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

ELEKTRONİK SEÇİM SİSTEMLERİNDE GÜVENLİK AMAÇLI ALGORİTMA ÖNERİSİ

(Yüksek Lisans Tezi)

Tezi Hazırlayan :

Halis SALMAN

İstanbul 2016

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

ELEKTRONİK SEÇİM SİSTEMLERİNDE GÜVENLİK AMAÇLI ALGORİTMA ÖNERİSİ

Yüksek Lisans Tezi

Tezi Hazırlayan :

Halis SALMAN

Öğrenci No:

140820003

Danışman:

Yrd. Doç. Dr. Turhan KARAGÜLER

İstanbul 2016

YEMİN METNİ

Yüksek Lisans tezi olarak sunduğum "**Elektronik seçim sistemlerinde güvenlik amaçlı algoritma önerisi**" 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. 18.04.2016

Halis SALMAN

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 140829003....no'lu HALİS SALMAN'ın .../.../... tarihinde yapılan tez savunma sınavı[1] sonucunda 45 dakika süreyle sunduğu ve savunduğu tezi hakkında[2] oybirliğiyle, ...kararı verilmiştir.

Bilgilerinize saygılarımızla arz ederiz.

Anabilim Dalı : BİLGİSAYAR MÜHENDİSLİĞİ
Programı : BİLGİSAYAR MÜHENDİSLİĞİ
Tez Başlığı[3] : Elektronik Seçim Sistemlerinde Güvenlik Amaçlı Algoritma Önerisi

---

Tez Sınav Jürisi	**Öğretim Üyesi**	**İmza**
Danışman	**: YRD.DOÇ.DR. TURHAN KARAGÜLER**	
Üye	**: YRD.DOÇ.DR. EDİZ ŞAYKOL**	
Üye	**: DOÇ.DR. GÖKHAN SİLAHTAROĞLU**	

[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] İleridedoğabilecekaksaklıklarınengellenmesiiçintezinbaşlığınınyazılmasıgerekmektedir.

Adı ve Soyadı : Halis SALMAN

Danışmanı : Yrd. Doç. Dr. Turhan KARAGÜLER

Türü ve Tarihi : Yüksek Lisans, 2016

Alanı : Bilgisayar Mühendisliği

Anahtar Kelimeler : Elektronik Seçim, Algoritma, Yöntem , Güvenlik, Seçim, Seçim Yöntemi, Algoritma Önerisi

ÖZ

ELEKTRONİK SEÇİM SİSTEMLERİNDE GÜVENLİK AMAÇLI ALGORİTMA ÖNERİSİ

Hazırlanan çalışma uygulanmakta olan elektronik seçim sistemlerine yeni bir güvenlik önerisi olarak elektronik seçim sistemlerinde kullanılabilmesini hedeflemiştir. Yapılan araştırmalar sonucunda, uygulanmakta olan elektronik seçim sistemlerine güvenlik kaygılarından dolayı güven az olup, uygulanan seçimlerde şüphe ile bakıldığı gözlemlenmiştir. Şüpheler ve güvenlik kaygıları göz önüne alınarak bu çalışmada seçimlerin kayıt edilme yöntemi ile ilgili elektronik seçim sistemlerine farklı bir yöntem katmak hedeflenmiştir. Bu amaçla düşünülen algoritma tanıtılmış olup, detayları tez içinde verilmiştir.

Name and Surname : Halis SALMAN

Supervisor : Asst. Prof. Turhan KARAGÜLER

Degree and Date : Master, 2016

Major : Computer Engineering

Key Words : Elektronic Voting, Algorithm, Method , Security, Vote, Voting Method, Algorithm Proposal

ABSTRACT

SECURITY ALGORITHM ADVICE ON ELECTRONIC VOTE SYSTEM

The study in hand is aimed to present a new security suggestion for the current electronic election systems. As a result of researches, it is observed that people have less confidance to the current electronic systems and they mostly take a suspicious and security concerns stance towards them due to security concerns. In this study, which has been contucted by taking these concerns into consideration , it is aimed to bring a new way of registration method to the current electronic election systems. The algorithm designed for this purpose is introduced and its details are presented in the thesis.

İÇİNDEKİLER

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR

YSK : Yüksek Seçim Kurulu
DRE : Direct Recording Electronic Systems
VVPAT : Voter Verified Paper Audit Trail
VVAATT : Voter Verified Audit Transcript Trail
HSM : Hardware Security Module
HTTPS : Secure Hypertext Transfer Protocol
MIT : Massachusetts Institue of Technology
CALTECH : California Institute of Technology
TCP : Transmission Control Protocol
IP : Internet Protokol
PIN : Personal Identification Number
DES : Data Encryption Standard
3DES : Tiple Data Encryption Standard
AES : Advanced Encryption Standard
VTP : Voting Technology Protocol
ABD : Amerika Birleşik Devletleri
IDS : Intrusion Detection System
IPS : Intrusion Prevention System
DoS : Denial of Services
DDoS : Distributed Denial of Services
CPU : Central Processing Unit
RAM : Read Access Memory
ICMP : Internet Control Message Protocol
UDP : User Datagram Protocol
DHCP : Dynamic Host Configuration Protocol
SMTP : Simple Mail Transfer Protocol
HTTP : Hypertext Transfer Protocol
DNS : Domain Name System
BGP : Border Gateway Protocol
UDP : User Datagram Protocol

CAPTCHA	**:** California Institute of Technology
SQL	**:** Structured Query Language
UTF-8	**:** 8 bit Unicode Transformation Formats
ID	**:** Identification Data

1. GİRİŞ

Oylama sistemi, kendilerini yönetecek veya temsil edecek bir veya birden fazla kişiyi seçmek amacıyla belli kurallara göre yapılan ve oy çoğunluğu esas alınarak sonuçlanan ve seçilen kişi veya kişilerin ülke yönetimi veya farklı kurum veya kuruluşları geçici yönetme yetkisi verildiği sistemdir. Seçimler daha önceden seçilmek için aday olan aday adaylarının, aday durumuna gelerek seçimlerde yarışmaları ortaya çıkan seçim sonucuna bağlı olarak sonuçlanır. Oylama sonucunda seçmenlerin çoğunluğunu alan aday veya adaylar geçici olarak yönetme veya temsil etme yetkisine sahip olurlar. Geçici süre ile seçimlerde en çok oyu alarak yetkilendirilen adaylar seçimleri yöneten bağlı bulundukları kurum veya kuruluş tarafından süresi belli olarak yönetme yetkisini alırlar.

Gelişen teknoloji her alanda olduğu gibi oylama sisteminde de etkili olmaya başlamıştır. Bazı ülkelerde oylamalar elektronik ortamlarda yapılmaya başlanmış, bazılarında ise fiilen kullanılmaya başlanmıştır. Diğer yandan elektronik seçim sistemleri gelişen teknoloji ile kullanımı artsa da şüpheleri tam olarak gidereememektedir. Genellikle elektronik ortama geçilmesine rağmen klasik yöntem seçimlerde olduğu gibi elektronik ortamda seçmenlerin seçtikleri aday, parti veya temsilcileri gösteren kağıt çıktıya ihtiyaç duyulmaktadır. Bu ihtiyaçlardan dolayı elektronik seçim sistemleri de güvenlik gerekçeleri ile farklı yöntem, algoritma ve mimarilerle geliştirilmeye devam edilmektedir. Geliştirmelerle ve yeni yöntemlerin kullanılması ile elektronik seçim sistemleri daha da yaygınlaşsa bile alanda güvenlik ve şüphelerden dolayı yeni düşünce ve fikirlerle yeni yöntem ve teknikler denenmeye devam etmektedir. Bu gerekçelerle Mercuri ve Chaum güvenlik elektronik seçim sistemlerinde denetim yapılabilecek kendi çözümlerini üretmişlerdir. Mercuri elektronik seçim sistemlerine güvenilemeyeceğini savunduğundan elektronik çıktıların gerekliliğini savunarak geliştirdiği sistemlerde oylamalar elektronik ortamda yapılmasına rağmen oylama sonucunda seçmenlerin görebileceği elektronik çıktılar üretilmektedir[1]. Chaum, kullandığı yöntemde ise pusulalarda şifreli bilgiler kullanmayı tercih etmiştir[2]. Oy kullanımı sonucunda kendileri için üretilen çıktıda, daha sonra kullandıkları oyları doğrulayabilecekleri şifreli pusulalar bulunmaktadır.

Elektronik oylamalarda yöntemlerle birlikte mimarilerin gelişiminde ve güvenilirliğinin denetlenmeleri için farklı kurum ve kuruluşlarda var olmaktadır.

Bunlardan bazıları, Massachusetts Institue of Technology/California Institute of Technology (MIT/CALTECH) üniversitelerinin ortaklaşa geliştirdikleri FROG mimarisi ve bunun yanı sıra Group2 mimarisi ve Evox mimarisi en çok bilinen mimarilerdir[3][4].

Elektronik seçim sistemlerinin denetlenebilirliğini gerçekleştirmek için bazı seçim denetleme yöntemleri geliştirilmiştir. Bu yöntemler seçmen 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 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 .

Elektronik seçim sistemleri geliştirilmeye devam ederken güvenlik ve güvenilirliğin ön planda olması gerekmektedir. Bu yüzden seçimler elektronik ortamda ve genellikle ağ iletişim sistemi kullanıldığından ağ güvenliğinin öncelikli olması gerekmtedir.

Bu tezin amacı var olan elektronik seçim sistemlerini inceleyerek, karşılaşılmış olunan güvenlik sorunlarına farklı bakış açısıyla TCP/IP kullanılarak güvenli yapılabilecek seçim sistemleri için yeni bir yöntem ve akış sunarak elektronik seçim sisteminin güvenlik şekilde uygulanmasına katkı sağlamayı hedeflemiştir.

Tez içerisinde, uygulanmakta olan klasik kağıt seçim sistemleri ve elektronik seçim uygulamalarının yöntem, mimarileri ve güvenlikleri konusunda bilgiler verilerek farklı bir bakış açısıyla kağıt yönteminden beslenen TCP/IP altyapısı kullanan bir elektronik seçim sistemi anlatılmıştır.

2. GENEL SEÇİM SİSTEMLERİ

Seçimler, belirli kurallar ve temsil edilme durumlarına belli sistemlerle yapılmaktadır. Bu sistemler çoğunluğu esas alarak yüzde veya sayısal olarak isimlendirilmektedir.

2.1 Çoğunluk Sistemi

Demokratik parlamenter rejimlere en uygun seçim sistemidir. Kuvvetli iktidarların doğması ve bir partinin tek başına iktidara gelmesine yol açar. Umumiyetle iki partili sistemleri doğurur. Kolay ve basit bir sistemdir. Oyların çoğunluğunu alan aday kazanmış olur. Liste varsa, liste kazanmış olur: a) Nispi çoğunluk, b) Mutlak çoğunluk, c) Barajlı çoğunluk olmak üzere üç çoğunluk sistemi vardır [5].

