Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi
BAUNSOBED Aralık 2024, Cilt:27 Sayı:52
https://dergipark.org.tr/tr/pub/baunsobed
Araştırma Makalesi / Research Article

E-Devlet üzerinden güvenli ve etkin bir dijital seçim sistemi modeli: Öneriler ve uygulama stratejileri
A secure and effective digital election system model through e-Government: Recommendations and implementation strategies

Gönderim Tarihi / Received: 15.05.2024
Kabul Tarihi / Accepted: 02.09.2024
Doi: 10.31795/baunsobed.1484568

Kübra CANBAZ AKÇA[1]
Tahsin GÜLER[**2]

ÖZ: Teknolojide yaşanan yenilikler sayesinde demokrasi ve demokrasinin kullandığı araçlarda ciddi dönüşümler yaşanmaktadır. Bilhassa katılımcı demokrasi alanına büyük fayda sağlayan teknoloji sayesinde dünya genelinde birçok yeni uygulama faaliyete geçmektedir. Katılımcı demokrasinin dünya genelinde önemini ortaya koyan yeni uygulamalara bakıldığında dijital seçim sistemleri dikkat çekmektedir. Bu çalışmada e-Devlet temelinde bir dijital seçim sistemi modeli önerisi öneriler ve uygulama stratejileriyle birlikte tartışılacaktır. E-Devlet sisteminin sürdürülebilir hizmet anlayışından yola çıkarak yönetişim alanının önemli bir noktasını temsil eden katılımcı demokrasinin de teknoloji destekli artırılması gerektiği düşünülmektedir. Bu kapsamda ülkeler için oldukça önemli bir yeri olan e-Devlet uygulamalarının katılımcı demokrasinin en üst seviyesini yansıtan seçim uygulamalarına uyarlama düşüncesi önemli görülmektedir. Bu çalışmada vatandaşların bulundukları yerde kolaylıkla oy kullanabildikleri, bağımsız, etkin ve güvenli bir dijital seçim sisteminde nelere dikkat edilmesi ve hangi sorunlara nasıl bir güvenlik çemberi oluşturulması gerektiği üzerinde önerilerde bulunulacak, e-Devlet üzerinden uygulanabilir bir dijital seçim sisteminin tasarım ve uygulama noktalarında yapay zekâ ve makine öğrenimi tabanlı güvenlik çözümlerine odaklanılacaktır.
Anahtar Kelimeler: Dijital seçim sistemi, E-Devlet, Yapay zekâ, Katılımcı demokrasi, Teknoloji

ABSTRACT: Thanks to innovations in technology, there are serious transformations in democracy and the tools used by democracy. Thanks to technology, which provides great benefits, especially to the field of participatory democracy, many new applications are becoming operational around the world. When we look at new applications that reveal the importance of participatory democracy around the world, digital election systems attract attention. In this study, a proposal for a digital election system model based on e-Government will be discussed along with suggestions and implementation strategies. Based on the sustainable service understanding of the e-Government system, it is thought that participatory democracy, which represents an important point in the field of governance, should be increased with technology support. In this context, the idea of adapting e-Government applications, which have a very important place for countries, to election practices that reflect the highest level of participatory democracy, is considered important. This study will offer suggestions on what to consider in an independent, efficient, and secure digital election system that allows citizens to vote easily from their current location, as well as propose security frameworks to address various issues. The study will focus on artificial intelligence and machine learning-based security solutions in the design and implementation phases of a digital election system that can be operated through e-Government platforms.
Keywords: Digital election system, E-Government, Artificial intelligence, Participatory democracy, Technology

[1] Doktora Öğrencisi, Uludağ Üniversitesi, Sosyal Bilimler Enstitüsü, kubrac12345@gmail.com, https://orcid.org/0000-0002-1903-7941
[**] Sorumlu Yazar / Corresponding Author
[2] Doç. Dr., Balıkesir Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, tahsin.guler@balikesir.edu.tr, https://orcid.org/0000-0002-7729-5172

EXTENDED ABSTRACT

Literature review

The concept of digital voting systems is a new term that has entered our lives with the rapid advancement of technology, and many countries worldwide have begun using digital voting systems with designs of their own choosing. Also referred to as electronic voting or e-voting, this new voting system has a broad definition, but in general, it refers to processes where information and communication technologies are used in place of traditional paper ballot voting for the casting, recording, or counting of votes (Telciler, 2007: 237; IDEA: 2011: 6).

Initially in the United States, Brazil, Japan, Estonia, and Switzerland, along with the Netherlands, which have been joining the ranks since 2004, and countries such as Lithuania, Malaysia, the United Kingdom, and India, which have transitioned to digital voting systems in recent years, it can be seen that the use of technological innovations in this field has become quite widespread worldwide (Çetinkaya and Çetinkaya, 2006:114). It is observed that even in populous and developing countries, it can be successfully and widely implemented. Most recently, Iran has also joined the countries implementing digital voting systems by conducting electronic voting in 8 cities, including the capital Tehran, during the parliamentary elections held in May 2024.

It is observed that the most emphasized topics in digital voting system applications, which have become widespread in the literature in the last twenty years, are the reliability of the developed voting system and how the secrecy of the voter's choice will be ensured.

In this context, Vural Dinçkol and Işık (2019) examined electronic voting and the example of Estonia in the context of participation. International IDEA (2011), Telciler (2017), and Akın (2006) provided evaluations on the security, issues, and solution proposals of digital voting systems, while Çetinkaya and Çetinkaya (2006) conducted studies on the requirements and design principles of digital voting systems. On the other hand, it is observed that numerous national and international organizations specializing in information technologies (such as the Presidency's Digital Transformation Office, National Securities Depository Limited (NSDL), verifiedvoting.org) are interested in and conducting studies on digital voting systems.

Methodology

In this study, a model proposal for a secure and effective digital voting system via e-Government will be discussed, along with design and implementation recommendations. Advantages and opportunities will be presented in designing a secure and effective digital voting system model, and alternative proposals will be provided to ensure security, taking into account potential security vulnerabilities and threats that may arise during the integration of this model into the existing active e-Government system.

It is believed that designing a new digital voting system model for Turkey, integrated with e-Government, where currently 65,470,800 users have direct and secure access to 8,246 digital services provided by 1,041 institutions, would address the existing issue of distrust in digital platforms among citizens. It can be said that adapting a digital voting system actively provided by the government and tailored to the e-Government portal, which has been in use for years, is important in instilling confidence and rapid adoption of the new system.

In the study, which utilized Document Analysis Management as the method, the framework of the proposed digital voting system model was determined by examining models of countries actively using digital voting systems worldwide, such as the United States, Switzerland, Brazil, and Estonia, and taking into account the integration of the E-Government system expressed in the preparations for the transition to digital voting systems, which has been emphasized in our country in recent years, as well as the development of new security technologies aimed at digital voting systems.

Findings and discussion

Digital voting systems offer several advantages over traditional voting systems, including broader accessibility, encouraging participation, being more suitable for the elderly and people with disabilities, reducing election costs in the medium to long term, being environmentally friendly, requiring less manpower, and providing more secure, accurate, and faster results. As an alternative to the digital voting applications designed in various forms by each country, it is recommended that a digital voting system model developed for our country be maintained via e-Government.

The security-focused design principles that can be proposed for managing a highly secure election process through a digital voting system developed via e-Government are as follows:
End-to-End Encryption, known as a solution for ensuring the privacy and security of data in digital voting systems, can be recommended. With end-to-end encryption in a digital voting system, the voter's voting process can be securely conducted. To enhance encryption, data can be encrypted using SSL/TSL Protocols, providing secure communication via HTTPS (HTTP Secure) connection to protect encryption (Turk.net, 2024). Time stamping, used in determining protocols, allows ensuring data integrity of transmitted data and can contribute to retrospective election auditing (KamuSM, 2024).

Multi-factor authentication (MFA) and authorization are considered important for securely maintaining a digital voting system conducted via e-Government.

In a digital voting system, it is necessary to establish the authorized authority that accesses the system from various stakeholders in a neutral manner, without allowing any suspicion or manipulation. It is considered important that this authority and control personnel are included in the system logs and that their system activities are recorded with time stamping. This is seen as an important method for identifying the person responsible for potential security breaches and detecting violations.

One of the security-focused design principles that can be established against security issues in digital voting systems could be in the field of artificial intelligence and machine learning. Considering that artificial intelligence, which can be utilized for the security of digital voting systems, will also support cybersecurity, it is believed that problems related to the misuse of personal data can be prevented (TR. Presidency's Digital Transformation Office, 2024). In this context, it is believed that integrating artificial intelligence into a digital voting system conducted via e-Government could prevent many problems that may occur during the election process.

Results and recommendations

In this study, a proposal for a digital voting system model that can be implemented via e-Government was discussed, taking into account the security issues of digital voting systems. Therefore, by highlighting the potential problems that a digital voting system model created via e-Government might encounter, firstly, problem identification was conducted. Considering security threats that concern countries worldwide regarding digital voting systems, the possible issues of the proposed digital voting system were identified.

For the implementation of a digital voting system conducted via e-Government, it is crucial to determine the election authorities and their powers who will have access to the system through End-to-End Encryption, multi-factor authentication, and authorization. During the implementation phase, it is suggested that the digital voting system model, designed considering the easy usability for citizens, should be compatible with different devices such as computers and mobile phones, and different interfaces that can adapt to various devices should be designed. Necessary recommendations for easy usability have been expressed at this point.

Moreover, although the technical infrastructure is sufficient for designing and implementing a digital voting system via e-Government in Turkey, its realization will depend on the determination of decision-makers on this issue and the change in the perception of distrust towards digital voting systems in society.

Giriş

Günümüzde hız kesmeden gelişen teknoloji sayesinde her alanda ciddi değişimler yaşanmaktadır. Yaşanan değişimlerin en önemli olanları ise devlet yapılanması ve demokrasi sistemi içinde gerçekleşen teknolojik uygulamalardır. Teknolojinin devlet yönetimine entegre edilmesiyle hayatımıza giren e-Devlet kamu yönetimi alanında yönetişimi güçlendirmiş, etkinliği ve verimliliği artırmış, zaman tasarrufu sağlamış ve en önemlisi hem devlet eliyle sürdürülen görev ve sorumluluklarda iş yükünü hafifletmiş hem de vatandaşların hizmetlere daha kolay ulaşmasına olanak sağlamıştır.

Teknolojinin hızla gelişmesi dolayısıyla kamu hizmetlerinin etkinliğini ve verimliliğini artıran bu yeni nesil teknolojik sistemlerde demokrasinin daha etkin şekilde işleyebilmesi amacıyla yeni dijital seçim uygulamaları da kullanılmaya başlanmıştır. Günümüzün teknolojik şartlarına uygun ve güvenilir şekilde tasarlanmaya çalışılan dijital seçim sistemlerinin geliştirilmesi, geleneksel seçim sistemlerinin içinde barındırdığı zaman sorunu, yüksek maliyet ve yaşanan şaibeli durumlar gibi uygulama zorluklarını ortadan kaldırması bakımından gereklilik arz etmektedir. Yeni kamu yönetimi anlayışı temelinde üzerinde önemle durulan yönetişimin sağlanması, etkin, verimli, adil, katılımcı ve şeffaf bir seçim sistemi kurulmasıyla da doğrudan ilişkilidir. Bu kapsamda hem teknoloji çağını yakalayabilmek hem de etkin bir yönetim modelinin temellerini güvenilirliği ve katılımcılığı esas alacak güçlü bir şekilde atabilmek gereklidir.

