ele alınmış ve analiz edilmiştir. Bunun yanısıratezde günümüze değin, dünyadaki e-seçim örneklerinin ve yaygın modellerinin kısa bir tarihçesi verilmiş olupgeçirdikleri evrim ve temel unsurları tanıtılmıştır.

Name and Surname : Haluk Alemdaroğlu

Supervisor : Yrd. Doç. Dr. Turhan Karagüler

Degree and Date : Master, 2014

Major : Computer Engineering

Key Words : E-Election, Electronic Voting, IP Based Electronic Elections, Election Systems, DRE Systems, Mercuri Model

ABSTRACT

AN APPLICATION OF ELECTRONIC VOTING BASED ON MERCURI'S MODEL

The aim of this work to introduce and analyse Mercuri Model which is one of the most reliable and secure IP based electronic election systems. The model simply assumes that it is almost impossible to achieve trustable and safe an electronic election. Therefore the model suggests providing and saving a paper output of vote along with electronic and digital devices used at all the steps of election process. Consideringpracticalityand applicability of the model, the rector election of a university is taken as the sample case to analyse. Additionally, the worldwide examples of electronic election applications are briefly introduced.A short history of electronic election is also given.

İÇİNDEKİLER

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR

ABD: Amerika Birleşik Devletleri

AES: Advanced Encryption Standard

ARP: Address Resolution Protocol

BGP: Border Gateway Protocol

CALTECH: California Institute of Technology

CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart

CBC: Cipher Block Chaining

CD: Compact Disk

CPU: Central Processing Unit

DMZ: Demilitarized Zone

DNS: Domain Name System

DoS: Denial of Services

DDoS: Distributed Denial of Services

DRE: Direct Recording Electronic

FOO: Fujioka,Okamoto, Ohta Protocol

FTP: File Transfer Protocol

G.SHDSL: Global Standard High-Bit-Rate Digital Subscriber Line

HDD: Hard Disk Drive

HTML: Hypertext Markup Language

HTTP: Hypertext Transfer Protocol

HTTPS: Secure Hypertext Transfer Protocol

ID: Identification Data

IDS: Intrusion Detection System

IP: Internet Protocol

IPS: Intrusion Prevention system

LAN: Local Area Network

MIT: Massachusetts Instıtute of Technology

NAS: Network Attached Storge

PC: Personal Computer

RAM: Read Access Memory

ROM: Read Only Memory

RSA: Rivest-Shamir-Adleman Algorithm

RV: Registration Verifier

SAN: Storage Area Network

SQL: Structured Query Language

SSH: Secure Shell

SSL: Secure Sockets Layer

STK: Sivil Toplum Kuruluşu

TC: Türkiye Cumhuriyeti

UDP: User Datagram Protocol

UTF-8: 8 bit Unicode Transformation Formats

UYAP: Ulusal Yargı Ağı Bilişim Sistemi

VPN: Virtual Private Network

VRDB: Vote Registration Database

VTP: Voting Technology Protocol

VVPAT: Voter Verified Paper Audit Trail

VVAATT: Voter Verified Audit Transcript Trail

YSK: Yüksek Seçim Kurulu

1.GİRİŞ

Siyasal partiler ve özgür seçimler, demokrasinin vazgeçilmez unsurlarıdır. Demokratik rejimlerde siyasal partiler, savundukları düşünceleri gerçekleştirmek için birbirleriyle mücadele ederek yarışırlar. Siyasal partiler, gerekli olan yetkiyi yapılan seçimler sonucunda halktan alırlar. Demokratik yönetimin olduğu ülkelerde yönetim yetkisinin ve meşruiyetinin temeli seçimlerdir. Çok partili demokrasilerde genel seçimlerin amacı, belirli bir süre için ülkeyi yönetecek olan siyasi partinin hangi parti olacağı, denetim görevi yapacak olan muhalefet partisinin kim olacağını belirlemektir. Fakat halk tarafından partilere verilen bu sıfatlar, geçici süre ile ülkeyi yönetme yetkisi verir. Çünkü iktidar ve muhalefet partileri, bir sonraki seçimde yer değiştirebilir. Değişiklik, seçim mekanizması ile gerçekleşir. Bu yüzden seçim sistemi elektronik veya alışılagelmiş olan yöntemlerle yapılmış olsun demokratik rejimin sağlıklı işleyişi bakımından yaşamsal bir önem taşır [1].

Elektronik seçim sistemleri bazı ülkeler tarafından seçim ve referandumlarda başarı ile kullanılmıştır. Ancak bu sistemler pratikliğinin yanında güvenlik sorununu da getirmiştir.Bu yüzden elektronik oy verme sistemlerinde güvenlik denetimininyapılabilmesi gerekmektedir. Mercuri ve Chaum yapmış oldukları çalışmalarda güvenlik denetiminin yapılabilmesi için kendilerine has çözümler üretmiştir. Mercuri, hiçbir elektronik sisteme tam olarak güvenilemeyeceğine ve bu yüzden seçmenin kullanmış olduğu oyun bir kağıt çıktısının alınarak güvenliği sağlayabileceğini savunmaktadır [2]. Chaum ise, şifreli bilgileri üzerinde barındıran pusula sistemini önermektedir. Pusula her kişi için tek olarak üretilmekte olup şifrelidir. Oy kullanımı bittikten sonra seçmenler oyların doğruluğunu görebilmek için kullanılan oyların yayınlandığı bir web sitesinden karşılaştırarak denetleyebilmektedirler [3].

Elektronik seçim sistemleri mimarisi üzerine bir çok kuruluş ve üniversite sistemin güvenilirliğine ve denetlenebilirliğine izin veren projeler geliştirmişlerdir. Bunların arasında Massachusetts Institue of Technology/California Institute of Technology (MIT/CALTECH) üniversitelerinin ortaklaşa geliştirdikleri FROG

mimarisi ve bunun yanısıra Group2 mimarisi ve Evox mimarisi en çok bilinen mimarilerdir.

Elektronik seçim sistemini ve değerlendirme kıstaslarını uygulayabilmek için,sistemin kullanılabilirliğinin, sistemin güvenliğinin ve sağlamlığının ve tüm sistem gereksinimlerinin sağlanması gerekmektedir. Elektronik seçim sistemi için gerekli olan tüm güvenlik sorgulamaları ilgili tüm kuruluşlarca yapılabilmelidir. Bu kuruluşlar gerektiğinde yasal mekanizmaları çalıştırabilecek yetkinliğe sahip olabileceği gibi bağımsız kişilerce de yapılabilmelidir.

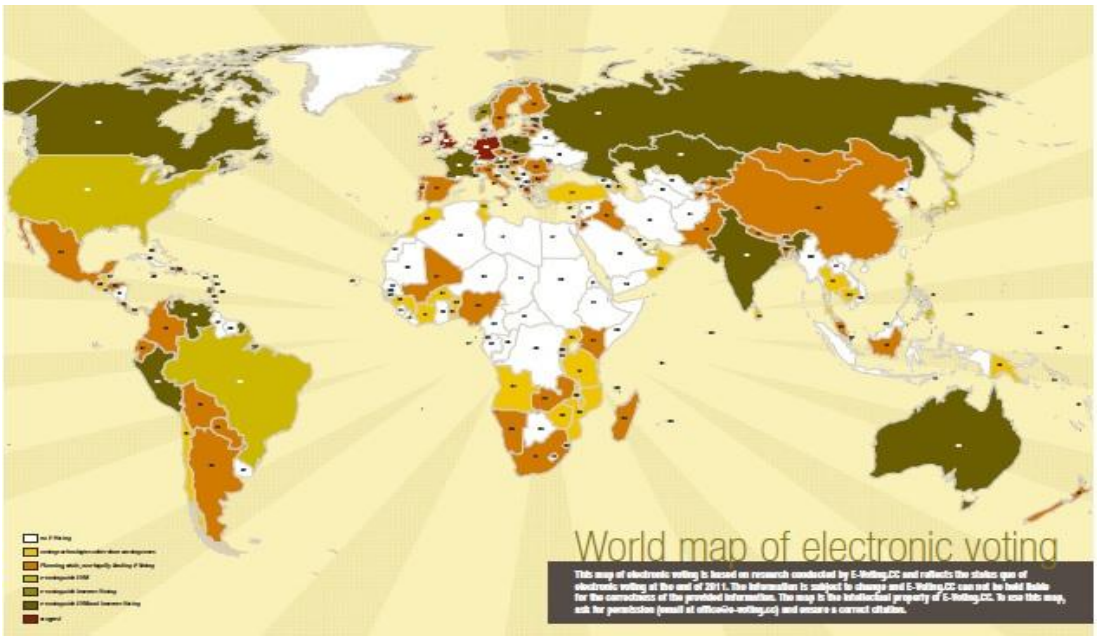
Elektronik seçim sistemlerinin denetlenebilirliğini gerçekleştirmek için bazı seçim denetleme yöntemleri geliştirilmiştir. Bu yöntemlerseçmen doğrulamalı kağıt denetim sistemi ve seçmen onaylı ses denetleme suret izidir. Seçmen doğrulamalı kağıt denetim sistemi Rebecca Mercuri' nin "Physical Verifiability of Computer Systems" adlı eserinden [2] yola çıkılarak gerçekleştirilen bir yöntemdir. Seçmen onaylı ses denetleme suret izi ise daha yeni bir düşünce olup, Ted Selker'in yayınlamış olduğu "Fixing the Vote" adlı bilimsel makalesinde bu yöntem tanıtılmıştır [4].

Yapılacak olan elektronik seçim sisteminin erişim alt yapısının da güvenli bir şekilde tasarlanması gerekmektedir. Sisteme erişimin engelleneceği, Denial of Services (DoS) ve Distributed Denial of Services (DDoS) gibi saldırılara karşı etkin bir ağ güvenliğinin sağlanabilmesi gereklidir.

Bu tezin amacı geçmişten günümüze elektronik seçim çalışmalarını incelemek, karşılaşılan güvenlik sorunlarını ve çözümlerini araştırmak ve Mercuri Modeli örnek alınarak IP tabanlı bir seçim sisteminin üniversitelerde ki rektörlük seçimlerine uygun hale getirerek uygulamasını sunmaktır.

1.1. Dünyada Elektronik Seçim Çalışmaları

Bilgisayar ve internet ortamının hızlı şekilde gelişmesi sonrasında e-demokrasi, e-seçim fikirleri ortaya atılmış ve bunların ihtiyaç olduğu savunulmuştur. E-seçim sisteminde ortaya çıkan en büyük sorun sistemin güvenilirliğidir. Bu soruna iki şekilde çözüm getirilebilir. Bunlar " Chaum Modeli " ve " Mercuri Modeli " dir. Dünyadaki bazı ülkeler e-seçim fikrini benimsemiş ve ülke genelindeki seçimleri elektronik ortamda yapmışlardır. Bu ülkelere Avusturalya, ABD, Kanada, Belçika, Estonya, Brezilya, Hindistan, Venezuela ve Finlandiya' yı örnek gösterebiliriz. Aşağıdaki şekilde elektronik seçim sistemini test eden, kullanan veya kullanmayan ülkeler harita üzerinde gösterilmiştir [5].



Şekil.1. Elektronik Seçim Sistemini Kullanan Ülkeler Haritası

Şekil.1' de verilen haritada: Beyaz hiç e-seçim yapılmamış bölgeleri, sarı oylarını başka oylama teknolojileri ile yapanları, portakal rengi planlamalar, denemeler ve yasal bağlayıcılığı olmayan e-seçimi, açık yeşil elektronik oy verme makinesi ile elektronik seçimi, yeşil internet üzerinden elektronik oy verme işlemini, koyu yeşil

internet oylaması ve elektronik oy verme makinesi ile elektronik seçimi, kırmızı yasal olarak durdurulmuş veya yasaklanmış yerleri göstermektedir.

Elektronik seçim sistemini en başarılı şekilde uygulayan ülkeler arasında, Estonya öne çıkmaktadır.Estonya 1991 yılında bağımsızlığını kazanmış olup, kısa zaman dilimi içinde, teknolojiye sahip çıkarak pek çok köklü devletin ulaşamadığı noktalara gelmiştir. 1 milyon 340 bin kişinin yaşadığı küçük bir ülke olan Estonya' da nüfusun büyük bölümü teknolojiyi hayatına sokmuştur. Eğitimden sağlığa, bankalardan iş hayatına kadar her hizmet X-road ismi verilen dijital bilgi otoyolunu ve ID-card adı verilen yongalı vatandaşlık kartını temel alarak yapılmaktadır. Estonya ekonomi ve ulaştırma bakanlıklarının ortak girişimleriyle geliştirilen X-road herkesin ulaşabileceği açık bir platform. Herkes kendi sistemini X-road platformuna entegre edebilmektedir. Bu yapı, kamu ve özel sektörün verdiği hizmetlerin temel taşıdır.

Estonya' da elektronik seçim sistemi çalışmaları 2003 yılında başlatılmıştır. İki yıl gibi kısa süre sonra 2005 yılında yerel seçimleri elektronik olarak gerçekleştirmiştir. Bu seçimde 9300 kişi mikro yongalı ve özel şifreli kartlarını, şahsi bilgisayarlarına takılan özel bir okuyucu yardımıyla sisteme tanıtarak kullanmıştır. 2007 yılı genel seçimlerinde bu rakam otuz bine, 2009 yerel seçimlerinde ise yüz beş bine yükselmiştir.

Estonya' da vatandaşlık hizmetlerinin tamamı %80 kullanım oranına sahip ID-card olarak anılan bir mikro yongalı kartla yürütülmektedir [6].Hindistan' da elektronik seçim kısmen 1999 yılında elektronik seçim makineleri ile yapıldı. Elektronik seçim makineleri, hükümete ait olan savunma araçları yapaniki birim tarafından üretildi. Elektronik seçim sistemi, seçmenin kullandığı seçim ünitesi ve seçim memuru tarafından idare edilen kontrol ünitesinden ibaret olan iki parçanın birleşiminden oluşmaktadır. 16 aday kapasitesine sahip olan oy verme birimi her aday için mavi bir butona sahiptir. Gerektiğinde bir denetim birimine dört adet oy verme birimi bağlanarak 64 adaya kadar çıkabilmektedir. Oy kullanma işlemi oy pusulasına mühür basar gibi bir butona basarak gerçekleştirilmektedir. Sistem basit,

ucuz ve yeniden programlanamayan mikroişlemciler kullanılarak oluşturulmuştur.Bu mikroişlemciler içerisinde oluşturulan yazılımın sonradan değiştirilebilmesi mümkün değildir. Bu sayede, yazılım değiştirilmesi gibi hilelerin önüne geçilmiştir.

İşlemcinin farklı bir işlemci ile değiştirilmesini engellemek için de kapağı açılmaya çalışılınca kendisini otomatik olarak kapatması hile olasılığını önlemektedir.

