بسم الله الرحمن الرحيم

انتخابات الکترونیکی

(بایسته‌ها و شیوه‌ها)

دکتر محمد فتحیان

مهندس منیرالسادات تقوی

دفتر مطالعات فناوری‌های نوین

مرکز پژوهش‌های مجلس شورای اسلامی

فتحیان، محمد
انتخابات الکترونیکی: (بایسته‌ها و شیوه‌ها)/ مؤلفان محمد فتحیان، منیرالسادات تقوی.-- تهران: مجلس شورای اسلامی، مرکز پژوهش‌ها، ۱۳۸۷.
ح، ۱۹۲ ص.: مصور، جدول، نمودار.- (مرکز پژوهش‌های مجلس شورای اسلامی؛ ۱۳۸۷/۵۶)
ISBN: 978-964-8427-42-4: ۳۰۰۰۰ ریال
فهرست‌نویسی براساس اطلاعات فیپا.
کتابنامه: ص. [۱۸۹]ـ۱۹۲.
۱. انتخابات. الف. تقوی، منیرالسادات، نویسنده همکار. ب. مجلس شورای اسلامی، مرکز پژوهش‌ها، دفتر مطالعات فناوری‌های نوین. ج. عنوان.
JF ۱۵۲۵/ آ۸ف۲
۱۳۸۷

عنوان: *انتخابات الکترونیکی* (بایسته‌ها و شیوه‌ها)
مؤلفان: دکتر محمد فتحیان و مهندس منیرالسادات تقوی
ناشر: مرکز پژوهش‌های مجلس شورای اسلامی
مدیر نشر: عبدالرضا فاضلی
نوبت چاپ: اول، تابستان ۱۳۸۷
تیراژ: ۱۰۰۰ نسخه
چاپ: نگاران‌شهر
قیمت: ۳۰۰۰۰ ریال

فهرست مطالب

پیشگفتار ناشر

با پیروزی انقلاب شکوهمند اسلامی ایران، ملت بزرگ ایران به قرن‌ها سلطهٔ حکومت‌های جور پایان داد و با استعانت از خداوند متعال و پیروی آگاهانه از مرجعیت دینی، امام خمینی (ره)، با اتحاد و همدلی پرچمی را برافراشت که به الگوی بی‌نظیری برای جهانیان بدل گشته است و هر روز مشتاقان بیشتری را به‌سمت خود جلب می‌کند.

در اصل نخست قانون اساسی جمهوری اسلامی ایران این شکوه ملی به تصویر کشیده شده و حکومت اسلامی نظامی معرفی شده که متکی بر آرای مردمی است که با پیروی از احکام مقدس اسلام در تعیین سرنوشت خود نقش مستقیمی ایفا می‌کنند. این اصل انکارناپذیر به روشنی در اصل ششم تبلور یافته است:

«در جمهوری اسلامی ایران امور کشور باید به اتکای آرای عمومی اداره شود، از راه انتخابات، انتخاب رئیس جمهور، نمایندگان مجلس شورای اسلامی، اعضای شوراها و نظایر اینها، یا از راه همه‌پرسی در مواردی که در اصول دیگر این قانون معین می‌گردد».

ویژگی برجستهٔ این اصل آن است که نحوهٔ اجرای این امر نیز به‌خود مردم واگذار شده است و راه آن هم قانون‌گذاری قرار داده شده که منتخبان ملت به آن همت می‌گمارند.

طی سه دههٔ اخیر با درک حساسیت و جایگاه بنیادی قوانین راجع به انتخابات، منتخبان ملت قوانین موجود را با شرایط زمانی خود آزموده‌اند و بارها به تصویب اصلاحیه‌ها و الحاقیه‌ها مبادرت ورزیده‌اند. تنها طی دههٔ گذشته (از سال ۱۳۷۸ تا ۱۳۸۶) ۲۲ بار قوانین انتخابات مجلس شورای اسلامی، شوراها و ریاست جمهوری دستخوش تغییراتی شده‌اند.

تردیدی نیست که این میزان حساسیت و البته آزادی عمل منتخبان ملت ستودنی است و جلوه‌ای بی‌نظیر از مردم‌سالاری را بازتاب می‌دهد، ولی نباید این مسئله را نادیده

انگاشت که ثبات قوانین لازم‌الاجرای این حوزه خود از ارکان زیربنایی مـردم‌سـالاری بـه شمار می‌آید و ماهیت متغیر و متحول این قوانین می‌تواند ناشی از ناکارآمدی قـانون یـا نحوهٔ اجرای آن باشد.

باوجود رویکردها و اندیشه‌های گوناگون راجع به چگونگی نهادینه‌سازی مردم‌سالاری و تثبیت آن در نظام حاکمیت ملی، یک موضوع مـورد اجمـاع اسـت و آن اینکـه رویـه و ابزار برگزاری انتخابات باید بـه‌گونـه‌ای تعریـف و تهیـه شـود کـه حـداکثر «شـفافیت» و «بی‌طرفی» در آن لحاظ شده و این‌گونه نباشد که این رویه‌ها و ابزارها بر گـزینش مـردم تأثیر بگذارند و به آن جهت بدهند و در عمل زمینـهٔ اسـتفاده‌هـای ناصـواب و مغـایر بـا اهداف نظام مقدس جمهوری اسلامی ایران فراهم آید.

یکی از ابزارهایی که طی دههٔ اخیر نظر سیاست‌گذاران حاکمیتی و اجتمـاعی را در توسعه و ارتقای همه‌جانبهٔ امور به‌خود جلب کرده، «فناوری اطلاعات و ارتباطـات» اسـت. ماهیت به‌اصطلاح «خنثی»، انعطاف‌پـذیر و تواناسـاز ایـن فنـاوری و تـأثیر شـگرف آن در افزایش کارایی و اثربخشی باعث شده دست‌اندرکاران حوزه‌های خرد و کـلان جامعـه در الکترونیکی کردن امور خود تردیـد نکننـد و ایـن رویـه در میـان کشـورهای جهـان بـه جایگاهی دست یافته که به معیاری برای توسعه‌یافتگی تبدیل شده است.

یکی از موضوعاتی که به‌طور جدی نظر سیاست‌گذاران را به‌خود جلب کرده، نحوه و میزان به‌کارگیری این فناوری در امر حکمرانی است. در این خصوص هیچ استثنایی هـم لحاظ نشده و سعی بر این است که از همهٔ ظرفیـت‌هـای آن اسـتفاده شـود. هـم‌اکنـون مباحثی نظیر پارلمان الکترونیکی و قانون‌گذاری الکترونیکی مباحـث نخسـتین خـود را پشت سر گذاشته‌اند و به تکامل خود نزدیک می‌شوند.

در این میان، یکی از شاخه‌های مورد توجه، برگزاری انتخابات به شیوهٔ الکترونیکی یا همان «انتخابات الکترونیکی» است. شاید اکنون بحث راجع به مزایای این فنـاوری بـرای برگزاری یک انتخابات مردم‌سالارانهٔ تمام‌عیار دیر شده باشد و به راستی باید از «ضرورت» آن صحبت کرد. آیا در جامعه‌ای که قرار است زیربنای حـوزه‌هـای مختلـف آن در بسـتر الکترونیک شکل گیرد و توسعه یابد، می‌توان نسبت به برگزاری انتخابات به شیوهٔ مرسوم اصرار کرد. هرچند آگاهی از مزایای به‌کارگیری این فنـاوری در مراحـل مختلـف فراینـد

انتخابات و رفع بسیاری از نواقص و اشکالات اجرایی مرسوم می‌تواند حصول این مهم را آسان سازد. تضمین مشارکت مردم در انتخابات و حق امنیت رأی آنان، سلامت انتخابات در کنار سرعت و امنیت شمارش و امکان سریع اعلام نتایج همگی مواردی است که اعتماد متقابل مردم و حکومت را در حضور مستقیم مردم در تعیین سرنوشتشان تضمین می‌کند.

مرکز پژوهش‌های مجلس شورای اسلامی در راستای وظیفهٔ قانونی خود به‌عنوان بازوی مشاور و کارشناس قوهٔ مقننه که یکی از مخاطبان اصلی قانون انتخابات و رأساً متولی آن به شمار می‌آید، پژوهش حاضر را که مطالعه‌ای تطبیقی در راستای شناسایی تجربه‌های دیگر کشورهای جهان در اجرایی کردن انتخابات الکترونیکی محسوب می‌شود، انجام داده است. امید است این مجموعه پیش‌درآمدی در راه پرثمر نهادینه‌سازی انتخابات الکترونیکی در ایران اسلامی بوده و زمینهٔ همراهی و همفکری تمامی مسئولان و دست‌اندرکاران این حوزه را برای رسیدن به نتیجه‌ای مطلوب فراهم آورد.

معاون پژوهشی مرکز

مقدمه

رأی‌گیری اصلی‌ترین شکل واژه دمکراسی است که در سطوح مختلف از جمله گروه‌های شغلی، انجمن‌ها، شرکت‌ها و به‌خصوص در سطح ملی و سیاسی قابل اجرا می‌باشد.

به‌نظر می‌رسد که توسعه فناوری اطلاعات می‌تواند چهره فرایندهای انتخاباتی را تغییر دهد. اگرچه رأی‌گیری الکترونیکی به شکل استفاده از ماشین‌های خودکار رأی‌گیری از سال‌ها پیش وجود داشته، اما توسعه اینترنت زمینه جدیدی را برای انتخابات از راه دور فراهم کرده است.

در سال‌های گذشته شکست انتخابات الکترونیکی در برخی از کشورها توجه متخصصان زیادی را به‌خود معطوف داشته است. بسیاری از مشکلات پیش آمده به‌دلیل نقایص موجود در تجهیزات انتخابات و سیستم‌های به‌کار گرفته شده، بوده است، به‌گونه‌ای که تجهیزات معیوب، تعرفه‌های به‌هم ریخته، بروز خطا در فعالیت‌های حوزه‌های انتخاباتی و معضلات دیگر سبب از بین رفتن چهار میلیون رأی در انتخابات ریاست‌جمهوری آمریکا در سال ۲۰۰۰، در ایالت فلوریدا گردید.[۱]

چنین معضلاتی سبب خدشه‌دار شدن اعتماد ملت‌ها به فرایند دمکراسی در کشورها می‌گردد. به این دلیل، بسیاری از دولت‌ها در سراسر جهان تصمیم گرفتند که بودجه لازم را برای اصلاح و بهبود تجهیزات انتخابات و نیز به‌کارگیری روش‌های نوین مدیریت انتخابات تدارک ببینند. در اکتبر سال ۲۰۰۲، دولت فدرال آمریکا ۳/۹ بیلیون دلار برای بهسازی تجهیزات انتخاباتی درنظر گرفت.[۲] در حال حاضر بسیاری از کشورهای عضو اتحادیه اروپا، به شکلی انتخابات الکترونیکی را تجربه کرده و استراتژی‌های لازم را برای پیاده‌سازی این نوع انتخابات تدوین نموده‌اند.

امروزه در جهان بحث‌های فراوانی در زمینه سهولت کاربرد، مزایا و مخاطرات مرتبط با انتخابات الکترونیکی مطرح است. اگرچه این نوع انتخابات به‌دلیل عدم شفافیت ذاتی بحث و جدل‌های زیادی را به‌دنبال دارد، اما در صورت پیاده‌سازی صحیح، نسبت به سایر روش‌های رأی‌گیری از مزایای فراوانی برخوردار است که از جمله آنها می‌توان به‌سرعت بالا، صحت و دقت نتایج، سهولت بیشتر برای رأی‌دهندگان، تجزیه و تحلیل سریع آرا و هزینه پایین اشاره کرد.

انتخابات الکترونیکی می‌تواند علاوه بر مدرنیزه کردن فرایند انتخابات، ضمن به‌کارگیری فناوری‌های نوین اطلاعات و ارتباطات، امکان مشارکت الکترونیکی افراد را فراهم نموده و سبب بهبود ارتباط و تعامل ملت و دولت گردد. از طرفی استفاده از تمامی مزایای انتخابات الکترونیکی مستلزم به‌کارگیری معیارهای امنیتی پیشرفته و افزایش اعتماد رأی‌دهندگان و مسئولان انتخابات به این روش است.

رأی‌گیری الکترونیکی از ضروریات قرن حاضر محسوب می‌شود و به همین دلیل، برای استفاده از این فناوری نوین، لازم است عوامل مستقیم و غیرمستقیم به‌عنوان زیربنا در امر توسعه رأی‌گیری الکترونیکی مورد بررسی و مطالعه قرار گیرد. همچنین مسئولان و دست‌اندرکاران باید این امر مهم را شناخته و ضرورت آن را درک نمایند.

در این کتاب ابتدا در فصل اول سیر تکامل ابزارها و تعرفه‌های انتخاباتی در دنیا به‌طور مختصر شرح داده شده و در ادامه سوابق اخذ و شمارش آرا در ایران بررسی می‌شود. در فصل دوم نقش و جایگاه فناوری اطلاعات و ارتباطات در فعالیت‌های دولتی بررسی می‌گردد. در فصل سوم به مزایا و معایب انتخابات الکترونیکی، انواع روش‌ها و ابزارهای رأی‌گیری الکترونیکی و نیز ابعاد انتخابات الکترونیکی اشاره می‌شود. در فصل چهارم تجارب برگزاری انتخابات الکترونیکی در چند کشور مورد بررسی قرار می‌گیرد. در فصل پنجم ضمن مطالعه گسترده منابع و مقالات علمی، سه پروتکل معروف انتخابات الکترونیکی تشریح می‌شود؛ این پروتکل‌ها برای انتخابات مختلف با مقیاس‌های گوناگون طراحی شده‌اند. همچنین نحوه رمزنگاری و رمزگشایی کارت‌های هوشمند مورد اشاره قرار می‌گیرد؛ در انتخابات با حساسیت بالا، از این کارت‌ها برای احراز هویت رأی‌دهندگان استفاده می‌شود. در فصل ششم تجربیات انتخابات الکترونیکی در برخی از کشورها بررسی

می‌شود. در فصل هفتم، استانداردها و انتخابات الکترونیکی بررسی شده و سرانجام در فصل هشتم نتیجه‌گیری مباحث ارائه می‌گردد.