Literatür taraması

Dijital seçim sistemi kavramı günümüzde teknolojinin hız kesmeyen ilerlemesiyle birlikte yaşamlarımıza giren yeni bir kavramdır. Dijital seçim, elektronik seçim veya e-seçim isimleriyle anılan bu yeni seçim sisteminin oldukça geniş bir tanımı olmakla birlikte en genel anlamda geleneksel kâğıt pusulayla yapılan seçim işlemlerinin yerine oyların kullanılması, kaydedilmesi veya sayılmasında bilgi ve iletişim teknolojilerini içeren sistemlerin kullanıldığı süreçleri ifade etmektedir (Telciler, 2007: 237; IDEA: 2011: 6). Oy verme ve oy sayma işlemleriyle birlikte süreç kapsamında sürdürülen her işlemin insan müdahalesinden arındırılması esas alınmaktadır.

Dünya genelinde birçok ülke, kendi belirledikleri tasarımlarla dijital seçim sistemlerinin kullanımına başlamıştır. Başta ABD, Brezilya, Japonya, Estonya, İsviçre olmak üzere 2004 yılından beri bu ülkeler arasına katılan Hollanda ve yakın tarihlerde dijital seçim sistemine geçen Litvanya, Malezya, İngiltere ve Hindistan gibi ülkeler dikkate alındığında dünya üzerinde teknolojik yeniliklerin bu alanda da kullanımının oldukça yaygınlaştığı (Çetinkaya ve Çetinkaya, 2006: 114), kalabalık ve gelişmekte olan ülkelerde bile başarıyla ve yaygın olarak uygulanabildiği görülmektedir (Akın, 2006: 45).[3] 10 Mayıs 2024 tarihinde İran'da gerçekleştirilen 12. Dönem milletvekili seçimlerinin de dijital seçim sistemiyle gerçekleştirildiği bilgisi dünya basınında yer almıştır. İran'ın 12. Dönem milletvekili seçimlerinde ilk kez Tahran dahil 8 seçim bölgesinde elektronik sandıklarda oylama gerçekleştirilmesi dijital seçim sistemlerine yönelimin arttığını göstermektedir (Anadolu Ajansı, 2024).

Dijital seçim sistemleri içerisinde yukarıda da ifade edildiği üzere farklı tasarımlar bulunmaktadır. Ülkeler özelinde farklı tasarım ve kullanımlara sahip bu dijital seçim sistemi teknolojileri arasında Doğrudan Kayıt Sistemi, Delikli Katlı Sistem, İşaret Tanıyıcı (Optik) Sistem ve internet üzerinden oylama bulunmaktadır (Telciler, 2017: 110-111). Adı geçen bu farklı teknolojilerin farklı içeriklere sahip avantajları ve dezavantajları bulunmaktadır.

Çalışmada oluşturulacak olan e-Devlet tabanlı dijital seçim sistemi modeliyle dünya genelinde farklı ülkelerin kullandıkları dijital seçim sistemleri arasındaki farklılığın ortaya konması amacıyla yukarıda sıralanan dijital seçim sistemi teknolojilerini açıklamakta yarar vardır.

[3] ABD, Brezilya ve Hindistan gibi dünyanın en çok nüfusa sahip olan ülkelerinin elektronik seçim sistemlerini tercih etmelerinin bir nedeni de 100 milyonları bulan (2024 Hindistan seçimlerinde 970 milyon seçmen) seçmen sayısıyla gerçekleştirilecek geleneksel bir seçimin maliyetinin ve zorluklarının çok fazla oluşudur. Diğer taraftan Brezilya ve Hindistan'ın teknolojik altyapı ve toplumun teknolojik duyarlılığı noktasında Türkiye'den daha ileri olmadıkları halde bu sistemleri uygulayabilmeleri, ülkelere özgü tasarımlarla -ki çalışmada Türkiye için e-Devlet sistemi önerilmiştir, dijital seçim sistemlerinin uygulanabilir olduğunu göstermektedir.

✓ ***Doğrudan Kayıt Sistemi (DRE):*** Dijital seçim sistemleri arasında en çok tercih edilen sistem DRE olarak bilinmektedir. DRE'nin kullanımı ATM'lere benzemektedir. Seçmene anlık bilgi sağlayan, geçersiz oy kullanımlarında seçmeni uyaran, oy kullanımı sonrasında oyların sayılması işlemini gerçekleştiren DRE oy kullanımı aşamasında yazıcıdan her seçmen için oy pusulası almakta ve seçim işlemini bu şekilde doğrulamaktadır. Teknolojinin seçim sistemlerine entegre edildiği bu model pratik ve hızlı bir seçim süreci gerçekleştirse bile kendi içinde handikaplar barındırmakta, örneğin makinede olan herhangi bir mekanik arıza durumunda etkisiz kalmaktadır. DRE'nin olumlu yanı açık kaynak kodlu yazılım barındırmasıdır. Bu sistem kendi içinde şeffaflık sağlarken üretici firmanın makine egemenliğini bertaraf etmektedir (Zissis, 2011: 243).

✓ ***Delikli Kartlı Sistem:*** Bu sistem ABD'de 2002 yılında oldukça şikâyet alan bir sistem olarak bilinmektedir. Bu seçim sisteminde seçmen hazırlanmış delikli kartlarda kendi tercihini belli edecek şekilde kartı delmektedir. Üretici firmalar tarafından 2 farklı model olarak üretilen bu makineler kullanışlı bulunmamıştır (Telciler, 2017: 111).

✓ ***İşaret Tanıyıcı (Optik) Sistem:*** Bu modelde ise seçmen oy pusulasını işaretleyip belirlenen alana koyar. Oyların sayım aşamasında faaliyete geçen makinede optik okuyucu sayesinde oylar otomatik algılanır ve sayımı gerçekleştirilir. Pusulada yer alan yanlış işaretler dolayısıyla çok fazla soruna yol açmıştır (Telciler, 2017: 111).

✓ ***İnternet Üzerinden Oylama:*** Bu modelde ise seçmen bir web arayüzüyle çevrim içi oy kullanır. Bu modele elektronik posta yöntemi de denmektedir. Seçmen seçim günü bir bilgisayardan seçim sitesine girerek kimlik denetimi yapıldıktan sonra boş oy pusulasını görür. Oy pusulasını tercihine göre dolduran seçmen "gönder" butonuna basarak oyunu kullanır. Kişisel bilgisayarların ve telefonların barındırdığı güvenlik açıklarından dolayı sistemin kötü niyetli kişiler tarafından ele geçirilmesi endişesi sebebiyle eleştirilen bu modelde oy verme işlemi sırasında gizlilik ilkesinin de sağlanamayacağı ileri sürülmektedir (Wheaton, 2010).

Tüm bunlarla beraber teknolojinin her gün gelişmesi ve gün geçtikçe farklı çalışmaların ortaya çıkması dijital seçim sistemlerinin artık kaçınılmaz olduğunu göstermektedir. Geleneksek seçim sistemlerinin de 100% güvenilir olmadığı ve dünya genelinde hemen her seçimde söylemlerle yayılan şaibeli durumların varlığı insan müdahalesinin en aza indirildiği seçim sistemlerinin geliştirilmesinin gerekliliğini vurgulamaktadır.

Dijital sistemlerin hem devlete hem vatandaşlara sağladığı avantajlar dikkate alındığında Dijital seçim sistemlerinin önemi ve gerekliliği daha net anlaşılmaktadır. Bu kapsamda dijital seçim sistemlerinin önemi ve gerekliliği şu şekilde sıralanabilir (Erol, 2021: 430-433).

✓ Dijital seçim sistemleri seçmenler için daha geniş bir erişim olanağı sağlamaktadır.
✓ Dijital seçim sistemleri geleneksel yöntemlere kıyasla katılımı teşvik edicidir.
✓ Dijital seçim sistemleri engelliler ve yaşlılar için katılımcı demokrasiyi genişletmektedir.
✓ Dijital seçim sistemleri kamusal maliyetleri azaltmaktadır.
✓ Dijital seçim sistemleri kâğıt israfı olmadığı için çevre dostudur.
✓ Dijital seçim sistemleri daha az insan gücüne ihtiyaç duyar.
✓ Dijital seçim sistemleri sonuçların daha güvenli, doğru ve hızlı şekilde açıklanmasını sağlar.
✓ Dijital seçim sistemlerinde güçlü bir teknolojik alt yapı ve güvenilir şifrelemelerle seçim gizliliği ve sonuç şeffaflığı en üst düzeyde sağlanabilir.
✓ Dijital seçim sistemleriyle seçim yolsuzluklarının önüne geçilebilir.

Dijital seçim sistemlerinin yukarıda sıralanan maddelerden de görüleceği üzere birden çok faydası bulunmaktadır. Bu kapsamda seçim sistemlerinin yeni nesil teknoloji çağına uygun biçimde tasarlanıp kullanıma sunulması gerekliliği göze çarpmaktadır. Her ülkenin farklı biçimlerde tasarladığı dijital seçim uygulamalarına alternatif olarak bu çalışmada ülkemiz bünyesinde geliştirilecek bir dijital seçim sistemi modelinin e-Devlet üzerinden sürdürülmesi önerisi yapılacaktır. Dünya genelinde dijital seçim sistemleri arasında yer alan *internet üzerinden oy kullanma* modeline benzerlik gösteren bu modelin ayırt edici yanı, içerisinde yapay zekâ desteği ve e-Devlet entegrasyonu barındırmasıdır. Bu kapsamda çalışmanın bundan sonraki kısmında e-Devlet üzerinden gerçekleştirilen bir dijital seçim sisteminde ne

gibi fırsatların yer aldığına, karşılaşılabilecek olası sorunlara, bu sorunlara karşı geliştirilebilecek çözüm önerilerine ve tasarım ve uygulamada gerekli olan noktalara odaklanılacaktır. Çalışma kapsamında önerilen her fikir geleneksel seçim sistemlerinde yer alan sorunlara, dünya genelinde sürdürülen dijital seçim sistemi modellerinde karşılaşılan sorunlara ve teknolojinin sağlayacağı alternatif güvenlik sistemlerine göre oluşturulacaktır.

Yöntem

Bu çalışmada e-Devlet üzerinden güvenli ve etkin bir dijital seçim sistemi model önerisi tasarım ve uygulama önerileriyle birlikte tartışılmıştır. Güvenli ve etkin bir dijital seçim sistemi modelinin tasarlanmasında avantajlar ve fırsatlar ortaya koyularak bu modelin hali hazırda aktif kullanım sunan e-Devlet sistemine entegre edilmesi kapsamında oluşabilecek güvenlik açıkları ve tehditler dikkate alınarak güvenliği sağlayabilecek alternatif öneriler sunulmaktadır.

Oluşturulabilir yeni dijital seçim sistemi modelinin günümüzde 65.470.800 kullanıcının 1.041 kurumun sunduğu 8.246 dijital hizmete doğrudan ve güvenle ulaşabildiği e-Devlet entegrasyonlu olarak tasarlanmasının vatandaşlarda var olan dijitale güvensizlik sorununa çözüm olacağı düşünülmektedir. Devlet eliyle aktif şekilde hizmet sunulan ve yıllardır kullanımına alışılmış e-Devlet portalına uyarlanmış bir dijital seçim sisteminin güven verme ve yeni sistemi hızlı benimseme açısından önemlidir.