Brezilya, yapmış olduğu bir seçimde ülkenin bütününde, elektronik cihazları kullanarak dünyada bir ilki başarmıştır. 1996 yılından beri elektronik seçim cihazları Brezilya' da kullanılmaktadır. Yapılan elektronik seçimlerde meydana gelen usulsüzlükler nedeniyle oy pusulasının da ayrıca bir yazıcıdan çıktısı alınmıştır. Bu yeni sistem oy verme işleminden sonra seçmen Mercuri yöntemindeki [2] gibi basılmış bir oy pusulasını cam arkasından görmektedir. Eğer seçmen yazıcıdan oyunun doğru çıkmadığını görürse oyunu iptal ederek yeniden oy verebilmektedir. Seçmenin onaylamış olduğu oy pusulası, el değmeden özel bir plastik torbaya aktarılmakta ve daha sonradan istendiğinde oy sayımını denetleyebilmek için kullanılabilmektedir.

1.2.Türkiye' de Elektronik Seçim Çalışmaları

Türkiye'de elektronik seçim çalışmaları ilk defa 1986 yılında gerçekleştirilmiştir. Bu çalışmaya Bilgisayar Destekli Merkezi Seçmen Kütüğü Bilgi Sistemi denilmiştir.Dünyada ilk yapılan elektronik seçim sistemi çalışmaları arasında yeralır. Bu çalışma seçimle ilgili her türlü bilginin ve verinin saklanıp muhafaza edildiği bir bilgi sistemidir.

Dünyada bir ilk olan proje, 90' lı yıllarda yöneticilerin ilgisizliği, yetersiz alt yapı ve teknolojik nedenlerden dolayı bir ilerleme kaydedememiştir. Yeterli özveri gösterilmeden çok ağır şekilde ilerlemesine neden olunan proje 2007 yılında tamamlanabilmiştir [7].

2. ELEKTRONİK SEÇİM

Elektronik seçim, seçmeninklasik yöntemlerle yapmış olduğu seçimin elektronik ortamda toplanıp değerlendirilmesi işlemidir. Yani, elektronik sistemlerle yapılan seçim şekline elektronik seçim denir. Elektronik seçim ayrıca e-seçim olarak bilinen optik tarama seçim sistemleri (optical scanning vote systems), delikli kartlar (punched cards), oy verme kabinleri ki (voting kiosk) bu kabinler bilgisayar, telefon ve internet içeren bir sisteme sahiptirler. Bu oy verme kabinleri, DRE (Direct Recording Electronic Voting System) diye adlandırılan kendi kendine yeten sistemleri içermektedir.

İki tür elektronik seçim sistemi yaklaşımı vardır. Birincisi, fiziksel olarak bağımsız seçim otoriteleri ya da hükümet temsilcilikleri tarafından denetlenen elektronik seçim (e-voting) sistemidir.İkincisi ise hükümet veya bağımsız otoriteler tarafından fiziksel olarak denetlenmeyen telefon, internet veya kişisel bilgisayar vasıtasıyla yapılan seçim sistemidir[8].

2.1. Elektronik Seçim Sistemi Elemanları

Elektronik seçim sistemi elemanları seçmen, kayıt otoritesi ve sayım otoritesidir.

-Seçmen: Ülke yasalarına göre oy verme hakkına sahip olan kişilerdir.

-Kayıt Merkezleri: Ülke yasalarına göre oy verme hakkına sahip olan seçmenleri seçim öncesinde kaydedildiği yerlerdir. Bu merkezler, sadece kayıtlı seçmenlerin seçim gününde yalnızca bir kez oy verebilmesini sağlarlar. Kayıt

merkezleri; nüfus memurları, yetkilendiriciler, oy pusulası dağıtıcıları veya şifreli anahtar (key generator) üreticileri olabilirler.

-Sayım Merkezleri: Verilen oyları toplarlar ve seçim sonuçlarını hesaplarlar. Sayım merkezleri; sayıcılar, toplayıcılar ya da hesaplayıcılar olabilirler.

2.2 Elektronik Seçim Sistemi Parametreleri

Elektronik seçim sistemi parametreleriyerleşke,kimlik saptanması, oy kullanma arayüzleri, oyların aktarılması ve oyların sayılmasıdır.

-Yerleşke: Seçmenlerin oyunu kullanacağı yerdir; ev, okul, fakülte, enstitü, işyeri, seçim kurulunun belirleyeceği kamusal yerler.

-Kimlik Saptanması: Seçim görevlilerince yapılacak olan kimlik kontrolü, yüz tanıma sitemleri, göz retina taraması, parmak izi kontrolü ile özel geliştirilmiş biometrik kimlik belirleme sistemleri, yongalı kart sistemleri ile kimlik saptaması yapılabilir.

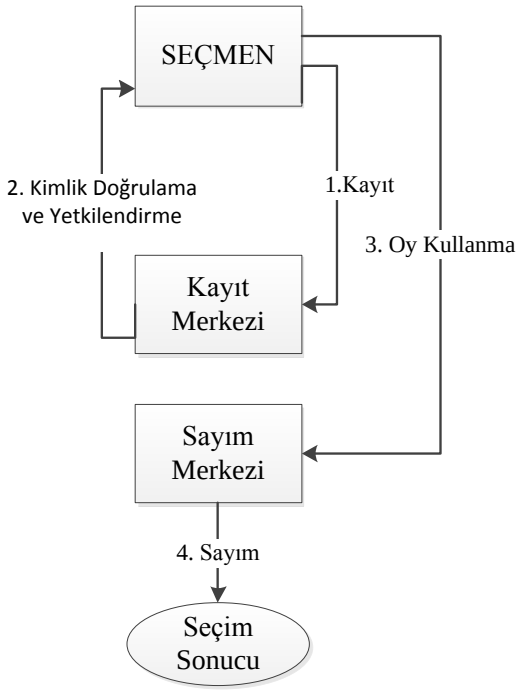
-Oy Kullanma Ara Yüzleri:Masaüstü bilgisayar, dizüstü bilgisayar, özel olarak tasarlanmış bir oy verme makinesi, telefon, sayısal televizyon ya da banka ATM' leri gibi benzeri araçlar.

-Oyların Aktarılması: Kullanılan oy fiziksel bir çıktı olarak, internet üzerinden, noktadan noktaya tasarlanmış bir ağ üzerinden veya özel sanal ağ (VPN) üzerinden aktarılabilir.

-Oyların Sayılması: Oyların sayılması oy kullanılan yerlerde, oyların aktarıldığı bölgesel noktalarda ve oyların toplandığı merkezi bir noktada yerel yada ulusal seviyede yapılabilir.

2.3. Elektronik Seçim Sistemi Aşamaları

Elektronik seçim sistemi aşamaları kayıt, yetkilendirme ve onaylama, oy verme ve sayma şeklindedir. Şekil.2' de elektronik seçim sistemi işleyiş aşamaları gösterilmektedir.



Şekil.2. Elektronik Seçimin Genel İşleyiş Şekli

-Kayıt: Seçmenler kayıt merkezlerince kaydedilir ve ülke yasalarına göre oy vermeye hak kazanan seçmenler seçimden önce listeler halinde ilan edilir.

-Yetkilendirme ve Onaylama: Kayıtlı seçmenler seçim gününde oy pusulalarını kayıt merkezlerinden talep ederler. Kayıt merkezleri seçmenin sadece bir kez kullanabileceği oy verme hakkına sahip olup olmadığını kontrol etmek için gerekli kimlik kontrollerini yapar. Kimlik kontrolü doğrulaması sonrasında seçmenin oy verme işlemi için onay verilir.

-Oy Kullanma: Seçmenler oylarını verirler.

-Sayım: Sayım yetkilileri oyları sayar ve seçim sonuçlarını ilan ederler [8].

2.4. Elektronik Seçim Sistemi Gereksinimleri ve Değerlendirme Kriterleri

International Association for Cryptologic Research (IACR), kriptoloji biliminin tanıtımına destek veren kar amacı gütmeyen uluslararası bir organizasyondur. IACR' nin kabul gördüğü herhangi bir elektronik seçim sistemi minimum aşağıdaki gereksinimlerikarşılamalıdır [9].

-Sistem yazılımı açık kaynak kod (open-source) olmalıdır.

-Sistem kullanıcı dostu (user-friend) olmalıdır. Yani, seçmenler oylarını mümkün olan en az sayıda cihaz ve en az beceri gereksinimi ile hızlıca kullanabilmelidir.

-Sistemin yönetimi ve sürdürülmesi denetleyiciler için (IACR gönüllüleri gibi) kolay olmalıdır.

-Oy verme işlemi için uygun olan seçmenler kesinlikle bir kez oy verebilmelidirler. Sistem, seçmenlerin bilgilerinin doğruluğunu kanıtlayabilmelidir.

-Bireysel oylar gizli kalmalıdır. Sistem, saldırganın verilen oyları öğrenmesine engel olmalıdır.

-Sistem, seçim sonuçlarının bütünlüğünün evrensel doğrulanabilirliğine sahip olmalıdır. Yani, sistem açık denetime (open audit) izin vermelidir.

-Sistem erişilebilir, mevcut ve güvenilir olmalıdır. Sistemin herhangi bir teknik arızaya karşı yedekleme ve fiziksel koruma mekanizması olmalıdır. Tek bir elektronik cihaza güvenilmemelidir.

-Denial of Services (DoS) saldırılarına karşı bir direnç mekanizmasına sahip olmalıdır.

-Sistem, virüs ve kötü amaçlı yazılımların sisteme vereceği tahribata ve muhtemel sızmalara karşı bir koruma sunabilmelidir.

-Sistem seçmenin baskı altına alınmasını önlemelidir. Bir seçmenin oyunu nasıl ve kime kullandığını herhangi bir kimse öğrenememelidir ve sahte oy kullanımını önleyici mekanizmalara sahip olmalıdır.

-Seçimde esnekliğin sağlanabilmesi için, kullanılan cihazlar değişik oy formlarına izin vermeli, değişik standart platformlar ve teknolojilerle uyumlu olmalı ve özürlülere erişim hakkı vermelidir.

-Oy kullananların oy kullanma süreci hakkında genel bilgiye sahip olmaları için önceden hazırlanmış eğitsel dokümanlar seçmenlerin anlayacağı en basit şekilde hazırlanmalı ve seçmenlere bu bilgiler öğretilmelidir. Seçmenler bu şekilde genel bilgi ve anlayışa sahip hale getirilmelidir.

-Seçmen oy kullanmak istemediği takdirde oy kullanmama hakkı olmalıdır. Bu durumda oy vermeyen seçmenin yerine bir başkasının oy kullanması engellenmiş olmalıdır.

-Seçmenin boş oy kullanabilme hakkı olmalı ve bu oylar da diğer oylar gibi silinememeli, değiştirilememeli ve kopyalanamamalıdır.

-Seçim sonuçları ve gerekli bilgiler seçim sonunda basın yoluyla ve internet aracılığıyla ilan edilmelidir.

-Seçimin ve sayımın doğru şekilde yapıldığı gösterilebilmelidir.

-Seçmenin oyunun sayıldığından emin olabilmesi bireysel doğrulamadır. Klasik kağıt oy pusulalı seçim sistemlerinde bireysel doğrulama yapılamamaktadır,

ancak sistemin akışı itibariyle seçmenin sandığa oyunu bizzat atması bir çeşit bireysel doğrulama olarak kabul edilebilir.

-Kayıt, seçim ve sayım gibi işlemlerin tamamı etkin bir şekilde yapılmalı, bekleme süreleri en aza indirilmelidir. Klasik seçimlere göre oylar daha kısa sürede sayılmalıdır.

-Oyların ve seçmenlerin gizliliğine zarar vermeden, e-seçim sistemlerinde en üst düzeyde şeffaflık hedeflenmelidir.

-Oylar ve gerekli seçim bilgileri sayım sonrasında, elektronik ve basılı ortamda saklanmalıdır. Hem elektronik hem de basılı ortamda saklanan oylar gerekirse yeniden sayılabilmelidir.

-Seçmenler istedikleri ortamdan rahat bir biçimde oy kullanabilmelidir. İnternet olan herhangi bir yerden, cep telefonundan, banka ATM' lerinden...

-Oy verme sistemleri kabul edilebilir bir maliyete sahip olmalıdır. Kabul edilebilir maliyet, elektronik seçim maliyetinin klasik seçim maliyetinden daha az olmasıdır.

-Sadece klasik anlamda çoktan seçmeli oy pusulalarının yanı sıra değişik seçim sistemleri, oylama ve anket uygulamaları için de gerekli alt yapı sağlanarak oy pusulalarının esnekliği sağlanmalıdır.

-Tasarım aşamasında e-seçim sistemi ve temel unsurlar, kullanılan programlama dilinden, uygulama geliştirme ortamından, işletim sisteminden ve kullanılacak teknolojilerden bağımsız olarak üst düzey modellenmelidir. Uygulama geliştirme aşamaları birbirinden ayrılmalıdır. Aşamalardan birinde yapılacak değişiklik sonrasında, diğerleri herhangi bir kaynak kod düzeltmesine gerek kalmadan üst düzeyde güncellenebilmelidir.

-Elektronik oy pusulaları kopyalanmaya karşı korunmalı ve özel olarak üretilmeli ve imzalanmalıdır.

-Elektronik seçim sistemi herhangi bir ek çalışma gerektirmeden küçük, orta ve büyük ölçekli seçimlerde kullanılabilmelidir.

2.5. Elektronik Seçim Sistemi Özellikleri ve Riskleri

Elektronik seçimler seçimsürecini birçok yönden iyileştirebilmektedir. Fakat tamamen sorunsuz birsüreçsunduğuda söylenemez. Elektronik sistemler üzerinde programlanan yazılım, seçim sürecini etkileyen yeni bir risk kümesi meydana getirir. Elektronik seçim sistemi özellikleri; elektronik seçim sandığı olarak kullanılacak olan e-seçim programı, veri iletişiminin işleyişi, yasama ve hukuki boyutları, kullanılacak olan standartlar, güvenlik sistemleri, oluşacak olan maliyet, personelin eğitilmesi konularıdır. Bu özelliklerden yola çıkarak meydana gelebilecek riskleri 4 kategoride sınıflandırabiliriz.

2.5.1. Yasamave Hukuki Boyuttaki Riskler

Yasama riskleri elektronik seçimler içintanımlanması gereken bir dizi seçim yasasını içerir. Var olan geleneksel seçim sistemleri için tanımlanmış yasalar elektronik seçimler için geçerli değildir. Elektronik seçimler bilişim kapsamına girdiğinden ilgili ülkenin bilişim alanındaki suçlarla ilgili yasalar uygulanmalıdır.