مطالعه این کتاب به کلیه دانشجویان مقاطع کارشناسی و تحصیلات تکمیلی به ویژه در رشته‌های مرتبط با فناوری اطلاعات، کارشناسان، مدیران و همه دست‌اندرکاران در حوزه انتخابات توصیه می‌شود. پیشاپیش از راهنمایی‌های ارزنده و نظرات اصلاحی کلیه خوانندگان گرامی که ما را در شناسایی و رفع اشکالات این اثر یاری خواهند کرد، تقدیر و تشکر می‌کنیم.

در اینجا لازم است از مساعدت و همکاری مرکز پژوهش‌های مجلس شورای اسلامی به ویژه استاد بزرگوار جناب آقای دکتر پورسید و جناب آقای مهندس باقری اصل سپاسگزاری نماییم.

فصل اول

تاریخچه انتخابات در جهان

۱-۱ انتخابات بدون تعرفه

نحوه برگزاری انتخابات در ۲۰ سال گذشته تغییرات زیادی را به همراه داشته است. دامنه این تغییرات در مقایسه با انتخابات امروزی به‌خوبی قابل لمس می‌باشد.

شکل ۱-۱ انتخابات در یک بخش

شکل ۱-۱ یک نقاشی از جورج بینگهام[1] است که محل اخذ رأی را روی پله‌های دادگاهی در شهر میسوری در سال ۱۸۴۶ نشان می‌دهد. در این نقاشی، رأی‌دهنده درحالی‌که دستش را روی انجیل قرار داده، سوگند می‌خورد که تاکنون رأی نداده است.

---

1. George Caleb Bingham

هیچ سازوکاری برای کنترل رأی‌دهنده وجود ندارد و تنها سوگند رأی‌دهنده و شهادت حضار در محل است که از رأی‌دهی مجدد رأی‌دهنده جلوگیری می‌کند.

در این سیستم رأی‌ها مخفی نبوده و رأی‌دهنده انتخابش را به منشی انتخابات که در روی ایوان و در پشت قاضی نشسته است اعلام می‌کند. منشی در یک دفتر نام رأی‌دهنده و انتخابش را می‌نویسد. در نقاشی چند نفر نیز با کاغذهایی در دست دیده می‌شوند. این کاغذها، تعرفه‌های انتخاباتی نیستند؛ زیرا در شهر میسوری تا سال ۱۸۶۳ انتخابات به‌صورت گفتاری صورت می‌گرفته است. مبارزات انتخاباتی در حوزه‌های اخذ رأی نیز قانونی و متداول بود. در نقاشی مردی دیده می‌شود که کارتش را به یکی از رأی‌دهندگان نشان می‌دهد تا به او رأی دهد.

۱-۲ اولین تعرفه‌های انتخاباتی

کلمه تعرفه[1] از واژه Ball مشتق شده است؛ زیرا تعرفه‌های اولیه به شکل توپ‌های کوچکی بودند. در دوره رنسانس گروه‌های مخفی مثل فراماسون‌ها درانتخابات خود برای پذیرش عضو جدید و یا ادامه عضویت اعضای موجود از توپ‌های کوچک سیاه و سفید استفاده می‌کردند. این توپ‌ها توسط اعضای گروه به صندوق رأی ریخته می‌شد، به‌نحوی‌که توپ سفید به‌معنای رأی اعتماد و توپ سیاه به‌معنای رأی عدم اعتماد بود.

در اواخر قرن نوزدهم، طراحان ماشین‌های رأی‌گیری نیز در طرح‌های خود از توپ‌های کوچک استفاده می‌کردند. در این ماشین‌ها توپ‌ها به‌عنوان رأی در محفظه‌های خاصی ریخته می‌شد. هدف از این سازوکار جلوگیری از رأی‌دهی مجدد رأی‌دهندگان و اختصاص صندوق‌های مجزا به هریک از کاندیداها بود.

۱-۲-۱ تعرفه‌های کاغذی

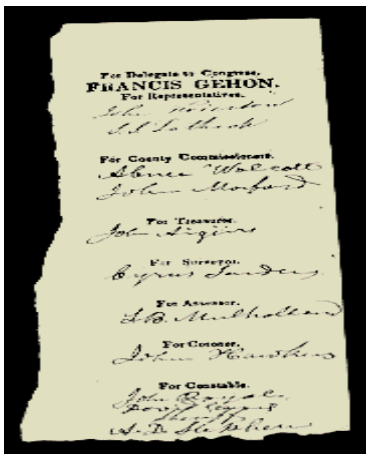
اولین مورد به‌کارگیری تعرفه‌های کاغذی در انتخابات به ۱۳۹ سال پیش از میلاد مسیح بازمی‌گردد، درحالی‌که در ایالات متحده آمریکا، اولین‌بار این تعرفه‌ها در سال ۱۶۲۹ برای انتخاب یک کشیش در یک کلیسا[2] مورد استفاده قرار گرفت.

---

1. Ballot
2. Salem Church

اولین تعرفه‌های کاغذی، تکه‌هایی از کاغذ بود که توسط شخص رأی‌دهنده تهیه می‌شد. پس از مدتی، این تعرفه‌ها توسط کاندیداها و یا گروه‌های سیاسی چاپ شده و در هنگام انتخابات در اختیار رأی‌دهندگان قرار گرفت.

نمونه‌ای از یک تعرفه کاغذی در شکل ۲-۱ دیده می‌شود که توسط کاندیدای[1] انتخابات کنگره آمریکا در سال ۱۸۳۹ به چاپ رسیده است. گوشه‌های پاره کاغذ حاکی از آن است که این تعرفه ممکن است به‌عنوان یک آگهی در روزنامه چاپ شده باشد.



شکل ۲-۱ تعرفه کاغذی مربوط به سال ۱۸۳۹

این نوع تعرفه‌های رأی‌گیری انتظارات رأی‌دهندگان را برآورده نمی‌کرد. از جمله اشکالات این تعرفه‌ها، عدم محرمانگی رأی‌دهنده، مخفی نبودن آرا و امکان رأی‌دهی چندباره رأی‌دهندگان بود.

یکی از روش‌های حفظ محرمانگی در انتخابات، استفاده از صندوق آرا بود، اما باوجود این، رأی‌دهنده می‌توانست به‌جای یک رأی، یک مشت رأی در صندوق بریزد و حتی کارکنان حوزه‌ها نیز می‌توانستند آرایی را به صندوق اضافه کنند. در این خصوص هیچ‌گونه سازوکار کنترلی وجود نداشت.

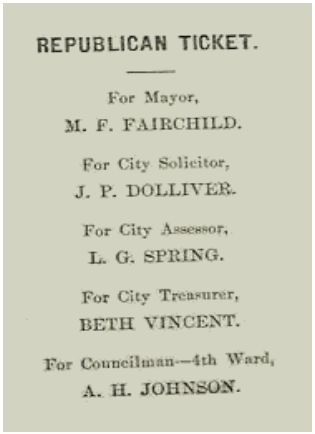
---

1. Francis Gehon

از اشکالات دیگر این سازوکار آن بود که رأی‌دهندگان می‌توانستند با درج علائم خاص در روی برگه‌ها کاری کنند که آرایشان در هنگام شمارش کاملاً مشخص باشد. حتی در صورت عدم شمارش این آرا طبق قانون، رأی‌دهنده می‌توانست با استفاده از کاغذهای خاص و یا به‌کارگیری شکل نوشتاری خاص، رأی خود را برای ناظران احزاب مشخص نماید. به همین دلیل احزاب سیاسی به‌سرعت شروع به چاپ اسامی کاندیداهای خود بر روی کاغذهای خاص نمودند، به‌طوری‌که تمام رأی‌دهندگانی که از این تعرفه‌ها استفاده می‌کردند، به‌راحتی قابل شناسایی بودند.

علی‌رغم تمامی مشکلات، رأی‌گیری با استفاده از این نوع تعرفه‌های کاغذی تا اواخر قرن نوزدهم رواج داشت. در اواسط قرن نوزدهم چاپ تعرفه در بین احزاب سیاسی متداول شد. این تعرفه‌ها به نام «بلیت حزب»[1] نامیده می‌شدند. علت به‌کارگیری واژه بلیت، به‌دلیل شباهت این تعرفه‌ها به بلیت‌های قطار بود.

در شکل ۳-۱ نمونه‌ای از این تعرفه‌ها که به‌وسیله حزب جمهوری‌خواه چاپ شده دیده می‌شود. در این دوره رأی‌دهندگان می‌توانستند از کاغذهای خود برای نوشتن رأی استفاده کنند اما احزاب سیاسی آنها را به استفاده از این تعرفه‌های چاپی تشویق می‌کردند.


REPUBLICAN TICKET.

For Mayor,
M. F. FAIRCHILD.

For City Solicitor,
J. P. DOLLIVER.

For City Assessor,
L. G. SPRING.

For City Treasurer,
BETH VINCENT.

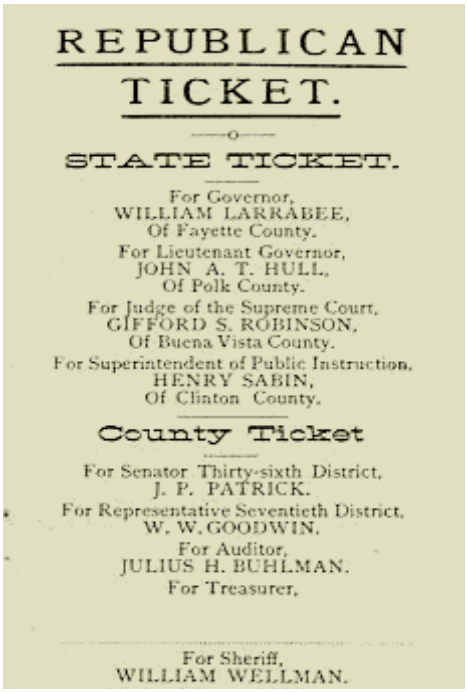
For Councilman—4th Ward,
A. H. JOHNSON.

شکل ۳-۱ تعرفه انتخاباتی در شهر آیووا در سال ۱۸۸۰

1. Party Ticket

اگر رأی‌دهنده می‌خواست به افرادی از سایر احزاب رأی دهد، می‌توانست اسامی موجود در روی تعرفه را خط زده و اسامی مورد نظر خود را بنویسد. برای رفع این اشکال، در دهه ۱۸۸۰، احزاب سیاسی تعرفه‌های خود را به‌صورت بسیار باریک چاپ کردند، تا کسانی که اسامی کاندیداها را خط می‌زنند، هیچ فضای خالی برای نوشتن نام کاندیدای دیگر نداشته باشند. شکل ۴-۱ یک تعرفه با این چارچوب را نشان می‌دهد.

با مقایسه این تعرفه با تعرفه شکل ۳-۱ درمی‌یابیم که فاصله بین خطوط حذف شده است. ویژگی جالب تعرفه اخیر صفحه‌بندی آن می‌باشد. نوشته‌های داخل تعرفه به‌صورت بسیار ریز چاپ شده است؛ زیرا ازنظر احزاب مهم این بود که مردم به احزاب رأی دهند و نه به کاندیدای خاص. بنابراین، نام احزاب به‌راحتی در روی تعرفه‌ها قابل مشاهده و انتخاب بود.



REPUBLICAN
TICKET.

STATE TICKET.

For Governor,
WILLIAM LARRABEE,
Of Fayette County.
For Lieutenant Governor,
JOHN A. T. HULL,
Of Polk County.
For Judge of the Supreme Court,
GIFFORD S. ROBINSON,
Of Buena Vista County.
For Superintendent of Public Instruction,
HENRY SABIN,
Of Clinton County.

County Ticket

For Senator Thirty-sixth District,
J. P. PATRICK.
For Representative Seventieth District,
W. W. GOODWIN.
For Auditor,
JULIUS H. BUHLMAN.
For Treasurer,

For Sheriff,
WILLIAM WELLMAN.

شکل ۴-۱ تعرفه انتخاباتی آیووا در سال ۱۸۸۸

به‌دلیل اینکه احزاب از تعرفه‌های مختلف با اشکال و رنگ‌های مختلف استفاده می‌کردند، نیازی به شمارش آرای تک‌تک کاندیداها در روی تعرفه‌ها نبود، بلکه در اولین مرحله از شمارش آرا، تعرفه‌ها براساس شکل و اندازه‌شان جدا شده و سپس تعرفه‌های متحدالشکل شمارش می‌گردید. البته در حین شمارش، تعداد و اسامی کاندیداهایی که نامشان در روی تعرفه خط خورده بود نیز یادداشت می‌شد. در مرحله آخر افرادی که نامشان در فهرست کاندیداهای احزاب نبوده اما به‌صورت دست‌نویس روی تعرفه‌ها نوشته شده بود، شمارش می‌شد.

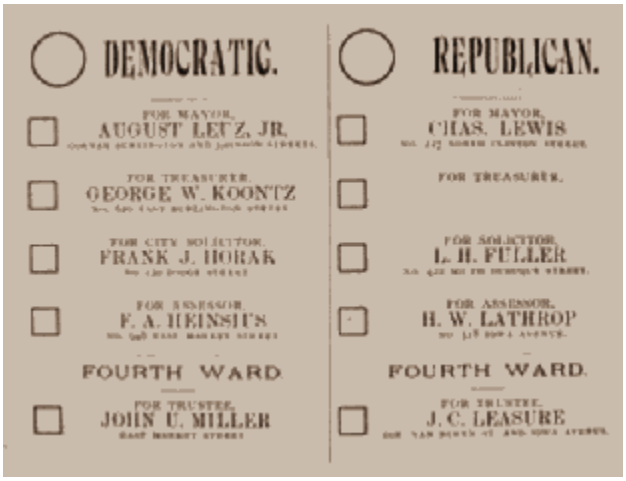
تمامی تعرفه‌ها روی کاغذهای ارزان‌قیمت مثل کاغذهای کاهی چاپ می‌شد، اما بسیاری از احزاب تعرفه‌هایشان را روی کاغذهای خاص و رنگی چاپ می‌کردند تا ناظران احزاب در حوزه‌ها بتوانند به‌راحتی تشخیص دهند که هر فرد به چه حزبی رأی داده است. صندوق‌های رأی نیز به‌صورت شفاف ساخته می‌شد تا رأی‌دهنده نتواند رنگ تعرفه را مخفی نگه دارد.