2.2 Nispi Çoğunluk

Örneğin, A,B,C partilerinin listeleri 25.000, 22.000 ve 15.000 oy alsın. En çok oy alan liste veya aday kazanmış olur. Partilerin çokluğu halinde en çok oy alamamış olan parti, mecliste çoğunluğu alabilir. Türkiye'de 1950-60 arası uygulanan nispi çoğunluk sistemiyle toplam oyları muhalefet partileri oylarından az olan bir parti, büyük bir çoğunlukla iktidar olmuştu. (1957 seçimlerinde oyların % 48'ini alan D.P. 424; oyların % 52'sini alan muhalefet partileri ise toplam 186 milletvekili çıkarmışlardır.)

2.3 Mutlak Çoğunluk

Bu sistemde, kullanılan oyların yarıdan fazlasını alan aday veya aday listesi seçimi kazanmış olur. Mesela, kullanılan oyların toplamı: 42.000 olsun. Kazanabilmek için 21.001 oy almak gerekir. Mutlak çoğunluğu almak çok zordur. Bazı ülkelerde birinci seçimde uygulanır. Kazanan olmazsa ikinci seçim yapılır.

2.4 Belli yüzde çoğunluğu sistemi

Buna n çoğunluk da denir. Kazanabilmek için aday veya aday listesinin; kullanılan oyların belli bir yüzdesinin çoğunluğunu alması gerekir. Mesela, oyların % 40'ının, % 50'sinin, % 80'inin alınması halinde kazanılmış olacağı gibi.

2.5 Seçim Kurulları

Seçim kurulları oylama öncesi hazırlıklar ve kuralları belirlemek, oylama sırasında veya sonrasında oluşabilecek usulsüzlüklerin oluşmasını engellemek amacıyla oluşturulan veya atanan kurullardır.

Seçim kuruluna örnek olarak ülkemizde bulunan Yüksek Seçim kurulu örnek olarak ele alınabilir. Yüksek Seçim kurulu (YSK), Ankara'da bulunur. Seçimlerin başlangıcından sonuna kadar düzen içinde geçmesini sağlar. Seçimlerin dürüstlüğü ile ilgili bütün işlemleri yapma ve yaptırma seçim süresince ve seçimden sonra seçimlerle ilgili bütün şikayet, itiraz ve yolsuzlukları inceler, kesin karara bağlar ve Türkiye Büyük Millet Meclisi Üyelerinin seçim tutanaklarını kabul eder. Yedi asil, dört yedek üyeden meydana gelen bir kuruldur. Bu üyelerin altısı Yargıtay, beşi Danıştay genel kurullarınca kendi üyeleri arasında gizli oyla seçilir. Bunlar aralarından gizli oyla ve salt çoğunlukla bir başkan ve bir başkan vekili seçerler. İki Yargıtay ve iki Danıştay üyesi kura ile yedek üyeliğe ayrılır. Başkan ve başkan vekili ad çekmeye dahil değildir.Seçim Kuruluna bağlı alt kurullar oluşturulmuştur. Bunlar İl Seçim Kurulu, İlçe Seçim Kurulu ve Sandık Kurullarıdır.

2.5.1 İl Seçim Kurulu

İl seçim çevresinde kanunla tespit edilen vazifeleri görür. Seçimleri düzenle yürütür. İl merkezindeki derecesi en yüksek hakim, başkandır. Diğer iki yüksek dereceli hakim de üye olur. Yargı organında iki hakim de yedek üyedir.

2.5.2 İlçe Seçim Kurulu

Her ilçe çevresinde, kanunun verdiği görevleri yapar. Seçimi düzenle yaptırır. İlçenin en yüksek dereceli hakiminin başkanlığı ile diğer altı üyeden meydana gelir. Dördü siyasi partilerden ikisi de başkanca seçilen kıdemli memurlardandır. İki de memur yedek üyesi vardır.

2.5.3 Sandık Kurulu

Sandık çevresinde seçimi yapan ve İlçe Seçim Kurulu tarafından kurulan bir başkan ve dört üyeden meydana gelir.

Seçim sonuçları hakkında şikayet ve itirazlar kanunla tespit edilmiş olup, kurullara aşağıdan yukarı doğru yapılır.

3. OY KULLANIM ESASLARI

Seçimlerin hilesiz ve adil olabilmesi için bazı esaslara uygun olması gerekmektedir [6]. Bunlar ;

- **Yeterlilik ve doğrulama**: Sadece oy kullanma hakkı olanlar oy kullanabilmelidirler;
- **Teklik:** Hiçbir seçmen birden fazla oy kullanmamalıdır;
- **Doğruluk:**Seçim sistemi oyları doğru bir şekilde kayıt etmelidir;
- **Bütünlük :**Oylar sayılmadan önce ve sonra değiştirilmemeli, taklit edilmemeli veya silinmemelidir;
- **Doğrulanabilme ve denetlenebilme:** Oyların sayımı sırasında kullanılan bütün oylarındoğru şekilde sayıldıklarını sağlamak mümkün olmalıdır. Güvenilir ve gerçekliği ispatedilebilir sayım kayıtları olmalıdır;
- **Güvenilirlik:**Seçim sistemleri herhangi bir arıza durumunda örneğin oy kullanma makinelerinin arızalanması veya internet bağlantısının tamamen kesilmesi durumunda oy kaybetmeden çalışabilir olmalıdır;
- **Gizlilik ve baskı altına alınmanın önlenmesi:**Herhangi bir seçmenin oyunu nasıl kullandığını hiç kimse öğrenememelidir. Aynı şekilde oy satılmasını veya seçmenin iradesi üstünde baskı kurulmasını zorlaştırmak için seçmenlerin nasıl oy kullandıklarını ispat edebilmeleri de engellenmelidir;
- **Esneklik :** Seçimde kullanılan aygıtlar değişik oy formlarının (örneğin adayların adının yazılması, anket soruları gibi) kullanılmasına izin vermelidir, değişik standart platformlar ve teknolojilerle uyumlu olmalı ve özürlülere erişim olanağı tanımalıdırlar;
- **Kolaylık:**Seçmenler oylarını mümkün olan en az sayıda aygıt ve en az beceri gereksinimi ile hızla kullanabilmelidirler;
- **Onaylanabilme:**Oy verme sistemleri seçim görevlileri tarafından gerekli ölçütleri sağladıklarının saptanması için test edilebilir olmalıdır;

- **Saydamlık :** Oy kullananlar oy kullanma süreci hakkında genel bilgiye ve anlayışa sahip olmalıdırlar;
- **Kabul edilebilir maliyet:**Oy verme sistemleri etkin ve kabul edilebilir bir harcama yapılarak temin edilebilmeli ve kullanılabilmelidir.

4. ELEKTRONİK SEÇİM (OYLAMA)

Elektronik Seçim, seçmenlerin dünya genelinde halen çok büyük oranda kullanılmakta olan ve sadece kağıt ortamında daha önceden belirlenen adayları genel olarak mühürle seçtikleri seçimin veya seçimlerin daha hızlı, etkili ve teknolojiden yararlanılarak yapılabilmesi için bilgisayar veya benzeri elektronik cihazlar kullanılarak yapabildikleri seçim türüdür.

4.1 Elektronik Seçim Sisteminin Uygulanışı

Elektronik Seçim sistemleri bir bilgisayar, mobil cihaz veya özel tasarlanmış cihazlarla genel olarak güvenli internet protokolü kullanılarak yapılan oy verme işlemidir. Elektronik seçim sistemlerinde oy kullanan kişilerin daha hızlı, güvenliği arttırılmış ve bir veya birden fazla platform üzerinden bir defa olmak üzere oy kullanmalarını hedeflemektedir. Halen dünyada yaygın olarak kullanılan seçimlerde belirli yerlere sandıklar kurulup, daha önceden belirlenen adayların bilgilerinin olduğu pusulalar (Şekil 1) oy kullanan kişilere verilere gizli şekilde oy kabini içinde kullandırılmaktadır. Elektronik oy kullanımında ise kimlik doğrulaması sonucunda gizli ve çok hızlı oy kullanımı yapılabilmesi hedeflenmektedir.

Şekil 1- Pusula Örneği

4.2 Elektronik Oy Kullanımındaki Ana Esaslar

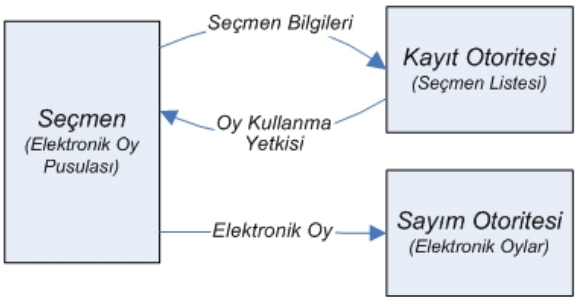
Elektronik Seçim Sistemleri oy kullanımı ve sayımı açısından kolaylıklar sağlamasına rağmen bazı esaslara öncelikli uyulmak zorundadır. Uyulması gereken esaslar hatasız çalışması için gerekli unsurlardır [7].Bunlar;

- **Seçmen:** Kayıt yaptırır ve oy kullanır.

- **Kayıt Otoritesi:** Seçmenlerin kayıtlarını yapar ve oy kullanma yetkisini verir.
- **Elektronik Oy Pusulası:** En basit anlamda adayların (iki veya daha çok) isimlerini içeren elektronik ortamdaki bilgidir.
- **Sayım Otoritesi**: Seçmenler tarafından kullanılan elektronik oyları toplar, sayar ve sonuçları ilan eder.

Diğer yandan elektronik seçim sisteminde en azından olması gereken aşamalar ve temel model aşağıdaki gibi sıralanmıştır ;

- **Ön Kayıt Aşaması:**Oy kullanmaya hakkı olan seçmenler seçim gününden önce seçim için kayıt otoritesine kayıt olurlar, gerekli hazırlıklar yapılır.
- **Kayıt Aşaması:**Seçmenler daha önce kayıt otoritesine kendilerini tanıttıkları için, seçim günü oy kullanmak için yetki isterler.
- **Oy Kullanma Aşaması:**Seçmen kendisine verilen yetki ile oyunu kullanır.
- **Sayım Aşaması:** Sayım otoritesi oyları sayar ve sonuçları ilan eder.



Şekil 2- Genel Bir Seçim Modeli

4.3 Elektronik Oy Kullanımındaki Gereksinimler

Elektronik oylama için gerekli olan temel gereksinimler bulunmaktadır. Bu gereksinimler sistemler ve seçmenler arasındaki şüphesiz güven için yerine getirilmesi gerekmektedir [7]. Bunlar;

- **Seçmenin Gizliliği:** Seçmen ile kullandığı oy arasında bir bağlantı kurulamamasıdır. Sistem tamamen bozulsa ve saldırılara maruz kalsa bile, bütün şifreler ele geçirilse bile, hatta otoriteler anlaşıp seçimi bozmaya çalışsa bile, hiçbir kurum, kuruluş veya kişi tarafından seçmenin

kullandığı oy ortaya çıkarılamamalıdır. Ayrıca seçmenin gizliliği seçim sırasında olduğu gibi, seçim sonrasında da korunmaya devam etmelidir.