Bu çalışmadaki model dünya genelinde dijital seçim sistemini aktif olarak kullanan ABD, İsviçre, Brezilya, Estonya gibi ülkelerin modellerinin incelenmesi, dijital seçim sistemine geçiş için başlatılan e- Devlet sistemi entegrasyonu ve dijital seçim sistemleri için geliştirilmesi hedeflenen yeni güvenlik teknolojileri dikkate alınarak belirlenmiştir. Doküman Analizi Yöntemi kullanılarak hazırlanan çalışmada önerilen dijital seçim sistemi modelinin çerçevesinin belirlenmesi için Vural Dinçkol ve Işık (2019), Telciler (2017) ve Çetinkaya ve Çetinkaya'nın (2006) çalışmalarından, konuyla ilgili çalışılmış diğer akademik çalışmalardan ve güncel olarak kamuya sunulan teknolojik yenilik haberlerinden yararlanılmıştır.

Bulgular ve tartışma

E-Devlet üzerinden dijital seçim sistemi: Avantajlar ve fırsatlar

Uluslararası konjonktürde teknolojiye uyum sağlamak ve teknolojinin sağladığı avantajları fırsata çevirmek ülkeler için oldukça önemli hale gelmiştir. Uluslararası rekabet gücünü belirleyen faktörler arasında yer alan teknolojinin hayat standartlarının gelişmesinde, devamlı yükselişte, beşerî ve ekonomik gelişmenin artmasında ve hem ulusal hem de uluslararası yönetim etkinliğinin gelişmesindeki rolü oldukça büyüktür. Her ülkenin, vatandaşlarının siyasal sisteme olan güvenini sağlamada teknolojiden önemli ölçüde yararlandığı göz önüne alındığında günümüzde teknolojinin her alanda etkisinin yadsınamaz bir gerçek olduğu görülmektedir.

Ülke yönetimlerinin en temel görevleri arasında her alanda güven ortamı oluşturmaları gelmektedir. Siyasal güven ortamının oluşturulması ise yönetsel, sosyal ve ekonomik pek çok alanı doğrudan etkilemesi bakımından önceliğe sahiptir. Vatandaşların siyasal sisteme ve siyasal sistemin kurumlarına duyacağı güvensizlik toplumda moral bozukluğunun yaygınlaşmasına, geleceğe olan güvensizliğe, siyasal yabancılaşmaya ve uzun vadede siyasal katılım düzeylerine doğrudan etki etmektedir (Akgün, 2001: 2-3). Dolayısıyla siyasal sistemin sağlıklı işleyişi adil, yarışmacı ve demokratik bir seçim ortamını gerektirdiği kadar şeffaf, etkin ve güvenilir bir seçim sisteminin varlığını da gerektirmektedir. Siyasal katılımın üst düzeyde olduğu ve vatandaşların güvenilir bir ortamda yöneticilerini seçtiklerine inandıkları bir siyasal sistem içinde siyasal güven ortamının sağlanması ve ülke içi istikrarın her alana sirayet etmesi kolaylaşmaktadır.

21. yüzyılda yeni yönetim anlayışı ve bilgi iletişim teknolojilerindeki değişimler, siyasi karar vericileri, kamu yönetimini yeni ilke ve değerlere göre yeniden keşfetmek zorunda bırakmış, hizmet sundukları alanlarda toplumsal taleplere doğrudan ve etkin şekilde cevap verebilecek, daha iyi hizmet için daha yaratıcı olan, süreç geliştiren ve risk alan bir pozisyona zorlamıştır. Bu bağlamda, küresel ekonominin önemli aktörleri olarak bilinen G-20 ülkeleri arasında yer alan Türkiye'de 1990'ların sonlarında başlayan dijital dönüşüm önemli bir ivme kazanmıştır. Bu süreçte başta kamu hizmetleri olmak üzere sağlık,

eğitim, ticaret, dijital ve siber güvenlik, ulaşım ve lojistik gibi pek çok alanda etkinlik ve verimliliğin artırılması için bilgi iletişim teknolojilerinin iş modellerine entegrasyonuna ağırlık verildiği, süreç içerisinde çok sayıda projenin hayata geçirildiği görülmektedir. Bu projeler arasında en başarılı ve dikkat çeken proje ise toplumun geneline hitap eden ve genel kamu hizmetlerinin dijital dönüşümünü sağlayan (OECD, 2023) e-Devlet Kapısı'dır. 18 Aralık 2008 tarihinde kullanıma açılan ve "türkiye.gov.tr" adresinden erişilebilen uygulama, tek bir kimlik doğrulama işlemiyle tüm hizmetlerin ortak bir noktadan hızlı bir şekilde kullanıcıya ulaştırılmasını sağlamaktadır (Şahnagil, 2017: 83).

Türkiye'de yönetişim alanında kullanılan en büyük ve etkin teknolojik uygulama olan e- Devlet'in devlet ve vatandaş özelinde kamu yönetiminin işlerliğinde son derece önemli yararları olduğu görülmektedir. Bu yararlardan bazıları aşağıdaki gibi özetlenebilir (Güler, 2023: 119- 120):

✓ ***Kamu hizmetlerine kolay erişim*:** Uygulama, günümüz itibariyle 1048 farklı kuruma ait 8000'den fazla hizmete tek bir platformdan erişim sağlamaktadır.
✓ ***Zaman tasarrufu*:** Vatandaşlar ihtiyaç duydukları kamu hizmetlerini sunan kurumlara fiziksel olarak gitmeden, dolayısıyla zaman ve para harcamadan, kuyruk beklemeden ev, işyeri ya da bulundukları herhangi bir yerden 7/24 kamu hizmetine ulaşabilmektedirler. Nitekim hizmet alabilmek için geleneksel yöntemdeki gibi kurumun açık olduğu mesai saatlerine uyma mecburiyeti bulunmamaktadır.
✓ ***Maliyetleri düşürmesi:*** Başlangıçta yatırım maliyetleri ve süreç içerisinde bakım, güvenlik vb. birtakım maliyetler olmasına rağmen orta ve uzun vadede gerek vatandaş gerek devlet açısından kırtasiye ve posta giderlerinin vb. azaltması, işlemlerin hızlanması dolayısıyla birim iş başına düşen maliyetin de düşmesi söz konusudur.
✓ ***Hızlı sonuç alma:*** Kullanılan yazılımlar binlerce aynı ya da farklı işlemin (başvurular, belge talepleri, güncellemeler) çok kısa sürede sonuçlandırılmasını sağlayarak bir yandan kamu görevlilerinin iş yükünü diğer yandan da vatandaşın bekleme sürelerini minimuma düşürmektedir.
✓ ***Çevre dostu olması:*** İşlemlerin elektronik olarak gerçekleşmesi, kâğıt, mürekkep, plastik dosya vb. araç gerecin kullanımını, arşivleme ve süresi dolan arşiv ve belgelerin imha sorununu ortadan kaldırması çevre üzerinde olumlu etki yaratmaktadır.
✓ ***Devlet ile iletişimi artırması***: Uygulama yoluyla vatandaşların talep, istek, öneri, görüş ve şikayetlerini hızlı bir şekilde bildirebilmesi ve bunlara yanıt alabilmesi vatandaşın kamu yönetimine güven duymasını ve memnuniyetinin artmasını sağlamaktadır.
✓ ***Güven sağlaması***: Uygulamanın kimlik doğrulama ve şifreleme teknolojileri kullanılarak kişisel verilerin güvenliğini sağlaması, vatandaşın tüm başvuru ve taleplerinin kendisi tarafından da görülebilir ve ispatlanabilir şekilde elektronik olarak kayıt altına alınması, dolayısıyla vatandaşların uygulama süreçlerini izleyebilmesi işlem süreçlerine güven duyulmasını sağlamaktadır.
✓ ***Etkin yönetimi desteklemesi***: Uygulama bugün geldiği noktada 8000'den fazla uygulamadan yararlanan 65 milyonu aşan kullanıcı sayısı ile çok büyük bir verinin sağlandığı/üretildiği bir yapı haline dönüşmüştür. Dolayısıyla bu büyük veri iyi analiz edildiğinde kamu yönetiminin gelecek projeksiyonlarını doğru oluşturmasına, kamu kurum ve kuruluşlarının politika kararlarının ve hizmetlerinin geliştirilmesine dayanak teşkil edecektir.

Yukarıda sayılan, E-Devletin sahip olduğu tüm bu avantajlar dikkate alındığında geliştirilerek sisteme entegre edilecek e- seçim sisteminin siyasal alanın meşruiyetini daha da güçlendirebileceği düşünülmektedir.

Dijital seçim sistemlerinin dünya çapında birden fazla uygulama modeli bulunmaktadır. Dijital seçim sistemleri arasında yer alan bu farklı tasarımlara alternatif olarak önerilen e-Devlet üzerinden gerçekleştirilecek bir dijital seçim sisteminin söz konusu olan diğer tasarımlara ve geleneksel seçim sistemine göre belli avantaj ve fırsatlar içerdiği düşünülmektedir. Bu avantajlar ve fırsatları şu şekilde sıralamak mümkündür:

✓ Dünya genelinde uygulanmakta olan dijital seçim sistemlerinin tasarım ve uygulamaları teknolojik olarak üretilen makinelerden oluşmaktadır. Bu makineler İşaret Tanıyıcı (Optik) Sistem, Delikli Kartlı Sistem veya DRE olarak adlandırılan ve ATM'lere benzer sistemler olarak bilinmektedir

(Telciler, 2017: 110-111). E-Devlet üzerinden tasarlanan bir dijital seçim sistemiyle üretilmesi veya temin edilmesi gereken dijital makinelerin maliyetlerinden kaçınılması söz konusu olabilir.

✓ Dijital seçim sistemleri için kullanılan ve yukarıda adı geçen dijital makineler özel sektör tarafından üretilmektedir (Telciler, 2017: 110-111). Yazılım ve donanımı özel şirketlere bağlı olan bu makinelerin dijital seçim sistemi bünyesinde kullanılması durumunda seçmenin tüm sistemin doğruluğuna ve dürüstlüğüne inanması gerekmektedir. Satıcı firmanın sistem üzerindeki egemenliğinin bertaraf edilmesi açık kaynak kodlu yazılımlarla sağlansa bile e-Devlet üzerinden gerçekleştirilecek olan bir dijital seçim sistemi modelinin tasarlanması yerli ve milli standartların sağlanmasında ve sürecin vatandaşın daha rahat güvenebileceği şekilde sürdürülmesinde etkili olabilir.

✓ Dijital seçim sisteminin e-Devlet üzerinden hizmete sunulmasıyla e-Devletin kendi bünyesinde barındırdığı avantajlardan yola çıkarak birçok alanda avantaj ve fırsat sağlayacağı ön görülebilir (Türkiye.gov.tr, 2024). Bu kapsamda e-Devletin dijital seçimlerde erişilebilirlik meselesine kolaylık sağlayacağı düşünülmektedir. Seçmenlere her yerde oy kullanma imkânı sunan bu model sayesinde dünya genelinde uygulanmakta olan diğer dijital seçim sistemi teknolojilerine göre siyasal katılımın daha da artacağı öngörülebilir.

✓ Oylama sürecinin yönetilmesi, oy sayımı ve sonuçların açıklanması gibi süreçlerin e-Devlet hizmeti kapsamına alınması durumunda seçim süreçlerinde hız ve verimlilik sağlanacağı söylenebilir.