۱-۱-۲-۱ تعرفه‌های کاغذی استرالیایی

یکی از مهم‌ترین ابداعات در فناوری انتخابات مربوط به شهر ویکتوریا در کشور استرالیاست. در سال ۱۸۵۸ انتخاباتی در آن شهر برگزار شد که در آن از تعرفه‌های کاغذی استانداردی که حاوی لیست اسامی تمامی کاندیداها بود، استفاده گردید. این تعرفه‌ها با هزینه دولت چاپ شده و در حوزه‌های انتخاباتی در اختیار رأی‌دهندگان قرار گرفت. این تعرفه‌ها به نام تعرفه‌های استرالیایی مشهور است.

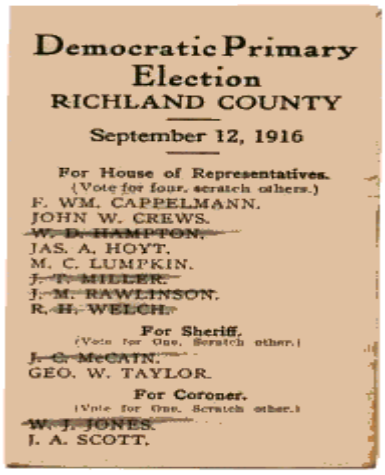
استفاده از این فناوری، مستلزم صرف هزینه دولت برای چاپ، نگهداری و توزیع آن در بین حوزه‌های انتخاباتی بود. در ایالات متحده آمریکا این تعرفه‌ها اولین‌بار در سال ۱۸۸۸ در شهرهای نیویورک و ماساچوست مورد استفاده قرار گرفت. نمونه‌ای از این تعرفه‌ها در شکل ۵-۱ نشان داده شده است:

در این روش رأی‌دهنده می‌توانست با درج علامت X در دایره بالا در کنار نام حزب، تمامی کاندیداهای حزب را انتخاب نموده و یا در صورت انتخاب بعضی از کاندیداها، تنها جلوی اسم آنها علامت X را بگذارد.



شکل ۵-۱ تعرفه استرالیایی مربوط به انتخابات شهر آیووا در سال ۱۸۹۳

شکل ۶-۱ نوع دیگری از تعرفه‌های استرالیایی را که در سال ۱۹۱۶ به‌کار گرفته شد نشان می‌دهد: در این تعرفه‌ها، رأی‌دهنده به استثنای کاندیداهای مورد نظر خود، روی بقیه اسامی خط می‌کشید.



شکل ۶-۱ تعرفه انتخابات کارولینای جنوبی در سال ۱۹۱۶

معمولاً سیاست‌مداران فاسد، پس از ارائه روش‌های نوین رأی‌گیری، به‌سرعت درصدد یافتن نقاط ضعف احتمالی و رسوخ در سیستم و سوءاستفاده از آن می‌گردند. البته مدیریت صحیح این‌گونه تعرفه‌ها مانع رأی‌دهی مجدد افراد و یا ریختن آرای قلابی توسط مسئولان انتخابات به صندوق‌ها می‌گردید.

بزرگ‌ترین ضعف این تعرفه‌ها در نحوه شمارش آنها (آرا) بود. ازطرف دیگر، پذیرش این آرا منوط به تفسیرهای ذهنی علائم درج شده در روی تعرفه بود. بنابراین، اگر سیاست‌مداران فاسد در حین ریختن آرا به صندوق نمی‌توانستند کنترلی بر روی آن داشته باشند، هنوز می‌توانستند در هنگام شمارش آرا نظر خود را تحمیل نمایند.

برای رفع این اشکال، هیئت نظارتی مرکب از احزاب سیاسی مختلف انتخاب می‌شدند تا در هنگام شمارش آرا بر عملکرد یکدیگر نظارت و کنترل داشته باشند، اما باوجود تمامی اقدامات احتیاطی، باز هم دست‌اندرکاران انتخابات قادر به دستکاری ماهرانه در آرا بودند.

در مراحل بعد، استانداردهای خاصی برای علامت‌گذاری در داخل خانه‌ها تعریف شد، به‌طوری‌که رأی‌دهندگان تنها مجاز به استفاده از علائم X و ✓ بودند. البته محل تقاطع علامت X و یا گوشه‌های علامت ✓ باید دقیقاً در داخل خانه قرار می‌گرفت. این استاندارد از تقلب‌های زیادی جلوگیری نمود، اما اشکالاتی را نیز به‌دنبال داشت، از جمله اینکه علامت ✓ با رأس گرد و یا علائم X و ✓ که بخشی از آنها در خارج از خانه قرار می‌گرفت مجاز شناخته نشده و در نتیجه آرای مربوط به آنها شمارش نمی‌گردید.

مشکل این نوع تعرفه‌ها تا حدودی با بازشماری مجدد آرا قابل رفع بود. به این نحو که هیئت بررسی آرای صندوق، آرای تأیید شده و آرایی را که به‌دلیل استفاده از علائم نامناسب باطل اعلام شده بودند، مجدداً شمارش می‌کردند.

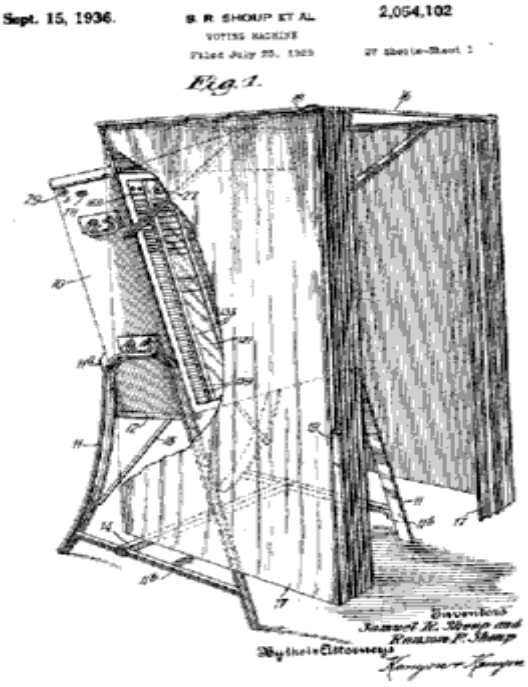
تعرفه‌های کاغذی استرالیایی در بسیاری از انتخابات مورد استفاده قرار گرفته و از استاندارد بالایی نیز برخوردار بوده است. اما در یک انتخابات عمومی که ممکن است نام بیش از ۵۰ کاندیدا در یک تعرفه ذکر گردد، شمارش آرا به این طریق بسیار کند و پرهزینه خواهد بود.

۳-۱ ماشین‌های رأی‌گیری اهرمی[1]

اولین نمونه از فرایندهای رأی‌گیری الکترونیکی مربوط به استفاده از ماشین‌های اهرمی است که توسط توماس ادیسون اختراع شد و اولین‌بار در سال ۱۸۹۲ مورد استفاده قرار گرفت. این ماشین‌ها به‌منظور جلوگیری از تقلب رأی‌دهندگان، حفظ سادگی فرایند رأی‌دهی و محرمانگی رأی‌دهنده طراحی گردید. شکل ۷-۱ نمونه اولیه این ماشین‌ها را نشان می‌دهد که شامل یک اتاقک است.

این ماشین‌ها از یک طرح جدولی استفاده می‌کردند، به‌نحوی‌که اهرمی که در محل تقاطع سطر و ستون خاص قرار می‌گرفت، رأی مربوط به کاندیدای خاص از حزب خاصی را ثبت می‌کرد. در این ماشین‌ها علاوه بر حفظ محرمانگی رأی‌دهنده، امکان رأی‌دهی چندباره افراد نیز وجود نداشت.

در این ماشین‌ها زمانی که رأی‌دهنده اهرم مربوط به کاندیدای مربوط به حزب خاصی را می‌کشید، یک واحد به شمارنده‌ای که جمع آرای مربوط به آن کاندیدا را نگهداری می‌کرد، اضافه می‌شد. پس از خاتمه رأی‌دهی و کنار زدن پرده، اهرم به‌صورت اتوماتیک، به حالت اولیه خود برمی‌گشت، به‌طوری‌که با ورود رأی‌دهنده بعدی به اتاقک، هیچ‌گونه اثری از رأی قبلی باقی نمی‌ماند.



شکل ۷-۱ تصویری از ماشین رأی‌گیری اهرمی

1. Lever Voting Machine

متأسفانه سازوکار این ماشین‌ها طوری بود که نمی‌توانست آرای رأی‌دهندگان را حفظ نماید، بلکه تنها تعداد آرای مربوط به هر کاندیدا توسط شمارنده‌ای که در پشت دستگاه قرار داشت ثبت می‌گردید. درواقع این ماشین، عملکردی مشابه کیلومترشمار اتومبیل داشت.

در این سیستم‌ها نه تنها تکنیسین‌های پشتیبان دستگاه می‌توانستند آنها را دستکاری نمایند، بلکه دستگاه دارای قطعات متحرک بی‌شماری بود که می‌توانست در هر لحظه به‌دلیل خرابی، نتایج نامطلوبی را به‌بار آورد. ماشین‌های رأی‌گیری اهرمی تا اواسط قرن بیستم به‌طور گسترده‌ای مورد استفاده قرار می‌گرفت.

۴-۱ کارت‌های پانچ برای رأی‌گیری[۱]

کارت‌های پانچ در سال ۱۸۸۶ توسط هرمن هالری[۲] اختراع شد و اولین‌بار برای استخراج جداول آماری توسط انجمن سلامتی بالتی‌مور و پس از آن در سرشماری سال ۱۸۹۰ مورد استفاده قرار گرفت.

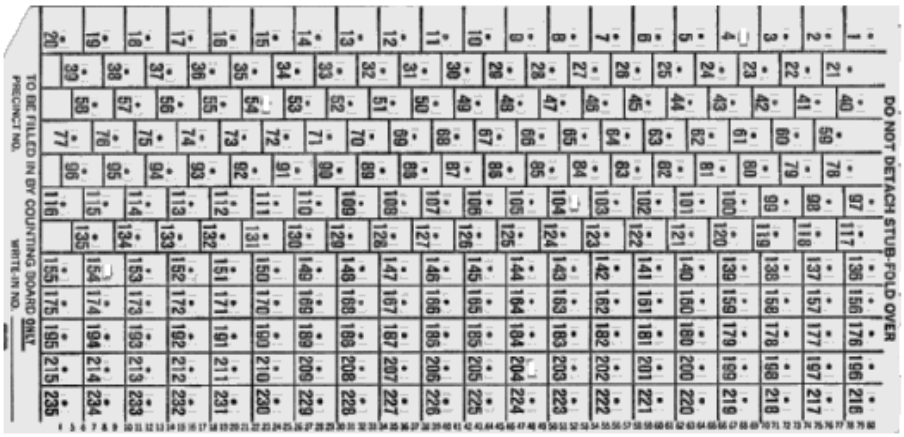
در این سیستم‌ها، رأی‌دهندگان گزینه انتخابی خود را به‌وسیله سوراخ کردن محل‌های خاص روی کارت انتخاب کرده و سپس کارت پانچ شده را به صندوق رأی می‌انداختند. پس از پایان رأی‌گیری، کارت‌ها توسط شمارشگر کامپیوتری شمارش می‌شد. در سال‌های بعد شرکت آی‌بی‌ام کارت‌هایی را به نام «پورت - ای- پانچ»[۳] طراحی نمود.

در اوایل دهه ۱۹۶۰ دو پروفسور از دپارتمان علوم سیاسی دانشگاه برکلی کالیفرنیا کارت‌های پانچ را برای انتخابات پیشنهاد کرده و به کمک یک مهندس از دپارتمان مهندسی مکانیک با اعمال اصلاحاتی در کارت‌های «پورت ـ ای ـ پانچ»، کارت‌های «وتوماتیک»[۴] را طراحی نمودند. کارت «وتوماتیک» که در شکل ۸-۱ نشان داده شده دارای ۲۳۵ محل رأی‌دهی است.

---

۱. Punched Card: نوعی وسیله ورودی رایانه است که امروزه از رده خارج شده است. این کارت از کاغذ ساخته می‌شد تا اطلاعات بیتی به‌صورت عمودی و به شکل سوراخ‌های ایجاد شده در کاغذ ذخیره شود.

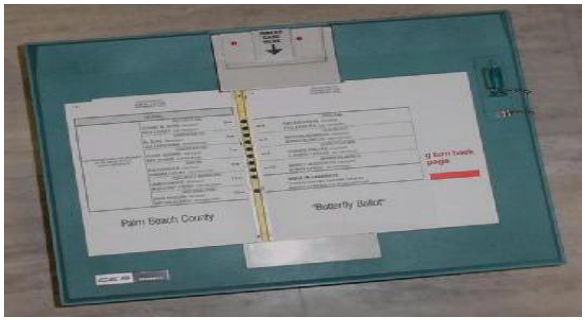
2. Herman Hollerith
3. Port-a-punch
4. Votomatic



شکل ۸-۱ تعرفه رأی «وتوماتیک» بدون قسمت انتهایی (تەبرگ)

در این شیوه، اسامی کاندیداها در روی تعرفه‌ها چاپ نمی‌شد، اما به‌صورت برچسب‌هایی روی ماشین‌های رأی‌گیری «وتوماتیک» نصب شده و یا به‌صورت کتابچه در اختیار رأی‌دهندگان قرار می‌گرفت و هر شماره در روی کارت متناظر با نام یک کاندیدا بود.