2.5.2. Sosyo-politik Riskler

Elektronik seçim yönteminin seçmen üzerinde olumsuz olabilecek etkilerinin sonuçları sosyo-politik sonuçlar doğurmaktadır. Buda beraberinde bazı sosyo-politik riskler getirmektedir. Dijital bölünme diye adlandırabileceğimiz bu riskler teknolojiye erişebilme/erişememe sorunu, seçmenleri olumlu/olumsuz yönde

etkileyecektir. Bunun yanısıra, teknolojiye erişebildiği halde okuma yazma bilmeyen bir seçmen oy kullanma hakkından mahrum kalacaktır.Bu nedenle seçmen oy kullanamadığından seçime katılan adaylarda alabilecekleri oyu alamayacaktır.

2.5.3. Ekonomik Riskler

Ekonomik risk, yapılacak olan seçim sistemi maliyetidir. Seçimler tüm ülkeyi kapsayacak şekilde ve devamlı olarak tekrarlanacağından, gelecekte de kullanılacağı düşünülerek yapılacak tercihler maliyeti çok etkileyecektir. Bu nedenden dolayı, sistem tasarımı yapılırken kullanılacak olan donanım ve yazılımın maliyetinin çok dikkatli bir şekilde irdelenmesi gerekmektedir. Bu maliyetleri aşağıdaki gibi sıralayabiliriz.

-Okullarda kullanılması planlanan bilgisayarların hazır hale getirilmesi ve maliyeti.

-Hukuki çalışmalar ve standartların oluşturulmasında oluşacak maliyet.

-Personel eğitimi maliyeti.

-Elektronik veri iletimi, güvenlik yazılımları, işletim sistemi ve programlar için ödenecek olan lisans bedeli maliyetleri.

2.5.4. Teknolojik Riskler

Teknolojik riskler, elektronik seçim sisteminin (e-seçim programı, e-seçim programı veritabanı ve e-seçim haberleşme ağı) güvenliği, gizliliği, şeffaflığı ve kullanılacak olan standartların düzgün bir şekilde uygulanmamasıdır. Elektronik seçimler geleneksel, fiziksel oylama metodlarından kullanılan araçlar ve izlenen yöntemler gereği çok farklıdırlar. Bu farklılıklar nedeniyle, elektronik seçimlerin teknolojik risk kaynakları aşağıdaki gibi listelenebilir.

-Oy pusulalarının dijital yapısı.

-Kullanılan sistemlerin karmaşıklığı.

-Kullanılan sistemlerin seçmenlere ve seçim otoritelerine karşı şeffaflıktan yoksun olması.

-Kullanılan sistemlerde ayrıcalıklı kullanıcıların olması.

Yukarıda sıralanan bu dört risk çok sayıda saldırının kaynağı olabilir. Örneğin;

-Elektronik sistemde (bilgisayar vb.) arıza olabilir.

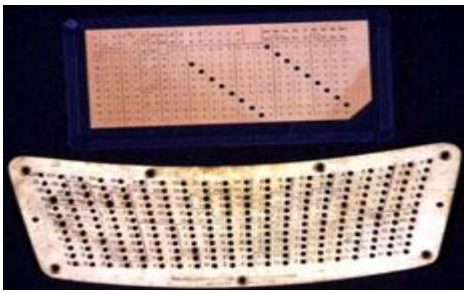
-Kullanılan yazılım kötü niyetli veya niyetsiz hatalar içerebilir.

-Oy pusulaları ayrıcalıklı kullanıcılar tarafından silinebilirveya değiştirilebilir, seçmenlerin gizliliğisağlanamayabilir.

2.6. Elektronik Seçimlerde Kullanılan Aygıtlar

Geçmişten günümüze kullanılan aygıtlar delikli kartlar, optik tarayıcılar, Lever makineler ve doğrudan kayıt yapan elektronik sistemlerdir (DRE).

Delikli Kartlar:1880 yılının sonlarına doğru Herman Hollerith tarafından Baltimore Sağlık Kurulu (Baltimore Board of Health) için istatistiki bilgileri tablolaştırmak maksadıyla tasarlanmıştır. Delikli kart oylama sistemiyle, küçük delikler içeren kart panoya eklenir. Seçmenler deliklerden kaleme benzer kayıt iğnesi ile sertçe bastırırlar. Oy verme işlemi tamamlandıktan sonra, seçmen oy pusulası kutusuna oy pusulasını bırakır [10].



Şekil.3. Delikli Kart

İki çeşit delikli kart vardır. Bunlar "votomatic" ve "datavote" diye adlandırılmıştır. Votomatic kartların her deliğe uygun sayıları vardır. Deliklerin sayısı kart üzerinde basılmış olan tek bilgidir. Aday listesi veya oy pusulaları oy kullanılan standın içinde basılı halde durmaktadır. Datavote, diğer taraftan, doğrudan olarak delik çukuruna yakın basılmış oy pusulalarına veya adayların isimlerine sahiptir.

-Optik Tarayıcı Oylama Sistemi: Genellikle optik tarayıcılar olarak adlandırılan Mark Sense oy verme sistemleri adayların isimlerini içeren önceden basılmış oy pusulaları veya dikdörtgen, daire şeklinde boş oy pusulaları şeklindedir. Seçmen siyah bir işaretleyici ile kutuyu veya daireyi doldurmak zorundadır. Optik tarama sistemi 1980' lerde kullanılmaya başlanmıştır. Kağıt pusulalar optik tarayıcıya yerleştirilir ve bilgisayar tarafından okunarak kaydedilir. Bilgisayarda bulunan zararlı bir yazılım ile kaydedilen bilgiler değiştirilebilir ve bu yüzden bir zaafiyet içerir [10].

Şekil.4. Optik Tarayıcı Oylama Sistemi

-Lever Makineler: Lever Makineler tamamen mekanik sistemlerdir. İlk lever makinesine "Myers Automatic Booth" adı verilmiştir. Bu Lever Makineleri ile 1892 yılında Newyork seçimleri yapılmıştır. Lever Makinelerinde oy pusulalarına işaret koymak için kol hareket ettirilir ve bu şekilde oy kullanılır. Oy kullanımından sonra verilen oya göre ilgili sayaç bir artar ve sayım işlemi bu şekilde gerçekleştirilir. Seçim görevlileri makinelerde ki kayıtları okur ve bunların sayımı ile sonuç elde edilir. Bu sistemde oyların denetlenmesine imkan yoktur. Çünkü sistem üzerinde oylara ait olan herhangi bir bilgi veya belge yoktur. Seçim sonunda yapılacak olan herhangi bir itiraz karşısında tekrar sayım yapmanın imkanı yoktur. Buda sistemin güvenirliğinin sorgulanmasına neden olmaktadır [10].

Şekil.5. Lever Makine

-Doğrudan Kayıt Yapan Elektronik Sistemler: Elektronik seçim insan kaynaklı kusur ve hataların önüne geçmek için işlemleri kolaylaştırmak adına kullanıma sunulmuş bir seçim sistemidir. Doğrudan kayıt sistemleri (Direct Recording Electronic Systems - DRE) bu hata ve kusurları elimine etmek için tasarlanmış cihazlardır. Bu sistemler 1980' lerde kullanılmaya başlanmış olan bilgisayar temelli ilk sistem olma özelliğini taşır.

DRE sistemleri kullanabilmek için bir Kişisel Kimlik Numarası (Personal Identifier Number – PIN)veya akıllı karta (smart card) ihtiyaç duyulur. İlgili görevliye kimlik kartı ibraz edilmek şartıyla PIN veya akıllı kart alınır ve bu şekilde sisteme giriş yapılır. Yapılan tercih sonrası bilgiler ekrana gelir ve seçmenin son kararını vermesi için onay bekler. Onay verilir verilmez oy kaydedilir.

DRE’ ler seçmene kullanılan oyun sadece bir yansıması olan elektronik görüntüyü ekrana getirir, gerçek oy pusulasını getirmez. Bu da kullanılan oyun gerçekten seçmenin vermiş olduğu oy olup olmadığı sorusunu akla getirir. Sistemde bulunan herhangi bir kötü amaçlı yazılım ile onay işleminden sonra bu oy değiştirilebilir. Günümüzde halen tam güvenilir bir DRE sistem yoktur [10].

Şekil.6. Doğrudan Kayıt Yapan Elektronik Sistemler

2.7. Kriptografik Araçlar

İnternet üzerinde bilgi ve haber gizliliğini sağlamanın başlıca yolları kriptografi ve stenografi’ dir. Kriptografi verinin çalınmasını önleyen önemli bir parçadır. Bilginin gönderen tarafında özel bir program ile şifrelenmesi ve alıcının da aynı programı kullanarak şifreyi çözmesidir. Verinin anlamını gizlemeye ek olarak kriptografi şifreleme, kimlik doğrulama, gizlilik ve bütünlük içeren veri için diğer güvenlik gereksinimlerini gerçekleştirir.

Kriptografi ayrıca, mesaj gönderen kişinin gerçek mi yoksa sisteme sızmaya çalışan birismi olduğunu saptamak için kimlik bilgilerini doğrulamada kullanılır. Şifreleme ayrıca kimlik doğrulamasına benzer kabul etmeme işlemi de sağlar ve

birisinin fiilen bir mesaj gönderip göndermediğini veya başka bir işlemin olup olmadığını ispatlamak için de kullanılır. Şifreleme bilimi (cryptography), sadece düzgün deşifreleme algoritmasıyla bir okuyucu ya da şifrelenmiş mesajları bir anahtar okuyabildiğinden, gizlilik sağlar. Sonunda şifreleme bilimi mesajların değiştirilmemesini sağlayarak bilgi bütünlüğünü koruyabilir.

Kriptografi, şifreli metin (ciphertext) diye adlandırılan şifrelenmiş veriyi şifresiz metine (cleartext) ya da okunabilen veriye dönüştürür. Kriptografi, tanımı gereği yetkisiz kullanıcıların metinleri okuyamasınlar diye tanımlanmış olan bilgiyi saklama bilimidir.

Kriptografinin geçmişi eski Mısır uygarlığına değin uzanır. Ancak kullanımı günümüzde hala güvenlik için kritiktir. Aslında şifreleme internet gibi çok güvensiz ortamlarda veri iletimi sağlanmak istendiğinde kesinlikle gereklidir. Şifreleme için simetrik, asimetrik ve hashing algoritmaları kullanılmaktadır [11].

2.7.1. Simetrik Kripto Sistemleri

Simetrik kriptolama sistemleri, şifreleme (encryption) ve deşifreleme (decryption) işlemlerinin her ikisinde de aynı anahtarı kullanarak işlem yaparlar. Gizli bir anahtarın karşılıklı olarak paylaşılmasıyla şifreleme ve deşifreleme işlemleri gerçekleştirilir. Veriyi gönderenin ve alanın anahtarı aynıdır. Bu iki işlem birbirine benzemesine rağmen bazı noktalarda birbirine ters sırayla uygulanır. Örneğin; Advanced Encryption Standard(AES).

Simetrik şifreleme veriyi küçük bloklar halinde böler ve kullandığı gizli bir anahtar ile bölmüş olduğu küçük blokları tek tek şifreler. Şifreleme işleminden sonra küçük küçük bloklara bölünen veriler bir araya getirilerek bir bütün halinde alıcıya gönderilir.Veriyi alan taraf deşifre işlemi için aynı anahtarı kullanır ve şifrelenmiş veriyi açar. Simetrik algoritmalar, asimetrik algoritmalara nazaran çok daha hızlı çalışmaktadırlar. Büyük veri akışlarında şifreleme dönüşümleri gerçekleştirmek

istendiğinde ideal bir şifreleme sistemidir. Bazı popüler simetrik şifreleme algoritmaları şunlardır: Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), International Data Encryption Standard, Rivest Cipher, Blowfish [11].

2.7.2. Asimetrik Kriptolama Sistemleri

Asimetrik şifreleme algoritmalarında anahtar ile şifre çözme anahtarı birbirinden farklıdır. Şifreleme yapan anahtar açık anahtar, şifreyi çözen anahtar ise özel anahtardır. Açık anahtarlar herkese dağıtılabilir, ancak hangi anahtarın kime ait olduğundan da emin olunmalıdır. Bu yüzden asimetrik algoritmalar ile sertifikalar kullanılmaktadır. Sertifika açık anahtar ile sahibi arasındaki bağlantının bir belgesidir. Özel anahtar ise sadece şifreyi çözecek kullanıcıda bulunur, açık anahtar ise gizli değildir. Bu yüzden asimetrik şifreleme güvenlik açısından simetriğe göre çok daha başarılıdır. Az sayıda anahtar kullanarak simetrik şifreleme yapan çok kullanıcılı uygulamalarda ortaya çıkabilecek anahtar fazlalığı durumunu engeller. Bununla birlikte hız ve donanımsal uygunluk gibi konularda asimetrik şifreleme simetriğe göre geri planda kalmıştır. Asimetrik algoritmaların güvenliğini sağlayabilmek için çok büyük asal sayılar kullanılmaktadır. Bu da zaman açısından çok büyük problemler getirmektedir. Asimetrik bir algoritmayı kullanan sistemler simetrik algoritmaları kullanan sistemlere göre çok daha yavaştır. Ayrıca asimetirk şifreleme algoritmalarının çok büyük sayılar kullanmasından dolayı donanımsal yapılara uyum sağlaması çok zor olmaktadır.

Güçlü yönleri; bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir. Anahtarı kullanıcı belirleyebilir.Zayıf yönleri; şifre uzunluğundan kaynaklanan algoritmaların yavaş çalışması ve anahtar uzunluklarının sorun çıkarabiliyor olmasıdır.

Günümüzde bazı sistemler hem asimetrik şifrelemeyi hem de simetrik şifrelemeyi birlikte kullanabilmektedir. Bu tür şifreleme sistemine melez sistem adı verilmektedir. Diffie-Helman ve Rivest-Shamir-Adleman algoritmaları asimetrik kripto sistemlere örnek verilebilir [11].

2.7.3. Hashing Algoritması

Algoritma, yapısı gereği tek yönlü gerçekleşen bir matematiksel işlemdir. Hash işlemine tabi tutulan bir metin sonucunda elde edilen çıktıdan yola çıkılarak orjinal metin elde edilemez çünkü hashing tek yönlü bir işlemdir. Hash işlemi sonucunda elde edilen çıktı büyük oranda bir birine benzersizdir. Ama bazen farklı uzunluktaki

metinlerin, sabit uzunlukta bir çıktıya çevrilmesinde aynı çıktılar elde edilebilmektedir. Buna "collisison" denilmektedir.

Güvenilir ve zor kırılır bir hashing için daha uzun karakter kümesi ve daha fazla bit sayısı gerekir. SHA-256 veya SHA-512 hashing algoritmasını örnek olarak verebiliriz [12].