- **Seçme Hakkı:** Sadece seçmen olanların oy kullanabilmesidir. Bu özellik seçim gününden önce seçmen kütüğü kayıt otoritesine sadece kendisine kanunlarla seçme hakkı verilen kişilerin kayıt yaptırabilmesini ve seçim günü önceden kayıt olmuş seçmenlere oy kullanabilme yetkisinin verilmesini kapsar. Bu durumda seçmen olmayan kişiler oy kullanamamalıdır.
- **Seçimin Dürüstlüğü:** Seçim sonuçlarının seçim bitmeden sayılamamasıdır. Seçim sürerken ve oylamalar devam ederken, oyları sayacak olan otorite de dahil olmak üzere hiçbir kurum, kuruluş, veya kişi seçim sonuçları hakkında bilgi edinememelidir. Böylece seçmenin her hangi bir şekilde yönlendirilmesi engellenmiş olur.
- **Tek Oy:**Bir seçmenin sadece bir oyunun sayılmasıdır. Seçmen değişik nedenlerden dolayı birden fazla oy kullanabiliyorsa, sadece bir oyu geçerli olmalıdır.
- **Oyun Zorla Kullandırılamaması:**Bütün otoriteler dahil hiçbir kurum, kuruluş veya kişi, seçmeni belli bir yönde oy kullanmaya zorlayamamalıdır. Seçmen oyunu özgür bir biçimde, hiç kimsenin etkisi altında kalmadan ve buna zorlanmadan kullanabilmelidir.
- **Sistemin Doğruluğu:**Oyların doğru sayılmasıdır. Seçim sisteminin doğruluğunun sağlanabilmesi için;
  - Kullanılan bütün oylar sayılmalıdır,
  - Herhangi bir oy değiştirilememelidir,
  - Herhangi bir oy silinememelidir,
  - Herhangi bir oy kopyalanıp çoğaltılamamalıdır,
  - Herhangi bir oy silme, değiştirme veya kopyalama girişiminden sistem haberdar olmalıdır,
  - Bir seçmenin yalnız bir oyu sayılmalıdır ve
  - Geçersiz oylar sayılmamalıdır.
- **Sistemin Sağlamlığı:**Kötü niyetli seçmenler, seçmen olmayan kişi veya kuruluşlar, otoriteler vb. sistemi ve seçimi bozamamalıdır. Seçim sisteminin sağlam olabilmesi için aşağıdakiler sağlanmalıdır.

- Kriptografik teknikler sadece bugün için değil gelecek için de geçerli olmalıdır. Daha güçlü ve hızlı işlemcilerle şifreler çözülememelidir.

- Teknik altyapı sağlam olmalıdır. Uygulamaya temel teşkil eden e-seçim protokolünde, kesintisiz hatlar, anonim kanallar, ...vb. kullanıldığı varsayılıyorsa bu teknik altyapı sağlanmalıdır.

- Bellek ve iletişim gereksinimleri çok iyi hesaplanmalı ve herhangi bir yetersizliğe meydan verilmemelidir.

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

- **Oy Kullanmama Hakkı:**Seçmenin oy kullanmak istemediği taktirde oy kullanmamasıdır. Bu durumda seçmen yerine bir başkası veya otoriteler oy kullanamamalıdırlar. Ayrıca seçmenin oy kullanmama hakkı olmakla birlikte, oy kullanmamaya zorlanamamalıdır ve seçme hakkı elinden alınamamalıdır.
- **Oy Kullanmaktan Vazgeçme Hakkı:**Seçmenin oylama işlemine başladıktan sonra ve oyunu göndermeden önce herhangi bir zamanda oy kullanmaktan vazgeçebilmesidir. Bu durumda seçmen yerine bir başkası veya otoriteler oy kullanamamalıdırlar.
- **Boş Oy Kullanma Hakkı:**Seçmenin boş oy kullanabilmesidir. Boş oylar da diğer oylar gibi silinememeli, değiştirilememeli ve kopyalanamamalıdır.
- **Sonuçların İlan Edilmesi:**Seçim sonuçları ve gerekli bilgiler seçim sonunda basın yayın yoluyla ve İnternet aracılığıyla ilan edilir.
- **Sistemin Geçerlenebilirliği:**Sayım sonucunun doğru olduğunun gösterilebilmesidir.
- **Sistemin Doğrulanabilirliği:**Seçimin ve sayımın doğru şekilde yapıldığının gösterilebilmesidir.
- **Bireysel Doğrulama:** Seçmenin oyunun sayıldığından emin olabilmesidir. Klasik kağıt oy pusulalı seçim sistemlerinde bireysel

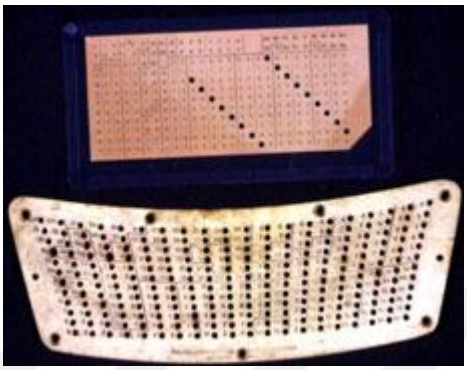
doğrulama yapılamamaktadır, ancak sistemin akışı itibariyle seçmenin sandığa oyunu bizzat atması bir çeşit bireysel doğrulama olarak kabul edilebilir.

- **Sistemin Etkinliği:**Kayıt, seçim ve sayım gibi işlemlerin tamamı etkin bir biçimde yapılmalı, bekleme süreleri en aza indirilmelidir. Klasik seçimlerle kıyaslanınca en azından oylar daha kısa sürede sayılmalıdır.
- **Kolay Kullanım:**Seçmenin oyunu kullanabilmesi için özel yeteneklere sahip olmak zorunda olmaması ve oy kullanmak için ekstra cihaz veya ekipman kullanmamasıdır. Ayrıca kullanıcı ara yüzlerinin ve seçim ortamının ergonomik olmasına dikkat edilmelidir. Ek olarak, seçmenin oyunu kullandıktan sonra, tekrar bir şey yapmasına gerek duyulmamalıdır.
- **Açık Yazılım:**Açık yazılım yapılmalı ve kaynak kod incelemeye açık olmalıdır. Sistemin güvenliği kaynak kod gizliliğine bağlanamaz. Sadece şifreler gizli olmalıdır ve iyi saklanmalıdır.
- **Yedekleme ve Fiziksel Koruma:**Sistemin herhangi bir teknik arızaya karşı yedekleme ve fiziksel koruma mekanizması olmalıdır. Tek bir elektronik cihaza güvenilmemelidir. İlan panoları kullanılarak işlemler kayıt altına alınabilir.
- **Seçimin Şeffaflığı:**Oyların ve seçmenlerin gizliliğine zarar vermeden, e-seçim sistemlerinde maksimum şeffaflık hedeflenmelidir. İlan panoları, herkes tarafından görülebilen elektronik listeler, ...vb kullanılarak seçimin herkes tarafından izlenebilmesi sağlanmalıdır. Sistemin güvenliği kullanıcılar ve otoriteler arasındaki mesajların gizliliğine bağlanamaz.
- **Oyların Saklanması:**Oyların ve gerekli seçim bilgilerinin sayım sonrasında, elektronik ve basılı ortamda saklanmasıdır.
- **Oyların Tekrar Sayılabilmesi:**Hem elektronik hem basılı ortamda saklanan oyların gerekirse yeniden sayılabilmesidir.

4.4 Elektronik Oylamada Denenmiş Olan Sistemler ve Donanımlar

Elektronik seçim sisteminde denenmiş olan sistemlerin uygulanışı ile ilgili farklı donanım ve yöntemler vardır. Bunlar aşağıdaki gibidir;

Delikli Kartlar:1880 yılının sonlarına doğru Herman Hollerith tarafından Baltimore Sağlık Kurulu (Baltimore Board of Health) için istatistik bilgilerini tablolaştırmak maksadıyla tasarlanmıştır. Delikli kart (Şekil 3) 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 [8].



Şekil 3- Delikli Kart Örneği

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 : Genellikle optik tarayıcılar olarak adlandırılan Mark Sense oy verme sistemleri adayların isimlerini içeren önceden basılmış oy pusulaları veya dikdörtgen, daire Çeklinde boş oy pusulaları şeklindedir. Seçmen siyah bir işaretleyici ile kutuyu veya direyi 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 [7].

Şekil 4- Optik Tarayıcılı Oy Kullanma 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 [7].

Şekil 5- Lever Makinesi

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 [7].

Şekil 6 – Doğrudan Kayıt Yapan Elektronik Sistemler

5. ELEKTRONİK SEÇİM SİSTEMLERİNDE KULLANILAN OYU SAKLAMA YÖNTEMLERİ VE GÜVENLİK

Seçim sistemlerinde kullanılan elektronik yöntemler belli özellikler içermektedir. Saklama yöntemleri, denetleme yöntemleri, sayım esasları gibi durumlar güvenli bir elektronik seçim sisteminin niteliklerini oluşturur.

5.1 Kriptolama Sistemleri

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 [9].

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 veya 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) veya 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 [10].

5.1.1 Simetrik Şifreleme 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 iĢlem 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 bölmü 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 [10].

5.1.2 Asimetrik Şifreleme 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 [10].

5.1.3 Hashing Algoritması

Algoritma, yapısı gereği tek yönlü gerçekleşen bir matematiksel işlemdir. Hash iĢlemine 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 birinden 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 [11].

5.2 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.

5.2.1 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.

Tamlık ve doğruluk ile etkileşime geçme yöntemidir. Sır vermemek ise kanıtlama yöntemidir.

Sıfır bilgi protokolü matematiksel bir ispatlama yöntemi değildir. Bu ispatlama yönteminde bilgi manipüle edilerek alıcıya ispatlamak için çalışılır [12].

5.2.2 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 [13].

5.2.3 Kör İmzalar

İnternet ortamında kişisel hakların korunmasından doğan kaygılar üzerine, 1982 yılında D. Chaum "Kör Sayısal imza" 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 [14].

5.2.4 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. eki tane kriptolanmış sayının toplamının, o sayıların toplamının kriptolanmış Çekline 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.

5.2.5 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 [15].

6. ELEKTRONİK SEÇİM SİSTEMİNDE KULLANILAN YÖNTEM VE MİMARİLER

Elektronik Seçim sistemleri kullanılmasıyla seçimler elektronik olarak yapılsada güven her zaman sorulanmıştır. Bu sorgulamadan dolayı yeni yöntem ve mimariler veya mevcut yöntemler üzerine yeni tezler ortaya çıkmaktadır. Günümüzde en çok kullanılan yöntem ve mimarileri aşağıdaki gibi sıralayabiliriz;

6.1 Mercuri Yöntemi

Bu yönteme göre, seçim sistemi, bilgisayar kullanılarak yapılan seçimlerin bir yazıcı yardımıyla kagıt üzerinde yeniden üretildigi bir mekanizma içermelidir. Üretilen bu çıktı cam bir fanus içerisinde yer almalıdır. Seçmen çıktıyı kontrol ederek tercihinin dogru kaydedilip edilmedigini denetleyebilir. Eger bir sorun varsa, seçmen seçim görevlisine basvurur ve çıktı yok edilir. Seçmene yeni bir oy hakkı verilir. Seçim sonunda resmi sonuçlar, kagıt pusulaların da sayılmasından sonra ilan edilir. Mercuri Yöntemi, seçmenlere oylarının dogru bir biçimde kaydedilip edilmedigini kontrol etme olanagı verir. Ancak, bu uygulama sistem maliyetini arttıracaktır [1].