ماشین «وتوماتیک» که در شکل ۹-۱ نشان داده شده به‌صورت عمودی بر روی یک قاب در اتاقکی نصب می‌گردید. در هنگام رأی‌دهی، کارت توسط رأی‌دهنده در محل خاصی از ماشین (قسمت بالا) قرار گرفته و به‌وسیله سوزن مخصوصی (سمت راست شکل) سوراخ می‌گردید.



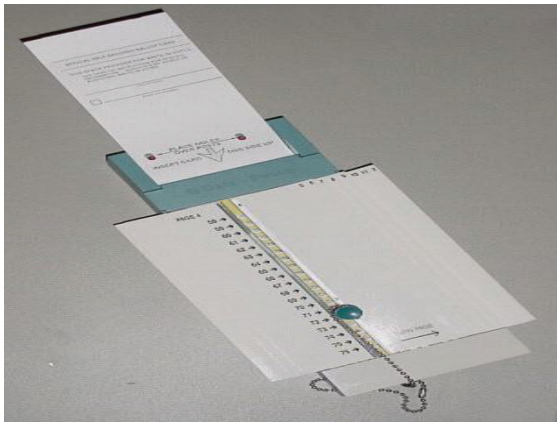
شکل ۹-۱ ماشین رأی‌گیری «وتوماتیک»

تعرفه استفاده شده در شکل ۹-۱ یک مدل دوصفحه‌ای معروف به تعرفه پروانه‌ای[1] است که در انتخابات عمومی سال ۲۰۰۰ در فلوریدا مورد استفاده قرار گرفت.

مدل نشان داده شده در شکل ۱۰-۱ نوع دیگری از ماشین‌های «وتوماتیک» می‌باشد که از کارت‌پانچ استفاده می‌کند.[2] این مدل به‌جای نصب در اتاقک رأی‌گیری، در روی میز قرار می‌گیرد. ماشین نشان داده شده در شکل، دارای ۲۲۸ محل برای انتخاب رأی است که این محل‌ها در هنگام انتخابات به کمک سوزن مشخص (در شکل) توسط کاربر سوراخ می‌گردید. در شکل، سوزن در موقعیت ۷۲ قرار گرفته است.

در قسمت انتهایی تعرفه، ته‌برگی وجود داشت که به‌صورت سریال شماره‌گذاری شده بود. در زمان دادن تعرفه به رأی‌دهنده، شماره روی ته‌برگ یادداشت می‌گردید تا پس از پانچ شدن تعرفه و تحویل آن به مسئول مربوطه، اطمینان حاصل شود که این تعرفه همان تعرفه واگذارشده به رأی‌دهنده بوده است. به‌این‌ترتیب، امکان فروش و تقلب در آرا از بین می‌رفت.

یکی از مشکلات این تعرفه‌ها آن بود که در برخی موارد به‌خصوص هنگام خواندن کارت‌ها توسط دستگاه کارت‌خوان، به‌طور اتفاقی یک رأی به آرای کاندیداها اضافه می‌شد.

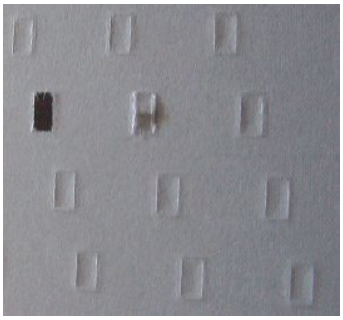


شکل ۱۰-۱ ماشین رأی گیری

1. Butterfly Ballot
2. Data Punch Voting Machine

به‌دنبال مسایل پیش آمده در انتخابات سال ۲۰۰۰ که در آن از فناوری رأی‌گیری «وتوماتیک» استفاده شده بود، انتقادات بسیار گسترده‌ای مطرح گردید. یکی از مهم‌ترین اشکالات، مربوط به نحوه برخورد با کارت‌هایی بود که در چندین خانه آنها علامت پانچ مشاهده می‌گردید. نمونه‌ای از این کارت‌ها در شکل ۱۱-۱ نمایش داده شده است.

در این شکل یک خانه پانچ شده کامل و یک گودی دیده می‌شود. مشکل شمارش آرا در این روش، مشابه مشکل موجود در هنگام شمارش تعرفه‌های استرالیایی بود. با نگاه اجمالی به گودی روی تعرفه نمی‌توان از قصد و نیت رأی‌دهنده آگاه شد.



شکل ۱۱-۱ پشت یک تعرفه «وتوماتیک»

معمولاً این حالت زمانی اتفاق می‌افتاد که رأی‌دهنده پس از انتخاب کاندیدای مورد نظر خود، در هنگام پانچ کردن خانه متناظر با کاندیدا، از تصمیم خود منصرف می‌گردید. این امکان که در هنگام سوراخ کردن خانه مربوطه مانعی در مقابل سوزن قرار گرفته باشد، تقریباً غیرممکن بود.

۵-۱ اسکنرهای نوری[1]

این اسکنرها اولین‌بار در سال ۱۹۶۲ در کالیفرنیا مورد استفاده قرار گرفت. نمونه‌ای از این اسکنرها در شکل ۱۲-۱ نشان داده شده است.

1. Optical Mark Sense Scanner

شکل ۱۲-۱ اسکنر نوری

این دستگاه دارای دو بخش اساسی است. جعبه مخصوص آرا و بخش بالایی دستگاه. جعبه پایینی محفظه مطمئنی برای نگهداری آرای شمارش شده می‌باشد، درحالی‌که در قسمت بالایی، اسکنر و اجزای الکترونیکی قرار دارند. جعبه تعرفه‌ها شامل سه محفظه جداگانه می‌باشد. یک محفظه آرایی را که به‌وسیله ماشین اسکن نشده‌اند نگه می‌دارد. این محفظه در موارد اضطراری و درحالتی که اسکنر کار نمی‌کند به‌کار می‌رود و در حالت عادی بسته است. محفظه دوم برای نگهداری تعرفه‌هایی است که باید توسط مسئولان مورد بازبینی قرار بگیرند و محفظه سوم برای تعرفه‌هایی که نیاز به بازبینی مجدد ندارند به‌کار می‌رود.

در هنگام شمارش آرا، تعرفه‌ها در سینی مخصوص قرار گرفته و سپس به‌صورت اتوماتیک به قسمتی که رأی را می‌خواند رانده شده و در نهایت به سمت خروجی هدایت می‌شوند. در ساختمان اسکنر یک سیستم کامپیوتری کامل وجود دارد.

۱-۶ ماشین‌های رأی‌گیری با ثبت هم‌زمان آرا[1]

این دستگاه شامل یک صفحه نمایش تماسی،[2] یک بسته نرم‌افزاری رأی‌گیری و یک بدنه مطمئن است که مانع از اتصال غیرمجاز صفحه‌کلید (کیبورد) و یا موش‌واره (ماوس) در هنگام استفاده در حوزه‌های انتخاباتی می‌شود. همچنین این دستگاه از طریق یک هاب،[3] به شبکه مرکزی متصل بوده و به‌منظور جلوگیری از قطع احتمالی

---

1. Direct Recording Voting Machines

۲. Touch Screen: صفحه نمایش رایانه‌ای که برای تشخیص محل یک تماس بر روی سطح خود طراحی شده و پس از برقراری تماس با صفحه نمایش، کاربر می‌تواند یک انتخاب داشته باشد یا مکان‌نما را حرکت دهد.

۳. Hub: ابزاری در شبکه و برای اتصال خطوط ارتباطی به سرور مرکزی است. این وسیله، اتصالی عمومی به تمامی دستگاه‌های شبکه به‌وجود می‌آورد.

برق از یک دستگاه برق اضطراری نیز استفاده می‌کند. نمونه‌ای از این دستگاه در شکل ۱-۱۳ مشاهده می‌شود.

پس از پایان انتخابات، آرا از طریق شبکه برای شمارش به حوزه ستادی ارسال می‌شود. امروزه بسیاری از کشورهای دنیا در انتخابات مختلف از این روش استفاده می‌کنند. در فصل سوم به نحوه عملکرد این دستگاه به‌طور کامل اشاره شده است.

شکل ۱-۱۳ ماشین رأی‌گیری به‌کار گرفته شده در کشور برزیل

۱-۷ انتخابات در ایران

در سالیان اخیر اکثر انتخابات عمومی کشورمان از جمله انتخابات ریاست‌جمهوری، انتخابات مجلس شورای اسلامی و انتخابات مجلس خبرگان رهبری به شیوه سنتی برگزار شده است. اگرچه در برخی از موارد شمارش آرا در شهرهای بزرگ به‌صورت الکترونیکی بوده، اما به‌دلیل مشکلات پیش‌آمده، شمارش الکترونیکی تاکنون مورد تأیید کامل شورای نگهبان و ستاد انتخابات کشور قرار نگرفته است.

۱-۷-۱ سوابق اخذ و شمارش آرا

شمارش آرا، در انتخابات ریاست‌جمهوری که تنها نام یک فرد در روی تعرفه درج می‌گردد و یا در انتخابات مجلس شورای اسلامی و مجلس خبرگان در حوزه‌های دارای یک یا دو نامزد کار چندان دشواری نیست و در ساعات اولیه به پایان می‌رسد، اگرچه احتمال تقلب و جعل آرا وجود دارد. اما در حوزه‌هایی مانند تهران بزرگ که می‌بایست حدود ۳۰ نفر نماینده از بین بیش از ۱۰۰۰ کاندیدا انتخاب شوند، شمارش دستی آرا کار بسیار طاقت‌فرسا و مشکلی بوده و گاهی تا چند روز هم به‌طول می‌انجامد. با طولانی شدن زمان شمارش، ضریب خطای انسانی و امکان تقلب در شمارش آرا هم افزایش

می‌یابد. یکی از اشکالات دیگر شمارش دستی آرا این است که در برخی از موارد افراد منتخب برای شمارش آرا ــ به‌دلیل خستگی ــ با نفرات دیگری تعویض می‌شوند که در بعضی از موارد ممکن است این افراد مورد تأیید هیئت‌های اجرایی و نظارتی نباشند.

امکان استفاده از شناسنامه افراد فوت شده، رأی دوباره، انداختن برگ رأی اضافی در صندوق اخذ رأی، عدم ثبت رأی بعضی از کاندیداها در شمارش دستی، تنظیم غلط و یا غیرقانونی صورت‌جلسات و موارد دیگر، از جمله تخلفات انتخاباتی در دوره‌های قبل بوده است.(۳)

به‌منظور افزایش سرعت و دقت در شمارش آرا، در سال ۱۳۷۲ برای انتخابات دوره ششم ریاست‌جمهوری نزدیک به چهارصد دستگاه مارک‌خوان[1] خریداری شد و انتخابات در تهران با استفاده از فرم‌های مخصوص به این روش انجام گرفت. رأی‌دهندگان ملزم بودند که علاوه بر نوشتن نام کاندیدای مورد نظر، شماره کاندیدا را در محل تعبیه شده (به‌صورت پرکردن خانه مربوط به هر عدد) با مداد درج نمایند. اما در عمل این روش با مشکلات زیر مواجه گردید:

۱. برخی از افراد نسبت به درج کد کاندیدا اقدام نکرده بودند که این موضوع باعث کندی در شمارش آرای صندوق‌ها گردید.

۲. به‌علت تعداد محدود دستگاه‌ها، عمل شمارش به کندی انجام شد.

۳. نرم‌افزار تهیه شده دارای اشکالات فراوانی بود و همه احتمالات و خطاها در آن پیش‌بینی نگردیده بود، که این موضوع نیز باعث کندی در شمارش آرای صندوق‌ها شد.

۴. نوع کاغذ، تاخوردگی برگ رأی، پر کردن نامناسب خانه‌های مربوط به اعداد، نوع قلم، کثیف شدن و مرطوب شدن برگ رأی و عوامل بسیار دیگر، از اشکالات این طرح بود که باعث کندی شمارش آرا گردید.

در نهایت، به گفته دست‌اندرکاران و مسئولان وقت وزارت کشور و شورای نگهبان، طرح فوق نه تنها باعث افزایش سرعت و دقت در اخذ و شمارش نگردید، بلکه در بعضی از موارد اثر منفی و کاهنده نیز داشت.

در برخی از دوره‌های انتخابات برای شمارش آرا، از روش داده‌آمایی[2] استفاده شد. در این روش، رأی‌گیری به‌صورت دستی، یعنی نوشتن نام کاندیدا بر روی تعرفه انجام

---

1. Mark Reader
2. Data Entry

می‌گرفت. پس از پایان زمان اخذ آرا، صندوق رأی باز شده و اسامی کاندیداها به‌ترتیب هر برگ رأی، وارد رایانه می‌شد. سپس اطلاعات الکترونیکی با حفظ محرمانگی، از طریق خطوط ارتباطی به ستاد انتخابات ارسال می‌شد تا تجمیع نهایی گردد.

در این روش نیز امنیت اخذ رأی همانند روش دستی است، ولی شمارش آرا نسبت به روش دستی از امنیت بالاتری برخوردار است، ضمن اینکه درصدی خطا به‌عنوان خطای اپراتور نیز وجود دارد.

۲-۷-۱ اهمیت و ضرورت استفاده از فناوری‌های جدید

امروزه نقش و جایگاه فناوری اطلاعات به‌عنوان ابزاری برای طراحی، پیاده‌سازی و اجرای برنامه‌های توسعه از اهمیت خاصی برخوردار است. با گسترش فناوری اطلاعات، امروزه شاهد تأثیر فراوان آن بر بهبود عملکرد سازمان‌ها و دستیابی سریع‌تر به اهداف آنها هستیم.

در دهه‌های گذشته روش‌های متنوعی برای شمارش صحیح و دقیق آرا ابداع و مورد استفاده قرار گرفته است که از آن جمله می‌توان به دستگاه‌های مارک‌خوان و دستگاه‌های تصویربردار[1] اشاره کرد.