✓ Geleneksel seçimlerin gerçekleştirilebilmesi için ihtiyaç duyulan insan gücünün fazlalığı göz önüne alındığında e-Devlet üzerinden gerçekleştirilen bir dijital seçimin insan hatalarını minimuma indirerek doğruluk ve güvenilirliği artıracağı düşünülmektedir. Dolayısıyla insan müdahalesinin en aza indirilmesi doğruluk oranlarının artmasına ortam sağlayabilecektir.

✓ E-Devlet aracılığıyla gerçekleştirilecek bir dijital seçim sisteminin engelli ve uzakta olan seçmenlere kolaylık sağlayacağı ve siyasal katılımı dezavantajlı gruplar açısından da artıracağı öngörülmektedir.

Tüm bunlarla beraber e-Devlet bünyesinde geliştirilen bir dijital seçim sisteminin hem devlet açısından hem de seçmenler açısından birden fazla fayda sağlayacağı söylenebilmektedir. E-Devlet sistemi kapsamında sunulan kamu hizmetlerinden memnuniyet ve vatandaşların yaşadığı hizmet deneyimi gün geçtikçe pozitif anlamda artış göstermektedir. Kamu kurumları açısından maliyet ve iş gücünde azalma sağlayan e-Devlet sisteminde bilgi ve iletişimin hızlanması, işlem sürelerinin azalması, hizmetin 7/24 gerçekleşebiliyor olması, güvenilir bir ortam sağlaması ve şeffaflık barındırması (Türkiye.gov.tr, 2024) gibi özelliklerin de bulunması dolayısıyla dijital seçim sistemi ve vatandaşlar açısından büyük fırsatlar sağlayacağı öngörülebilmektedir.

E-Devlet tabanlı dijital seçim sisteminin karşılaşacağı muhtemel sorunlar: Güvenlik sorunları ve tehditler

Gün geçtikçe artan teknolojik yeniliklerle hayatımıza giren ve dünya genelinde birçok ülkede uygulamaya koyulan dijital seçim sistemleri günümüz şartlarında artık gerekli görülmektedir. Ancak hala geleneksel seçim sistemi yürüten ülkelerce bu geleneksel olanın sürdürülmesindeki en büyük itici gücün dijital seçim sistemlerine karşı kamuoyunda hâkim olan güvensizlik algısının olduğunu söylemek mümkündür. Çeşitli makineler veya internet tabanlı arayüzler vasıtasıyla geliştirilen dijital seçim sistemi modellerinde güvenlik endişelerinin bulunması bu alandaki çekingen tavrın en geçerli sebebi olarak değerlendirilebilmektedir. Bununla birlikte dijital seçim sistemi fikrinin kendisine duyulan güvensizliğe ek olarak sistem içi güvensizlik de bu alanda atılacak adımlarda ülkeleri ve vatandaşları çekingen kılmaktadır (Vural Dinçkol ve Işık, 2019: 721).

Dijital seçim sistemlerinin uygulama alanları dijital araç, gereç ve makinelerdir. Dijital ortamda verilen oyların toplanması, sayılması ve sonuçlarının güvenli bir şekilde açıklanması sistemin sağlaması gereken en temel hizmettir. Ancak dijital araç gereçler vasıtasıyla gerçekleştirilecek bir seçimde en başından itibaren kimlik doğrulama, anonimlik, mahremiyet, güvenilirlik ve denetlenebilirlik faktörleri güvenli bir seçimin dijitalde nasıl sağlanacağı hususunda birçok soruyu beraberinde getirmektedir. Bu sistem üzerinde önemle durulan ilk sorunun mahremiyet hususu olduğunu söylemek yanlış olmayacaktır. Çünkü dijital seçim sistemlerinde seçmenlerin oylarının sayılıp sayılmadığını kontrol etmek istemesi durumunda seçmenin nasıl oy kullandığını açıklamadan bu kontrolün yapılamayacağı düşünülmektedir (Gibson vd., 2016: 281). Bu duruma ek olarak dijital seçim sistemlerinin seçim

sonuçlarının yakın olduğu durumlarda meşruiyet sorunsalı oluşturması, psikolojik etkiler sebebiyle seçmenin uzaktan oy kullanması durumuna bağlı olarak seçiminin etkilenmesi ve dijital seçim sistemlerinde kullanılan oyun gizlilik barındırmadığı iddiaları dijital seçim sistemleri üzerinde oluşmuş bazı sorunların başında gelmektedir (Buchstein, 2004: 40).

E-Devlet sistemi üzerinden sağlanacak dijital bir seçim sisteminin de bu bağlamda muhtemel sorunlarına dikkat çekmek yerinde olacaktır. Sorunların büyük çoğunlukla teknolojinin hızlı gelişimine bağlı olarak oluşabilecek kötü niyetle gerçekleştirilen tehditler ve bundan kaynaklanacak güvenlik sorunları temelinde gerçekleşeceği düşünülmektedir. Bu kapsamda sorunlar şu şekilde sıralanabilir (Çetinkaya ve Çetinkaya, 2006: 114-120).

✓ ***Korsan saldırıları:*** Dijital seçim sistemleri internet tabanlı yapılarıyla ön plana çıkan sistemlerdir. Bu sebeple oluşabilecek en ciddi sorun sisteme yönlendirilen siber saldırılar olarak ifade edilebilir. Kötü niyetli kişi veya grupların dijital seçim sistemi üzerine yönlendirdiği siber saldırılar güvenlik tehditleri oluşturabilir.

✓ ***Verilerin manipülasyona uğraması:*** İster geleneksel seçim sistemi ister dijital seçim sistemi olsun bir seçim sistemindeki en önemli noktalardan biri seçmen iradesinin doğru şekilde sonuçlara aktarılmasıdır. Bu kapsamda dijital seçim sistemlerinde sistem içindeki verilerin manipüle edilmesi veya seçmen iradesinin olandan farklı şekilde yansıtılması sorunları ortaya çıkabilir. Seçim sonuçlarını yanıltan bu durum seçimin doğruluğu ve güvenilirliği açısından tehdit unsuru olarak değerlendirilir.

✓ ***Seçmen verilerinin çalınması:*** Kötü niyetli kişiler tarafından gerçekleştirilen siber saldırılarla seçmene ait kimlik bilgilerinin çalınıp kötü niyetle kullanılması mümkündür. Elde edilen kimlik bilgileriyle sahte hesaplar açılabilir, mevcut hesaplar ele geçirilebilir ve seçim sonuçlarına müdahale edilip sahte oy kullanılabilir.

✓ ***Sosyal mühendislik:*** Sosyal mühendislik bir psikolojik saldırı türüdür. Saldırganın akıllıca ve kuşku uyandırmayarak, hatta çoğu kez kurbanın güvenini sağlayarak gerçekleştirdiği kötü niyetli bilgi edinme girişimidir (Siberay, 2024). Dijital seçim sistemlerinde de saldırganların seçmeni veya seçim görevliklerini kandırarak sistemdeki verileri elde etmesi ve kötüye kullanması olasıdır.

✓ ***Fiziksel interferans ve engelleme girişimleri:*** İnterferans; bir sisteme dışarıdan girerek iletişimi olumsuz yönde etkileyen sinyallere verilen genel isimdir (Beyaz.Net, 2024). Dijital seçim sistemleri de yapısı gereği bu tarz kötü niyetli girişimlere müsaittir. Fiziksel olarak müdahale edilen dijital seçimin normal işleyişi engellenebilir ve sonuçların güvenliği tehlikeye girebilir.

✓ ***Otomatik saldırılar:*** Kötü niyetli kişilerce sisteme düzenli olarak yapay zekâ temelli otomatik siber saldırılar gerçekleştirilebilir. Sisteme aşırı yüklenilmesine sebep oluşturabilecek bu saldırılar sonucunda sistem çökebilir, veriler ele geçirilebilir, seçim sonuçları engellenebilir veya değiştirilebilir.

✓ ***Olası ve kasti elektrik kesintileri*:** Dijital bir seçim sisteminin var olan sorunları ve tehditleri arasında elektrik kesintileri de bulunmaktadır. Belirli bir süre içerisinde gerçekleştirilmesi hedeflenen seçimlerin kötü niyetli kişiler tarafından sabote edilmesi elektrik kesintileriyle de sağlanabilir. Sisteme giriş sağlayacak cihazların elektrik kesintisi sebebiyle kullanılamaması seçimlerinin belirsiz bir süre kapsamında ertelenmesine yol açabilir. Bu elektrik kesintileri kötü niyetli kişilerce kasti bir saldırı niteliğinde olabileceği gibi doğal sebeplerden kaynaklanacak elektrik kesintileri de dijital seçim sistemleri için sorun ve tehdit teşkil edebilir.

✓ ***Yetkilendirme sorunları:*** Dijital bir seçim sisteminin dikkate alınması gereken bir diğer önemli sorunu yetkilendirme meselesidir. Tasarlanmış bir dijital seçim sisteminde seçim öncesinde, esnasında ve sonrasında sisteme erişim kontrolü sağlayabilecek kişi ve kuruluşların güvensizliğe mahal vermeden belirlenmesi gerekir (Çetinkaya ve Çetinkaya, 2006: 120). Yetkili kişi veya kurumun doğru politikalarla belirlenmediği durumlarda ciddi güvenlik açıkları oluşabileceği gibi seçimin güvenilirliği de zedelenebilir.

E-Devlet üzerinden gerçekleştirilen bir dijital seçim sisteminin olası sorun ve tehditleri dikkate alınmalıdır. İçinde bulunduğumuz teknoloji çağında dijital dünyada her geçen gün yeni gelişmeler yaşanmakta ve bu gelişmeler her zaman iyi niyetli olarak şekillenmemektedir. Dijital bir seçim sisteminin oluşturulması aşamasında da olası tehditlerin belirlenmesi tasarlanacak olan dijital seçim sisteminin güvenilirliğini artıracaktır.

Güvenlik odaklı tasarım ilkeleri: E-Devlet üzerinde dijital seçim sistemlerinin güvenliğini sağlamak için öneriler

Yukarıda bahsedildiği üzere dijital seçim sistemlerinin güvenli ve sağlıklı bir seçim sisteminin sürdürülmesinde bazı şüpheli güvenlik açıkları olduğu ileri sürülmektedir. E-Devlet üzerinden gerçekleştirilecek bir dijital seçim sisteminin de bu güvenlik şüpheleri göz önünde bulundurularak tasarlanması önemlidir. Bu kapsamda üzerinde durulan güvenlik sorunları ve tehditler dikkate alınarak güvenlik odaklı tasarım ilkeleri belirlenmelidir. E-Devlet üzerinden geliştirilebilecek bir dijital seçim sistemiyle üst düzey güvenlikli bir seçim sürecinin yönetilmesinde önerilebilecek güvenlik odaklı tasarım ilkeleri şu şekildedir:

- **End-to-end encryption ve güvenli iletişim protokolleri**

Dijital seçim sistemlerinin güvenliğine dair ileri sürülen ilk sorun bu sistemlerin mahremiyet ve anonimlik barındırmayacağı ve seçim sürecindeki verilerin gizli kalamayacağı yönündedir. Bu güvenlik sorununa çözüm olarak End-to-End Encryption önerilebilir. Uçtan uca şifleme olarak da bilinen End-to-End Encryption iletişim sürecindeki verilerin alıcıya ulaşana kadar tüm noktalarda şifrelenmesini sağlayan bir yapıdır. Bu şifrelemede verilerin iletim aşamasında başka sunucu veya üçüncü partiye aktarılmasının önüne geçilmiş olur. Her çeşit elektronik verinin okunamaz bir biçimde dönüştürülerek aktarıldığı bu şiflemede yalnızca gerekli şifreye sahip olanlar veriye ulaşabilir (Vr, 2015). Dijital bir seçim sisteminde uçtan uca şifreleme sayesinde seçmenin oy kullanma işlemi güvenli bir şekilde gerçekleştirilmiş olur. Seçmenin cihazında şifrelenen ve güvenli şekilde veriyi ileten bu sistemle seçmen bilgileri çalınamaz, mahremiyet korunur ve manipülasyon riski en aza indirilir.