- Seçmen dokunmatik bir ekran yardımıyla oyunu kullanır.
- Sistem seçmenin oyunu elektronik olarak kaydeder. Ancak kesin kayıt kağıt pusulada yapılır. Sistem seçmenin oyunu kagıt pusulaya basar ve bir cambölmenin arkasında gösterir.
- Seçmen pusulaya görür ve kontrol eder. Eger pusula seçmenin tercihlerini yansıtmıyorsa pusulanın geçersiz sayılması için seçim görevlisini çagırır veyeniden oyunu kullanır. _slem sorunsuzsa, makine kagıt pusulayı kutuya gönderir.

Şekil - 7 Mercuriy Seçim Sistemi Uygulanışı[1]

6.2 Chaum Yöntemi

Chaum karmaĢık 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 [2].

6.3 Biyometrik Tabanlı E-Seçim Sistemi

Bu sistemde Asp.Net Framework 2.0, Java Script, Xml ve bunların ortak kullanımını sağlayan XSL dili kullanılmıştır. Ayrıca daha önceden yazılmış bazı hazır kütüphaneler de kullanılmıştır. Seçmenlerin parmak izi görüntülerini almak için kullanılan parmak izi okuma cihazı Unifinger SFR300-S'tir [19].

Şekil – 8 Parmak izi okuyucusu[19]

Biyometrik seçim sistemi, internet tabanlı olarak gerçekleştirilmiştir. Böylelikle seçmenlerin kullandıkları oylar çok fazla masrafa gerek kalmadan internet ağı üzerinden bir merkezde toplanmıştır. Sisteme girişte parmak izi okutulduktan sonra elde edilen parmak izi şablonları ikili kodlara çevrilerek veritabanına kaydedildiğinden dolayı bilgilerin güvenliği sağlanmış olmaktadır. Sistem ilk çalıştığında kullanıcı ara yüzü olarak ekrana gelen görüntü Şekil 2'de gösterilmiştir. Sisteme 3 farklı giriş yapılabilir. Bunlardan ilki sistem yöneticisidir. Sistem yöneticisi sistemle ilgili tüm ayarlamaların yapılabildiği yetkilerin belirlendiği kısımdır. Seçim tanımlama, parti tanımlama, bölge tanımlama, mahalle tanımlama, seçmen tanımlama, seçim işlemleri, seçim ekranı, seçim sonuçları ve aktif kullanıcıların görünebildiği ekranlardan oluşmaktadır [19].

Şekil – 9 Parmak izi okuyulu Sistem Ekran Görüntüsü[19]

Sisteme giriş yapıldıktan sonra Seçmen karşısına gelen elektronik oy pusulasından (Şekil 10) istediği partinin yanında bulunan Evet butonuna tıklayarak oy verme işlemini başlatabilir. Seçmenimiz yanlışlıkla evet butonuna basarak oy verme işlemini tamamlamasın diye son bir mesaj penceresiyle seçmenin tercihinden emin olması sağlanır. Oy verme işlemi bittikten ve karşımıza mesaj geldikten sonra sistem tarafından otomatik olarak parmak izi giriş ekranı kullanıcının karşısına gelir. Artık oy verme işlemi seçmen için bitmiştir [19].

Şekil – 10 Elektronik oy pusulası[19]

Yapılan seçimin sonuçlarını sistem yöneticisi istediği an istediği bölgenin veya tüm Türkiye'nin olmak üzere görebilir. Sistem yöneticisi bunlar ile ilgili işlemleri Şekil 6'da gösterilen sistem yöneticisi penceresinde bulunan seçim sonuçları kısmından gerçekleştirebilir. [19].

Yapılan seçimin sonuçlarını sistem yöneticisi istediği an istediği bölgenin veya tüm Türkiye'nin olmak üzere görebilir. Sistem yöneticisi bunlar ile ilgili işlemleri Şekil 11'de gösterilen sistem yöneticisi penceresinde bulunan seçim sonuçları kısmından gerçekleştirebilir [19].

Şekil – 11 Seçim Sonuç Ekranı[19]

6.4 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. KuruluÇundan bu yana, VTP üyeleri ABD ve yurtdışında tüm seçim süreç durumunu araştırmıştır. VTP fakültesi, araÇtırma 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 veya mekanik cihazlar, ses kayıt cihazı veya kağıt olabilir [3].

6.4.1 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 veya 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 veya 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 iÇlemi 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 [16].

```
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
```

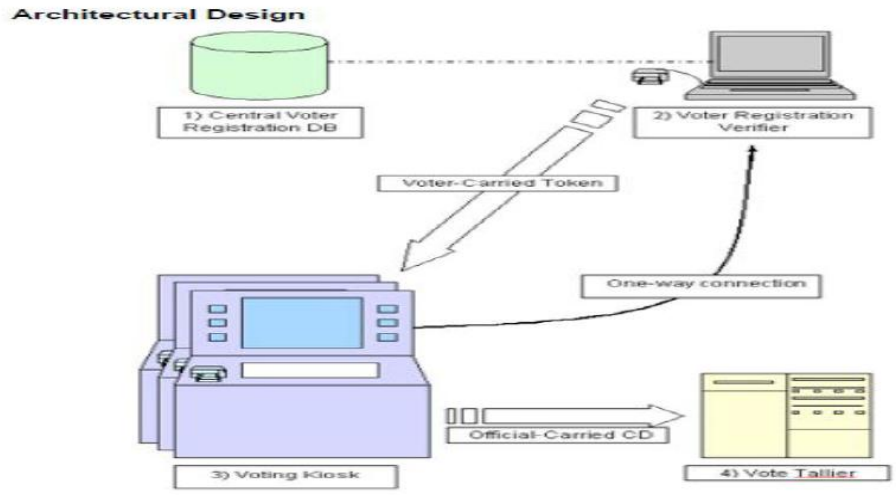
Şekil – 12 Evox Mimarisi UTF-8 Formatı[16]

,

6.4.2 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[4].

- Seçimler bir veya bir kaç gün sürebilir.
- Bu sistem sadece eyalet çapında veya 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
- Tüm cihazlar, seçimler arasında ürün yükseltme ve yeniden kuruluma katlanmak zorundadır.
- Tüm cihazlar, kullanım halinde, stoklamada ve nakil halinde iken güvenliği sağlanmak zorundadır.



Şekil – 13 Grup 2 Mimarisi[4]

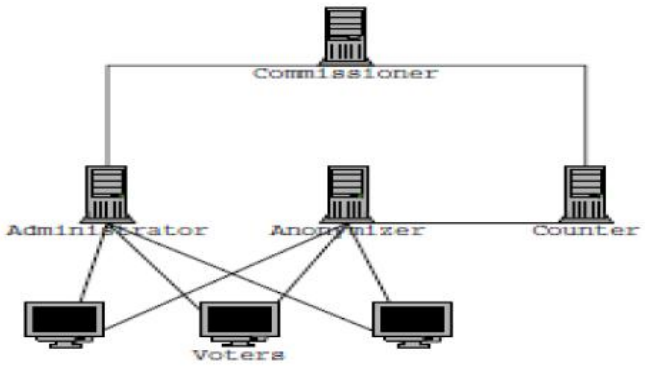
6.4.3 Evox Mimarisi

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 [17]. 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 – 14 Evox Mimarisi Tasarımı[17]

7. ELEKTRONİK SEÇİM SİSTEMLERİNDE OYLARIN DOĞRULANMASI VE GÜVENLİK

Elektronik oy kullanımı yeni yöntem ve mimarilerle artmasına rağmen oyların sayımı ve denetimi konusunda kağıt kullanımından tam olarak vazgeçilememektedir. Oylamada elektronik olarak kullanılan mimari ve yöntemler yeni olsada denetim ve konusunda güvensizlikler devam etmektedir. Oyların sayımı ve doğrulamalarında yöntemler kullanılmaktadır. Bunlar;

7.1 Kağıt Denetim Sistemi

Kağıt denetimi, kullanılan elektronik oylama yöntemde sistemlerin oy kullanıcılarının işleminin sonunda başarılı ise sistemin oluşturduğu kağıdın el değmeden bir sandık veya sistem haznesinde biriktirmesi ile oluşan oyların elektronik sayım haricinde klasik yöntemlerde olduğu gibi sayılmasıdır. Kağıtlar elle sayılarak sistemin doğruluğu sağlanmış olmaktadır.

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 [18].

7.2 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 [18].

7.3 Elektronik Seçim Sistemi İnternet Tabanlı Sistemlerde Saldırı Yöntemleri ve Güvenlik

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 15’ de gösterilmektedir [20].

-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 veya yazılım olarak üretilmiş IPS ve/veya Firewall engelleyemez. Bu saldırıları devletler, hacker' lar ve sıradan bilgisayar kullanıcıları yapabilirler [20].

DoS/DDoS saldırıları amacına ve yapılış şekline göre farklılık göstermektedir. Amaca göre DoS/DDoS iki farklı şekilde yapılır. Bunlar; bant genişliği (bandwidth) tüketimi ve kaynak (source) tüketimidir (CPU, RAM...). YapılıG Gekline 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 (CompletelybAutomated Public Turing test to tell Computers and Humans Apart, CAPTCHA) bir bölüm konularak sistemin güvenliği sağlanır.

-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.

-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 veya yetersiz olmasından kaynaklanan güvenlik açıklarıdır. iyi bir yetki yönetimi ile bunun önüne geçilebilir.