2.8. Kriptografik Elektronik Seçim Protokolleri

Kriptografi sadece bilgi saklaması ve aktarması problemine güvenli bir çözüm aramaktan ibaret değildir. Elektronik imza, elektronik para ve elektronik seçim gibi farklı kullanım alanları da bulunmaktadır. Bu problemlere çözüm getiren protokoller, bahsi geçen şifreleme sistemlerine ek olarak, "kriptografik temel taşları" diyebileceğimiz yöntemler kullanmaktadır.

2.8.1. Sıfır Bilgi İspatları

Bu algoritmanın temel prensibi “bilinen bilgiyi bir başkasına, bilgiyi ona vermeden ispat etmektir”.

Aşağıdaki üç özellik ile sıfır bilgi kanıtı yerine getirilmelidir.

-Tamlık: Eğer verdiğimiz kanıt doğru ve eksiksiz ise alıcı bilgiye sahip olduğunuzdan emin olacaktır.

-Doğruluk: Eğer kanıtımız yanlış ise hilekarlık yapmadan alıcıyı ikna edebiliriz.

-Sır Vermemek: Eğer ifade doğru ise alıcı bunu anlayacaktır. Alıcıya verdiğimiz örnek ile bunu ispat edebiliriz.

Yukarıda vermiş olduğumuz ilk iki örnek alıcı ile etkileşime geçme yöntemidir. Üçüncüsü ise kanıtlama yöntemidir.

Sıfır bilgi protokolü matematiksel bir ispatlama yöntemi değildir. Bu ispatlama yönteminde bilgi manipüle edilerek alıcıya ispatlamak için çalışılır [13].

2.8.2. Dijital İmzalar

Gündelik hayata kullandığımız imzalar gibi, elektronik ortamda kullandığımız dijital imzalar da gönderilen bilginin kime ait olduğunu göstermek için kullanılır. Dijital imzanın oluşturulmasında ve doğrulanmasında dijital sertifikalar kullanılır. Dijital imzalar basitçe iletilebilir, başka biri tarafından asla taklit edilemez ve otomatik zaman damgalıdır. Orijinal imzalı mesajın yerine ulaştığını sağlama yeteneği, mesajı gönderenin daha sonradan reddetmesinin basit olmayacağı anlamına gelir.Bir dijital imza, mesajın şifreli olup olmadığına bakmaksızın çok çeşitli mesajla kullanılabilir. Bir dijital sertifika, herkesin gerçek olduğuna onay vereceği bir sertifika üretim yetkilisinin dijital imzasını içerir. Dijital imza bir kullanıcı, sunucu

veya bilgisayardan gönderilen bilgilerin kesinlikle gönderene ait olduğunu doğrular ve verinin başkası tarafından yollanmadığını garanti eder.

Dijital imza, veri alışverişi sırasında bilgilerin içeriğini korur, bir başka kişinin eline geçmesini engeller, bilginin sadece alıcıya gittiğini ve sadece alıcı tarafından okunacağını garanti eder.

Sayısal imza veriyi gönderenin ve alanın kim olduğunun kanıtlanmasına imkan tanır. Yani imzalanmış bir dokümanı yollayan kişi onu yolladığını inkar edemez ve alıcı da aldığını inkar edemez [14].

2.8.3. Kör İmzalar

İnternet ortamında kişisel hakların korunmasından doğan kaygılar üzerine, 1982 yılında D. Chaum "Kör Sayısal İmza" kavramını ileri sürmüştür. Bu protokolde iki taraf bulunmaktadır. İstemci taraf ve imzalayıcı taraf. Bu yöntem ile mesajı imzalayan kişi mesajın içeriğini bilmez, sadece kendisine güvenli bir şekilde ulaşan mesajı imzalar ve alıcıya yollar. Alıcı mesajın kendisine doğru ulaştığını her zaman için imzalayıcıdan kontrol edebilir. Bu şekilde mesajı imzalayan ve alan arasında güvenli bir kanal oluşturulur. Kör imza protokolünün gerçekleşmesi için gerekli olan bazı zorunluluklar vardır.

-Doğruluk: Mesaja ait olan imzanın doğruluğu imzalayıcının açık anahtarı ile gösterilebilir.

-Körleştirme: Mesajın içeriği imzalayıcıya gösterilmemelidir, kör sayısal imzanın sahibi mesaj içeriğini göremez.

-Taklit Edilemezlik: İmza, imzalayan için bir kanıttır ve başka biri taklit imza kullanarak doğrulama aşamasını geçemez.

-İzlenemezlik: Kör sayısal imza sahibi imza yayımlandığında imzanın atıldığı mesajla imza arasında bir bağ kuramaz [15].

2.8.4. Benzer Yapılı Şifreleme

Benzer Yapılı Şifreleme(Homomorfizm) özellikle elektronik seçim siteminde yararlı bir cebirsel özelliktir. Çünkü deşifreye gerek kalmadan şifreli oy pusula setleri üzerinde işlem yapmaya izin verir. İki tane kriptolanmış sayının toplamının, o sayıların toplamının kriptolanmış şekline her zaman eşit olmasını sağlayan bir özelliğe sahiptir. Elektronik oylama şemalarında aşağıdaki kavramlar kullanılır.

Örneğin; M ve C birer tamsayıdır. E() de kriptolama fonksiyonudur.

E (M + C) = E(M) + E (C) eşitliği her zaman için sağlanacaktır.

2.8.5. Mix-Net

Seçmenler oy sandığını kullanarak bir düzen içerisinde oy verirler ve seçim bittiğinde verilen oylar farklı bir sırada gelir. Bu seçmenin anonim olmasını sağlar. Bunu sağlamanın bir diğer yöntemi de Chaum tarafından ileri sürülen "mix-net" kullanımıdır. Bu protokolün temel amacı gelen ve giden mesajlar arasında gizliliği sağlamaktır. Üç farklı tipte pek çok tanım ve yapıda "mix-net" vardır.

Mix-net kullanan elektronik seçim protokollerinde, her biri bir ortak anahtar ve gizli eş bir anahtara sahip olan mix-sunucuları yetkilidir. Oy pusulaları, mix-sunucularının ortak anahtarını kullanan seçimlerden önce hazırlanmak zorundadır. Seçim aşamasında, her oylama mix-sunucuların gizli anahtarıyla başarılı bir şekilde deşifre edilerek mix-net aracılığıyla oylanır [16].

3. ELEKTRONİK OY VERME SİSTEMLERİNDE GÜVENLİK DENETİMİ

Oy verme işlemi cihazların tasarımı ile başlayıp seçimden sonra cihazların saklanmasıyla sona eren çok aşamalı bir süreçtir. Bu sürecin her aşamasında güvenlik riskleri doğabileceği için güvenlik denetimi cihazlarla sınırlı kalmayıp her aşamada yapılmalıdır.

Elektronik oy verme cihazları genellikle hem donanım hem de yazılım bileşenleri olan karmaşık sistemlerdir. Yukarıda verilen ölçütleri sağlayıp sağlamadıklarının seçim kurullarınca denetlenebilmesi ancak sistemin açık olması halinde ve o zaman da bir dereceye kadar mümkündür. Bugüne kadar görülen uygulamalarda elektronik cihazlar genellikle kar amacı güden ticari firmalarca ve özellikle yazılımları ticari sır oldukları gerekçesi ile denetime açılmamaktadır. Bu durumda sistemin denetlenmesi yalnızca dışarıdan kullanılarak mümkün olmaktadır.

Sistemlerin denetleme sırasındaki davranışlarıyla gerçek seçim sırasındaki davranışlarının aynı olup olmadığının anlaşılamaması da başka bir sorundur. Örneğin; kötü amaçlı bir kullanıcının belirli tuşlara belirli sırada basıp yazılım

dünyasında “Paskalya Yumurtası” adı verilen bir programı çalıştırarak birden fazla oy kullanması ya da rakiplerin aldıkları oyları silmesi gibi bir durumun oluşup oluşmadığının denetlenmesi imkansızdır.

3.1. Mercuri Yöntemi

Mercuri, yapılacak olan bir elektronik seçime şüphe ile yaklaşılması gerektiğini ve bu sayede sistemin iyileştirilebileceğini ve güvenilirliğinin arttırılabileceğini ileri sürmektedir [2]. Seçmenin kullanacağı elektronik oyun ve sistemde kaydedilen oyun aynı olabileceğini ve tam olarak kanıtlanabilmesini sağlayabilecek bir elektronik sistemin olmayacağını düşünmektedir.

Kriptolama sistemleri kullanılarak internet üzerinden bir elektronik seçim gerçekleştirilmesi durumunda servis reddi (Denial of Service) saldırılarına maruz kalınacağını ve saldırılara açık bir yapı oluşacağını ileri sürer. Ayrıca, kriptolama sistemlerinin kullanılması durumunda pusula üzerinde ki bilgilerin gizliliğinin sağlanabileceğinin düşünülmemesi gerektiğini ve bunun garantisinin verilemeyeceğini iddia eder [2].

Elektronik sistemlerin ne kadar güvenilir olursa olsunlar, hatalara eğilimleri olduklarını ve seçmenin zihninde herhangi bir güvensizliğeneden vermemek adına, elektronik olarak kullanılan oyların bir çıktısının kağıt olarak alınmasının gerekliliğini şart koşar. Bu yüzden, bu yöntemde seçmen oyunu elektronik olarak kullandıktan sonra ayrıca üretilen kağıt oy pusulasını bir cam arkasında görmekte, bu pusula seçmenin onayından sonra ayrı, güvenli bir kutuda biriktirilmektedir. Eğer seçmen oyunun yanlış kaydedildiğini saptarsa seçim görevlileri oyu iptal etmekte ve seçmen yeniden oyunu kullanmaktadır. Güvenli haznede biriktirilen bu kağıt pusulalar seçimden sonra gerekirse yeniden sayım veya sistemlerin denetimi için kullanılabilmektedir.

Mercuri yöntemi tercih edilerek yapılan bir elektronik seçimde, verilen tüm oyların ispatı olarak kağıt bir çıktı alınmasından dolayı en güvenilir ve en kapsamlı bir yöntemdir diyebiliriz. Fakat bu yöntem süre ve işlemler açısıdan artı maliyetler getireceğinden uygulamada diğerlerine göre bir miktar yavaşlık ve ilave kağıt kullanımı gibi sorunları beraberinde getireceği öngörülebilir..

3.2. Chaum Yöntemi

Chaum karmaşık bir pusula sistemi önermektedir. Bu sistemde bazı şifreleme yöntemleri kullanılarak seçmene oyunu kullandıktan sonra yanında götüreceği bir pusula basılmaktadır. Pusula üstündeki bilgiler şifreli olduğu için seçmenin kime oy verdiği belli olmamaktadır. Ancak her seçmen için tek olarak üretilmektedir.

Seçimden sonra oy makinesinin kaydettiği oylar bir web sitesinde yayınlanmakta ve seçmen isterse kendi verdiği oyun bu oylar arasında olup olmadığını bu pusulayla karşılaştırarak denetleyebilmektedir. Ancak bu sistem karmaşıklığı ve denetleme için seçmenin bir internet erişimi olmasını gerektirmesi nedeniyle kısa vadede uygulanabilir görünmemektedir.

Kağıt pusula kullanımının seçmenlerin oylarının doğru olup olmadığına bakmadan pusulayı onaylamaları, onaylamanın işlemin süresini uzatması ve Mercuri yönteminde ise bir itiraz halinde seçmenin oyunun belli olması gibi sakıncaları da vardır [3].

3.3. Elektronik Seçim Mimarileri

Burada inceleyeceğimiz Massachusetts Institute of Technology **(**MIT) /California Institute of Technology **(**CALTECH)üniversitelerinin ortaklaşa geliştirdikleri FROG mimarisi ve bunun yanısıra Group2 mimarisi ve Evox mimarileridir.

3.3.1. MIT/CALTECHSeçim Teknolojisi Projesi

Voting Technology Protocol (VTP) fakültesi,CALTECH başkanı David Baltimore ve MIT başkanı Charles Vest tarafından 2000 yılı Amerika Birleşik Devletleri (ABD) seçimlerindeki tehdit problemlerinin tekrarını önlemek için, 2000 yılı aralık ayında kuruldu. Kuruluşundan bu yana, VTP üyeleri ABD ve yurtdışında tüm seçim süreç durumunu araştırmıştır. VTP fakültesi, araştırma kuruluşları ve öğrencilerle pek çok çalışma yapıp, akademik makaleler ve kitaplar yayımlamış ve büyük özel bir dizi projeler geliştirmiştir.

MIT/CALTECH projesinde kullanılan her bir oyun fiziksel bir biçim taşıması gerektiği savunulmaktadır. Kullanılan oyların elektronik sistemlerde kayıt altına alınması yeterli görülmemektedir. Bu yüzden adına "FROG" denen bir nesne icat edilmiştir. FROG, kayıt cihazının fiziksel şeklinin nasıl olduğunun bilinmediği varsayılarak türetilmiş olan bir terimdir. FROG, bilgisayar ekranı, elektronik ya da mekanik cihazlar, ses kayıt cihazı ya da kağıt olabilir [17].

3.3.1.1. FROG Mimarisi

FROG mimarisi pek çok yol ile desteklenebilir. FROG mimarisi, oy pusulalarının bazı elektronik cihazlarda saklanması yerine ayrı fiziksel bir ortamda tutulmasını önermektedir. Her oy pusulası "FROG" diye adlandırılan bir nesnede kaydedilir.

Bir FROG' u, üretim maliyeti 20 cent civarında olan 1-2 Kbyte' lık veriyi bünyesinde barındırabilecek kartvizit boyutlarında küçük bir kart olarak düşünebiliriz. FROG okuma/yazma hafızası ve ayrıca bir kilide sahip olan veya

içindeki verinin değiştirilmesini engelleyen “freeze” diye adlandırılan teknolojiye sahip olmalıdır. Yani sadece içindeki verinin değiştirilmesine izin vermeyen (dumb memory) bir mekanizmaya sahip olan ama bir işlemcisi olmayan küçük bir kart olmalıdır. FROG bu sayede delikli kartların ya da kağıt oy pusulalarını ikame eder. Bununla birlikte, güvenilir bir şekilde okunabilsin diye elektronik ve dijitaldir. Sistem boş FROG’ ları kullanır. Kağıt oy pusulaları gibi kağıt çıktı maliyeti yoktur. Bir seçimde kullanılmayan FROG’ lar bir sonraki seçimde kullanılabilirler. FROG’ lar küçük olduğundan saklama maliyetleri de minimum düzeydedir. Seçimin sonunda, kilitli FROG’ lar yeniden saymak ya da denetim yolları için muhafaza edilir.FROG’ un içerisinde ki veri formatı basit bir düz dosyasıdır.Oy verme işlemi için 3 farklı adım vardır:

-Kayıt (Sign in): Seçmen FROG’ u alır.
-Oy Üretimi (Vote Generation): Seçmen seçimi ile FROG’ ta ki dosyayı doldurur
-Oy Dökümü (Vote-Casting): Seçmen seçimini onaylar ve FROG’ u kilitler ve oy kutusuna bırakır.