در این میان، ضروری است که سازمان‌های درگیر در امر انتخابات با استفاده از مباحث جدید مطرح در زمینه فناوری اطلاعات و تجربیات سایر کشورها، در زمینه الکترونیکی شدن انتخابات گام مؤثر برداشته و به‌منظور صیانت از آرای مردم و جلوگیری از تقلب، اهداف زیر را تعقیب نمایند:

۱. کاهش زمان اجرا و شمارش آرا و اعلان سریع نتایج،

۲. کاهش تقلب و جعل آرا و دستکاری نتایج انتخابات،

۳. جلوگیری از بروز بحران‌ها و تنش‌های منطقه‌ای و قبیله‌ای،

۴. حفظ منزلت و شأن جمهوری اسلامی ایران در استفاده از فناوری اطلاعات و ارتباطات در عرصه انتخابات،

۵. جلوگیری از اتلاف وقت، نیروی انسانی و سرمایه کشور به‌دلیل طولانی شدن فرایند شمارش دستی آرا،

۶. تهیه بانک اطلاعاتی از انتخابات برگزار شده.

---

1. OCR

پی‌نوشت‌ها

1. B. Watt, *Implementing Electronic Voting* 2002, [online]: http://www.lcd.gov.uk/elections/e-voting/pdf/legal-report.pdf
2. Ibid.
۳. *سوابق اخذ و شمارش آراء انتخابات در ایران*، گزارش اداره کل رایانه شورای نگهبان، آذر ۱۳۸۴.

فصل دوم

دولت الکترونیکی و دمکراسی

فناوری اطلاعات مجموعه‌ای از سخت‌افزار، نرم‌افزار و مغزافزار است که گردش و بهره‌برداری از اطلاعات را امکان‌پذیر می‌سازد. گسترش این فناوری و پیدایش شبکه‌های گسترده ارتباطی در دنیا مباحث تازه‌ای را مطرح نموده که از آن جمله می‌توان به کاربرد دمکراتیک این ابزارها و شبکه‌های ارتباطی و نیز شیوه‌های جلوگیری از انحصاری شدن اطلاعات و در نهایت تبعیض اطلاعاتی اشاره کرد. مفهوم رأی‌گیری الکترونیکی، بر شکلی جدید از رفتار دمکراتیک دلالت دارد که حاصل فناوری‌های جدید اطلاعاتی و ارتباطاتی است.

در این فصل ضمن معرفی اجمالی دولت الکترونیکی و دمکراسی الکترونیکی، مزایای به‌کارگیری فناوری‌های نوین اطلاعات و ارتباطات در فعالیت‌های دولتی را مورد بررسی قرار می‌دهیم.

۱-۲ دولت و اشکال آن

در فرهنگ *لالاند* «حکومت» به‌معنای مجموعه ارگان‌هایی است که به‌واسطهٔ آن، حاکم به اعمال اقتدار می‌پردازد. این واژه به‌صورت کلی نمایشگر اجرای اقتدار عمومی توسط حاکم بوده و حاکمیتی به جریان افتاده محسوب می‌شود. لذا تجسم‌بخش موجودیت یک کشور و عامل اجرای حاکمیت موجود در آن است که از آن به‌عنوان رژیم سیاسی نیز یاد می‌شود. رژیم‌های سیاسی براساس تعداد فرمانروایان و نحوهٔ قانون‌گذاری به سه دسته تقسیم می‌شوند:[1]

۱. **یک‌تن‌سالاری (مونوکراسی)**: در این نوع رژیم، قدرت در دست یک نفر بوده و با نهادینه کردن قدرت آن را موروثی می‌کند. نظام‌های پادشاهی و دیکتاتوری از این نوع است.

۲. **چندتن‌سالاری (آریستوکراسی)**: حکومت شمار معدودی که در اقلیت به سر می‌برند، لکن به سبب حوادث مختلف قدرت را به‌دست گرفته‌اند. فئودالیسم که در آن طبقهٔ حاکم زمین‌دارهای جامعه‌اند، از این نوع است.

۳. **مردم‌سالاری (دمکراسی)**: دمکراسی زمانی شکل می‌گیرد که اکثر مردم در ادارهٔ جامعه مؤثر باشند.

ازسوی دیگر، دولت به‌معنای جبهه فرمانروایان شامل هیئت حاکم، نهادهای فرمانروا و متصدیان سیاسی یک کشور در برابر تودهٔ مردم و شهروندان به‌کار می‌رود. این مفهوم بر کلیه کارگزاران و نهادهایی اطلاق می‌شود که بر مردم حکومت می‌کنند. گاهی نیز دولت در معنای لایه سیاسی قوه مجریه یا رده‌های فوقانی نظیر نخست‌وزیر و هیئت وزیران به‌کار برده می‌شود. با توجه به ساختار درونی کشورها، دولت ممکن است دارای شکل تک‌بافت یا چندپارچه باشد. دولت‌های تک‌بافت یا بسیط دارای مرکز واحد عملکرد سیاسی هستند و قدرت سیاسی توسط دولت مرکزی اعمال می‌شود، لیکن کشورهای چندپارچه (مرکب) دارای چند مرکز عملکرد سیاسی بوده و حاکمیت چندگانه‌ای در آنها حکم‌فرماست. اعمال حاکمیت توسط هر نوع رژیم سیاسی شامل مراحل زیر است:[۲]

- تدوین و تصویب قوانین،
- ابلاغ به شهروندان و دولتمردان،
- اجرا،
- نظارت و انتظام.

تدوین و تصویب قوانین می‌تواند توسط مجلس قانون‌گذاری، هیئت حاکم یا توسط آرای عمومی صورت گیرد، اما ابلاغ و اجرا و نظارت به‌عهدهٔ دولتمردان است. نظارت و انتظام، گسترهٔ وسیعی دارد. به‌طور مثال، دعاوی مردم علیه دولتمردان، دعاوی دولتمردان علیه مردم و دعاوی مردم علیه مردم، همگی جزء نظارت و انتظام می‌باشد، چون هر کدام مستلزم نقض قانون مصوبی است. بنابراین، اعمال حکومت شامل ارتباط چندلایه بین طبقات هیئت حاکم با یکدیگر و نیز مردم با طبقه حاکم و بالعکس است.

۲-۲ دولت الکترونیکی

از شروع به‌کارگیری اینترنت در سال ۱۹۹۰ بحث‌های زیادی در مورد نحوه استفاده از فناوری اطلاعات در دولت مطرح گردیده است. بدیهی است که تجربیات به‌دست آمده

در زمینه تجارت الکترونیکی نمی‌تواند به همان شکل در مدیریت دولت به‌کار رود. بنابراین، واژه دولت الکترونیکی به‌عنوان مقوله‌ای جدید در زمینه سیستم‌های اطلاعات دولتی به‌وجود آمد. در اروپا در زمینه دولت الکترونیکی تبلیغات گسترده‌ای آغاز شده است، اما هنوز بسیاری از افراد آن را با فعالیت‌های مدیریتی مبتنی‌بر فناوری اطلاعات و ارتباطات اشتباه می‌گیرند. دولت الکترونیکی ارتباط الکترونیکی دولت و شهروندان به‌خصوص در فرایندهای دمکراتیک مانند انتخابات است.

دولت الکترونیکی را می‌توان این‌گونه تعریف کرد: «دولت الکترونیکی عبارت است از استفاده از فناوری اطلاعات برای پشتیبانی از فعالیت‌های دولتی، ارائه خدمات دولتی و مشارکت شهروندان، که نه تنها شامل مدیریت الکترونیکی فرایندها، بلکه شامل مشارکت الکترونیکی شهروندان نیز می‌باشد».

دولت الکترونیکی به اشکال مختلف دیگر نیز تعریف می‌شود:[۳]

- گروهی دولت الکترونیکی را معادل کسب‌وکار الکترونیکی در یک کشور درنظر می‌گیرند. این نگرش از آنجا ناشی شده که دولت الکترونیکی و کسب‌وکار الکترونیکی از زیرساختی واحد استفاده می‌کنند. با این وجود، تفاوت‌های واضحی بین مدل‌های بازار در بخش‌های عمومی و خصوصی وجود دارد که باید دولت الکترونیکی را حوزهٔ جداگانه‌ای درنظر گرفت.
- دولت الکترونیکی سازماندهی مجدد خدمات شهروندی به کمک فناوری اطلاعات است.
- دولت الکترونیکی کاربرد فناوری اطلاعات و ارتباطات برای ارتقای کارایی، اثربخشی، شفافیت تبادلات و تعاملات اطلاعاتی بین دولت‌ها و همچنین درون دولت شامل سطوح مختلف ادارات دولتی اعم از محلی، شهری یا در سطح کشور، شهروندان و بنگاه‌های تجاری است که موجب ارتقای توانمندی شهروندان از طریق دسترسی و بهره‌گیری از اطلاعات می‌شود.
- از منظر کسب‌وکار، دولت الکترونیکی به‌صورت کاربرد فناوری اطلاعات و ارتباطات برای بهبود، انتقال و تعریف مجدد منابع و مبادله اطلاعات بین عاملان، نظیر شرکت‌ها، دولت و مشتریان تعریف می‌شود.
- دولت الکترونیکی صورتی از تجارت الکترونیکی است که توسط بخش دولتی مورد استفاده قرار می‌گیرد. دولت الکترونیکی به خدمات‌دهی و تبادل اطلاعات به‌صورت

درون‌سازمانی یا برون‌سازمانی اطلاق می‌شود که از طریق بهره‌گیری از ابزارهای مبتنی‌بر فناوری اطلاعات صورت می‌گیرد و به‌صورت ارتباط و تأثیر متقابل میان عناصر زیر است:

- دولت و شهروندان،
- دولت و بنگاه‌های کاری،
- دولت و کارمندان،
- دولت و دولت،
- دولت و مؤسسات غیرانتفاعی.

۱-۲-۲ اهداف و مزایای دولت الکترونیکی

تعیین اهداف مورد انتظار از دولت الکترونیکی اهمیت ویژه‌ای دارد؛ چراکه با شناسایی آن‌ها، می‌توان مسیر اجرای دولت الکترونیکی را تعیین نمود. شکی نیست که دولت‌های مختلف، اهداف متفاوتی را دنبال می‌کنند و برخی از این اهداف مشترک‌اند. به‌عنوان مثال، سرعت در اجرای امور، هدف همه دولت‌هاست. برخی دیگر از اهداف یا مزایایی که می‌توان از تحقق دولت الکترونیکی انتظار داشت، عبارت‌اند از:[۴]

۱. **کاهش تشریفات دست‌وپاگیر اداری**: برخورداری از دولت الکترونیکی موجب کاهش بوروکراسی و تشریفات دست‌وپاگیر مرسوم در سازمان‌های دولتی می‌شود.

۲. **تسریع در ارائه خدمات با استفاده از روش‌های الکترونیکی**: در دولت الکترونیکی، خدماتی که دولت از طریق کارگزاران خود به مشتریانش عرضه می‌کند، الکترونیکی است. در این دولت، دیگر مشتری ناچار نیست بسیاری از امور خود را در زمانی طولانی و با خستگی و سردرگمی انجام دهد. او می‌تواند توسط امکاناتی که دولت فراهم آورده است خدمات مورد نیاز خود را به‌صورت الکترونیکی در کوتاه‌ترین زمان ممکن و با کیفیت مناسب به‌صورت شبانه‌روزی دریافت نماید.

۳. **اطلاع‌رسانی الکترونیکی**: یکی از مهم‌ترین انتظارات شهروندان یک جامعه، دریافت به‌موقع اطلاعات مورد نیاز آنان است. این انتظار در دولت الکترونیکی با به‌کارگیری ابزارها و اطلاع‌رسانی به‌موقع و شفاف درباره عملکرد دولت، برنامه‌ها، رویدادها و سایر موارد دیگر برآورده می‌شود.

۴. **تأمین رضایت شهروندان**: ارائه خدمات به‌موقع و کیفی به شهروندان و سهیم‌کردن آنان در تصمیم‌گیری‌های عمومی موجب افزایش رضایت آنان می‌گردد.

۵. **افزایش اقتدار ملی**: دستیابی سریع به اطلاعات و بهره‌مندی مناسب از آن، همچنین اطلاع‌رسانی صحیح و شفاف و تقویت نقش ملت در تصمیم‌گیری‌ها موجبات افزایش اقتدار ملی را فراهم می‌آورد.

۶. **افزایش بهره‌وری**: ارائه خدمات مؤثر و کارآمد، کارایی بیشتر سازمان‌های اداری و کاهش هزینه‌ها و تلفات موجب افزایش بهره‌وری ملی می‌شود که برخی از مصادیق آن عبارت‌اند از:

ـ دولت‌ها می‌توانند با عرضه اطلاعات مورد نیاز به‌صورت الکترونیکی، در مناقصه‌ها و مزایده‌ها، هزینه‌های خود را کاهش دهند.

ـ اتوماسیون فعالیت‌ها، موجب کاهش هزینه نیروی انسانی و کوچک‌سازی دولت می‌گردد.

ـ با تحقق دولت الکترونیکی، هزینه اطلاع‌رسانی و بایگانی کاهش می‌یابد.

۷. **توسعه مشارکت مردمی**: تدارک شرایط مشارکت مستقیم همه شهروندان در فرایندهای تصمیم‌گیری و سیاست‌گذاری توسط دولت الکترونیکی از جمله اهداف تحقق آن به شمار می‌رود.

۸. **شفافیت امور و کاهش رشوه‌خواری**: دسترسی سریع به اطلاعات شفاف و امکان نظارت و ارزیابی دقیق، از فساد اداری و رشوه‌خواری می‌کاهد و این موضوع می‌تواند به‌عنوان یکی دیگر از اهداف تحقق دولت الکترونیکی محسوب شود.

۹. **تصمیم‌گیری سریع مبتنی‌بر اطلاعات**: در فرایند حل مسئله، اتخاذ تصمیم صحیح مبتنی‌بر نود درصد اطلاعات و ده درصد مهارت‌های فردی، تحقق دولت الکترونیکی و جمع‌آوری و پردازش اطلاعات در زمان کوتاه را میسر می‌سازد.