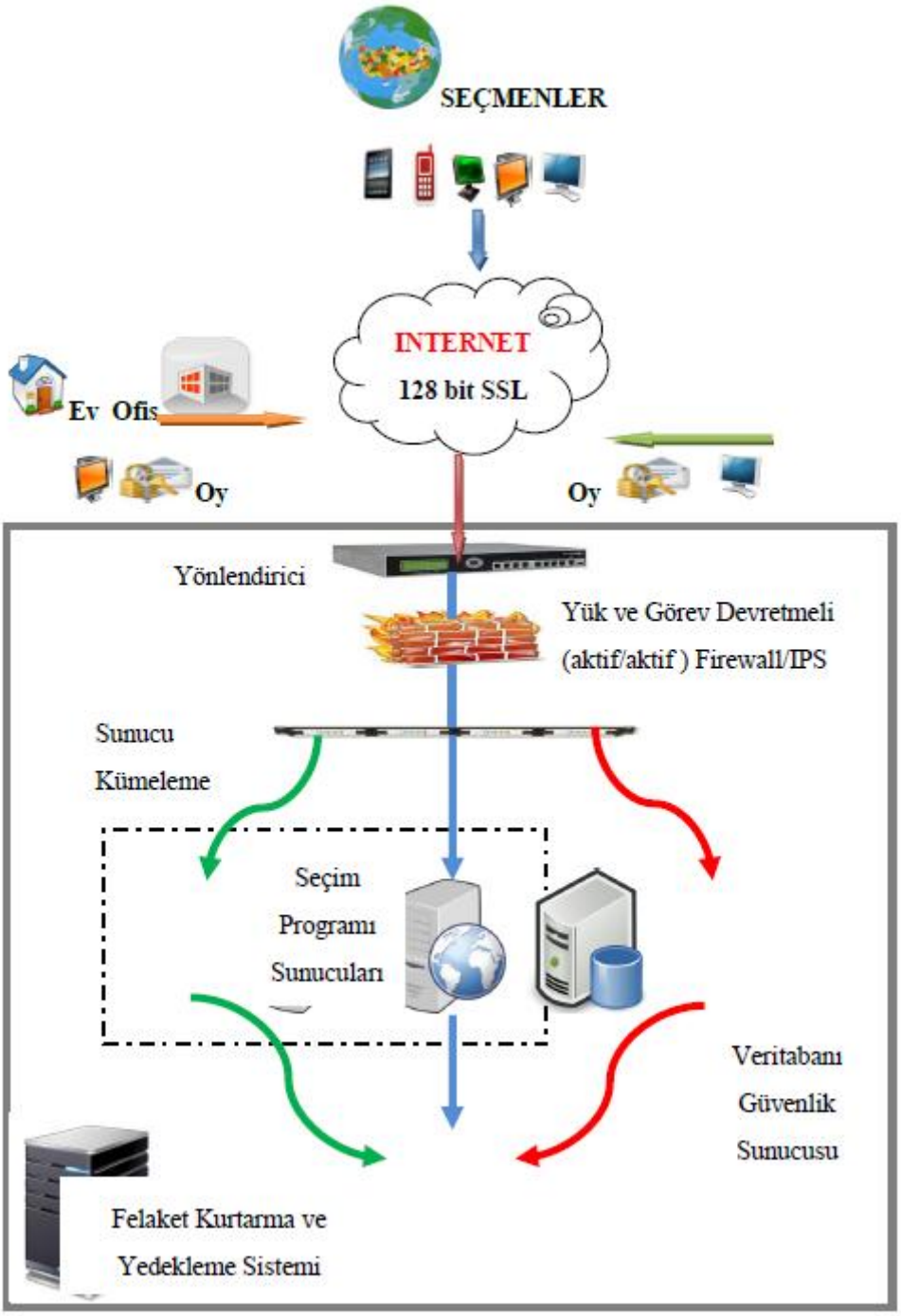
-Uzak Erişim Araçları Kullanılarak Sisteme İzinsiz Giriş: Genellikle bu tür saldırılar uzak erişim araçlarının (Remote Desktop, SSH, Telnet, FTP)parola ve IP bilgilerinin saldırgan tarafından ele geçirilmesi ile gerçekleştirilir. Güçlü parolalar kullanarak bu soruna çözüm üretebiliriz.

-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 veya 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.



Şekil – 15 İnternet Tabanlı Elektronik Seçim Sistemi[20]

8. ELEKTRONİK SEÇİM SİSTEMLERİNDE GÜVENLİK AMAÇLI ALGORİTMA ÖNERİSİ

Bu öneri uygulanacak olan genel seçimler veya herhangi bir seçimlerde elektronik seçim sisteminin uygulanabilmesi için kullanılan oyların daha güvenli saklanması hedeflenmiştir. Tasarlanan saklama algoritması ile genel ihtiyaçları karşılayarak, güvenlik ile ilgili sorunlara çözüm üretilmesi ve güvenli alt yapının hazırlanıp elektronik seçim sistemi uygulanabilirliğinin artması hedeflemiştir.

8.1 Tanım

Tasarlanan sistem, kullanımı basit fakat altyapısı karmaşık olup, uygulama esnasında ve sonrasında oluşabilecek hilelere karşı daha güvenli tasarlanarak, elektronik seçim sistemine olan genel şüpheli bakışı daha azaltmayı hedefleyen yapıda olmalıdır.

Sistem, genel olarak TCP / IP altyapısı kullanılarak kayıt etme sırasındaki farklı algoritma kullanımı ile hızlı sayım, net sonuçlar, şüphesiz işlem yaparak elektronik seçim sistemini tercih edilmesini bir adım daha kullanılabilir kılmaktadır.

Tasarlanan sistemin kullanılabilirliği için başlangıçda bazı gereklilikler aşağıdaki gibi sıralanmıştır;

- Oy kullanan seçmenlerin temel bilgisayar bilgisinin olması gerektiği ve oy kullanımına engel teşkil etmeyecek şekilde engelsiz yapıya sahiptirler.
- Seçmenlerin bağlı bulundukları seçim kurulları tarafından kimlik doğrulama için üretilmiş kendilerine ait kimlik kartları bulunmaktadır.
- Seçmenler, genel seçimler için bağlı bulunduğu yasa ve kurallara göre oy kullanabilir yaşta olması gerekmektedir.
- Oy kullanan seçmenler, ikinci defa oy kullanamazlar.
- Seçmenler bir başka seçimen yerine vekaletle veya doğrudan oy verme işlemi yapamazlar.

- Oy kullanımından sonra oy kullanım alanından çıkması halinde oyunda değişiklik yapamazlar.

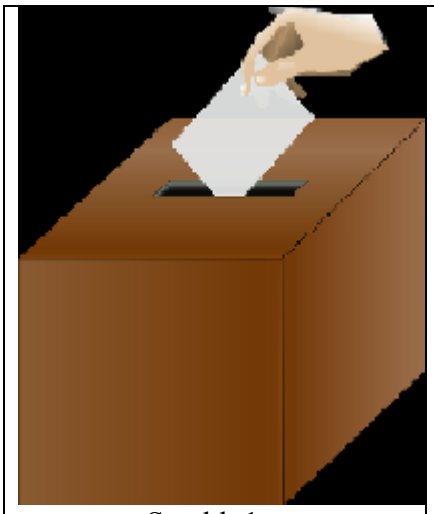
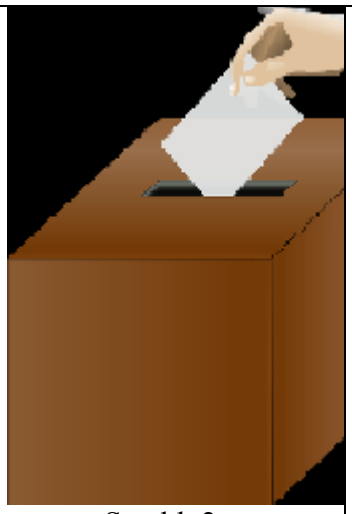
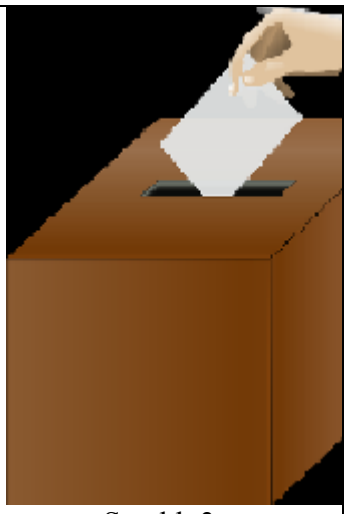
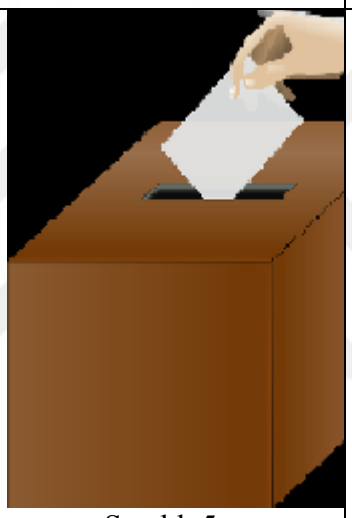
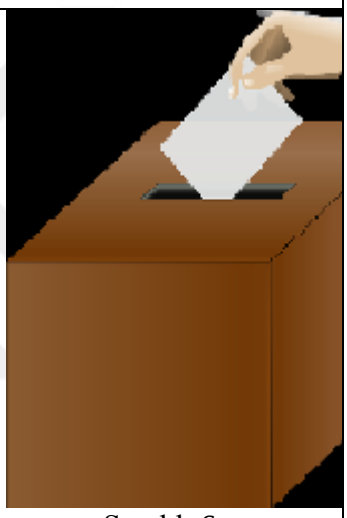
- Seçmenler kendileri için belirlenen oy verme alanı haricinde başka yerde oy kullamazlar.
- Seçmeler kendileri hariç oy kullandıkları alanda gizli oylama sebebi ile başka bir kimse bulunmaz.

8.2 Önerilen Algoritma İçin Elektronik Oylama Modelinin Genel Yapısı

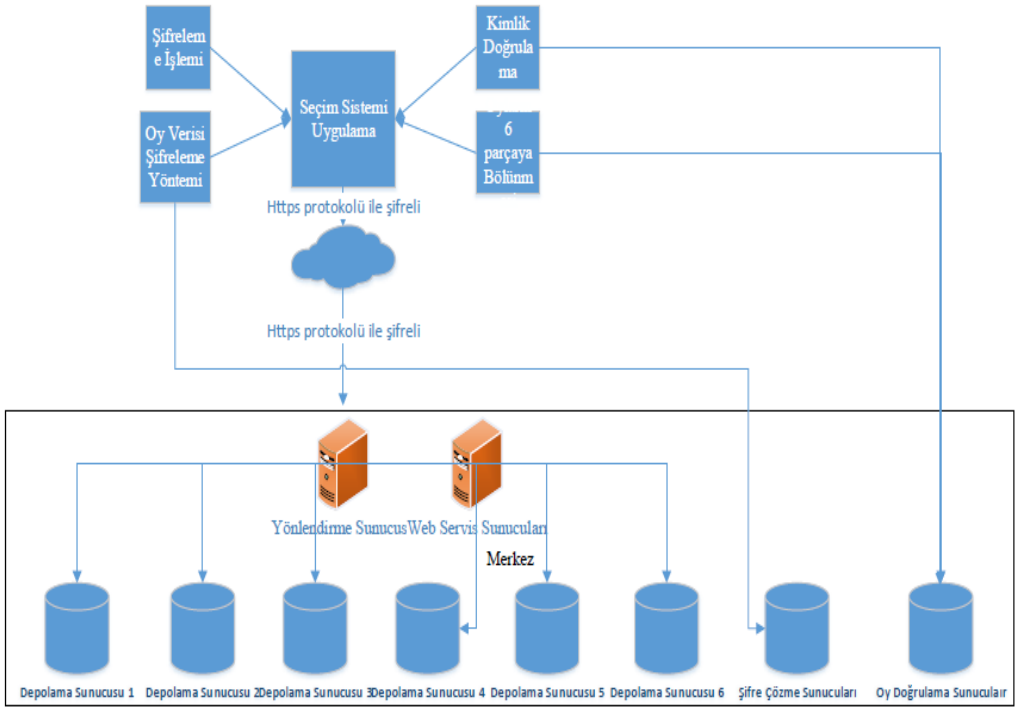
Tasarlanan yapı en basit ve günümüzde kullanılmakta olan kağıt sisteminin saklanma yöntemine yeni bir bakış getirerek bu bakışın elektronik olarak yapılmasını hedeflemiştir. Temel esas alınan yapı aşağıdaki kağıt pusulanın parçalanması ile başlamıştır. Aşağıdaki pusula belirli aralıklarla toplamda 6 parçaya bölünmüştür. Varsayım olarak pusulanın 6 parçaya bölünmesi (Şekil -16) ile her parçanın ayrı sandıklarda (Şekil – 17) ayrı odalarda saklanılması düşünülmüştür. Her parçanın arkasında birleştirilebilmesi için aynı sayılar olması varsayılmıştır. Bu sandıkların herhangi biri yerinden alındığından veya bir kısmı herhangi bir sandıktan alındığında pusula bütünlüğü olmadığından ve tam olarak hangi parti veya adaya oy verildiği bilinemeyeceğinden ve diğer yandan şüphelerin tam olmasından dolayı bir parçası alınmış oy pusulası herhangi bir anlam ifade etmeyecektir.