Yapılan oy verme işlemi kağıt oy pusulaları ile oy verme işleminde ki adımlarla benzerdir.FROG’ ta ki veri formatı uluslararası bir standarttır. Bu standart FROG’ larda oy kaydı için kullanılacaktır. Aşağıdaki şekilde uluslararası bir standart olan UTF-8 formatı gösterilmektedir [18].

```
State of Massachusetts, Middlesex County, Precinct 11
Ballot Initialized by Election Official 10
Election Closes November 7, 2004 at 8pm EST
Ballot: MA/Middlesex/1; English; No rotation

You have chosen:
     U.S. President: Mary Morris
     U.S. Vice President: Alice Applebee
     Middlesex Dog Catcher: Sam Smith (write-in)
     Proposition 1 (Casino): FOR
     Proposition 2 (Taxes): AGAINST
     Proposition 3 (Swimming Pool): FOR
     Proposition 4 (Road Work): NO VOTE
```

Şekil.7. UTF-8 Veri Formatı

3.3.2. Grup 2 Mimarisi

ABD' de ki Maryland eyaleti için tasarlanmış olan elektronik seçim sistemidir. Bu elektronik seçim sistemi eyalet çapında seçmenlerin oy kullanabilmesine olanak sağlamaktadır. Bu tasarım Maryland eyaleti için elektronik seçim sistemini ayrıntılı olarak ele almaktadır. Bu elektronik seçim sistemi eyalet çapında seçmenlerin geçerli oy verebilmelerini sağlar. Eyalet çapında her oy kullanım yeri özdeş mimariyi kullanacaktır. Merkezi oy kayıt veritabanı (Voter Registration Database) tüm seçmen bilgisini içerecektir. VRDB' nin bir kopyasıseçim zamanından önce her seçim

bölgesinde hazır olarak bulundurulmak zorundadır.Bu mimari bazı kısıtlamalara sahiptir.

-Seçimler bir ya da bir kaç gün sürebilir.

-Bu sistem sadece eyalet çapında ya da daha küçük birimler için tasarlanmış olup büyük yerler için uygun değildir.

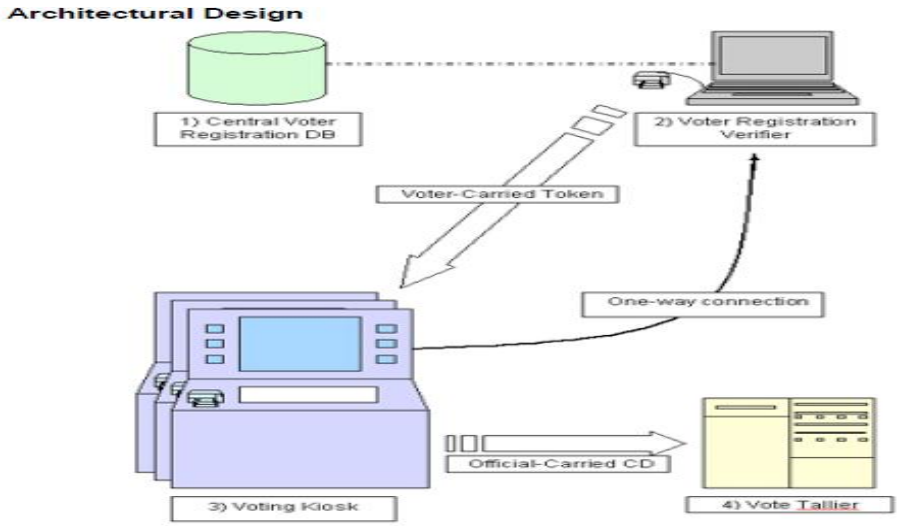
-Tüm seçim görevlileri seçmenlere yardımcı olabilmek için sistem hakkında eğitilmelidir.

-Tüm cihazlar kurcalandıkları zaman bunu açıkça belli edecek şekilde olmalıdır. Yani en ufak bir kurcalanma cihazlar üzerinde olmamalıdır.

-Rastgele seçilen cihazlar seçim öncesi ve sonrası ilave testleri başarıyla sonuçlandırmalıdır.

-Tüm cihazlar, seçimler arasında ürün yükseltme ve yeniden kuruluma katlanmak zorundadır.

-Tüm cihazlar, kullanım halinde, stoklamada ve nakil halinde iken güvenliği sağlanmak zorundadır [19].



Şekil.8. Grup2 Mimarisi

3.3.3. Evox Mimarisi

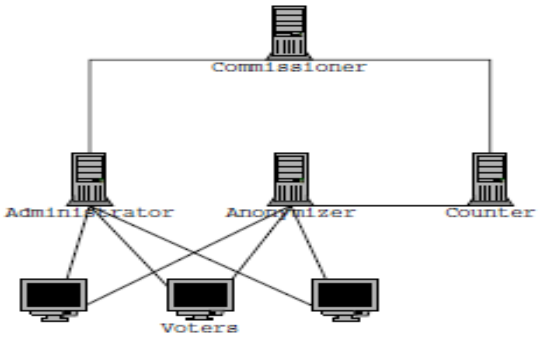
Bilgisayar bilimi için laboratuvar çalışmaları yapan araştırmacılar EVOX diye adlandırdıkları yeni bir elektronik seçim sistemi tasarlayıp uyguladılar. Bu sistem Fujioka, Okamoto ve Ohta tarafından teklif edilen bir taslağa dayanır.

EVOX protokolü Fujioka, Okamoto ve Ohta tarafından ileri sürülen FOO protokolüne dayanır [20]. FOO protokolü kırılamayan kriptgorafik fonksiyonları kullanmak kaydıyla ispat edilebilir güvenlik sağlar. Ancak, seçmenlere güvenli bir

seçim sağlamak için konuşlandırma talepleri gerçek bir seçimde uygulanamaz. Özellikle güvenli bir seçimi sağlamak, hatta oy vermemeyi seçen kişilerin bile oy verip vermedikleri kontrol edilmeli ve onlarda hesaba katılmalıdır.

EVOX protokolü bu gereksinimleri rahatlatır. Bir kez oy verildiğinde, seçmenin başka bir sorumluluğu kalmaz. Ama bu olası güvenlik zafiyetlerini ortaya çıkarır.

EVOX protokolü 5 safhada analiz edilebilir. Bunlar; hazırlık, yönetim, anonimleştirme, toplama ve sayımdır.



Şekil.9. EVOX Ağ Tasarımı

3.4. Elektronik Seçim Denetleme Yöntemleri

DRE oy makinelerini kuşatan tartışmalar Amerika Birleşik Devletleri (ABD) 2000 yılı başkanlık seçimini takiben önemli bir şekilde artmasına rağmen, Direct Recording Electronic (DRE) makineleri geliştirildi ve uzun süre kullanıldı.İlk DRE makineleri fiilen 1970' li yıllarda konuşlandırıldı ve fazlasıyla Lever makinelere benziyordu. 2000 yılı ABD başkanlık seçiminden önce DRE kullanımı oldukça yavaş gelişti. 2000 yılında yapılan ABD başkanlık seçiminin etkisi ile DRE kullanımı son

yıllara oranla pazarını arttırdı. Pazar paylaşımında Lever makineler ve delikli kart sistemleri düşüş gösterirken, DRE cihazlar ciddi bir pazar payına erişti.

Oylama cihazları gittikçe artan inceleme altına girdiğinden pek çok kişi, DRE oy verme sistemlerinde kullanılan oyun kağıt çıktı ile garanti altına alınmasında ısrar etmeye başladı. Epeyce siyasi grup tüm DRE makinelerin yazıcılarla donatılmasını zorlama amacıyla kuruldu. Bu grupların en ses getireni Doğrulanmış Seçim Kuruluşudur (Verified Voting Foundation).

3.4.1. Seçmen Doğrulamalı Kağıt Denetim Sistemi

Seçmen doğrulamalı kağıt denetim sistemi (Voter Verified Paper Audit Trail, VVPAT) DRE güvenliği üzerindeki tartışmalardan daha önce gelir. Rebecca Mercuri Mart 1992 yılında "Physical Verifiability of Computer Systems" adlı eserinde ilk olarak bu sistemi tanıtmıştır. VVPAT arkasındaki fikir oldukça basittir.

-Seçmenler seçimlerini yapmak için DRE' yi kullanır.

-Seçmenler seçimlerini bitirdiklerinde, DRE' de ki bir tuşa basarlar ve cam bir panelin arkasında yaptıkları seçimin bir çıktısı görünür.

-Seçmenler kağıt üzerine verdikleri oyun doğru bir şekilde çıkıp çıkmadığını kontrol ederek onay vermek için çıktıyı okurlar.

-Seçmen çıktıyı kabul ederse, yazıcıdan çıkan kağıt güvenli bir oy pusula kutusunda saklanır. Diğer yandan, seçmen çıktıyı kabul etmezse, tekrardan oy vermeye başlar. Kabul edilmeyen oy pusulaları kabul edilmediklerininanlaşılması için işaretlenir ve oy pusulası kutusunda saklanmaz.

Mercuri ilk defa bu sistemi önerdiğinde , hiçbir DRE tedarikçisi onu uygulamadı. İlk tekliften sonraki 10 yıldan daha fazla süre sonra Avi Rubin'in raporu ve artan güvenlik kaygıları ticari satıcıları VVPAT sistemini uygulamaya

sevk etti. Hali hazırda hemen hemen tüm DRE satıcıları VVPAT uygulamasının birkaç çeşidini desteklemektedir [4].

3.4.2. Seçmen Onaylı Ses Denetleme Suret İzi

Seçmen onaylı ses denetleme suret izi (VVAATT), daha ucuz ve muhtemel daha verimli seçim denetim aracı için yeni bir düşüncedir. Ted Selker yayınlamış olduğu "Fixing the Vote" adlı bilimsel akademik makalesinde "Seçmen onaylı ses denetim kopya izini (VVAATT) tanıtmıştır. VVAATT, VVPAT' ye bazı kritik farklılıklar hariç pek çok yönden benzemektedir. Bir seçmenin izlemesi gereken prosedürler aşağıdaki gibidir:

-Seçmen oy kabinine girer ve kulaklığı takar.

-Seçmen normal olarak oy verme işlemine başlar.

-Seçmen yaptığı her bir seçim için, kulaklıkta bir onaylama sesi duyar. Örneğin; seçmen A adayını seçtiğinde, DRE seçili adayın A olduğunu seçmene sesli olarak duyuracaktır. Bu ses onayı seçmenin yaptığı her önemli hareket için duyulacaktır. A adayını seçtiniz, A adayını seçmediniz, oyunuzu teslim ettiniz gibi.

-DRE ses çıktısı, bir ses kaseti gibi fiziksel bir ortamda seçim oturumunu kaydeden VVAATT kayıt birimine teslim edilecektir.

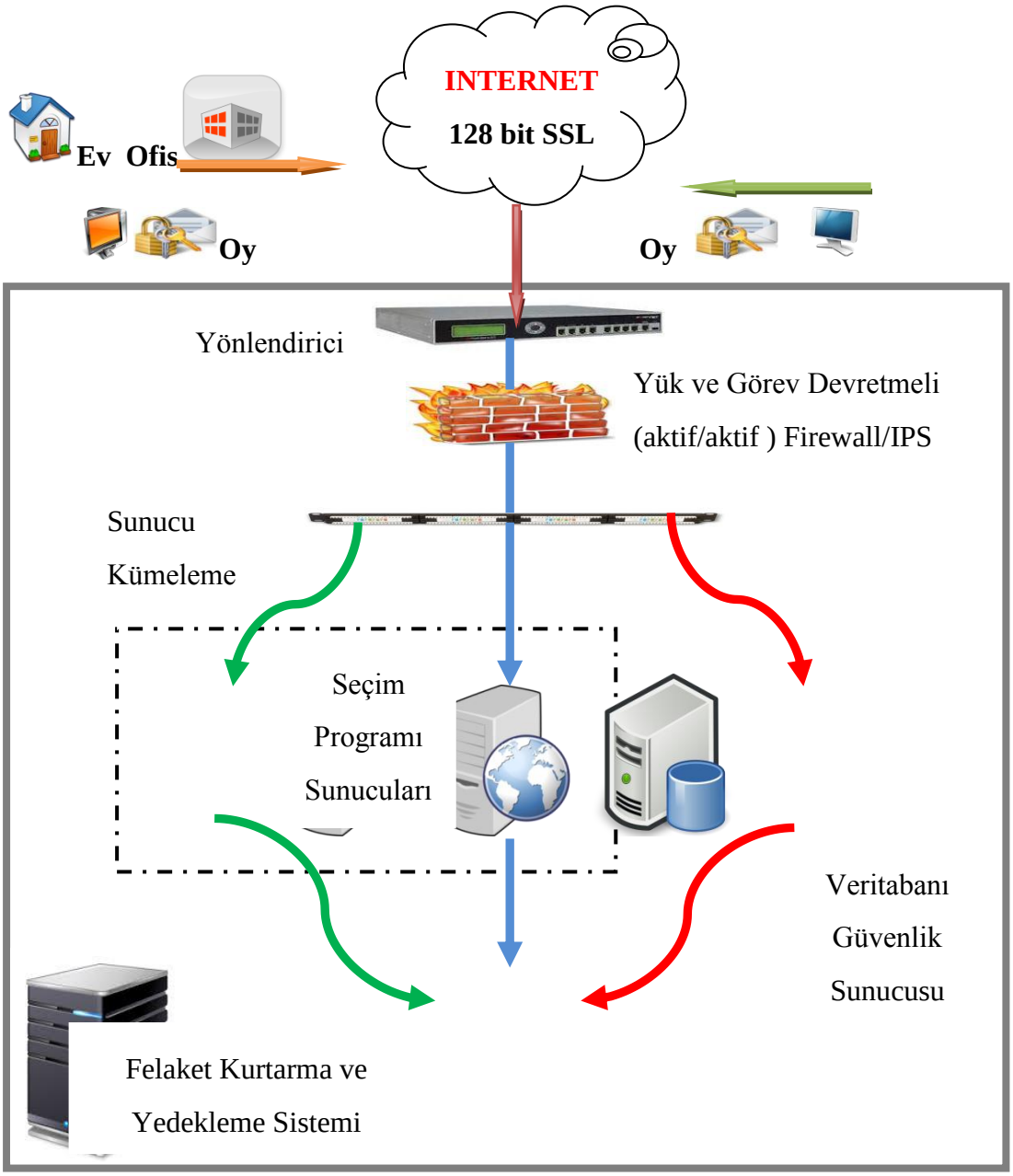
-Seçmenler oturum sonunda oylarını teslim ederler ve oy kabininden ayrılırlar.