۱۰. **اثرات مثبت زیست‌محیطی**: با تبدیل نسخه کاغذی پرونده‌ها، مدارک، کتب و غیره به نسخه الکترونیکی، کاغذ مصرفی کاهش یافته در نتیجه جنگل‌ها و منابع طبیعی کمتر آسیب می‌بینند. از طرفی، با کاهش حمل‌ونقل بین شهری، برای دستیابی به اطلاعات و خدمات دولتی سوخت کمتری مصرف شده و خطرات زیست‌محیطی کاهش می‌یابد.

۱۱. **کارآفرینی**: برای تحقق دولت الکترونیکی نیاز به توسعه زیرساخت‌هایی می‌باشد که ایجاد، بهره‌برداری و نگهداری از آنها نیازمند نیروی کار فناوری اطلاعات است.

۲-۲-۲ خدمات دولت الکترونیکی

بعضی از خدماتی که دولت الکترونیک در اختیار قرار می‌دهد عبارت‌اند از:[۵]

- خدمات پرداخت برخط نظیر پرداخت مالیات، عوارض و صورت‌حساب آب، برق، گاز و ...،
- خدمات یکبار مصرف دولتی،
- خدمات مشاوره از راه دور،
- خدمات واسطه‌گری (دلالی) الکترونیکی،
- فرم‌های الکترونیکی،
- نظرخواهی برخط،
- خدمات کاریابی الکترونیکی،
- ارائه داده‌های آماری برخط نظیر اطلاعات ترافیک،
- خدمات بازار و اجتماع الکترونیکی،
- خدمات پلیس الکترونیکی،
- خدمات سیاست‌گذاری الکترونیکی،
- رأی‌گیری الکترونیکی،
- خدمات ثبت الکترونیکی نظیر ثبت شرکت، ازدواج، طلاق، تولد و مرگ.

۲-۲-۳ قابلیت‌های دولت الکترونیکی

قابلیت‌هایی که انتقال از مدیریت عمومی و سنتی به مدیریت الکترونیکی ارائه می‌کند هنوز ناشناخته است، اما با این حال می‌توان به موارد زیر اشاره کرد:[۶]

- شکل‌های جدید تحویل اطلاعات،
- روش‌های جدید دسترسی شهروندان به اطلاعات،
- روش‌های جدید تعامل و مبادلهٔ اطلاعات با شهروندان،
- شکل‌های جدید ایجاد انجمن‌ها به‌صورت محلی و عمومی از طریق روش‌های برخط،
- شکل‌های جدید دخالت مردم در فرایند قانون‌گذاری و سیاست‌گذاری،
- راه‌های جدید توسعهٔ مهارت‌ها برای شرکت فعال مردم در دولت الکترونیک،

- شکل‌های جدید وکالت،
- روش‌های جدید ارائه اطلاعات برای دولت،
- روش‌های جدید کاهش شکاف دیجیتالی با توسعه خدمات همگانی در دسترسی به اطلاعات،
- روش‌های جدید رهبری.

برای تحقق موفقیت‌آمیز دولت الکترونیکی باید فرایندهای عملیاتی دولت تغییر کند و وظایف جدیدی برای کارکنان دولت، صاحبان مشاغل و شهروندان تعریف شود. بدیهی است که تمامی طرف‌های درگیر و دست‌اندرکاران باید با فناوری‌های نوین آشنا شده و مهارت‌های جدید بیاموزند.

۳-۲ دمکراسی الکترونیکی

توسعه سریع فناوری‌های اطلاعات و ارتباطات بر تمامی جنبه‌های زندگی اجتماعی تأثیرگذار است. این تأثیرات نه تنها در بخش‌های آموزش، اقتصاد و رسانه‌ها، بلکه در بعد سیاسی نیز مشهود می‌باشد. گستره تأثیرگذاری فناوری‌های اطلاعات و ارتباطات بر تغییرات اجتماعی آن‌چنان فراوان بوده که از آن می‌توان به عنوان «انقلاب» یاد کرد. اما در ابتدای قرن بیست‌ویکم نمی‌توان با اطمینان در مورد تأثیر این فناوری بر شکل نهایی جوامع اظهارنظر نمود. در دهه گذشته متخصصان علوم اجتماعی تحقیقات گسترده‌ای را در زمینه انقلاب اطلاعاتی انجام داده‌اند، به‌طوری‌که همگی آنها بر تأثیر فناوری‌های جدید بر ساختار و سازوکارهای اصلی زندگی اجتماعی از جمله الگوهای رفتاری افراد در اجتماع اذعان دارند.

از دیدگاه متخصصان علوم سیاسی، مهم‌ترین بحث مطرح در مورد انقلاب اطلاعاتی به وضعیت دمکراسی مدرن برمی‌گردد. آیا استفاده از اینترنت به توانایی‌های شهروندان خواهد افزود؟ آیا تعامل مردم و دولتمردان را افزایش خواهد داد؟ آیا فناوری‌های اطلاعات و ارتباطات می‌تواند بر بحران مشارکت سیاسی غلبه نماید؟ سؤالاتی از این قبیل، مبنای مباحثات و تحلیل پیامدهای سیاسی انقلاب اطلاعات است. تمامی این سؤالات را می‌توان در یک سؤال کلی خلاصه کرد: «فناوری‌های نوین اطلاعات و ارتباطات تا چه حد قادر است ساختار دمکراسی را تغییر دهد؟» به‌عبارت‌دیگر، حاصل انقلاب اطلاعاتی چه نوعی از دمکراسی خواهد بود؟

مشکل اساسی که در تحلیل انقلاب اطلاعاتی از بعد سیاسی وجود دارد، عدم همخوانی و تطابق بین نتایج حاصل از بررسی‌های انجام شده مختلف است. از طرفی، دیدگاه نظری و ایدئولوژیکی عصر جدید دمکراتیک وجود دارد و از طرف دیگر، مطالعات تجربی در دهه اخیر نشان می‌دهد که برخی از کشورها در استفاده از این پدیده نو با مشکلات عدیده‌ای مواجه بوده‌اند.

۱-۳-۲ واژه‌های مرتبط با دمکراسی

متخصصان علوم سیاسی در جستجوی واژه‌ای هستند که بتوانند از طریق آن پیامدهای انقلاب اطلاعات در حوزه دمکراسی را توضیح دهند. واژه «تله‌دمکراسی یا دمکراسی از راه دور» یکی از قدیمی‌ترین واژه‌هایی است که در دهه ۱۹۸۰ مورد استفاده قرار گرفت و هنوز طرفداران بسیاری دارد. تله‌دمکراسی، استفاده از فناوری ارتباطات برای سهولت در تبادل اطلاعات بین شهروندان و دولتمردان و نیز بیان عقاید و نظرات سیاسی آنهاست.(۷)

نوع دیگر دمکراسی به نام دمکراسی سایبر نامیده می‌شود. طبق نظریه تیلور، در این نوع دمکراسی از شبکه‌های رایانه‌ای و اینترنت برای مباحثات مردمی، تبادل نظرات و مشارکت در امور سیاسی استفاده می‌شود.(۸)

در ادبیات علوم سیاسی واژه‌ای به نام دمکراسی مجازی و دمکراسی دیجیتال نیز وجود دارد که به تأثیرات ناشی از استفاده از فناوری‌های نوین اطلاعات و ارتباطات در حوزه دمکراسی اشاره دارد. این واژه در عصر انقلاب اطلاعاتی به نام دمکراسی الکترونیکی نامیده می‌شود.(۹) تعاریف زیادی برای دمکراسی الکترونیکی وجود دارد، اما آنچه که مسلم است استفاده از فناوری‌های اطلاعات و ارتباطات سبب تقویت مشارکت مردمی و افزایش نقش مباحثات و همه‌پرسی‌های برخط در تصمیم‌گیری‌ها می‌گردد.

۲-۳-۲ تعریف دمکراسی الکترونیکی

با برخورداری از دولت الکترونیکی می‌توان دمکراسی یا مردم‌سالاری الکترونیکی را توسعه داد. مردم‌سالاری الکترونیکی به‌معنای به‌کارگیری فناوری اطلاعات برای پشتیبانی و توسعه مردم‌سالاری است. ابعاد موجود در مردم‌سالاری الکترونیکی عبارت‌اند از:

- **اطلاعات**: وجود اطلاع‌رسانی شفاف ازسوی حکومت به مردم،
- **ارتباطات**: تعامل دوطرفه بین حکومت و مردم،
- **مشارکت**: ایجاد فرصت برای توسعه مشارکت‌های مردمی،
- **آزادی**: شامل آزادی بیان، رسانه‌های آزاد، آزادی اجتماعات و انتخابات آزاد،
- **انتخابات و رأی‌گیری الکترونیکی**: که یکی از نتایج مردم‌سالاری الکترونیکی است.

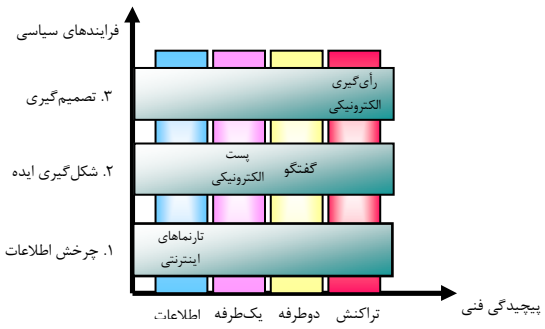
با گسترش دمکراسی الکترونیکی، ارتباط بین مردم و نمایندگان منتخب آنها افزایش یافته و مردم و احزاب سیاسی می‌توانند نقش مؤثرتری در فرایند سیاست‌گذاری داشته باشند. دمکراسی الکترونیکی به‌عنوان شکل الکترونیکی فرایندهای دمکراتیک به سه فرایند زیر تقسیم می‌شود: چرخش اطلاعات، شکل‌گیری ایده و تصمیم‌گیری.

در برنامه‌های کاربردی تحت اینترنت، با توجه به میزان پیچیدگی فرایندها، این سه مرحله قابل تشخیص‌اند. ترکیب پیچیدگی‌های فنی و فرایندهای سیاسی، چارچوب دمکراسی الکترونیکی را تشکیل می‌دهد. بنابراین، دمکراسی الکترونیکی دارای دو هدف اصلی است:

- مشارکت الکترونیکی که پیش‌نیاز تصمیم‌گیری است (فرایندهای اول و دوم).
- رأی‌گیری الکترونیکی (تصمیم‌گیری، یعنی فرایند سوم).

چهار نوع برنامه کاربردی در شکل ۱-۲ نشان داده شده است:

۱. تارنماهای اینترنتی به‌عنوان منبع اطلاعات برای شهروندان،
۲. ارتباط از طریق پست الکترونیک با سیاست‌مداران (که ارتباط یک‌طرفه ناهم‌زمان است)،
۳. گفتگوی اینترنتی با سیاست‌مداران به‌عنوان روش بحث و تبادل نظر هم‌زمان،
۴. رأی‌گیری الکترونیکی (هنگامی‌که در نهایت تصمیمی اتخاذ و گزینه‌ای انتخاب می‌گردد).



شکل ۱-۲ چارچوب دمکراسی الکترونیکی

۳-۳-۲ ویژگی‌های دمکراسی الکترونیکی

ویژگی‌های دمکراسی الکترونیکی عبارت‌اند از:

- در پرتوی دمکراسی الکترونیکی خدمات دولتی به‌صورت یکپارچه و الکترونیکی قابل ارائه است.
- سازمان‌های دولتی به‌جز ارائه خدمات پیوسته جاری، می‌توانند خدمات پیوسته و منسجم دیگری را هم عرضه کنند. آنها قادرند تا به‌جای سرگردان کردن مردم در ادارات یا پایگاه‌های اینترنتی مختلف برای به‌دست آوردن یک تأییدنامه دولتی، امکاناتی را فراهم کنند تا مردم امور خود را تنها از طریق یک نقطه به انجام برسانند.
- امکان دسترسی به فناوری جدید برای عموم مردم از طریق دوره‌های آموزشی مختلف فراهم گشته، آموزش مادام‌العمر امکان‌پذیر می‌شود و ایده تمام نشدن آموزش با پایان یافتن مدرسه محقق می‌گردد.
- دولت قادر به بازسازی روابط میان خود و مردم می‌شود و درواقع به‌جای ارائه خدمات یکسان به همه، می‌تواند به کمک فناوری جدید با مردم به‌صورت افرادی مستقل عمل کرده و به آنها خدمات شخصی ارائه دهد.
- شهروندان در رابطه خود با دولت، احساس مسئولیت بیشتری می‌کنند و اعتماد و اطمینان خود را نسبت به بخش دولتی تقویت می‌نمایند.
- مردم با نمایندگان خود ارتباط نزدیک‌تری پیدا می‌کنند. از این طریق هر کس می‌تواند بدون هیچ مشکلی در خانه خود نشسته و حرف خود را به گوش دولتمردان برساند، به‌ویژه برای افرادی که در نقاط دوردست کشور حضور دارند.
- تعهد افراد نسبت به دولت افزایش می‌یابد؛ چرا که راز تعهد، مشارکت راستین همه افراد است. اگر مشارکتی در کار نباشد، تعهدی نیز در کار نخواهد بود.
- همخوانی مؤثر رایانه‌ای بین بخش‌های دولتی و خصوصی باعث تسریع و پیشرفت امور می‌گردد.
- مشارکت مردم در تصمیم‌گیری‌های حکومتی افزایش می‌یابد؛ چرا که مردم همیشه خواستار برقراری ارتباط نزدیک و آسان با نهادهای حکومتی، نمایندگان و مشارکت در امر حکومت برای رفع مشکلات خود بوده‌اند.