Tasarlanan ve algoritma olarak farklı bir saklama yöntemi ile güvenirlilik ve kullanımını yukarı taşımayı hedefleyen bu tezde anlatılan temel prensip pusulayı paçalama yöntemini esas alarak bu işlemleri elektronik olarak (Şekil - 18) yapmaktadır.

Şekil – 16 Kağıt Pusulanın Parçalara Bölünmesi

		
Sandık 1 – Pusula Parça 1	Sandık 2 – Pusula Parça 2	Sandık 3 – Pusula Parça 3
		
Sandık 4 – Pusula Parça 4	Sandık 5 – Pusula Parça 5	Sandık 6 – Pusula Parça 6

Şekil – 17 Bölünmüş Kağıt Pusulanın Her Parçasının Farklı Sandıklarda Saklanması



Şekil – 18 Pusula Parçalama Yöntemi İle Genel Mimari

8.3 Seçim Sisteminin Elemanları

Tasarlanan ve farklı saklama algoritması ile uygulanmaya çalışılan sistemin elemanları bulunmaktadır. Bunlar ; Seçmen , şifreleme Yöntemi , denetleme , Kimlik doğrulama , depolama sunucusu, Web servis sunucusu, şifre çözme sunucusu, oy doğrulama sunucusu ve sayım sunucusudur.

- **Seçmen :** Daha önceden seçimi yöneten kurum veya ilgili kuruluş tarafından seçim yapacak olan kişilere kendilerine seçime katılabilecekleri belge veya bilgilendirme ile oy kullanabilecek kişilerdir.
- **Şifreleme Yöntemi :** Kullanılan oyları belli kurallara göre direkt olarak okunamayacak verilere dönüştüren sistem parçası.
- **Denetleme :** Kullanılan oyların doğruluğunun sağlanması için sayısal ve veri bütünlüğünün kontrol edilmesine imkan veren sistem parçası.
- **Kimlik Doğrulama :** Oy kullanacak seçmenlerin oylarını kullanma sırasında elektronik kart veya kimlik belgeleri ile kimliklerinin doğruluğunu kontrol eden sistem parçası.

- **Depolama Sunucu :** Kullanılan Oyların sayım öncesinde depolandığı, sunucu işletim sistemleri kurulu ve veri tabanlarını üzerinde barındıran sistemler.
- **Web Servis Sunucusu :** Kullanılan oyların , seçim işlemi bittikten sonra sistemden alınan dataların merkeze aktarımını sağlayan ara katman.
- **Şifre Çözme Sunucusu :** Oy kullanımı sonrası merkeze alınan okunamaz dataların oy sayım sırasında dataları çözümleyerek okunabilir parçalara dönüştüren sistem.
- **Oy Doğrulama Sunucusu :** Oy Kullanımı sonrasında merkeze gelen dataların, kullanım yeri parça bütünlüğü ve şifreleme yöntemini kontrol eden sistemler.
- **Sayım sunucusu :** Oy doğrulama ve oy çözme sunucularından geçen parçalı olarak okunabilir dataları birleştirerek sayılabilir ve okunabilir oy verisine dönüştürüp sonuç oluşturan sistem.
- **Seçim Sistemi Uygulaması :** Seçmenlerle sistem arasındaki fiziksel ve sistemsel, seçmen tarafında gerekli kullanım haricinde herhangi bir fiziksel veya yazılımsal zararlı kullanıma imkan vermeyen ve müdahale edilemeyen sistem.

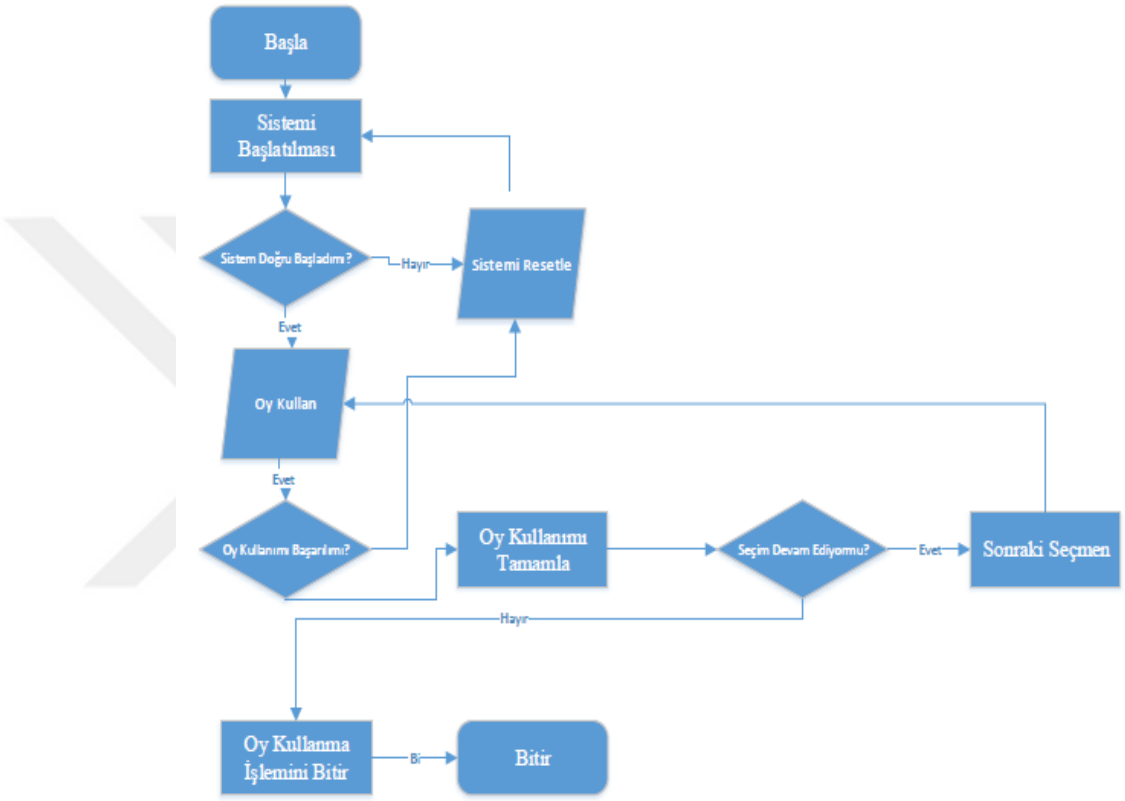
8.4 Sistemin İşleyişi

Seçmen kimlik doğrulaması ve oy kullanacağı yer bilgisi ile birlikte oylama işlemi gerçekleşir. Bu işlemler sonucunda arka planda oy kullanımı , oyun kaydedilmesi, oylamanın tamamlanması , oyların merkeze aktarılması , oyların doğrulanması ve oy sayım işlemleri gerçekleşmektedir.

8.4.1 Oy Kullanım Akışı

Seçmen oy verme işlemi için oy kullanım alanına geldiğinde kimlik doğrulamasından geçtikden sonra oy kullanım alanın girer ve sistemde seçim yapacağı seçeneği seçerek oy kullanımını adımlar yardımıyla tamamlar. Aynı seçme iki defa oy kullanamaz veya oy kullanımını tamamladıktan sonra tekrar seçim alanına gelerek tercihini değiştiremez.

Seçmen oyunu kullandıktan sonra , başka bir seçmen kimlik doğrulamasından sonra oyunu kullanır. Sistemde sorun olması durumunda görevli tarafından resetlenen sistem akışına Şekil – 19 daki gibi devam eder. Oy verme işlemi yeni seçmen geldikçe sistem kapatılmadığı sürece devam eder.



Şekil – 19 Oy Kullanımı Başlangıç Diyagramı

8.4.2 Oyların Şifrelenmesi ve Veri Tabanına Kayıt İşlemi

Oyların kullanımı sonrası veri tabanına kaydedilmesi sırasında parçalara bölünerek tek başına anlamsız veri olacak şekilde kayot işlemi gerçekleştirilir. Kayıt işlemi aşağıdaki algoritma ve örnek bir kayıt (Şekil - 20) aşağıdaki gibidir.

Kaydetme algoritmasındaki adımlarda herhangi bir parametrik değer almaması için ve şifreli ifadenin kaç parçaya (6) bölüneceği belli ve sabit

olduğundan yazılımsal güvenlik açısından parametrik olmaması için döngü kullanılmamıştır.

Kaydetme Algoritması :

1.Adım : Başla

2.Adım : Veriyi sayısal etiket ekle (id)

Etiket Eklenmiş veriyi 30 karakterli varchar (değişken ve karakterli) ifadeye dönüştür.

3.Adım : String ifadeyi 6 parçaya böl

4.Adım : Etkiketlenmiş her 1. veri parçasını asimetrik şifreleme ile şifrele

5.Adım : Şifrelenmiş 1. veri parçasını dosyaya kaydet.

6.Adım : Etkiketlenmiş her 2. veri parçasını asimetrik şifreleme ile şifrele

7.Adım : Şifrelenmiş 2 veri parçasını dosyaya kaydet.

8.Adım : Etkiketlenmiş her 3. veri parçasını asimetrik şifreleme ile şifrele

9.Adım : Şifrelenmiş 3. veri parçasını dosyaya kaydet.

10.Adım : Etkiketlenmiş her 4. veri parçasını asimetrik şifreleme ile şifrele

11.Adım : Şifrelenmiş 4. veri parçasını dosyaya kaydet.