VVAATT ve VVPAT arasındaki en önemli fark VVPAT oy kullanım oturumunun sonunda seçmenin gerçekleştirdiği gecikmeli onayın aksine VVAATT sisteminde meydana gelen hemen onaylamadır. Seçmen A adayını tuşladığı zaman, seçmen A adayı için denetleme izi kaydını doğrular. Seçmenin seçimi ve seçimin

onaylanması arasında zaman gecikmesi yoktur. Hemen onay, ayrıca, yanlış bir adayın tuşuna basılması gibi kazara yapılan hataları azaltacaktır [4].

3.5. Internet Tabanlı Elektronik Seçim Sunucularına Saldırı Teknikleri Ve Güvenliğinin Sağlanması

Internet tabanlı elektronik seçim sistemi programının çalıştığı web sunucularına aşağıdaki durumlarda erişilmesi ile kötü amaçlı yazılımlar yüklenerek, şifreler çalınarak, web sayfası ayarları değiştirilerek zarar verilebilir. Bu zararlar aşağıdaki olası saldırı yöntemleri kullanılarak verilir. Internet tabanlı elektronik seçim sistemi şekil 10' da gösterilmektedir.



Şekil.10.İnternet Tabanlı Elektronik Seçim Sistemi

-İşletim Sistemi ve Ağın Hatalı Konfigürasyonu: Sistem yöneticisinin bilgi yetersizliği sonucu bu tür hatalarla karşılaşılmaktadır. Yüklemeyi ve konfigürasyonu yapacak kişinin işinin ehli biri olması bu tür hataların önlenmesini sağlayacaktır.

-İşletim Sistemi Zayıflıkları: Elektronik Seçim programının üstünde çalışacağı işletim sisteminin tüm güncelleştirmelerinin yapılmış olması

gerekmektedir. İşletim sistemlerinin yeni sürümü çıktığında gözden kaçan açıklar ve zayıflıklar bu şekilde bertaraf edilecektir.

-İşletim Sistemini Kurulduğu Ayarlarla Bırakmak ve Güncellemeleri Yapmamak: Sistem yöneticisinin gerekli güvenlik ayarlarını ve güncellemelerini yapmaması sonrasında bu zayıflıkların saldırgan tarafından tespit edilerek sunucuya zarar vermesi işletim sisteminin güncel tutulmasıyla önlenecektir.

-Güvenlik Önlemlerinin Alınmaması: Yamaların uygulanmaması, firewall, Intrusion Detection Systems/Intrusion Prevent Systems (IDS/IPS) gibi güvenlik uygulamalarının olmaması, antivirüs yazılımlarının veya virüs veritabanının güncel olmaması sistemimizde açıklar oluşturacaktır. Bu yüzden sistem planlanırken teknolojinin getirmiş olduğu en güncel güvenlik yazılımları/donanımları kullanılmalıdır.

-Hizmet Reddi Saldırıları (DoS): Sistemleri çalışamaz hale getirmek için yapılan saldırı biçimidir. Saldırı sırasında kullanılan Internet Protocol' ler(IP) genellikle IP sahteciliği (IP spoofing) metodu ile değiştirilmiş IP' lerdir. Hizmet reddi saldırısı (DoS) ve DDoS saldırılarını, donanım ya da yazılım olarak üretilmiş IPS ve/veya Firewall engelleyemez. Bu saldırıları devletler, hacker' lar ve sıradan bilgisayar kullanıcıları yapabilirler.

DoS/DDoS saldırıları amacına ve yapılış şekline göre farklılık göstermektedir. Amaca göre DoS/DDoS iki farklı şekilde yapılır. Bunlar; bantgenişliği (bandwidth) tüketimi ve kaynak (source) tüketimidir (CPU, RAM...). Yapılış şekline göre DoS çeşitleri de şunlardır; ARP, Wireless, IP, ICMP, TCP, UDP, DHCP, SMTP, HTTP, HTTPS, DNS.

-Dağınık Hizmet Reddi Saldırıları (DDoS): Yüzlerce, binlerce farklı ortam ve sistemden eş zamanlı olarak yapılan DoS saldırılarıdır. Saldırıyı gerçekleştiren bilgisayarlara zombi bilgisayar denmektedir. Günümüzde dağınık hizmet reddi saldırısı **(**DDoS) için tercih edilen yöntemler; SYN Flood, HTTP Get/Flood, UDP Flood, DNS DoS, Amplification DoS Attacks, BGP protokolü kullanılarak yapılan

DoS, Şifreleme DoS saldırıları. Bu saldırıları gerçekleştirenleri bulmak ve önlemek şu anki teknoloji ile mümkün değildir. Çok güçlü firewall veya IPS sistemleri ile kısa bir süre hizmet devam edebilir.

Alan Adı Saldırıları: Hedef DNS sunucuya kapasitesinin üstünde DNS istekleri gönderilerek bant genişliğinin kullanılamaz hale getirilmesi yöntemidir. Bu tür saldırıda bir DoS saldırı türüdür. Güçlü firewalllar ile bu saldırı yöntemi bir süreliğine engellenebilir.

User Datagram Protocol Flood Saldırıları: User Datagram Protocol (UDP) kullanılarak oluşturulan bir DoS saldırı türüdür. Güçlü ateş duvarları tarafından bir süreliğine engellenebilir.

-Yetkili Hesaplara Brute Force Saldırıları: Deneme yanılma yöntemi ile şifrelerin ele geçirilmesi yöntemidir. Şifreleri ele geçirmek için yazılmış olan özel yazılımlar mevcuttur. Formlara güvenlik amaçlı insan mı yoksa zararlı bir yazılım mı olduğunu sorgulayıp anlayabilen (CompletelyAutomated Public Turing test to tell Computers and Humans Apart, CAPTCHA) bir bölüm konularak sistemin güvenliği sağlanır [21].

-Ortadaki Adam Saldırısı: Bir ağ üzerinde kurban ile ağ cihazları arasındaki verileri yakalayarak şifreleri ele geçirme işlemidir. En çok Address Resolution Protocol zehirlenmesi (ARP poisioning) metodu uygulanarak verilerin saldırganın eline geçmesi sağlanır.

Bu saldırıdan zarar görmemek için değerli bilgileri şifrelenmiş protokoller üzerinden göndermeliyiz. Saldırgan şifrelenmiş paketleri ele geçirse dahi içeriğini görüntüleyemez ve değiştiremez[22].

-WEB Yazılım Hataları: Web programcısının yaptığı yazılım hatalarından kaynaklanan güvenlik açıklarıdır. İyi bir test sürecinden geçirildiği takdirde gerekli açıklar giderilerek bu tür hataların sisteme zarar vermesi engellenir.

-Hatalı Atanmış Yetkiler: Sistem yöneticisi tarafından atanan yetkilerin yanlış ya da yetersiz olmasından kaynaklanan güvenlik açıklarıdır. İyi bir yetki yönetimi ile bunun önüne geçilebilir.

-Uzak Erişim Araçları Kullanılarak Sisteme İzinsiz Giriş: Genellikle bu tür saldırılar uzak erişim araçlarının (Remote Desktop, SSH, Telnet, FTP)parola ve IP bilgilerinin saldırgan tarafından ele geçirilmesi ile gerçekleştirilir. Güçlü parolalar kullanarak bu soruna çözüm üretebiliriz.

-SQL Injection: Web uygulamalarında ki en ciddi açıkların başında gelir. Bu saldırı yöntemi asp, php, cgi gibi veritabanından dinamik içerik sunan web uygulamalarına karşı yapılan bir saldırı yöntemidir. Bu saldırı web sayfalarına bir SQL sorgusu ya da komutunu enjekte etme hilesidir.

Web tabanlı uygulamalarda dinamik SQL cümlecikleri çalıştırılır. Örneğin; "SELECT * FROM musteriler;" sorgusu web uygulamasında bulunan tüm müşterileri getirecektir. Bu sorgu oluşturulurken araya herhangi bir meta-karakter girildiğinde bir SQL injection' a neden olunabilir. Meta-karakterden kastedilen programlama dillerinde kendine has özel anlam içeren karakterler akla gelmelidir. Örneğin; SQL için (') tek tırnak ve (;) karakteri bir meta-karakterdir. Bunlar SQL için çok kritik olan meta-karakterlerdir.

Web uygulama geliştiricileri SQL Injection' ı tam olarak anlamadıklarından dolayı çok ciddi hatalar yaparlar.

SQL injection veritabanından ve kullanılan dilden bağımsız olarak her türlü uygulama-veritabanı ilişkisine sahip sistemde bulunabilir ve bu veritabanlarının açığı değildir. SQL ' dan korunmak web program geliştiricisinin görevidir [21].

4. MERCURI TEMELLİ ELEKTRONİK SEÇİM MODELİ ÖNERİSİ

Bu model, bir üniversite veyabenzer bir eğitim kurumunda uygulanacak olan bir elektronik seçim sisteminin sağlaması gereken minimum ihtiyacı karşılamak için

tasarlanmıştır. Model, genel oy kullanım ihtiyaçları, güvenlik sorunlarına çözüm üretilmesi ve denetim için gerekli olan alt yapının hazırlanması ile ilgili bilgiler içermektedir.

4.1. Giriş

Seçim sistemi, oldukça karmaşık bir yapıya sahip olup uygulanacak olan seçim sistemi hiç kimsenin aklındabir şüphe bırakmayacak şekilde tasarlanmış olmalı ve denetime açık bir yapıya sahip olmalıdır.

Tasarlanan bu seçim modeli, Rebecca Mercuri' nin akademik doktorası referans alınarak hazırlanmıştır [2]. Ayrıca, kriptoloji biliminin tanıtımına destek veren ve kar amacı gütmeyen uluslararası bir organizasyon olan IACR' nin kabul gördüğü minimum elektronik seçim sistemi kriterlerine de uyulmuştur [9].

Tasarlanan bu modelde oy kullanabilecek öğretim görevlilerinde bulunması gereken şartlar aşağıda sıralanmıştır. Bunlar;

-Öğretim görevlilerinin hepsi bilgisayar kullanımına engel teşkil etmeyecek görme ve işitme duyularına sahiptir.

-Oy kullanacak olan öğretim görevlileri oy kullanımına izin veren özel olarak üretilmiş yongalı kartlara sahiptir.

-Seçim yapılacak üniversite veya yüksek teknoloji enstitüsünde herhangi bir kadroda görev yapan öğretim üyeleri oy kullanabilirler.

-2547 sayılı kanunun 40/b maddesi uyarınca kendi üniversitelerinden başka bir üniversite veya yüksek teknoloji enstitüsüne görevlendirilenler sadece kadroların bulunduğu üniversite veya yüksek teknoloji enstitüsünde oy kullanabilirler.

-2547 sayılı Kanunun 38. maddesi uyarınca görevlendirilenler kadrolarının bulunduğu yükseköğretim kurumunda oy kullanabilirler.

-2547 sayılı Kanunun 39. maddesi uyarınca yurtiçi ve yurtdışında uzun süre ile görevlendirilenler oy kullanabilirler.

-Doçent ve Profesor unvanına sahip ancak akademik başka bir kadroda bulunan öğretim elemanları oy kullanabilirler.

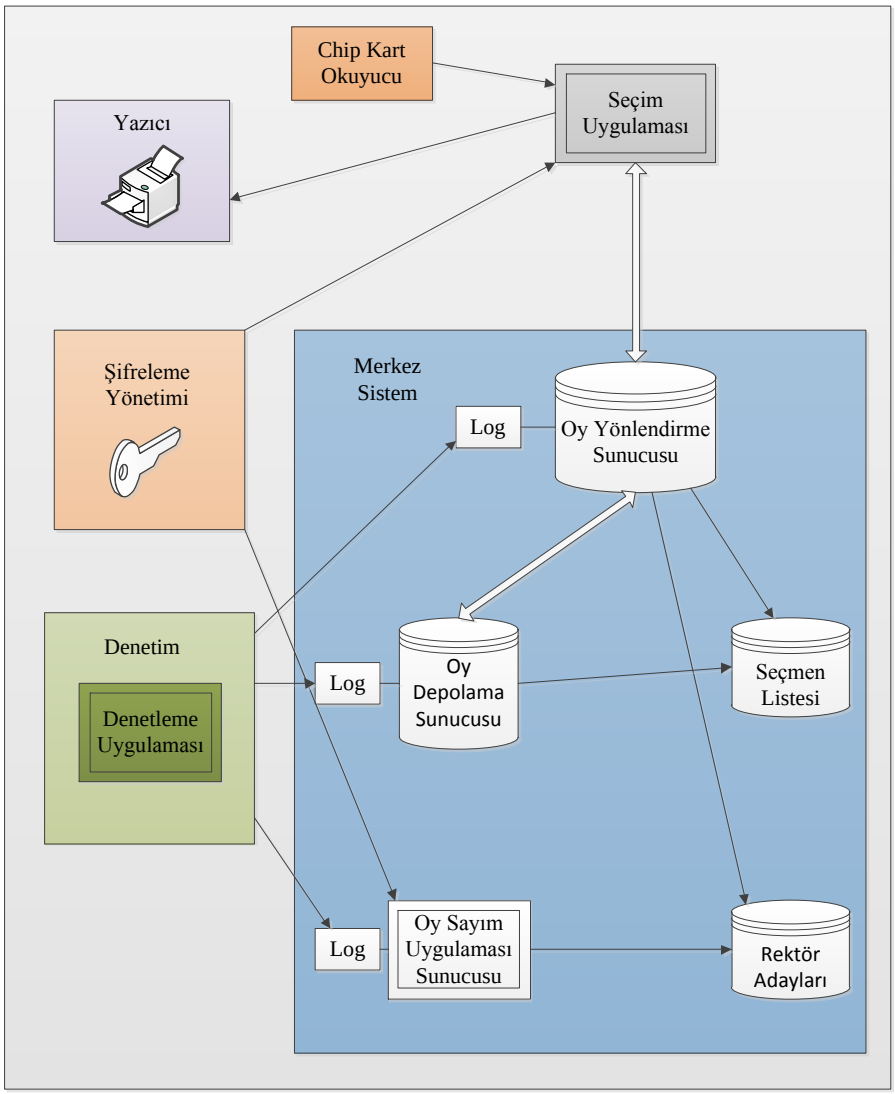
-Uzun süreli olarak bir başka üniversitede yan dal eğitiminde olan öğretim üyeleri, seçim esnasında üniversitede olmaları durumunda, oy kullanabilirler.

-Üniversitelerin kadrolu öğretim üyelerinden ücretli veya ücretsiz izinli olanlar seçim günü üniversitede olmaları halinde oy kullanabilirler.

-Askerlik görevini yapan öğretim üyeleri ile sağlık sebebi ile raporlu öğretim üyeleri de seçim günü üniversitede olmaları halinde oy kullanabilirler [24].