- رضایت عمومی مردم بیش از گذشته حاصل می‌شود.
- افزایش تعداد رأی‌دهندگان در انتخابات ادواری را به‌دنبال دارد.
- صرفه‌جویی در هزینه‌ها را به‌دنبال دارد. دمکراسی الکترونیکی می‌تواند سرمایه‌های هنگفتی را از طریق صرفه‌جویی ناشی از کاهش امور بدون بازده، هزینه‌های زائد و کاغذبازی‌های اضافی کشور نماید.(۱۰)

۴-۳-۲ راه‌حلی برای بحران دمکراسی

از میان جنبه‌های گوناگون بحران دمکراسی، دو جنبه آن از اهمیت بسزایی برخوردار است. این دو جنبه ارتباط تنگاتنگی با یکدیگر داشته و تعیین‌کننده میزان گرایش جامعه به مردم‌سالاری و حکومت مردمی است؛ روند صعودی کاهش مشارکت افراد در فرایندهای مردمی و وجود شکاف بین شهروندان و نظام حاکم، ساختار دمکراسی را آسیب‌پذیر می‌سازد. یکی از مهم‌ترین پیامدهای ناشی از چنین وضعیتی رشد روزافزون بی‌علاقگی و بی‌توجهی شهروندان به امور کشور و کاهش میزان مشارکت افراد در فعالیت‌های سیاسی است.

تأثیر روزافزون فناوری‌های اطلاعات و ارتباطات بر فرایندهای سیاسی، می‌تواند به‌عنوان راه‌حلی برای بحران دمکراسی تلقی شود. این تأثیر ناشی از دو ویژگی مهم دمکراسی الکترونیکی است که اولین آن تأثیر فناوری‌های جدید بر جنبش سیاسی جامعه می‌باشد. اگر جنبش سیاسی را فرایندی بدانیم که در آن شهروندان به شرکت در فعالیت‌های سیاسی ترغیب می‌شوند، آنگاه مهم‌ترین مانع در راه رسیدن به چنین جنبشی، هزینه بالای مشارکت سیاسی خواهد بود. استفاده از اینترنت و سایر فناوری‌های جدید این هزینه‌ها را به‌طور قابل ملاحظه‌ای کاهش می‌دهد. افرادی که تمایل به شرکت در فعالیت‌های سیاسی دارند، برای مبارزات انتخاباتی خود نیازی به برپایی گردهمایی‌های سیاسی در شهرهای مختلف نداشته و درحالی‌که در محل کار خود و در پشت رایانه نشسته‌اند، می‌توانند برنامه‌های کاری خود و حزبشان را به‌راحتی در اختیار همگان قرار دهند.

مزایای به‌کارگیری فناوری‌های اطلاعات و ارتباطات در فرایند دمکراسی عبارت است از: ارتباط مؤثرتر، هزینه کمتر و دسترسی به اطلاعات بیشتر. با به‌کارگیری صحیح

فناوری‌های جدید، حتی گروه‌های بسیار کوچک سیاسی با ساختار سازمانی بسیار ضعیف می‌توانند خود را معرفی نمایند.

ویژگی دیگر دمکراسی الکترونیکی که شاهدی بر نقش مؤثر استفاده از فناوری‌های اطلاعات و ارتباطات در غلبه بر بحران دمکراسی است، کاهش فاصله بین مردم و حکومت و از بین رفتن بوروکراسی اداری می‌باشد. دمکراسی الکترونیکی در قلب دولت الکترونیکی قابلیت آن را دارد تا بخش دولتی را تغییر شکل داده و رابطه میان دولت و شهروندان را از نو پایه‌ریزی کند. در چنین شرایطی شهروندان می‌توانند خدمات و اطلاعات مورد نیاز خود را در هر زمان و بنابر استانداردهای روز کسب نمایند. در این دولت و توسط این دمکراسی ارائه خدمات به شهروندان تسهیل می‌شود، ضمن آنکه لایه‌های اضافی مدیریت دولتی نیز قابل حذف است.

امروزه مردم از خدمات دولتی به‌عنوان فرایندی زمان‌بر، هزینه‌بر و پردردسر یاد می‌کنند، درحالی‌که ایده دمکراسی الکترونیکی می‌تواند این تصور را کاملاً تغییر دهد. دمکراسی الکترونیکی این قابلیت را دارد که رابطه میان دولت و مردم را به‌طورکلی متحول کرده و خدمات دولتی را بهبود بخشد؛ چرا که مردم همیشه خواستار برقراری ارتباط نزدیک با نهادهای حکومتی، نمایندگان و دولتمردان برای رفع مشکلات خود بوده‌اند. مردم می‌خواهند نقش مؤثرتری در فرایند دمکراسی ایفا نمایند.

۵-۳-۲ محرکی برای تشدید بحران دمکراسی

یکی از چالش‌های موجود در دمکراسی الکترونیکی، توانایی افراد مختلف در جامعه در استفاده از فناوری‌های جدید اطلاعات و ارتباطات و میزان نفوذپذیری این فناوری در جامعه است. قابلیت دسترسی به این فناوری‌ها و نیز توانایی استفاده از آنها را می‌توان در سه بعد مورد بررسی قرار داد:

۱. در بسیاری از نقاط دنیا از جمله قاره آفریقا افراد زیادی وجود دارند که علی‌رغم داشتن امکانات مالی فراوان و نیز تحصیلات بالا، به‌دلیل نداشتن شبکه‌های ارتباطی، قادر به استفاده از اینترنت نیستند.

۲. میزان استفاده از این فناوری‌ها تا حد زیادی به هزینه استفاده از آنها بستگی دارد. در کشوری مثل آمریکا ۱ تا ۲ درصد درآمد ماهانه افراد صرف استفاده از خدمات

اینترنت می‌شود، درحالی‌که در کشور بنگلادش این هزینه سهم بالایی از درآمد (بالغ بر ۱۹۱ درصد) ماهانه افراد را به‌خود اختصاص می‌دهند.

۳. کسی که تاکنون رایانه و یا سایر تجهیزات الکترونیکی را ندیده، مطمئناً قادر به گشت و گذار در دنیای اینترنت نخواهد بود. در چنین شرایطی حتی اگر استفاده از اینترنت مجانی بوده و به‌منظور استقرار جامعه اطلاعاتی، رایانه نیز به‌عنوان یک هدیه ازطرف دولت در اختیار افراد قرار گیرد، باز هم فقدان تخصص و تجربه مانع بزرگی در مقابل استفاده از فناوری‌های اطلاعات و ارتباطات خواهد بود.

تمامی ابعاد یادشده در موفقیت دمکراسی الکترونیکی از اهمیت بسزایی برخوردارند. اگر تمامی اقشار جامعه، صرف‌نظر از وضعیت اقتصادی-اجتماعی‌شان قابلیت استفاده یکسان از فناوری‌های جدید را داشته باشند، آنگاه می‌توان ادعا نمود که در دمکراسیِ الکترونیکی به روی همگان گشوده شده و افراد می‌توانند از پیامدهای مثبت آن به‌عنوان ابزار قدرتمندی در زندگی سیاسی استفاده کنند. باوجود این، اگر وضعیت اقتصادی-اجتماعی افراد در کشوری متناسب با الزامات فناوری‌های جدید نباشد، استفاده از این فناوری‌ها شکاف اجتماعی جدیدی را ایجاد نموده و خود محرکی برای تشدید بحران دمکراسی در آن کشور خواهد بود.

پی‌نوشت‌ها

۱. ابوالفضل قاضی‌شریعت‌پناهی، *بایسته‌های حقوق اساسی*، دانشگاه تهران، ۱۳۸۱.

۲. ابوالفضل قاضی‌شریعت‌پناهی، همان.

۳. محمد فتحیان و حاتم مهدوی، *مبانی و مدیریت فناوری اطلاعات*، تهران، دانشگاه علم و صنعت، ۱۳۸۵.

۴. محمد فتحیان و حاتم مهدوی، همان.

۵. محمد فتحیان و حاتم مهدوی، همان.

۶. همان.

7. R. Watson, S. Akselson, B. Evjemo, N. Aarsaether, *Teledemocracy in Local Government,* Association For Computer Machinery, Communications of ACM, 42(12), 1999.

8. J. Taylor. E. Burt, *Parliaments on the Web: Learning Through Innovation,* [In:] Coleman, S. Taylor. C., Van De Donk, W. eds, Parliament in the Age of the Internet, Oxford University Press, Oxford, 1999.

9. B. Hague, B. Loader, *Digital Democracy. Discourse and Decision Making in the Digital Age,* 1999.

۱۰. گروه مهندسین مشاور معمار و شهرساز عمران آب و انرژی ره شهر، بخش تحقیق و توسعه، ۱۳۸۳.

فصل سوم

انتخابات و رأی‌گیری الکترونیکی

گسترش استفاده از فناوری‌های پیشرفته، زمینه بهبود فرایند انتخابات را فراهم نموده است، به همین دلیل، در سال‌های اخیر، انتخابات الکترونیکی به شکل گسترده‌ای مورد توجه سیاست‌مداران و دست‌اندرکاران انتخابات و سایر متخصصان قرار گرفته است.

در سال‌های اخیر، به‌خصوص از سال ۲۰۰۰، مباحث مختلفی در سطوح دانشگاهی، دولتی و صنعتی درخصوص مزایا و معایب انتخابات الکترونیکی مطرح شده است. اگرچه بیشتر این مباحث مربوط به رأی‌گیری اینترنتی است، اما این بحث به سایر انواع انتخابات الکترونیکی از جمله استفاده از ماشین‌های رأی‌گیری نیز سرایت کرده است.

۱-۳ مفاهیم اولیه

برخی از واژه‌های مورد استفاده در مورد انتخابات و رأی‌گیری الکترونیکی به‌شرح زیر است:

۱. **انتخابات الکترونیکی یا رفراندوم الکترونیکی**:[1] انتخابات یا رفراندومی که در یک یا چند مرحله از آن از تجهیزات الکترونیکی استفاده می‌شود.

۲. **رأی‌گیری الکترونیکی**:[2] انتخابات یا رفراندومی که حداقل مرحله رأی‌گیری آن به‌صورت الکترونیکی است.

۳. **رأی‌گیری باجه‌ای**:[3] به‌معنای استفاده از ماشین‌های رأی‌گیری است که در باجه‌های مخصوص و یا مکان‌های از پیش تعیین شده نصب می‌شوند. در این روش، رأی‌دهندگان به‌صورت الکترونیکی (مثلاً با استفاده از صفحه نمایش تماسی)[4] رأی می‌دهند. عمل

---

1. E-election or E-referendum
2. E-voting
3. Kiosk Voting
4. Touch Screen

رأی‌گیری و شمارش آرا با استفاده از دستگاهی به نام ماشین رأی‌گیری با ثبت مستقیم[1] انجام می‌شود و سپس نتایج حاصل از شمارش آرا، از طریق شبکه‌های اختصاصی برای اعلام نتیجه نهایی به حوزه مرکزی ارسال می‌گردد.

۴. **رأی‌گیری الکترونیکی از راه دور**:[2] در حال حاضر ایدئال‌ترین روش رأی‌گیری است و به رأی‌دهندگان امکان می‌دهد که بدون نیاز به حضور در حوزه‌های انتخاباتی در انتخابات شرکت نمایند. در این روش برای ارسال رأی می‌توان از اینترنت، سرویس پیام کوتاه، تلویزیون‌های محاوره‌ای و یا تلفن‌های دکمه‌ای استفاده نمود.

۵. **رأی‌گیری برخط**:[3] به‌معنای رأی‌گیری الکترونیکی از طریق اتصال به یک سیستم مستقیم است. در این روش، آرای ارسال شده از راه دور و یا از طریق باجه‌های رأی‌گیری مستقیماً در بانک اطلاعاتی سرور مرکزی ذخیره می‌گردد.

۶. **رأی‌گیری اینترنتی**:[4] یکی از انواع رأی‌گیری الکترونیکی از راه دور است که از امکانات اینترنت و تارنماهای آن استفاده می‌کند.

۷. **شمارش الکترونیکی**:[5] استفاده از فناوری‌های مختلف که تعرفه‌ها را به‌صورت الکترونیکی شمارش می‌کند، مثل اسکنر نوری.

۸. **دستگاه مشتری**:[6] وسیله‌ای است که برای ایجاد ارتباط بین رأی‌دهنده و نظام انتخاباتی به‌کار می‌رود.

۹. **شناسایی**:[7] انجام اقداماتی برای تأیید هویت ادعا شده از طرف افراد.

۱۰. **تعرفه**: ابزاری قانونی که به‌وسیله آن رأی‌دهنده انتخابش را بیان می‌کند.

۱۱. **کاندیدا**: یک گزینه انتخابی که می‌تواند یک فرد، یک گروه و یا یک حزب باشد.

۱۲. **رأی‌دادن**:[8] ریختن رأی در صندوق.

۱۳. **صندوق رأی الکترونیکی**:[9] ابزارهای الکترونیکی که برای ذخیره‌سازی آرا پیش از

---

1. Direct Recording Electronic Machine (DREM)
2. Remote Electronic Voting (REV)
3. Online Voting
4. Internet Voting
5. Electronic Counting
6. Client
7. Authentication
8. Cast Vote
9. Electronic Ballot Box

شمارش به‌کار می‌رود.

۱۴. **رأی**:[1] بیان گزینه انتخابی.

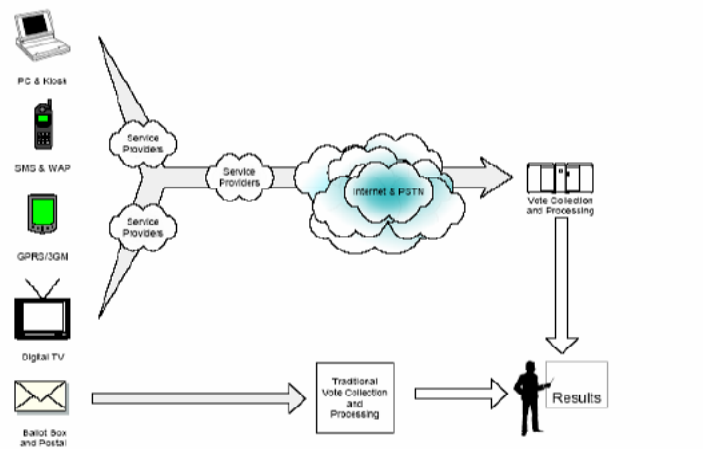
۱۵. **رأی‌دهنده**:[2] فردی که به او اجازه شرکت در انتخابات داده می‌شود.