Şifrelemenin korunmasında yapılması önerilen önemli bir nokta da güvenli iletişim protokollerinin belirlenmesidir. Dijital tabanlı bir sistemin kendine özgü güvenlik ağlarının devreye sokulması seçim güvenliğinin sağlanmasında önemli görülmektedir. Bu kapsamda iki cihaz arasında güvenli bir bağlantı oluşturan SSL/TSL Protokolleriyle verilerin şifrelenmesi güvenlik önlemi olarak sağlanabilir (Aws, 2024a). Tüm iletişim kanalları arasında güvenli bir iletişim sağlayan HTTPS (HTTP Secure) bağlantısı sağlanarak şifreleme güçlendirilebilir (Turk.net, 2024). Bunlara ek olarak Kriptografi protokolleriyle şifreleme ve gizlilik oluşturma sağlanabilir. Dünya üzerinde yaygın şekilde kullanılan kriptografi protokolleri üst düzey gizlilik sağlayan, verileri yetkisi olan kişiler dışında kimsenin anlamayacağı forma dönüştüren bir uygulama olarak bilinmektedir (Kara, 2009: 34). Protokollerin belirlenmesinde kullanılacak olan zaman damgalaması da iletilen verilerin veri bütünlüğünü sağlamaya olanak tanırken geriye dönük seçim denetimi imkânı sunmada katkı sağlayabilir (KamuSM, 2024). Sistem içinde sağlanacak güvenlik protokolleri arasında ağ düzeyinde uygulanabilecek güvenlik duvarları, ağ izleme sistemleri ve saldırı tespit sistemleri de sistem güvenliğinin sağlanmasında güvenli bir ağ katmanı oluşturulmasını sağlayacaktır.

- **Çok faktörlü kimlik doğrulama ve yetkilendirme**

Çok faktörlü kimlik doğrulama (MFA) ve yetkilendirme de e-Devlet üzerinden gerçekleştirilecek bir dijital seçim sisteminin güvenli bir biçimde sürdürülmesinde önemli görülmektedir. MFA, kullanıcıların bir sisteme paroladan daha fazla bilgi girmesini gerektiren, çok adımlı oturum açma süreci olarak bilinmektedir. Kullanıcıların hassas bilgilerinin çevrim içi depolandığı dijital mecralarda bilgilerin kötüye kullanılmasının, çalınmasının ve mahremiyet ihlallerinin önüne MFA ile geçilmektedir. Birden çok faktör dikkate alınarak tasarlanabilir bu kimlik doğrulama sisteminde bilgi faktörü, sahiplik faktörü ve katılım faktörüne göre kimlik doğrulaması yapılabilmektedir. Buna göre bilgi faktöründe kişinin kimsenin bilmediği bir bilgiyi kanıtlaması (ilk evcil hayvan adı, anne kızlık soyadı vb.), sahiplik faktöründe kişinin benzersiz olarak sahip olduğu bir şeyi veri olarak sisteme sunması (cep telefonu, e-posta hesabı ve donanım ve güvenlik anahtarı gibi fiziksel araçlar), katılım faktöründe ise kişinin biricik olan fiziksel özelliklerini (parmak izi, retina, ses, yüz) sisteme veri olarak sunması gerekir (Aws, 2024b). E-Devlet üzerinden tasarlanacak bir dijital seçim sisteminde seçmenlerin vatandaşlık hakkı olan seçme hakkını sağlıklı ve güvenli bir şekilde kullanması için çok faktörlü kimlik doğrulama sistem içinde sağlanmalıdır. Özellikle ileri teknoloji kullanarak belirlenen parmak izi, retina, ses ve yüz tanıma özellikleriyle biricikliğe sahip faktörler dikkate alınarak

oluşturulmuş bir giriş yöntemi dijital seçim sistemlerinin çok tartışılan "Ya bir başkası yerime oy kullanırsa?", "Kötü niyetli kişilerce sahte oylar sisteme işlenirse?" gibi endişeleri ortadan kaldıracaktır. Çünkü sistem içi kullanımlarda e-Devlet'te vatandaş olarak kayıt altında olan bireylerin sisteme girişleri ve seçime dair kararları başka kimselerce görülmeyecek şekilde tasarlansa bile o kişinin oy kullandığı sisteme yansıyacaktır. Bu da o kişi adına başka bir şekilde oy kullanılmasının önüne geçecektir.

Güvenlik sorunlarının bertaraf edilmesi konusunda önem arz eden bir diğer nokta da yetkilendirme meselesidir. Sisteme erişim sağlayan bir yetki otoritesinin varlığı dijital bir seçimde oluşabilecek sorunların hızlı şekilde çözümlenmesi için gereklidir. Ancak bu yetki otoritesi politikalarla belirlenmelidir (Çetinkaya ve Çetinkaya, 2006: 120-121). Bu kapsamda ilk olarak sistem içi erişim sağlayacak kişileri veya kurumları kapsayan bir politika belirlenmesi önerilebilir. Buna ek olarak ortak güven duygusunun sağlanması açısından seçim sürecinde seçmene hitap eden parti veya kurumların yetki otoritesinde donanımlı kontrol personeli bulundurma hakkının bulunması önerilebilir. Geleneksel seçimlerde bulunan farklı partilerin sandık görevlilerine benzer şekilde belirlenen donanımlı kontrol personelleri sayesinde kötü niyetle gerçekleştirilecek ve halkın iradesini gerçek dışı yansıtacak girişimlerin önüne geçilebilir. Bu kontrol personellerinin sistem içi kayıtlarda yer alması ve sistem içi hareketlerinin zaman damgalamasıyla kayıt altına alınması olası güvenlik ihlallerinde sorumlu tutulacak kişinin belirlenmesinde ve ihlalin tespit edilmesinde önemli bir yöntem olarak düşünülmektedir.

- **Fiziksel ve siber güvenlik altyapısı: Tehditlere karşı fiziksel ve dijital koruma**

E-Devlet üzerinden gerçekleştirilecek bir dijital seçim sisteminin muhtemel güvenlik tehditlerini bertaraf edecek biçimde tasarlanması ve uygulanması oldukça önemlidir. Bu kapsamda fiziksel ve siber güvenlik alt yapı ve kontrollerin en üst seviyede sağlanması gerekir. Dijital bir seçim her ne kadar dijital ortamda gerçekleştirilse de fiziksel olarak da korumaya alınmalıdır. Bu bağlamda seçim sisteminin özellikle yetkilendirilmiş birimlerce sürdürüldüğü merkezlerin fiziksel denetim altına alınması gerekir. Seçim, sayım ve denetim otoritelerinin bulunacağı ana merkezlerin güvenlik kameralarıyla denetlenmesi ve güvenlik personeliyle kontrol altına alınması önerilebilir. Ana merkeze yönelik fiziksel saldırılarla seçim sürecinin olumsuz etkilenmemesi fiziksel korumanın da önemini ortaya koyar nitelikte değerlendirilmektedir.

Fiziksel güvenlik alt yapısının dışında teknolojik güvenlik alt yapısının oluşturulması da güvenli bir seçim süreci için önem teşkil eder. Dijital seçim sistemlerinin kendi bünyesinde birinci dereceden siber tehditlerden uzak tutulması gerekir. Bu kapsamda tasarlanacak dijital seçim sisteminde güvenlik duvarları, ağ güvenliği, güncel yazılımlar, güncel işletim sistemleri, olay izleme, incident response planları ve gelişmiş tehdit koruma çözümleri bulunması gereklidir. Siber güvenlik alt yapısıyla sağlanacak dijital korumalarda sistemin ağ trafiğinin izlenmesi, zararlı içeriklerin filtrelenmesi, yetkisiz erişimlerin engellenmesi, kötü niyetli saldırıların tespit edilmesi, saldırılara karşı dirençli bir dijital alt yapının oluşturulması ve olası güvenlik ihlallerine karşı hazırlıklı olunabilecek planların oluşturulması sağlanabilmektedir. Özellikle son zamanlarda gelişmiş tehdit koruma alanında gerçekleştirilen çalışmalarla dijital saldırıların tespit edilmesi, saldırıların engellenmesi ve zararlı yazılımların sistem içinde açtığı yarıkların kapatılması konusunda gelişmeler sürmektedir (InfoSEC Bilgi Teknolojileri, 2024). E-Devlet üzerinden gerçekleştirilecek bir seçim sisteminin de bu hususlar dikkate alınarak tasarlanması önerilmektedir.

- **Yapay zekâ ve makine öğrenimi tabanlı güvenlik çözümleri**

Dijital seçim sistemlerinin güvenlik sorunlarına karşı oluşturulabilecek güvenlik odaklı tasarım ilkelerinden biri de yapay zekâ ve makine öğrenimi alanında olabilir. Teknolojik gelişmeyle doğru orantılı olacak şekilde tanımı ve işlevi her geçen gün değişen yapay zekâ ve makine öğrenimi günümüzde birçok alana önemli katkılar sağlamaktadır.Görüntü işleme, ses işleme, veri işleme, sağlık verilerinin analizi ve tedavi planlaması, insansız sürüş sistemleri, sigortacılık ve finans, siber güvenlik, eğitim, tarım ve hayvancılık gibi birçok farklı alanda yapay zekâ teknolojilerinin kullanımı artmaktadır (TC. Dijital Dönüşüm Ofisi, 2024).

Bir bilgisayar veya bilgisayar kontrolünde olan bir robotun akıllı varlıklarla ilişkili görevleri yerine getirme yeteneği olarak tanımlanan yapay zekâ, akıl yürütme, anlam keşfetme, genelleme ve deneyimlerle öğrenme gibi insana ait yeteneklerin donanımlı sistemlerle geliştirilmesi amacıyla kullanılmaktadır. Her geliştirilen teknoloji gibi yapay zekanın da kötü niyetle kullanılabileceği dikkate alınmakla birlikte her geçen gün güvenlik ve açıklanabilirlik ilkelerine sadık kalınarak etik ve ahlaki kurallar çerçevesinde yapay zekanın önemli bir teknolojik gelişmeyi ifade ettiği söylenebilmektedir (Britannica, 2024).