12.Adım : Etkiketlenmiş her 5. veri parçasını asimetrik şifreleme ile şifrele

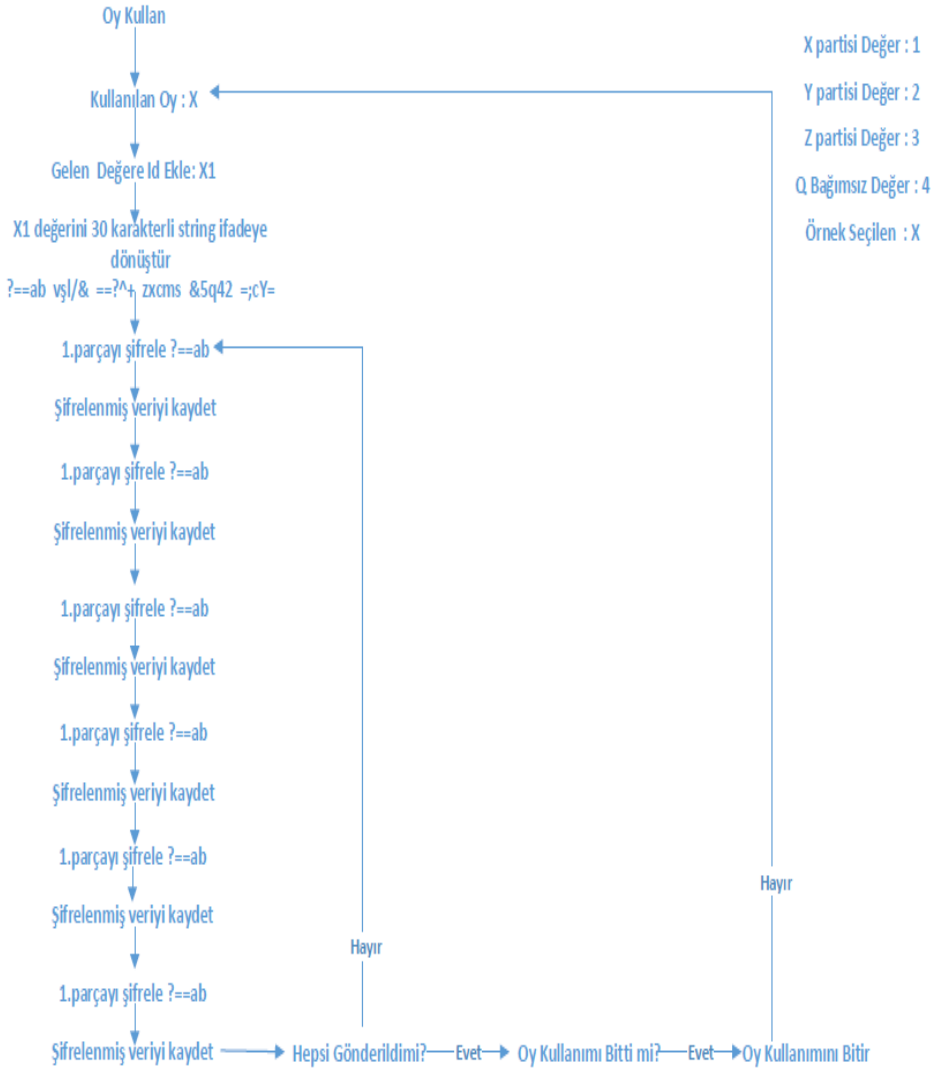
13.Adım : Şifrelenmiş 5. veri parçasını dosyaya kaydet.

14.Adım : Etkiketlenmiş her 6. veri parçasını asimetrik şifreleme ile şifrele

15.Adım : Şifrelenmiş 6. veri parçasını dosyaya kaydet.,

16.Adım : Kaydetme İşlemini Tamamla.

Örnek Oy Kaydetme



Şekil – 20 Oy Kullanımı Kayıt İşlemi

8.4.3 Sistemin Korunması

Sistem fiziksel olarak kullanıcıların herhangi yazılımsal veya donanımsal müdahalesine kapalı olarak tasarlanmıştır. Oy kullanım sırasında seçnmenlerin herhangi bir şekilde giriş yapabileceği donanımsal bir port bulunmamaktadır.

Oy kullanma işlemleri tamamlandıktan sonra ancak seçim görevlilerinin özel anahtarlarla ve ekrandan güvenlik girişleri ile veri aktarımı için kullanılacak network girişi bulunmaktadır.

Sistemin fiziksel olarak müdahale edilmesi durumlarına karşı kendisini kilitlemesi için hareket veya belirli bir güç kullanımında devreye giren HSM (Şekil - 21) cihazı kullanılmaktadır [21].

Şekil – 21 HSM Cihazları

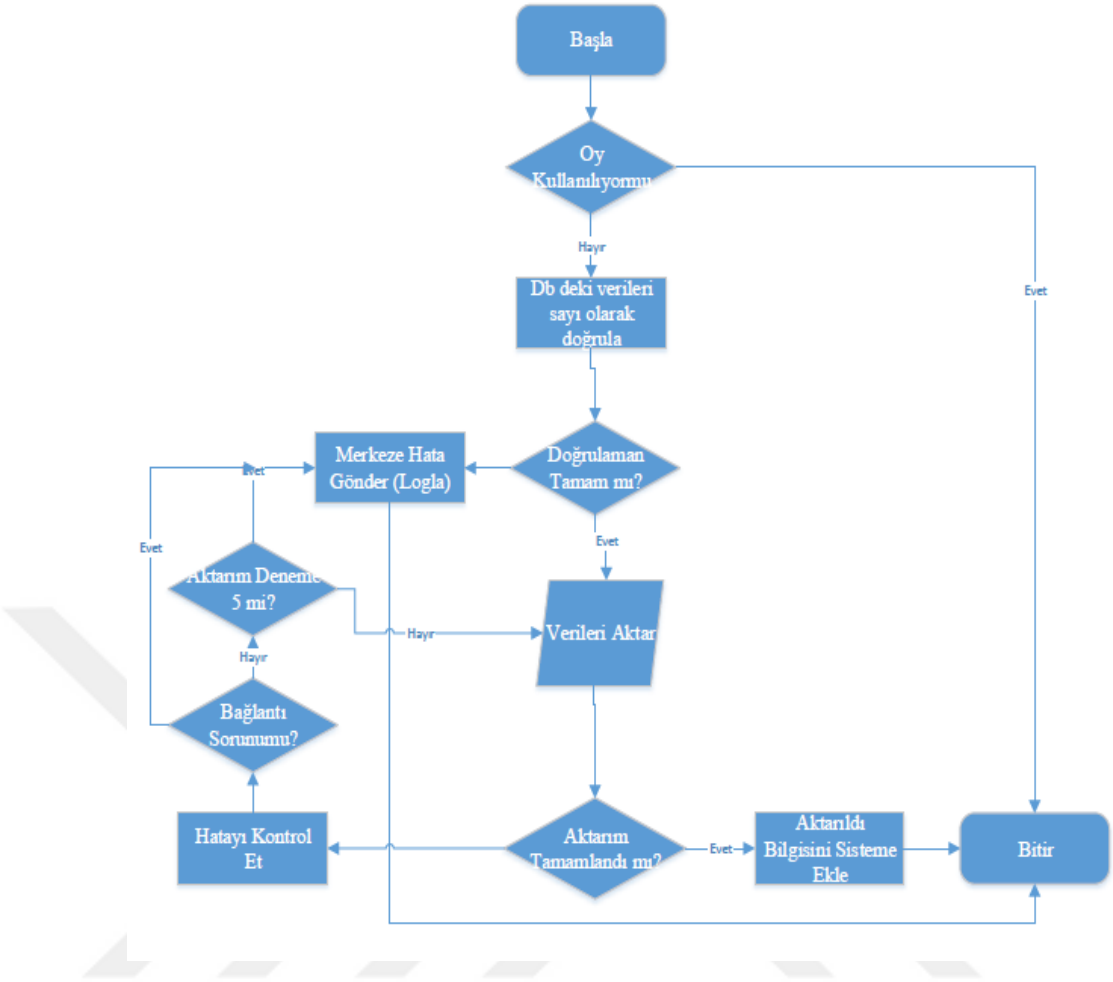
8.4.4 Oyu İptal Etmek

Elektronik oylamada iptal işlemi oy kullanım sırasında onay verilmediyse mümkündür. Oy kullanımı sonrasında oyu iptal etmek veya değiştirmek mümkün değildir.

Oy iptal işlemi oylama sürecini yürüten kurum veya kuruluş tarafından genel olarak yapılması gerekirse sistemdeki oylar toplandıktan sonra iptal edilebilir , veri tabanlarında oy durumları silinmiş olarak belirlenir.

8.4.5 Oyların Merkeze Gönderimi

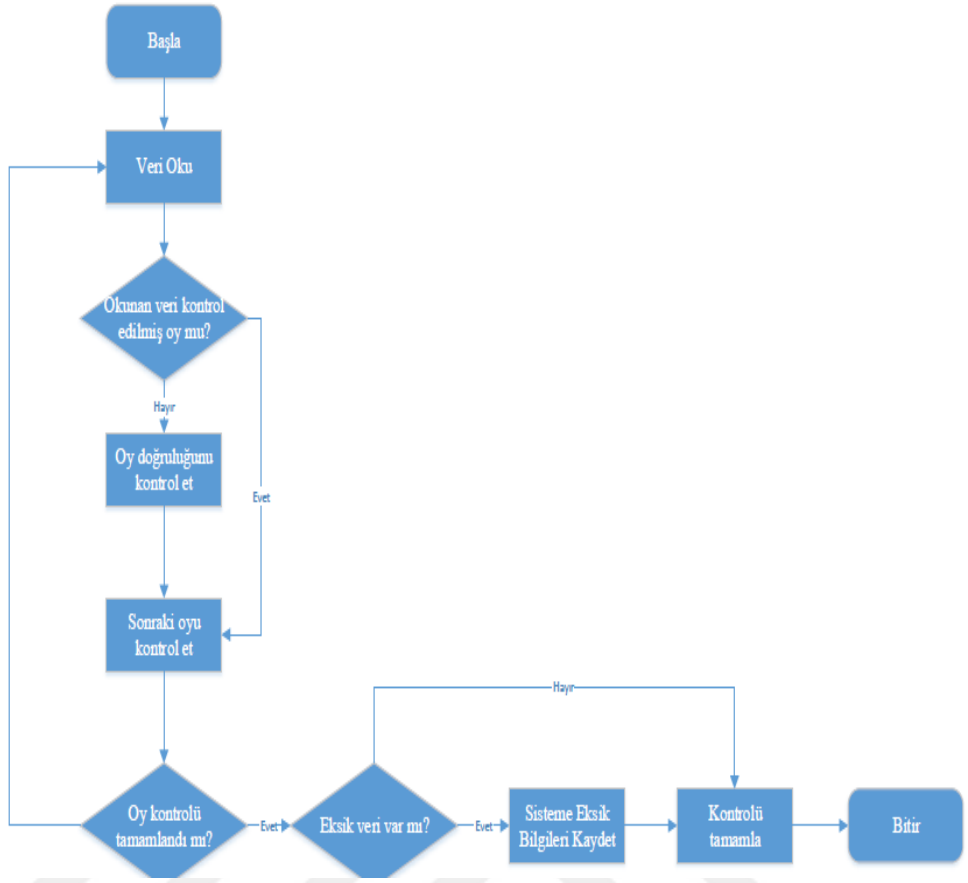
Elektronik oylama sistemi tamamlandıktan sonra oy verme işlemi görevli tarafından sonlandıktan sonra veriler sistem üzerinden parçalı şekilde merkeze gönderilir. Daha önce her birine id verilen ve parçalı olarak kaydedilen okunamaz veriler sistemin bağlanacağı web servis üzerinden https protokolü kullanılarak merkeze aktarılır. Aktarımın yapılacağı akış şeması **Şekil - X** deki gibidir. Aktarım sırasında hata yaşanırsa ve oy kullanılan sistemde kullanım sırasında sorun olmadığı varsayılırsa aktarımın başarısız olmasından dolayı cihaz ilgilileri tarafından sistemsel olarak incelenip oy aktarımının tamamlanması sağlanır.