4.2. Model Sistem Mimarisi

Model olarak sunulan elektronik seçim sisteminin sistem mimarisi aşağıda tasarlanarak anlatılmaktadır. Sistemde kullanılan yazılımın açık kaynak kodlu programlama dili olduğu varsayılmıştır. Sistem, incelemek ve denetlemek isteyen tüm ilgili birimlere açık olarak tasarlanmıştır. Bu ilgili birimler; siyasi partiler, üniversiteler,hukukçular, STK' lar, YSK ve özel denetleme kuruluşlarıdır.



Şekil.11. Model Sistem Mimarisi

4.3. Seçim Sistemi Elemanları

Tasarlanan bu model bazı seçim sistemi elemanlarına sahiptir. Bunlar; seçmen, merkezi sistem, şifreleme yönetimi, denetleme, oy yönlendirme sunucusu, oy depolama sunucusu ve oy sayım uygulamasıdır.

-Seçmen: Daha önceden rektörlük tarafından hazırlanan öğretim üyesi bilgi sistemi doğrultusunda, oy vermesinde herhangi bir engel olmayan kişi ya da kişiler seçmen olarak oy kullanabilecektir. Seçmen, seçim yerindeki (fakülte, rektörlük

binası gibi.) bilgisayarda sahip oldukları yongalı kartı bilgisayara okutarak şifreli veya dijital imzalı oyu kullanır ve merkezi sisteme gönderir.

-**Merkezi Sistem**: Sistem bileşenleri Rektörlüğün sorumluluğu altındadır. Seçimin birleşik sonuçlarının bilgisi alınana kadar, oyları alır ve işler.

-**Şifreleme Yönetimi**: Sistemin anahtar şifreleme çiftlerini (key pairs) oluşturur ve yönetir. Ortak anahtarlar (public keys) seçmenlerin uygulamalarına entegre edilmiştir. Özel anahtarlar (private keys) ise, oy sayım uygulamasına gönderilir.

-**Denetleme:** Merkezi sistemden gelen giriş bilgilerini kullanarak, ihtilafları ve şikayetleri çözer.

-**Oy Yönlendirme Sunucusu:**Seçmen bilgilerini doğrular, seçmene seçime katılan tüm rektör adaylarını gösterir ve dijital olarak imzalanmış ve şifrelenmiş elektronik oyları teslim alır. Elektronik oy, hemen oy depolama sunucusuna gönderilir ve oradan alınan onay seçmene iletilir.

-**Oy Depolama Sunucusu:** Oy yönlendirme sunucusundan elektronik oyları alır ve onları depolayarak saklar.

-**Oy Sayım Uygulaması:** Oy sayım sunucusu, elektronik oy verme işlemi çıktılarını ve oyları tasnif ederken sistemin özel anahtarını (private key) kullanır ve sayım bu şekilde gerçekleştirilir.

4.4. Mercuri Temelli Elektronik Seçim Modeli Prosedürleri ve İşleyişleri

Seçmenin oyunu kullandığı andan itibaren arka planda bir takım prosedürler çalışarak, kullanılan oyların şifrelenmesi, kaydedilmesi veya iptali, denetimi ve seçim mahallerinden sisteme erişim işlemleri gerçekleşir.

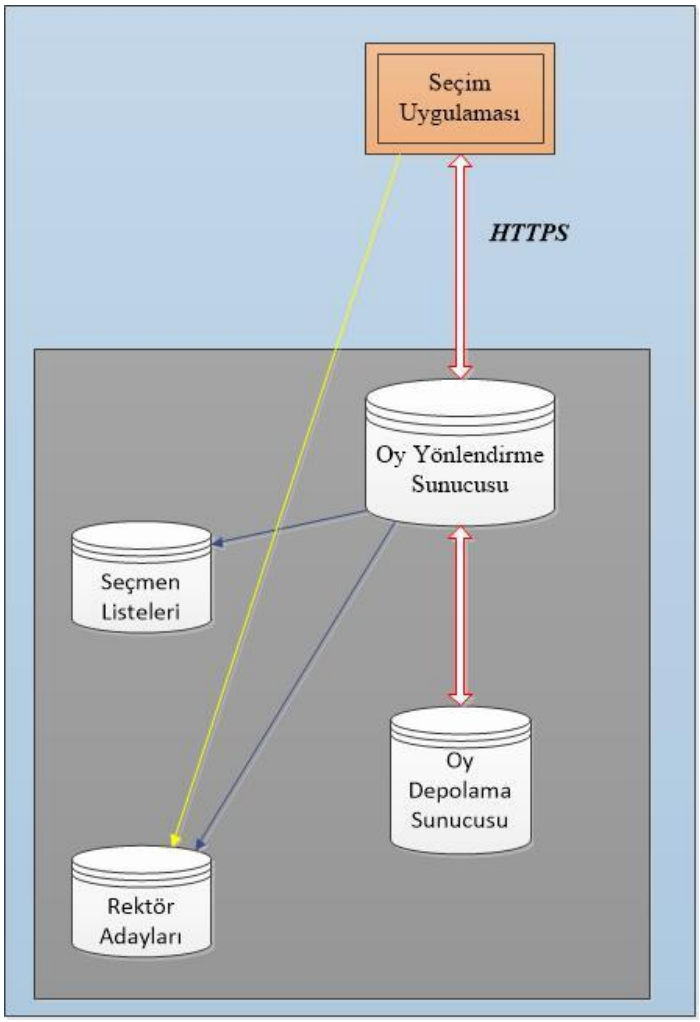
4.4.1.Şifreleme Yönetimi

Kullanılan şifreleme yönetim prosedürleri ve güvenlik sistemi, sistemin temel ihtiyaçlarının (oylamanın gizliliği ve kişiselliği) yerine getirilmesinde görev alan kritik bileşenlerden biridir.

Sistemde oylama gizliliğini garanti etmek için kullanılan kriptografi, asimetrik kriptografi teknolojisidir. Asimetrik kriptografi, simetrik kriptografiye göre şifre uzunluğundan kaynaklanan daha yavaş çalışmasına rağmen bütünlük, kimlik doğrulama ve gizlilik gibi daha güçlü yönler barındırdığından tercih edilmiştir. İstemci yazılımına entegre edilen ortak bileşen bir sistem şifreleme çifti (key pairs) oluşturur ve oyu şifrelemek için kullanır. Şifreleme çiftinin özel bileşeni, kullanılan oyun şifresini çözmek için oy sayım uygulamasında kullanılır.

4.4.2.Oylama ve Oyların Muhafazası

Oylama, seçmen ve oy yönlendirme sunucusu arasında gerçekleşen bir işlem olarak yapılır. Oy yönlendirme sunucusu, seçmen ve rektör adaylarını yerel veritabanında sorgular ve nihayetinde kullanılan oyu, oy depolama sunucusuna gönderir. Aşağıda bu işlemin nasıl gerçekleştirildiğini gösteren bir yapı çizilmiştir.



Şekil.12. Oy Verme

Seçmen uygulaması web ortamında (intranet, extranet ya da internet) çalışır. HTML sayfalarına ek olarak, imzalı bir applet, oyu şifrelemeye izin veren seçmenin tarayıcısına yüklenir ve dijital olarak sonucu şifreleyerek imzalar. Seçmen uygulaması seçmenin seçimini yapmadan önce son bir kez seçiminde değişiklik yapıp yapmayacağını sorar ve onay alır. Onay alırsa şifreleme işlemini gerçekleştirir. Genel kural olarak seçmene birden fazla adayı aynı anda seçebilme izni verilmemektedir. Seçmen birden fazla adayı aynı anda seçmeye çalıştığında ekrana bir uyarı gelmektedir. Ancak, seçmen istediği takdirde boş oy kullanabilmektedir. Kullanılan boş oylar geçersiz oy kabul edilmektedir.

Oy yönlendirme sunucusu, üzerinde çalışan uygulamalarla birlikte bir web sunucusu olarak tasarlanmıştır. Oy yönlendirme sunucusu internetten ya da noktadan-noktaya direkt erişime izin veren, merkez sistemin bir bileşenidir. Tüm diğer merkez sistem bileşenlerine oy yönlendirme sunucusu üzerinden erişilebilmektedir.

Oy kullanım işlemleri aşağıdaki gibi meydana gelir.

-Seçmen yongalı kartını seçmen uygulamasına okutur ve onay sonrasında oy yönlendirme sunucusuna erişir.

-Oy yönlendirme sunucusu seçmen listesi veritabanından seçmenin yongalı kartından bilgileri alır ve bir sorgu döner ve seçmenin bilgileri ekrana gelir.

-Oy yönlendirme sunucusu oy depolama sunucusundan böyle bir seçmenin daha önceden oy verip vermediğini öğrenmek için bir sorgu gerçekleştirir. Eğer böyle bir durum var ise seçmen bu konuda ikaz edilir ve tekrarlı oy kullandırılmaz.

-Oy yönlendirme sunucusu rektör adaylarını veritabanından bir sorgu gerçekleştirerek alır ve seçmene sunar.

-Seçmen bir adayı seçer.

-Seçmen seçtiği adayı onaylar.

-Uygulama, seçimi şifreler ve ortak anahtara rastgele bir sayı atanır.

-Seçmen uygulaması, dijital olarak imzalanmış oyu ve oturumun başlangıcı esnasında dijital imzayı veren kişinin yetkilendirilmiş aynı kişi olup olmadığını, resmi olarak doğrulayan oy yönlendirme sunucusuna iletir.

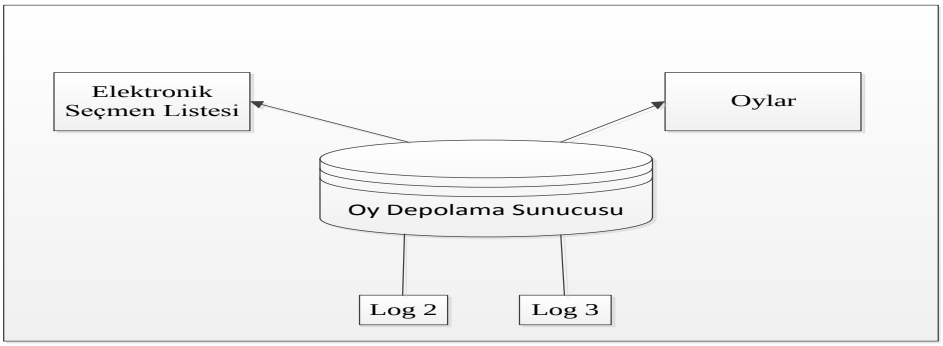
-Oy yönlendirme sunucusu, oy depolama sunucusuna kullanılan oyu gönderir. Oy depolama sunucusu, daha sonra imzalanan oya eklenen dijital imzanın geçerliliğini onaylayarak bir sertifika elde eder.

-Oy depolama sunucusu oyun alındığına dair bir onayı oy yönlendirme sunucusuna gönderir. Aynı mesaj seçmene de iletilir ve yazıcıdan kullanılan oyun bir çıktısı alınır. Kullanılan oy ve yazıcıdan alınan çıktı aynı ise oy verme işlemi tamamlanmış olur. Oyun alındığına dair gelen bilgi log 1 dosyasında saklanır.

-Elektronik seçim sonlandıktan sonra oy yönlendirme sunucusu tüm iletişimi durdurur.

4.4.3. Oy İptali

Oy depolama sunucusu üzerinde çalışan uygulama, oy iptal ve depolama safhası bileşenidir. Bu sürecin sonucu, elektronik oy veren seçmen listesi ve oylardır. Oy iptal edildiğinde, seçmen oy kullanma aşamasındaki tüm adımları baştan itibaren yapmak zorunda kalır. Her iptal edilen oy log 2 dosyasına kaydedilir.

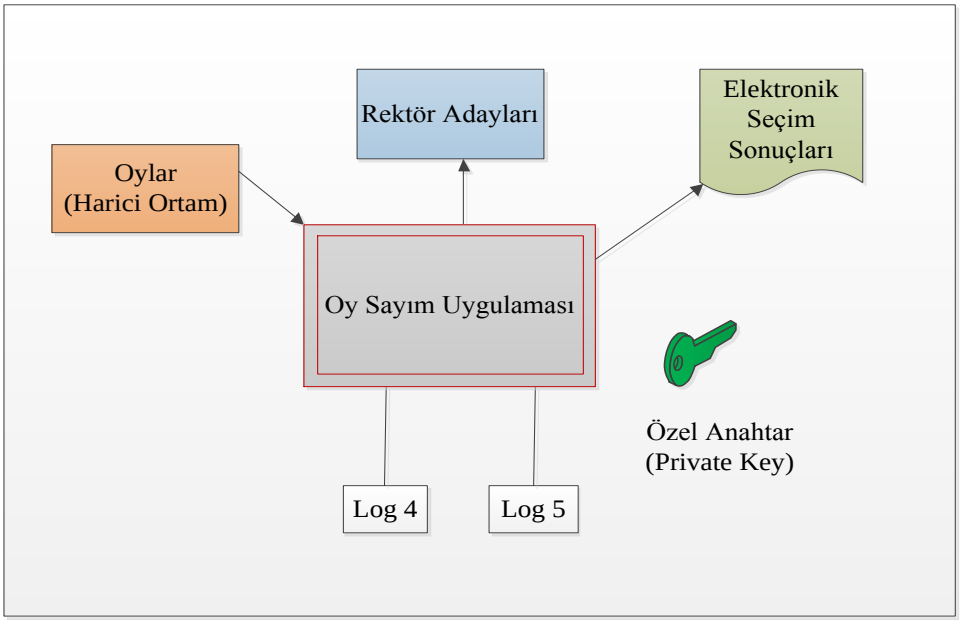


Şekil.13. Oy İptali

4.4.4. Oyların Sayımı

Oy sayım işleminin tekrarlanabilir olması gereklidir. Bu işlem, oy sayım uygulaması sonucunda oluşan bir donanımsal arızanın meydana gelmesi durumunda, bir başka bilgisayarda sayım yapılmasının mümkün hale getirdiğinden sigorta niteliği taşımaktadır.

Oyları saymak için, sistemin özel anahtarı, anahtar yönetim prosedürleri uyarınca anahtar yöneticisi tarafından çalıştırılır. Oy sayımı, oy depolama sunucusundan harici bir ortama (harici HDD, NAS, SAN gibi) aktarılarak elde edilen oylarla yapılmaktadır.



Şekil.14. Oy Sayımı

Özel anahtarlar (private keys) kullanılarak oyların şifreleri çözülür. Orijinal oylar muhafaza edilir. Şifresi çözülen oylar rektör adayları ile karşılaştırılarak kontrol edilir. Oy boş kullanılmışsa, geçersiz olduğu bildirilir ve aynı bildiri log 4 dosyasına kaydedilir. Geçerliliği saptanan oylar log5 dosyasına yazılarak kaydedilir.