Yaygın yanlış kanılar arasında bulunan "yapay zekâ sistemlerinin güvenilir olmadığı"na dair inançlar bu meseleye yaklaşımları etkilemektedir. Ancak özellikle güvenlik meselesine karşı 2018 yılında yürürlüğe giren Genel Veri Koruma Yönetmeliğiyle (GDPR) birlikte yapay zekâ algoritmalarında kişisel veri güvenliğini sağlayan diferansiyel mahremiyet, federe öğrenme ve homomorfik şifreleme gibi yaklaşımlar geliştirilmiştir (TC. Dijital Dönüşüm Ofisi, 2024). Dijital seçim sistemlerinin güvenliği amacıyla kullanılabilecek bir yapay zekanın da siber güvenliği destekleyeceği düşünüldüğünde kişisel verilerin kötüye kullanılmasına karşı çıkabilecek sorunlarının önüne geçileceği düşünülmektedir. Nitekim seçim sistemi için geliştirilmesi gereken yapay zekâ, veri güvenliğini sağlamak amacıyla tasarlanacaktır. Bu da dijital seçim sistemi için tasarlanan bir yapay zekanın seçim sisteminin güvenliğini sağlayacak önemli bir etken olduğunu düşündürmektedir.

Siber güvenlik alanlarında sistem içi zararlı yazılımların tespit edilmesinde, analiz edilmesinde ve anomali tespitlerinde yapay zekâ teknolojileri güvenilir çözümler sunmaktadır (TC. Dijital Dönüşüm Ofisi, 2024). Bu kapsamda yapay zekanın e-Devlet üzerinden gerçekleştirilecek bir dijital seçim sistemine entegre edilmesi durumunda seçim sürecinde yaşanabilecek birçok sorunun önüne geçileceği düşünülmektedir. Öyle ki seçim sırasında oluşabilecek muhtemel sorunlar kısmında tartıştığımız bazı sorunlarla birlikte yapay zekanın dijital seçim sisteminin güvenliği için yapabilecekleri şu şekilde düşünülmektedir:

- ✓ Korsan saldırılarına karşı yapay zekâ hızlı ve etkili güvenlik duvarları oluşturabilir.
- ✓ Fiziksel İnterferans olarak bilinen iletişim engelleyici sinyallerin olması durumunda sinyallerin tespit edilmesi, engellenmesi ve raporlanması yapay zekâ sayesinde gerçekleştirilebilir.
- ✓ Sistem içi tanımlı olmayan kişilerin sisteme girme girişimi olması durumunda bunların tespit edilmesi ve engellenmesi yapay zekâ ile hızlı ve etkili biçimde mümkün olabilir.
- ✓ Geçmiş deneyimlerle kendini geliştirme yeteneğine sahip olan yapay zekâ sisteme karşı yönlendirilebilecek otomatik saldırılara karşı hızlı, etkili ve güvenli önlemler alabilir ve sistem içi güvenliği sağlayabilir.
- ✓ Yetkilendirilen birimlerin sistem içi faaliyetlerini seçim süresi boyunca denetleyebilir ve olası bir kötü niyetli girişim algıladığında yetkilendirilen birimden yetkiyi alıp kişiyi veya kurumu sistem dışı bırakabilir.
- ✓ İleri bir yapay zekâ yetkilendirmesi olarak seçim süreci boyunca karar destek sistemine ve tasarım alt yapısına bağlı olarak tüm yetkiyi kendinde toplayabilir ve insani müdahaleden arındırılmış tamamen dijital bir seçim süreci hizmeti sunabilir.

Yapay zekanın dijital bir seçim sistemine entegre edilmesi güvenli, etkin, hızlı ve sürdürülebilir bir seçim sürecinin yönetilmesinde etkili olabilir. Ancak yapay zekanın yukarıda sıralanan potansiyel katkıları ahlaki ve etik kurallarla üretilen ve iyi eğitilen bir yapay zekâ algoritması için geçerlidir. Etik ve ahlaki hassasiyetlerle tasarlanmamış ve doğru şekilde eğitilmemiş bir yapay zekanın yanlış sonuçlar üretmesi ve potansiyel siber tehditleri yanlış yorumlaması mümkündür. Bu nedenle bu alan için üretilecek bir yapay zekanın doğru şekilde eğitilmesi ve sürekli güncellenmesi gerekmektedir. Buna ek olarak yapay zekâ teknolojilerindeki hızlı gelişmeye bağlı olarak yapay zekâ sistemlerinin anlaşılması zor bir yanı da bulunmaktadır. Bu kapsamda seçim sisteminin doğru şekilde işlemesi yapay zekanın şeffaflığına ihtiyaç duymaktadır. Karmaşık ve anlaşılması zor bir yanı olan yapay zekanın seçim sürecindeki işleyişi ve karar mekanizmasını nasıl sürdürdüğü izlenebilmelidir. Bu da büyük verileri kendinde toplayıp deneyimle karar verebilen bu algoritmaların denetim ve izleme alanlarında şeffaflık barındıran yapıda tasarlanmasını gerekli kılmaktadır.

E-Devlet üzerinden dijital seçim sistemi modeli: Tasarım ve uygulama önerileri

E-Devlet üzerinden gerçekleştirilecek bir dijital seçim sisteminin tasarım ve uygulama aşamasında çeşitli gereksinimleri karşılaması gerekmektedir. Bu kapsamda çalışmanın bu kısmında dijital seçim sistemlerinde dikkate alınması gereken güvenlik tedbirleri ve dijital seçimin güvenli şekilde başlatılıp sonlandırılması için gereken kullanım şekilleri dikkatealınarak tasarım ve uygulama gereksinimleri önerilerle desteklenecektir.

➢ **Tasarım gereksinimleri**

Dijital seçim sisteminde dikkate alınması gereken güvenlik tedbirleri ve seçim sisteminin kolay kullanımı göz önünde bulundurularak tasarım gereksinimleri şu şekilde belirlenebilir (Çetinkaya ve Çetinkaya, 2006: 116-119; Erzurumlu ve Koloğlu, t.y; Erol, 2021: 431-434).

- ✓ Dijital bir seçim sisteminde en önemli ilk güvenlik gereksinimi seçmen gizliliğinin sağlanmasıdır. Seçmen ile kullandığı oy arasında bağlantı kurulamamasını ifade eden seçmen gizliliği için dijital seçim sistemine uçtan uca şifleme yöntemi, güvenli iletişim ve kriptografi protokollerince belirlenen siber alt yapının sağlanması önerilir.
- ✓ Seçimin seçmenler için güvenilir olması ve seçmenlerin seçme hakkını güvenilir şekilde kullanabilmesi için çok faktörlü kimlik doğrulama ile sisteme giriş yapılması gereklidir. Bu sebeple tasarlanacak dijital seçim sisteminin üst düzey kimlik doğrulama metotlarından biri olan parmak izi tarama, retina veya yüz tanıma metotlarıyla hizmet vermesi önerilir.
- ✓ Dijital seçim sistemlerinin siber saldırılardan korunması için dağınık bir alt yapı kullanılması saldırı riskini azaltabilir. Bu sebeple merkezi bir sunucu yerine dağınık bir alt yapı kurulması güvenlik sorununa alternatif olabilir. Tek merkezli bir sistem denetimi yapılması durumunda ise merkezin fiziksel ve teknolojik kontrol mekanizmalarıyla güçlendirilmesi önerilmektedir.
- ✓ Seçim sürecinin bağımsız denetime uygun olarak tasarlanması sistemin güvenliği, bütünlüğü ve şeffaflığı açısından önem teşkil eder. Bu kapsamda yetki otoritesinin farklı paydaşlarla iş birliği yapacak şekilde tasarlanması önerilir. Yetki otoritesinde farklı parti, kurum ve kuruluşlarının belirleyeceği donanımlı kontrol personeli alternatif paydaşlar arasında olabileceği gibi sistemin tamamen siyasal alandan bağımsız kişilerce sürdürülmesi de alternatifler arasında değerlendirilebilir.
- ✓ Geleneksel seçim sisteminde geçerli olan "tek oy" dijital seçim sistemi için de geçerli olmalıdır. Sisteme giriş yapan her seçmenin tek bir oy hakkı olmalıdır. Bu durum seçim sürecindeki manipülasyonları engelleyeceği gibi seçimin dürüstlüğünü de sağlayacaktır. Tek oy kuralının işletilmesi için E-Devlet'te kayıtlı olan seçmen sayısının, oy kullanan seçmen sayısının ve oy kullanmayan seçmen sayısının ilçe, il, bölge ve ülke şeklinde seçmenin oy gizliliği korunarak raporlanması ve sonuçlara yansıtılması önerilebilir.
- ✓ Seçimde doğabilecek olası yanılmalara, şüpheli durumlara ve reddetme sorunlarına karşı oy verme işleminin kayıt altına alınması önemlidir. Seçmen oyunun gizliliği riske atılmadan zaman damgalaması kullanılarak verilen oyların geriye dönük kayıt altına alınması önerilebilir.
- ✓ Dijital seçim sisteminin doğruluğunun sağlanması için seçim dönemi süresince kullanılan her oyun sayılması ve bunun seçime katılan seçmen sayısı oranınca kanıtlanabilir olması önemlidir.
- ✓ Seçim işlemi yapan seçmenin seçim süreci boyunca oyunu değiştirme hakkı ve geçersiz oy kullanma hakkının bulunması baskı ortamında verilen oyların kişi iradesine göre değiştirilebilme hakkını koruyacaktır. Bu kapsamda her seçmenin belli güvenlik aşamalarıyla kimlik doğrulaması gerçekleştirip sisteme girmesi ve oyunu belirlenen seçim süresinde değiştirme hakkının bulunması önerilebilir. Ek olarak kaydedilen oyun yetkili otoritelerce seçim süreci boyunca görüntülenememesi, oyların değiştirilmesinin önüne geçeceği için gerekli siber alt yapının bu alanda sağlanması önerilmektedir.
- ✓ Dijital seçim sisteminin kötü niyetli kişiler, kurumlar ve otoriteler tarafından zarar görmemesi için dijital güvenlik duvarları oluşturulmalıdır. Bu kapsamda hem seçim öncesi hem de seçim sürecinde sistemin sürekli denetlenebilir ve güncellenebilir olması gerekir. Bu noktada siber

güvenliğe önemli katkılar sunan yapay zekâ alt yapısı alternatif olabilir. Sürekli iyileşme ve deneyimsel ilerleme yeteneğine sahip olan yapay zekâ sayesinde sisteme yöneltilen saldırıların veya manipülasyon girişimlerinin bertaraf edilmesi kolaylaşacaktır.