Şekil – 22 Oyların Merkeze Gönderim Akışı

8.4.6 Oy Sayım Öncesi Kontroller ve Doğrulama

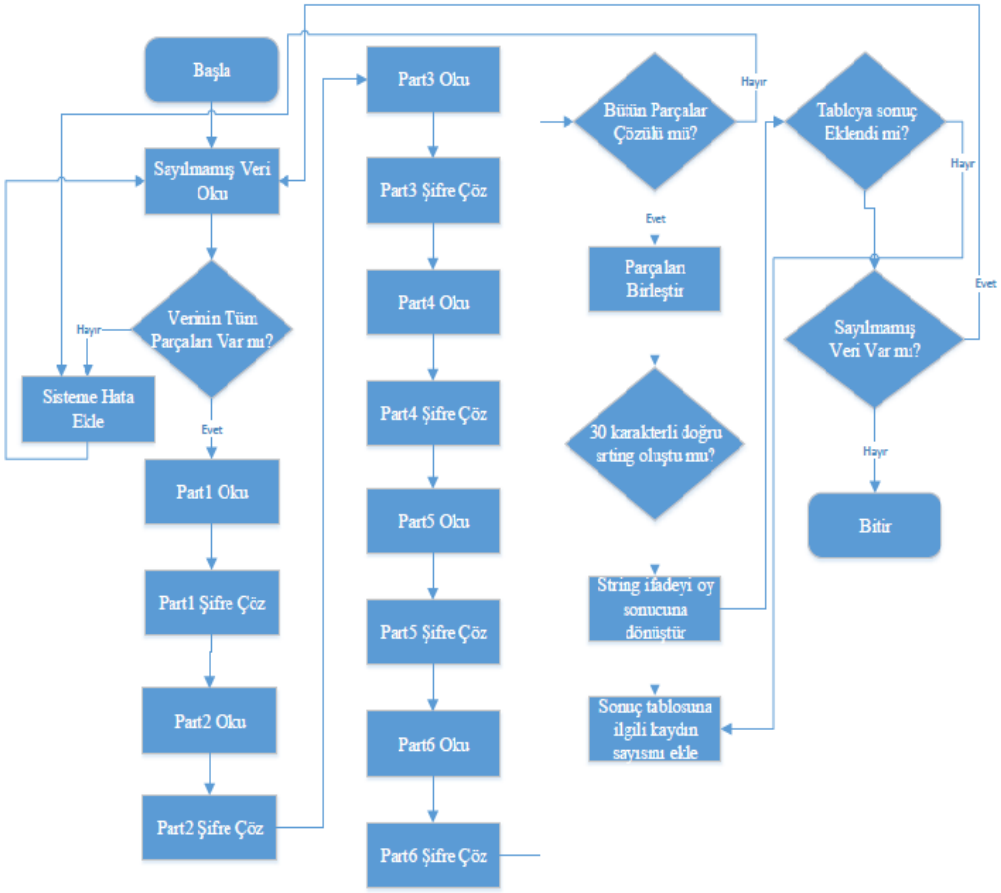
Verilerin tamamı veya büyük kısmı merkeze aktarıldığı varsayılarak sayım işlemi için gerekli kontroller yapılır. Kontrollerde aktarılan verilerle daha önce seçmenler için oluşturulan veriler sayısal olarak karşılaştırılarak, kullanılan oy, kullanılmayan oy sayıları toplanarak, seçimi yürüten kurum veya kuruluş tarafından seçmen sayısı doğrulanmış olur. Bu doğrulama sırasında gizli oylama esas olduğundan kişilerin hangi oyu kullandıkları tutulmamakta olup, sayısal olarak kaç kişinin oy kullanıp kullanmadığı kontrol edilmektedir. Doğrulama için ise parçalı okunamaz şekildeki verilerin toplamda 6 parça olarak okunamaz bir bütünü sağlama durumları kontrol edilir. Doğrulama için aşağıdaki akış şeması (Şekil - 23) takip edilir.



Şekil – 23 Oyların Merkeze Gönderim Akış Kontrolü

8.4.7 Oyların Sayımı

Oylama sisteminde veriler kontrol edildikten sonra verilerde herhangi bir sorun olmadığı varsayılarak sayım işlemi yapılır. Sayım sırasında, daha önceden seçim bölgelerinden gelen okunamaz ve anlam ifade etmeyen veriler, şifre çözen sunucularda anlamlı parçalara dönüştürülerek birleştirilir. Oluşan anlamalı 30 karakterli ifade tekrar tersine algoritma çalıştırılarak kullanılan oya dönüştürülür ve id oydan ayrılır. Oy sayımında seçmenin tercih ettiği aday veya parti puanı bir arttırılarak sonraki oy işlemi için aynı operasyonlar yürütülür. Oyların tamamı sayıldıktan sonra sonuçlar kontrol edilerek duyuruya hazır hale getirilir. Bu işlemler aşağıdaki akış şemasındaki gibi takip edilir.



Şekil – 24 Oyların Sayılması

SONUÇ

Tasarlanan bu elektronik seçim sistemi klasik kağıt kullanımından esinlenilerek kullanılan oyun okunamaz ve tek başına anlamsız parçalı şekilde saklanmasını ve saklanan her bir parçanın farklı veri tabanlarında saklanmasını sağlamaktadır.

Günümüzde kullanılan elektronik seçim sistemlerine güvenlik ve şüphe gibi sebeplerden dolayı tam olarak güvenilmemektedir. Tasarlanan bu modelde güvenlik klasik kağıt yöntemi için kullanılabilecek yöntemi elektronik model olarak kullanmayı sağlamaktadır. Saklama yönteminden dolayı olası saldırılara karşı daha güçlü olarak tasarlanmış ve herhangi bir saldırıda veriler şifrelenerek saklandığından çözülmesi ve değiştirilmesi çok güç olacaktır.

Önerilen model ve algoritma hem oy kullanma esnasında hem aktarım hem de sayım esnasında birden fazla doğrulama kullanıldığından sonuçlar hızlı ve güvenilir olmaktadır.

Dünya'da ve ülkemizde denemeleri yapılan ve bazı ülkelerde uygulanan elektronik seçim sistemi, üzerindeki şüphe ve güvensizlikler azaldığında kullanım alanı hızla artacağı görülebilmektedir. Hazırlanan bu tez elektronik seçim sistemindeki güvenlik sebeplerinden dolayı kullanımına engel teşkil eden şüpheleri en aza indirebilmeyi hedeflemekte ve elektronik seçim sisteminin tercih edilmesine katkı sağlamayı hedeflemiştir.

Bu çalışma, gerçek ortamda, uygun şartlar sağlandığında ve tezde bahsedilen akışlara uygun tasarlandığında, test edilebilir, güvenilir ve doğru somut sonuçlar alınabilir.

KAYNAKÇA

1. "**Elektronic Voting**" http://www.notablesoftware.com/evote.html , (Çevirimiçi 09.01.2010)

2. **Şahin, M., Karagüler T. "***Elektronik Seçim Sistemleri ve Mercuri Modeli***"** , Akademik Bilişim 2006, Pamukkale-Denizli, (1-3.02.2006)

3. **Baltimore, D., Vest, C. "***Voting Technology Project***"**. (2000). 06.05.2014, http://www.vote.caltech.edu/

4. **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_de sign.pdf

5. "*Seçim*" https://tr.wikipedia.org/wiki/Se%C3%A7im, (Çevirimiçi 16.11.2015)

6. "*Elektronik Oy Verme Sistemlerinde Güvenlik : Deneyimler ve Türkiye için Önriler*" http://eidergisi.istanbul.edu.tr/sayi3/iueis3m3.pdf (Çevirimiçi 11.12.2006)

7. "E-Seçim Uygulamaları için Gereksinimler ve Tasarım İlkeleri", XI. "Türkiye'de Internet" Konferansı (Çevirimiçi 21.12.2006)

8. "*History of Voting Machines*" http://www.glencoe.com/sec/socialstudies/btt/election_day/history.shtml (Çevirimiçi)

9. "*Steganografi*" http://e-bergi.com/y/Veri-Gizleme-Bilimi (Çevirimiçi)

10. "*What is Cryptography*?",(b.t),http://www.computer-network-security-training.com/what-is-cryptography/. (Çevirimiçi)

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

12.**Goldwasser, S., Micali, S., Rackoff, C.** 1985. **"***The Knowledge Complexity of Interactive Proof-Systems***".**

13. **Rouse, M**. **"***Digital Signature***"**. (2007). 01.05.2014, http://searchsecurity.techtarget.com/definition/digital-signature

14. **Chaum, D**. (1982). "*Blind Signatures for Untraceable Payments*". Department of Computer Science University of California Santa Barbara, CA.

15. **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,

16. **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

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

18. **Cohen, B. S.** (19.05.2005). **"***Auditing Technology for Electronic Voting Machines***".** Yayınlanmamış Yüksek Lisans Tezi, MIT.

19. "*Biyometrik Tabanlı E-Seçim Sistemi*", http://ab.org.tr/ab13/bildiri/40.pdf (Çevirimiçi)

20. **Haluk Alemdaroğulu** "*Mercuriy Modeline Dayal Örnek Elektronik Seçim Uygulaması"*, Beykent Üniversitesi FBE Yüksek Lisans Tezi, (2014)

21. "*HSM Nedir*?", http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/uygulama-ve-islem-guvenliginde-hsmlerin-onemi-ve-kullanim-alanlari.html, (Çevirimiçi)

ÖZGEÇMİŞ

Halis SALMAN, 15 Ocak 1989 yılı Tokat ili Zile ilçesinde doğdum. İlköğretim ve Ortaöğrenimi İstanbul Sultanbeyli'de tamamladım. 2006 yılında Bozok Üniversitesi Bilgisayar Teknolojisi ve Programlama Bölümüne yerleştikten sonra 2008 yılında mezun oldum. 2008 yılında bir bankanın iştirak şirketi Bilişim bölümünde çalışmaya başladım. 2010 yılında yapılan Dikey Geçiş Sınavı ile Beyken Üniversitesi Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği bölümünü tamamladım. 2014 yılında mezun olduğum Beykent Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı Bigisayar Mühendisliği yüksek lisans programına başladım.

2012 yılında iş değiştirerek başladığım kamu kuruluşunda yazılım geliştirici bilgisayar mühendisi olarak görev yapmaktayım. Orta seviyede İngilizce bilmekteyim.

Halis SALMAN