4.4.5. Denetim

Model olarak sunulan bu elektronik seçim sisteminde farklı safhalarda 5 adet log dosyası oluşturulmaktadır. Bunlar:

Log 1: Oyların alınması ile ilgili bilgileri barındırır.

Log 2: İptal edilen oyların bilgisini içermektedir.

Log 3: Sayılacak oyların bilgisini tutmaktadır.

Log 4: Geçersiz oyların bilgisini içermektedir.

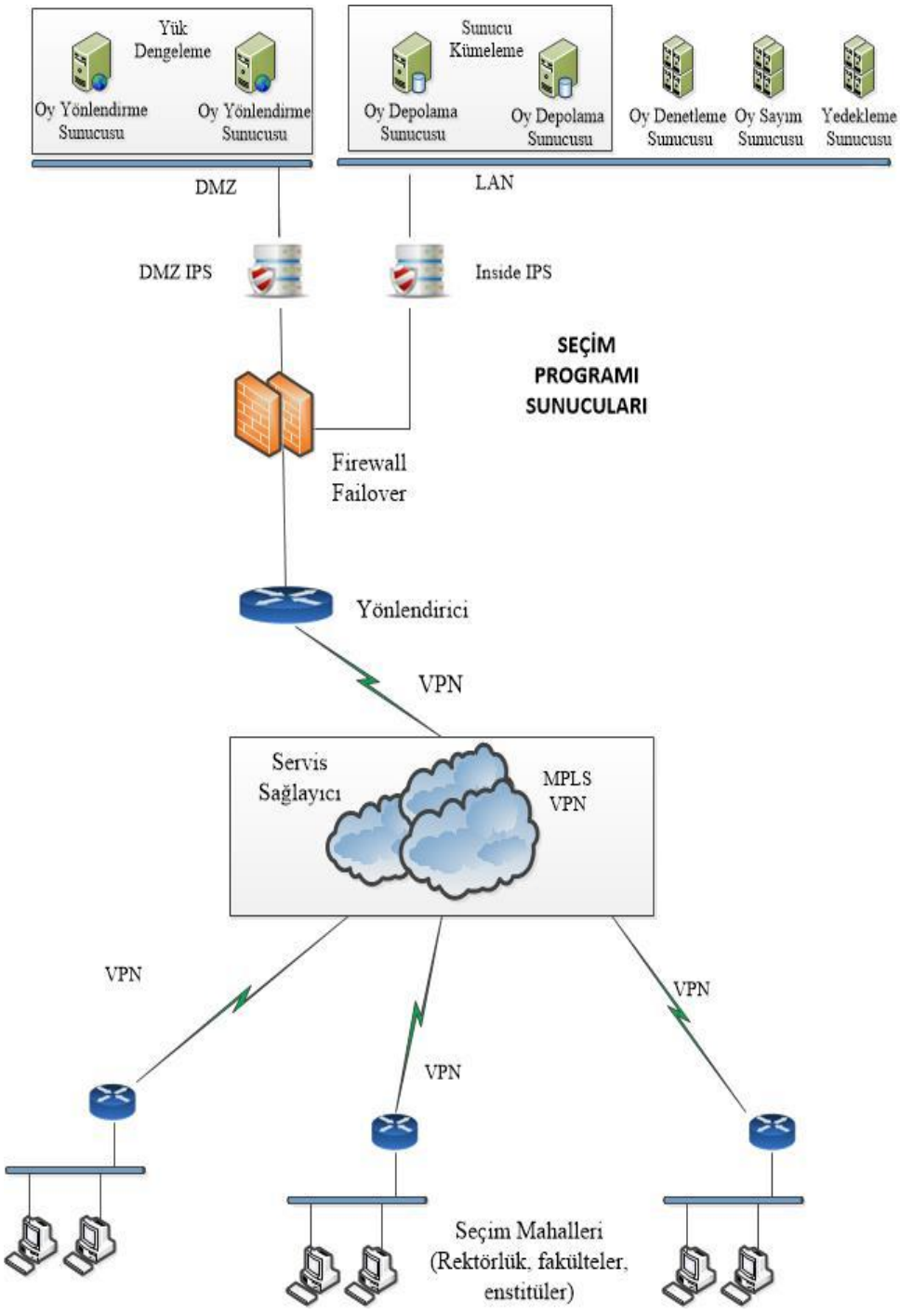
Log 5: Sayılan oyların bilgisi bu log dosyasında mevcuttur.

Tüm log dosyaları yaratıldığı zaman bilgisini taşımaktadır. Ayrıca kriptografik şifreleme ile hileyekarşı ispat niteliği taşımaktadırlar.

4.5. Seçim Sunucularına Erişim

Sunucuların bulundurulacağı merkez veya merkezlerde, web sunucular yük dengeleme sistemi (Load Balancing) ile çalışıyor olup oy depolama sunucularında da sunucu kümeleme teknolojisi kullanılmaktadır. Denetleme sunucusu ve oy sayım sunucusu için de gerek görülürse kümeleme mantığı uygulanabilmektedir. Yük dengeleme teknolojisi kullanılarak çalışan web sunucuları sistemin verimli şekilde çalışmasını sağlamakta ve erişimdeki yavaşlıkları gidermektedir. Oy depolama sunucularına uygulanan kümeleme teknolojisi (clustering) ile veritabanına kayıt işlemleri daha hızlı bir şekilde gerçekleşmekte ve gecikmelerin önüne bu şekilde geçilebilmektedir. Merkezde veya farklı yerlerde konuşlandırılmakta olan bir yedekleme sistemi ile de tüm sistemin yedeklemesi yapılabilmektedir. Sunucuların güvenliğini sağlamak için saldırı engelleme sistemi olan IPS sistemleri ve sunucu üzerinde çalışan programlara erişim sağlayabilmek için firewall' lar kullanılmaktadır. Noktadan noktaya bağlantı gerçekleştirilmekte olup, servis sağlayıcının MPLS VPN alt yapısı kullanılarak kiralık hat, G.SHDSL vb. iletişim hatları üzerinden VPN teknolojisi ile erişim sağlanmaktadır.

Seçmenlerin oy kullanacağı seçim noktalarında her bilgisayara bir yazıcı bağlanmıştır. Bu yazıcılardan alınan çıktı kullanılan oyun doğruluğunu garanti etmektedir. Seçmenin seçim sunucularına ulaşıp oy verebilmesi için, noktadan noktaya internete kapalı bir bağlantı gerçekleştirilmektedir. Seçmen bu şekilde bağlantı gerçekleştirip oyunu kullanabilmektedir.



Şekil.15. Seçim Sunucularına Erişim

5. SONUÇ

Tasarlanan bu modelde, seçmenlere seçim esnasında kullanacakları oyları kontrol edebilme hakkı verilmiştir. Bunu sağlamadığımızda, seçmenlerin yanlış oy kullandıklarında verdikleri oyu değiştirebilme veya iptal edebilme yeteneklerini ellerinden alınmış olur. Tasarlanan bu sistemde oy kullanım işlemi bittiğinde, yazıcıdan kullanılan oyun bir çıktısının alınmış olmasına rağmen kullanılan oyun iptal edilebilme hakkı da ayrıca seçmenlere tanınmıştır. Buradaki amaç; hiçkimsenin aklında şüphe kalmadan kullanılan oyun doğruluğundan emin olunması ve kötü amaçlı kişilerin sistemin düzgün çalışmadığı iddiası ile sisteme zarar vermesini engellemektir.

Önerilen bu model oyların sayılmasına ve denetlenmesine izin vermektedir. Herhangi bir itiraz halinde elektronik sistemdeki oy miktarı ile kağıt pusulalardaki oylar sayılarak karşılaştırılabilmektedir. Bu işlem sistemin güvenilirliğini ispat etmektedir.

Artık günümüzde elektronik seçim gibi modern bir teknoloji çok sayıda ülkede referandumlar, yerel seçimler ve genel seçimlerde çok başarılı bir şekilde uygulanmaktadır. Ancak yaşanan güvenlik sıkıntıları ve ihlaller pek çok üniversite ve ülkede elektronik seçimlerin güvenliği hakkında araştırmalar yapmaya yoğunlaştırmıştır. Elektronik seçimin zor ve karmaşık problemlere sahip olduğu düşünüldüğünde, bu çalışmaların gerekliliğini ispatlamaktadır.

Çok yakın gelecekte ülke çapında genel seçimler de dahil olmak üzere, birçok konuda kamuoyu yoklamaları ve referandumların hızlı bir şekilde sonuçlandırılabilmek için elektronik çözümler kullanılmaya başlanacaktır. Bu tez konuya ilişkin yapılacak olan çalışmalara katkı motivasyonu taşımaktadır.

KAYNAKÇA

[1] Electronic Voting. (2005). 21.11.2013,http://bravenewballot.org.

[2] Mercuri, R. (30 Nisan 2001). Electronic Voting Tabulation Checks&Balances. A Dissertation in Computer and Information Science for the Degree of Doctor of Philosophy. University of Pennsylvania.

[3] Karagüler. T,. Şahin, M. "Elektronik Seçim Sistemleri ve Mercuri Modeli" , Akademik Bilişim 2006, Pamukkale-Denizli, 1-3 Şubat 2006.

[4] Cohen, B. S. (19.05.2005). Auditing Technology for Electronic Voting Machines. Yayınlanmamış Yüksek Lisans Tezi, MIT.

[5] Computer Center for Electronic Voting and Participation. (2011). 13.03.2014, http://www.e-voting.cc/en/it-elections/world-map/

[6] Kuzuloğlu, M.S. (2012). İnternette Gerçekleşen Bir Başarı Öyküsü: Estonya.04.05.2014,http://www.radikal.com.tr/yazarlar/m_serdar_kuzuloglu/internetle_gerceklesen_bir_basari_oykusu_estonya-1107792

[7] Ulusoy,O. (2012). Türkiye'de e-seçim çalışmaları. 10.01.2014, http://www.andsecim.com/ esecim/4/turkiyede-e-secim-calismalari/

[8] Kwak, J., Deng, R, H., Won, Y., Wang, G (Eds.) . (23 Nisan 2010).Information Security Practice and Experience 6th International, ISPEC 2010 içinde "Conference Protection Profile for E-voting Systems" s(382-395) Seoul, Korea: Springer Science&Business Media

[9] Benaloh, J., Rivest, R., Wagner, D., Yung, M. (2008). E-Voting Systems for the IACR, Requirements and Evaluation Criteria. 16.03.2014, http://www.iacr.org/elections/eVoting/requirements.html

[10] History of Voting Machines. (b.t). 27.10.2013, http://www.glencoe.com/sec/socialstudies/btt/election_day/history.shtml

[11] What is Cryptography?,(b.t). 30.04.2014,http://www.computer-network-security-training.com/what-is-cryptography/.

[12] Concept of Hashing. (b.t). 30.04.2014, https://www.andrew.cmu.edu/course/15-121/lectures/Hashing/hashing.html

[13] Goldwasser, S., Micali, S., Rackoff, C. 1985. The Knowledge Complexity of Interactive Proof-Systems.

[14] Rouse, M. Digital Signature. (2007). 01.05.2014, http://searchsecurity.techtarget.com/definition/digital-signature

[15] Chaum, D. (1982). Blind Signatures for Untraceable Payments. Department of Computer Science University of California Santa Barbara, CA.

[16] Fouard, L., Duclos, M., Lafourcade, P. Survey on Electronic Voting Schemes. (b.t). 01.05.2014, http://www-verimag.imag.fr/~duclos/paper/e-vote.pdf,

[17] Baltimore, D., Vest, C. Voting Technology Project. (2000). 06.05.2014, http://www.vote.caltech.edu/

[18] Bruck, S., Jefferson, D., Rivest, R.L. A Modular Voting Architecture ("Frogs"). (2001). 25.04.2014, http://www.brunazo.eng.br/voto-e/textos/rivest-voting1.pdf

[19] Brown, J., Dickinson, D., Stinebach, C., Zhang, J. E-voting System: Specification and Design Document. (2003). 13.04.2014, http://www.cs.jhu.edu/~rubin/courses/sp03/group-reports/group2/group2_design.pdf

[20] DuRette, B. W. Multiple Administrators for Electronic Voting. (1999). 05.04.2014, http://groups.csail.mit.edu/cis/theses/DuRette- bachelors.pdf

[21] Önal, H. DoS, DDoS ve Korunma Yöntemleri. (2009). 25.01.2014, http://www.bga.com.tr/calismalar/ddos_ataklar_ve_korunma.pdf

[22] Man in The Middle Attack. (2009). 25.01.2014, https://www.owasp.org /index.php /Man-in-the-middle_attack

[23] SQL Injection Walkthrough. (2002). 25.01.2014, http://www.securiteam.com/ securityreviews/5DP0N1P76E.html

[24] Rektör Adaylarının Seçimle Belirlenmesine İlişkin Usul ve Esaslar. (04.11.1981). 04.07.2014, http://www.yok.gov.tr/documents/43971/46386/2547_kanun.pdf/300ddf15-dd83-45a6-9ad0-dff96f8ebfea

ÖZGEÇMİŞ

05 Nisan 1971 tarihi, Sakarya ili Adapazarı ilçesi doğumluyum. İlk, Orta ve Liseyi yine aynı ilçede tamamladıktan sonra askerlik görevimi yerine getirmek için askere gittim. Acemi birliğini 1991 yılında Manisa Kırkağaç 6. Jandarma Komando Alayında tamamladım.Akabinde, usta birliğim olan Siirt 3.Jandarma Komando Tugayına gittim. Buradan 1992 yılında terhis oldum ve askerlik hizmetimi tamamladım.

Çalışma hayatına başladıktan sonra, 1992 -1994 yılları arasında Adapazarı Batı Dilleri Eğitim Merkez' inde 2 yıl ingilizce dil eğitimi aldım. Bu sırada üniversite sınavına girdim ve Gazi Üniversitesi, Bilgisayar Programcılığı bölümünü kazandım. Bu bölümden 1997 yılında mezun oldum.Anadolu Üniversitesi İşletme Fakültesi, İşletme bölümü' nden 2011 yılında mezun odum. 2012 yılında da Beykent Üniversitesi, Bilgisayar Mühendisliği Dalında yüksek lisans eğitimine başladım.

Özel ilgi alanlarım, araştırma yapma, ağ ve sistem güvenliği, veritabanı ve proje yönetimidir.

Şubat 2007' den beri, turizm acentelerine tüm alt yapı hizmetlerini sağlayan Merlin Travel Group ve medya kuruluşlarına entegre çözümler üreten BMP TV, Broadcast Mühendislik, Global Access Software gibi firmaları bünyesinde barındıran Broadcast Group şirketlerinde IT Project Director olarak görev yapmaktayım.

Yabancı dilim ingilizce olup, evli ve bir çocuk babasıyım.

Aday: Haluk ALEMDAROĞLU