- ✓ Oyların satılma meselesi geleneksel seçimlerde ciddi sorun teşkil etmektedir. Bu kapsamda dijital seçim sisteminde bu durumun engellenmesi için karekod görüntüleme önerilmektedir. Sisteme giriş yapan seçmen oy pusulasını görüntülediğinde seçimi yaptığı anda seçmenin kişisel bilgileri ve verdiği oy arasında bağlantı kurularak kişiye özel bir karekod oluşturulabilir. Bu sayede oyların satılması meselesi söz konusu olamayacağı gibi seçmenin iradesini kanıtlayan bir belge bulunacağı için geriye dönük itirazlarda bu karekodla oyun sayılıp sayılmadığı da kontrol edilebilir.
- ✓ Dijital bir seçim sisteminin şeffaf şekilde olabilmesi için tasarım aşamasında açık yazılımla geliştirilmesi önerilir. Tasarlanan sistemin kaynak kodunun incelemeye açık olması seçimin şeffaf ve güvenilir şekilde sürdürülmesini sağlayacaktır.
- ✓ Tasarlanacak dijital seçim sistemi tek bir seçimde kullanılmayacağından dolayı her seçime uyabilecek uygun ölçekli bir tasarım yapılmalıdır.
- ✓ Dijital seçim sistemi en temelde internete daha sonra bilgisayar veya akıllı cep telefonuna ihtiyaç duyan bir sistem olduğu için bu imkanları sağlayamayan kesimlerin de tasarım aşamasında düşünülmesi gerekir. Bu kapsamda internet ve akıllı cihaza ulaşım sağlayamayan kesimler için elektronik oy verme kabinleri kurulabilir (Tarhan, 2023) ya da tespit edilen kısıtlı kesimlerin gezici araçlarla seçime katılımı sağlanabilir.
- ✓ Seçim süreci bittiğinde ve sonuçlar açıklandığında o seçime ait gerekli bilgilerin elektronik ve basılı ortamda saklanmasına özen gösterilmesi önerilmektedir.
- ✓ Dijital seçim sistemi tasarlanırken alt yapısında sürekli güncellemelerin bulunması gerektiği düşünülmelidir. Teknolojinin her an her dakika geliştirildiği dikkate alındığında sistemin sürekli olarak yeni tehditlere hazırlıklı, gelişmelere açık olması gerekmektedir. Bu kapsamda bu alanda da yapay zekâ sayesinde güncellemeler otomatik olarak yapılabilir ve denetim birimlerince geriye dönük takip sürdürülebilir.
- ✓ Dijital seçim sisteminin güvenli ve etkin şekilde sürdürülmesi seçim dönemi boyunca kesintisiz elektrik ile sağlanacaktır. Bu kapsamda seçim sürecine ve sonuçlarına müdahale etmek isteyen kötü niyetli saldırıları bertaraf etmek ve elektriği kesintisiz şekilde vatandaşların hizmetine sunmak önemlidir. Olası sorunlar arasında göz önünde bulundurulması gereken elektrik kesintilerine karşı alternatif olarak ülke geneline yedek güç kaynakları kurulabilir. Bu kaynaklar bölgesel veya ülkesel gerçekleşebilecek olası elektrik kesintileri durumunda sistemin devam etmesini sağlayacaktır. Bu kaynaklar yedek jeneratörler veya batarya destekli güç kaynakları gibi alternatif enerji kaynakları olabilir. Buna ek olarak elektrik sağlayıcılarla yapılacak ön iş birlikleri ve anlaşmalar kesinti durumunda sorunun en kısa sürede çözümünde katkı sağlayacaktır.
- ✓ Tasarlanan modelin seçmenlerin ve diğer paydaşların güven duyabileceği şekilde oluşturulması gereklidir. Bu kapsamda katılımcılar arası iletişim ve geri bildirim mekanizmasın sürdürülebileceği bir tasarım yapılması önerilir. Kullanıcıların sistemi daha iyi anlaması, güvenliğin daha kapsamlı şekilde oluşturulması ve sistemin kullanımının daha fonksiyonel olması noktasında sunabileceği öneriler sistemin sürdürülmesinde etkili olacaktır. İletişim ve geri bildirim sürecinin katılımcı demokrasiyi güçlendirecek biçimde sürdürülmesi için vatandaşların kolay şekilde iletişim kurup sorunlarını ve önerilerini kolaylıkla iletebildikleri Cumhurbaşkanlığı İletişim Merkezi (CİMER) gibi dijital iletişim platformlarına entegre edilebilecek bir dijital seçim öneri bloğu alternatif olabilir.
- ✓ Dijital bir seçim sistemi tasarımda üzerinde durulması gereken önemli bir nokta da tüm cihazlarla uyumlu bir platform geliştirmektir. Bu sebeple e-Devlet üzerinden uygulanabilecek

bir dijital seçim sisteminin bilgisayarlar ve cep telefonları için ayrı özelliklerde geliştirilmesi önerilmektedir. Bilgisayarlar üzerinden oyunu kullanmak isteyen vatandaşların karşılaşacakları ara yüz ve cep telefonları üzerinden oyunu kullanmak isteyen vatandaşların karşılaşacakları ara yüzün kullanılacak cihaza göre en kolay şekilde oluşturulması önerilmektedir.

- **Uygulama gereksinimleri**

E-Devlet üzerinden tasarlanacak bir dijital seçim sistemi için uygulama gereksinimleri ve uygulama önerileri ise şu şekilde sıralanabilir (Kozan, 2018):

- ✓ Dijital bir seçim sisteminde uygulama gereksinimi olarak her şeyden önce kolay bir arayüz kullanılmalıdır. Seçmenin özel yetenekler gerektiren cihaz ve ekipman kullanmamasına özen gösterilmeli, hemen herkesin kolay giriş sağlayabileceği bir sistem geliştirilmelidir.
- ✓ Bilgisayar ve cep telefonları için ayrı tasarım oluşturmak vatandaşların sistemi daha rahat ve etkili kullanmasını sağlayacağı için bu hususta tasarlanacak olan arayüzün sade ve basit şekilde uygulamaya yansıtılması önerilmektedir.
- ✓ Tasarlanan sistemin okunabilir metinleri ve yazı fontları kullanılan cihaza göre farklılık gösterebilir. Kullanıcıların daha kolay biçimde sistem adımları takip etmesi için önerilen yazı fontları dikkat alınmalıdır. Her cihaza uyum sağlayacak olan tasarımın genel geçer yazı fontlarıyla düzenlenmesi önerilmektedir.
- ✓ Mobil uygulamalar temelde dokunuş ve parmak hareketleri ile ön plana çıkan yapıya sahiptir. Bu sebeple özellikle cep telefonları için tasarlanacak olan dijital seçim sisteminin parmakla kolaylıkla ulaşılabilir boyutlarda olması kolay kullanım ve etkili bir seçim için önemli görülmektedir.
- ✓ Sonuçların ilanı sistem üzerinden verilebilir olmalıdır. Her seçmen sonuçların açıklanmaya başladığı anda e-Devlet üzerinden sonuçları ilçe, il, bölge ve ülke geneli olarak görüntüleyebilmelidir. Buna ek olarak seçim sonuçları halka açık alanlarla dijital tabelalarda da gösterilebilir.
- ✓ Seçim sürecinin başından sonuna kadar güvenli şekilde sürdürülmesi için sistem akışına bağlı kalınmalıdır. Bu kapsamda seçim sonuçlarının açıklanması sistemin oy sayımına bağlı olarak sürdürülmelidir. Yetki otoritesinin sayım aşamasında yalnızca süreci başlatması ve sayıma müdahale etmemesi gerekir. Dijital seçim sistemine girilen oyların hızlı ve güvenli şekilde sayılması sistem içinde yapay zekâ desteğiyle sağlanabilir.

Sonuç ve öneriler

Bu çalışmada, e-Devlet üzerinden güvenli ve etkin bir dijital seçim sistemi modeli önerilmiş ve bu modelin tasarım ve uygulama stratejileri detaylı olarak incelenmiştir. Dijital seçim sistemleri, geleneksel yöntemlere kıyasla birçok avantaj sunmakta ve katılımcı demokrasiyi güçlendirmede önemli bir araç olarak öne çıkmaktadır. Çalışmanın bulguları, dijital seçim sistemlerinin geniş bir erişim imkânı sağlaması, engelli ve yaşlı bireyler için katılımı artırması, seçim süreçlerini hızlandırması, maliyetleri düşürmesi, çevre dostu olması ve insan hatalarını minimize ederek sonuçların daha güvenilir olmasına katkı sağladığını göstermektedir.

Ancak, bu avantajlarına rağmen dijital seçim sistemlerine yönelik güvenlik endişeleri dünya genelinde hala yaygındır. Bu endişeler, büyük ölçüde kamuoyu algısıyla şekillenmekte olup, teknolojinin hızlı gelişimiyle birlikte giderilebileceği düşünülmektedir. Dijital seçim sistemlerinin güvenliği konusunda en çok tartışılan konular arasında verilerin gizliliği, seçmen iradesinin doğru bir şekilde yansıtılması, siber saldırılar, manipülasyon riski ve kimlik doğrulama süreçleri bulunmaktadır. Çalışmada bu sorunlara yönelik çeşitli güvenlik odaklı tasarım ilkeleri ve teknolojik çözümler önerilmiştir. Uçtan uca şifreleme, çok faktörlü kimlik doğrulama ve yapay zekâ tabanlı güvenlik çözümleri gibi ileri teknolojiler, dijital seçim sistemlerinin güvenliğini artırmada kritik rol oynayacaktır.

Önerilen model, e-Devlet platformu üzerinden entegre edilerek uygulanması planlanan bir dijital seçim sistemini kapsamaktadır. Türkiye'de dijital dönüşüm sürecinde önemli bir araç haline gelen e-Devlet, zaten güvenilirliği ve geniş kullanım ağıyla bilinen bir platformdur. Bu platform üzerinde geliştirilecek

bir dijital seçim sistemi, hem kullanıcıların mevcut güvensizliklerini gidermeye yardımcı olacak hem de teknolojinin sağladığı avantajlarla katılımı artıracaktır. Özellikle e-Devlet'in sunduğu güvenli kimlik doğrulama mekanizmaları, seçim sürecinde güvenliğin sağlanmasında önemli bir destek sağlayacaktır.

Dijital seçim sistemine geçişin başarılı olabilmesi için, toplumsal algının dönüştürülmesi ve bu yeni sistemin kabul edilmesi gerekmektedir. Bunun için kamuoyunun dijital seçim sistemlerine yönelik önyargılarının kırılması ve bu alandaki güvenin artırılması zorunludur. Toplumu bilinçlendirme kampanyaları, pilot uygulamalar ve şeffaf bir bilgilendirme süreci, bu güvenin sağlanmasında etkili olacaktır.

E-Devlet üzerinden uygulanacak dijital seçim sisteminin tasarımı sırasında dikkate alınması gereken en önemli unsurlar güvenlik, şeffaflık, erişilebilirlik ve kullanıcı dostu olmasıdır. Güvenlik konusundaki endişelerin giderilmesi için, sistemin her aşamasında ileri düzey güvenlik protokolleri uygulanmalı ve bu sistemlerin düzenli olarak güncellenmesi sağlanmalıdır. Aynı zamanda, yapay zekâ ve makine öğrenimi gibi teknolojilerden faydalanarak, sistemin olası tehditlere karşı dirençli olması sağlanmalıdır. Çalışmanın tüm bulguları birlikte değerlendirildiğinde e-Devlet üzerinden uygulanacak dijital seçim sistemi için şunlar önerilmektedir:

- Dijital seçim sistemine yönelik kamuoyu algısını değiştirmek ve sistemi kabul ettirmek için kapsamlı bilinçlendirme kampanyaları düzenlenmelidir. Bu kampanyalar, dijital seçim sistemlerinin güvenliği, işleyişi ve sunduğu faydalar hakkında toplumun her kesimini bilgilendirmeye yönelik olmalıdır. Bu süreçte, medya, sivil toplum kuruluşları ve eğitim kurumlarıyla iş birliği yapılabilir.
- Dijital seçim sisteminin tamamen uygulanmasından önce, belirli bölgelerde pilot uygulamalar gerçekleştirilebilir. Bu uygulamalar, sistemin işleyişi hakkında değerli geri bildirimler sağlayacak ve olası teknik ve güvenlik sorunlarının tespit edilmesine olanak tanıyacaktır. Pilot uygulamalar sırasında elde edilen veriler ışığında sistem üzerinde gerekli iyileştirmeler yapılmalıdır.
- Dijital seçim sistemlerinin güvenliğini sağlamak için, kullanılan güvenlik protokollerinin sürekli güncellenmesi gerekmektedir. Özellikle yapay zekâ ve makine öğrenimi teknolojilerinin entegre edilmesiyle, sistemin yeni ortaya çıkan tehditlere karşı dirençli hale getirilmesi sağlanmalıdır. Bu güncellemeler, sadece seçim dönemlerinde değil, sistemin sürekli olarak güvenli kalmasını temin etmek için periyodik olarak yapılmalıdır.
- Dijital seçim sisteminin hukuki altyapısı güçlendirilmelidir. Bu kapsamda, dijital oy verme işlemleri ve güvenlik protokolleriyle ilgili yasal düzenlemeler netleştirilmeli ve seçim sürecinde yaşanabilecek hukuki ihtilafların önlenmesi için gerekli adımlar atılmalıdır. Ayrıca, seçim sonuçlarının doğrulanabilirliği ve şeffaflığı açısından ulusal ve uluslararası standartlar belirlenmeli ve bu standartlara uygunluk sağlanmalıdır.
- Diğer ülkelerdeki dijital seçim uygulamalarının incelenmesi ve bu deneyimlerden yararlanılması önemlidir. Uluslararası iş birlikleri, özellikle güvenlik açıklarının tespiti ve giderilmesi konusunda değerli bilgiler sağlayabilir. Türkiye, dijital seçim sistemlerinin geliştirilmesi sürecinde, bu alandaki deneyimli ülkelerle bilgi alışverişinde bulunmalı ve uluslararası standartlara uygun bir sistem geliştirmelidir.
- Dijital seçim sisteminin tasarımı ve uygulanması sırasında, vatandaşların geri bildirimde bulunabileceği etkili bir dijital platform oluşturulmalıdır. Bu platform, vatandaşların sistemle ilgili deneyimlerini, önerilerini ve şikayetlerini doğrudan iletebileceği bir mecra olarak işlev görmelidir. Bu sayede, dijital seçim sisteminin sürekli iyileştirilmesi ve katılımcı demokrasinin güçlendirilmesi sağlanabilir.
- Dijital seçim sistemi, güvenilir ve kesintisiz bir hizmet sunmak için güçlü bir teknik altyapıya ihtiyaç duyar. Sistem altyapısının düzenli olarak denetlenmesi ve olası teknik sorunlara karşı yedek çözümler üretilmesi gerekmektedir. Elektrik kesintileri gibi olası problemlere karşı yedek enerji kaynakları ve alternatif teknolojiler devreye sokulmalıdır.
- Dijital seçim sistemi, herkesin kolayca erişebileceği şekilde tasarlanmalıdır. Özellikle engelli bireyler ve internet erişimi olmayan kişiler için özel çözümler geliştirilmelidir. Bu kapsamda, elektronik oy verme kabinleri veya gezici seçim araçları gibi alternatifler değerlendirilebilir.

Bu öneriler doğrultusunda, e-Devlet üzerinden uygulanacak dijital seçim sisteminin başarılı bir şekilde hayata geçirilmesi ve sürdürülebilirliğinin sağlanması mümkündür. Dijital seçim sistemlerinin güvenli, etkin, şeffaf ve katılımcı bir yapıda yönetilmesi, demokratik süreçlere katılımı artırarak toplumsal güveni güçlendirecektir. Türkiye'nin bu alandaki başarılı uygulamaları, diğer ülkeler için de bir model teşkil edebilir ve uluslararası arenada örnek bir dijital seçim sistemi olarak tanıtılabilir. Bu nedenle, dijital seçim sistemlerinin geliştirilmesi ve uygulanması sürecinde atılacak her adım, Türkiye'nin demokratik süreçlerini güçlendirme yolunda önemli bir ilerleme kaydetmesine katkı sağlayacaktır.

Kaynakça

Akgün, B. (2001). Akgün, B. (2001). Türkiye'de siyasal güven: Nedenleri ve sonuçları. *Ankara Üniversitesi SBF Dergisi,* 56(04), 2-23.

Akın, M. (2006). Elektronik oy verme sistemlerinde güvenlik: Deneyimler ve Türkiye için öneriler, *Ekonometri ve İstatistik Dergisi*, Sayı:3, 32- 47

Anadolu Ajansı, (2024). İran, Meclis Seçimlerinin ikinci turu için sandık başına giderken 8 kentte oy verme işlemi elektronik sandıkta yapılıyor, 12 Mayıs 2024 tarihinde aa.com.tr/tr/dunya/iran-meclis-secimlerinin-ikinci-turu-icin-sandik-basina-giderken-8-kentte-oy-verme-islemi-elektronik-sandikta-yapiliyor/3215309 adresinden erişildi.

Aws, (2024a). SSL ve TSL arasındaki fark nedir? 01 Nisan 2024 tarihinde amazon.com/tr/compare/the-difference-between-ssl-and-tls/ adresinden erişildi.

Aws, (2024b). Çok faktörlü kimlik doğrulama (MFA) nedir? 04 Nisan 2024 tarihinde amazon.com/tr/what-is/mfa/ adresinden erişildi.

Beyaz.Net, (2024). Enterferans (Interference), 29 Mart 2024 tarihinde beyaz.net/tr/ipucu/entry/713/enterferans-interference adresinden erişildi.

Britannica, (2024). Yapay zekâ nedir? 04 Nisan 2024 tarihinde britannica.com/technology/artificial-intelligence adresinden erişildi.

Buchstein, H. (2004). "Online democracy, ıs it viable? Is it desirable? Internet voting and normative democratic theory", in, *Electronic voting and democracy: A comparative analysis,* Eds: Norbert Kerstıng/Harald Baldersheım, Palgrave Macmillan, New York.

Çetinkaya, D. ve Çetinkaya, O. (2006). E-seçim uygulamaları için gereksinimler ve tasarım ilkeleri, XI. "*Türkiye'de internet" konferansı bildirileri* 21- 23 Aralık 2006 TOBB Ekonomi ve Teknoloji Üniversitesi, Ankara.

Erol, V. (2021). Yönetim bilişim sisteminin bir örneği olarak Türkiye'de elektronik seçim sistemi, *BŞEÜ Sosyal Bilimler Dergisi* 6 (2), 427-440.

Gibson, J. P, Krımmer, R., Teague, V., Pomares, J. (2016). "A review of e-voting: The past, present and future*" Annals of Telecommunications*, 71(7), 281.

Güler, T. (2023). *Değişim ve dönüşüm perspektifinden 21. yüzyılda Türk kamu yönetimi*, Ekin Yayınevi, Bursa.

InfoSEC Bilgi Teknolojileri, (2024). Dijital savunma: Siber güvenliğin 7 temel taşı, 04 Nisan 2024 tarihinde infosec.com.tr/dijital-savunma-siber-guvenligin-7- temel-tasi/ adresinden erişildi.

International IDEA, (2011). Introducing electronic voting: Essential considerations, (Policy Paper), International Institute for Democracy and Electoral Assistance, (International IDEA), Stockholm, Sweden 04 Mayıs 2024 tarihinde idea.int/sites/default/files/2023-09/introducing-electronic-voting.pdf adresinden erişildi.

KamuSM, (2024). Zaman damgası nedir? 01 Nisan 2024 tarihinde kamusm.bilgem.tubitak.gov.tr/urunler/zaman_damgasi/#:~:text=Zaman%20Damgalar%C4%B1%20belli%20bir%20verinin,belirli%20bir%20tarihteki%20varl%C4%B1%C4%9F%C4%B1n%C4%B1%20onaylar adresinden erişildi.

Kara, O. (2009). Kriptografinin yapıtaşları kriptografik algoritmalar ve protokoller, bilim ve teknik, 05 Nisan 2024 tarihinde services.tubitak.gov.tr/edergi/yazi.pdf;jsessionid=mmI99dY9l0qODZOvI20foFvf?dergiKodu=4&cilt=42&sayi=638&sayfa=34&yaziid=28094 adresinden erişildi.

Kozan, E. (2018). Mobil uygulama tasarımında 10 altın kural, 08 Nisan 2024 tarihinde tr.linkedin.com/pulse/mobil-uygulama-tasar%C4%B1m%C4%B1nda-10- alt%C4%B1n-kural-emrah-kozan adresinden erişildi.

Siberay, (2024). Sosyal mühendislik, 29 Mart 2024 tarihinde siberay.com/sosyal-muhendislik adresinden erişildi.

Şahnagil, S. (2017). Kamu politikası oluşturma sürecinde bilgi ve iletişim teknolojileri: E-Devlet uygulamaları, *Mersin Üniversitesi Sosyal Bilimler Enstitüsü e-Dergi,* Cilt 1, Sayı 1, s. 77- 89.

Tarhan, U. (2023). Seçimler yapay zekâ ile yapılabilseydi ne olurdu? 03 Mart 2024 tarihinde dunya.com/kose-yazisi/secimler-yapay-zeka-ile-yapilabilseydi-ne-olurdu/694352 adresinden erişildi.

TC. Dijital Dönüşüm Ofisi, (2024). Yapay zekâ, 04 Nisan 2024 tarihinde https://cbddo.gov.tr/sss/yapay-zeka/ adresinden erişildi.

Telciler, C. (2017). Elektronik seçim sistemleri, sorunlar, çözüm önerileri, *Nişantaşı Üniversitesi Sosyal Bilimler Dergisi,* 5(2), 106-122.

Turk.net, (2024). HTTP ve HTTPS nedir? 01 Nisan 2024 tarihinde turk.net/blog/http-ve-https-nedir/ adresinden erişildi.

Türkiye.gov.tr, (2024). E-Devlet- sıkça sorulan sorular, 22 Mart 2024 tarihinde turkiye.gov.tr/bilgilendirme?konu=sikcaSorulanlar adresinden erişildi.

Vr, (2015). End-to-end encryption (Uçtan uca şifreleme), 01 Nisan 2024 tarihinde vr.net.tr/teknik-makaleler/end-to-end-encryption-uctan-uca-sifreleme/ adresinden erişildi.

Vural Dinçkol, B. ve Işık, A. (2019). Katılımcı demokrasi ve online karar alma bağlamında e-oy ve estonya örneği, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,* 25(2), 716-726.

Wheaton, S. (2010, October 08). Voting test falls victim to hackers, The New York Times. 23 Mart 2024 tarihinde nytimes.com/2010/10/09/us/politics/09vote.html adresinden erişildi.

Zissis, D. L. (2011). Securing e-government and e-voting with an open cloud computing architecture, *Government Information Quarterly,* 28(2), 239-251.

Etik kurul onayı

Bu çalışmada anket, mülakat, odak grup çalışması, gözlem, deney, görüşme teknikleri, katılımcılardan veri toplanmasını gerektiren nitel ya da nicel yaklaşımlarla yürütülen araştırmalar, insan ve hayvanların (materyal/veriler dahil) deneysel ya da diğer bilimsel amaçlarla kullanılmasını gerektirecek herhangi bir araştırma ve kişisel verilerin korunması kanunu gereğince retrospektif çalışmalar kullanılmaması sebebi ile bu araştırma etik kurul izni gerektirmeyen çalışmalar arasında yer almaktadır.

Araştırmacıların katkı oranı beyanı

1. yazar %50 oranında, 2. yazar %50 oranında katkı sağlamıştır.

Çıkar çatışması beyanı

Bu çalışmada herhangi bir potansiyel çıkar çatışması bulunmamaktadır.