۱۶. **کانال رأی‌گیری**: روشی که از طریق آن رأی‌دهنده می‌تواند رأی دهد.

۳-۲ تجزیه و تحلیل مقدماتی

شکل ۱-۳ نشان می‌دهد که رأی‌گیری الکترونیکی در عمل چگونه کار می‌کند.

رأی‌دهندگان رأی خود را از طریق دستگاه مشتری ارسال می‌نمایند. این دستگاه‌ها از طریق یک سرویس‌دهنده به شبکه عمومی مثل اینترنت متصل می‌باشند. رأی داده شده به‌وسیله سرویس‌دهنده، از طریق شبکه عمومی یا اختصاصی به مرکز جمع‌آوری و پردازش آرا فرستاده می‌شود.



شکل ۱-۳ معماری رأی‌گیری الکترونیکی

۳-۳ ابزارها

امروزه بحث‌های مختلفی در زمینه به‌کارگیری ابزارهای مختلف رأی‌گیری وجود دارد؛ از ساده‌ترین ابزار یعنی تلفن گرفته تا رایانه‌های بسیار مجهز و پیچیده. در ادامه برخی از مباحث

---

1. Vote
2. Voter

مربوط به امنیت، سهولت کاربرد و سایر موارد مرتبط با این ابزار مورد بررسی قرار می‌گیرد.

۱-۳-۳ تلفن

۱-۱-۳-۳ تلفن‌های دکمه‌ای

۱. هر دستگاه تلفن که مجهز به سیستم تون باشد، می‌تواند برای رأی‌گیری الکترونیکی از راه دور مورد استفاده قرار گیرد.
۲. در شبکه‌های تلفن ثابت امکان حفظ محرمانگی و جامعیت آرا وجود ندارد؛ زیرا به‌راحتی می‌توان خط تلفنی را که مکالمه از طریق آن صورت گرفته تشخیص داد.
۳. استفاده از تلفن‌های دکمه‌ای در مواردی کاربرد دارد که رأی‌دهنده یک عدد منحصربه‌فرد را به‌عنوان رأی وارد می‌کند.

۲-۱-۳-۳ تلفن‌های تشخیص‌دهنده صدا

مشابه مکالمات تلفنی به‌روش تلفن‌های دکمه‌ای است، با این تفاوت که دارای نرم‌افزاری می‌باشد که کلمات اصلی مانند سه، دو، یک، خیر و بله را تشخیص می‌دهد. این نوع تلفن‌ها در عمل دارای اشکالات بسیاری هستند. بنابراین، برای انتخابات الکترونیکی پیشنهاد نمی‌گردند.

۳-۱-۳-۳ استفاده از سیستم پیام کوتاه

۱. امروزه تعداد کثیری از تلفن‌های همراه، دارای امکان استفاده از سیستم پیام کوتاه‌اند. این پیام‌ها شامل حروف بزرگ و کوچک، اعداد، سمبل‌ها و علائم نقطه‌گذاری می‌باشند، اما ریسک خواندن پیام‌ها همچون ریسک گوش کردن به مکالمات همچنان وجود دارد.
۲. در سیستم‌های پیام کوتاه، هیچ تضمینی برای ارسال موفقیت‌آمیز پیام وجود ندارد، درحالی‌که در سیستم‌های رأی‌گیری الکترونیکی، ضروری است که رأی‌دهنده از ارسال رأیش مطمئن شود. در چنین مواردی برای اطمینان از ارسال رأی، رأی‌دهنده ممکن است چندین مرتبه رأی خود را ارسال نماید. علاوه بر این‌که هویت رأی‌دهنده نیز می‌تواند مورد تردید واقع شود.
۳. سیستم پیام کوتاه در مواردی مناسب است که یک عدد منحصربه‌فرد به هر کاندیدا

اختصاص یابد (کد کاندیدا و کد رأی‌دهنده) و این کد به‌عنوان رأی از طریق سیستم پیام کوتاه ارسال گردد.

۲-۳-۳ تلویزیون‌های دیجیتالی محاوره‌ای[1]

۱. این نوع تلویزیون‌ها به دو صورت کابلی و غیرکابلی وجود دارند. در تلویزیون‌های غیرکابلی از خط تلفن برای ایجاد ارتباط استفاده می‌شود.
۲. برای رأی‌گیری الکترونیکی از یک نرم‌افزار استفاده می‌شود.
۳. این نرم‌افزارها دارای یک رابط کاربر است که امکان انتخاب گزینه مورد نظر را با استفاده از یک داده عددی فراهم می‌کند.

۳-۳-۳ اینترنت

با استفاده از توانایی‌های اینترنت، می‌توان رأی‌گیری الکترونیکی از راه دور را با استفاده از ابزارهای مختلف انجام داد. در ذیل به تعدادی از این ابزارها اشاره می‌شود.

۱-۳-۳-۳ فرم‌های ساده وب[2]

۱. یک صفحه وب است که داده عددی را به‌عنوان ورودی گرفته و پاسخ را برمی‌گرداند؛ مشابه سیستم‌های پیام کوتاه یا تلویزیون‌های محاوره‌ای.
۲. هر داده‌ای که در اینترنت جابه‌جا می‌شود در معرض ریسک تغییر توسط رایانه‌های میانی و شبکه بین دو نقطه ابتدایی و انتهایی است. بنابراین، احتمال تغییر آرا توسط افراد متقلب وجود دارد.

۲-۳-۳-۳ تارنماهای «اس اس ال»[3]

۱. تارنماهای محافظت شده‌ای هستند که مشابه سیستم‌های فروشگاهی عمل می‌کنند.

---

1. Interactive Digital TV
2. Simple Web Form
۳. Secure Socket Layer (SSL): یک فناوری استاندارد برای تأمین ارتباطی امن مابین یک وب‌سرور و یک مرورگر اینترنت است. این ارتباط امن از تمامی اطلاعات ردوبدل شده محافظت می‌کند تا در حین انتقال به‌صورت محرمانه و دست‌نخورده باقی بماند.

کاربر اطلاعات مربوط به‌خود را وارد کرده و پس از تأیید هویت، کاندیدای مورد نظر خود را از لیست کاندیداها انتخاب می‌کند.

۲. استفاده از این روش بسیار آسان است، اما توزیع کد کاربری و کلمه عبور[1] بین رأی‌دهندگان با مشکلاتی همراه می‌باشد.

۳. سرعت و دقت این روش بستگی به مرورگر وب[2] و سیستم‌عاملی دارد که کاربر از آن استفاده می‌کند.

۴. در این روش امکان سرایت ویروس به مرورگر وب و سیستم‌عامل وجود دارد، به‌طوری‌که ممکن است وجود ویروس سبب تغییر نتایج ارسالی به سرور مرکزی گردد.

۳-۳-۳-۳ استفاده از برنامه‌های جاوا[3]

کاربر می‌تواند با استفاده از تارنماهای «اس اس ال»، هویت خود را تأیید نموده و سپس از یک ریزبرنامه در روی مرورگر وب، برای انجام پردازش‌های محلی مثل امضای دیجیتالی رأی استفاده کند. هویت رأی‌دهندگان در این روش محفوظ می‌ماند.

۳-۳-۴ ماشین‌های رأی‌گیری با ثبت هم‌زمان آرا

این ماشین‌ها در حوزه‌های انتخاباتی نصب شده و به رأی‌دهندگان امکان می‌دهد که بتوانند آرایشان را به‌صورت مستقیم و با استفاده از صفحه نمایش تماسی[4] وارد نمایند. در فصول آینده این دستگاه‌ها به‌صورت کامل معرفی می‌گردند.

۳-۴ پیش‌نیازها

در حالت کلی می‌توان گفت که تمامی پیش‌نیازهای لازم برای برگزاری انتخابات کاغذ-محور در مورد انتخابات الکترونیکی نیز صادق است. این اصول در مورد تمامی انتخابات

---

1. Username, Password
2. Web Browser
۳. نوعی زبان برنامه‌نویسی برای ایجاد جلوه‌های گرافیکی است. کارتون‌ها، تصاویر متحرک در صفحه نمایش و فرم‌های هوشمند، همگی نمونه‌هایی از برنامه‌های جاوا هستند.
4. Touch-screen Monitor

دمکراتیک عمومیت داشته اما ممکن است در جزئیات با یکدیگر متفاوت باشند. این اصول از نقطه‌نظر انتخابات الکترونیک عبارت‌اند از:

۱. **انتخابات آزاد**: شهروندان باید بتوانند کاندیداهای خود را به‌صورت آزادانه و بدون اعمال فشار انتخاب کنند. این آرا باید بدون دستکاری و تغییر به‌دست مسئولان مربوطه برسد.

۲. **محرمانگی آرا**: هیچ‌کس نباید از رأی دیگری مطلع شود.

۳. **تساوی در حق رأی**: تمامی آرا از ارزش مساوی برخوردارند. هیچ رأیی به‌دلیل مشکلات فنی نباید باطل اعلام شود. حق رأی دادن افراد، تنها به آنچه که در قانون به‌صراحت بیان گردیده، وابسته است (مثل حق رأی افراد با محکومیت جنایی).

۴. **شفافیت**: کلیه مراحل رأی‌گیری باید شفاف و قابل تولید مجدد باشد.

۵. **قابلیت اطمینان**: تمامی بخش‌های سیستم رأی‌گیری باید با قوت به‌کار خود ادامه دهد، حتی در صورت قطع ارتباط اینترنتی و یا درست کار نکردن ماشین‌های رأی‌گیری.

۶. **قابلیت انعطاف**: سیستم باید قابلیت پیکربندی در انتخابات مختلف را داشته باشد (مثلاً زبان‌های مختلف و یا طرح سؤالات متنوع در تعرفه‌های انتخاباتی). همچنین این سیستم‌ها باید با سیستم‌عامل‌های مختلف سازگار باشند.

۷. **یگانگی**: هر رأی‌دهنده تنها مجاز به دادن یک رأی می‌باشد.

۸. **جامعیت**: هر نوع دستکاری، جعل و یا حذف آرا باید توسط سیستم قابل شناسایی باشد.

۹. **سهولت کاربرد**: استفاده از سیستم‌های رأی‌گیری نباید منوط به داشتن مهارت‌های خاص باشد.

۵-۳ انواع نظام‌های انتخاباتی

کشورهای توسعه‌یافته برخی از اشکال فناوری اطلاعات و ارتباطات را در فرایندهای انتخاباتی خود به‌کار می‌گیرند. در این نظام‌ها تنها عمل شمارش آرا به‌صورت الکترونیکی انجام می‌شود.[1]

در مقابل، در بسیاری از کشورها فرایند انتخابات کاملاً غیرالکترونیکی است.[2] در

---

1. Back-end Election Systems
2. Front-end Election Systems

این کشورها، تعرفه‌های رأی کاغذی بوده و پس از انتخاب کاندیداها، در پاکت‌های خاص مهروموم شده و سپس به صندوق رأی ریخته می‌شوند. در طول انتخابات مسئولیت کنترل و نظارت صندوق‌ها به‌عهده اعضای شورای انتخابات می‌باشد. پس از خاتمه مهلت انتخابات، این صندوق‌ها توسط اعضای شورا باز شده و عمل شمارش آرا در حوزه‌ها به‌صورت دستی انجام می‌شود. به‌این‌ترتیب، تعداد آرای هر حوزه به تفکیک مشخص می‌گردد. این شیوه سنتی انتخابات با هیچ‌گونه تجهیزات الکترونیکی سروکار ندارد.

در این روش، یک ارتباط محاوره‌ای مستقیم بین رأی‌دهندگان، اعضای شورای انتخابات و کارکنان حوزه‌ها وجود دارد. این سه گروه تنها با عناصر فیزیکی مانند تعرفه رأی، پاکت (در بعضی از کشورها) و صندوق آرا سروکار دارند.

در برخی از نظام‌های سنتی انتخابات، برای شمارش آرا از اسکنرهای نوری استفاده می‌شود. استفاده از این دستگاه‌ها منجر به افزایش سرعت شمارش آرا و اعلام سریع نتایج می‌گردد. باوجود این، این نظام‌ها هنوز به‌عنوان سیستم‌های کاغذ-محور[1] نامیده می‌شوند.

انتخابات الکترونیکی استفاده از فناوری اطلاعات و ارتباطات در نظام‌های انتخاباتی سنتی است. یک دستگاه الکترونیکی مستقیماً گزینه انتخابی رأی‌دهنده را به شکل دیجیتالی در محل مورد نظر ذخیره می‌کند. به این معنی که رأی‌دهنده به‌جای تعرفه‌های کاغذی از تعرفه‌های دیجیتالی مجازی استفاده می‌نماید. پس از انتخاب گزینه مورد نظر توسط رأی‌دهنده، نیازی به مراجعه او به حوزه‌های انتخاباتی نیست؛ زیرا می‌توان از اشکال مختلف فناوری اطلاعات و ارتباطات از جمله شبکه‌های ارتباطی برای ثبت آرا استفاده کرد. استفاده از تعرفه‌های دیجیتالی به‌جای تعرفه‌های کاغذی دارای مزایای زیر است:

- افزایش سرعت و دقت انتخابات،
- صرفه‌جویی در چاپ و توزیع تعرفه‌ها،
- امکان دسترسی آسان برای افراد معلول و ناتوان،
- انعطاف‌پذیری تعرفه‌ها، به‌طوری‌که حتی در آخرین دقایق مانده به شروع انتخابات نیز می‌توان تعرفه‌ها را تغییر داد،

---

1. Paper-centred

- امکان دستیابی به اطلاعات جامع در مورد کاندیداها،
- امکان نمایش تعرفه‌های انتخاباتی به زبان‌های مختلف،
- جلوگیری از خطاهای رأی‌دهندگان.

اصولاً انتخابات سیاسی از حساسیت بالایی برخوردار بوده و انتخاب شیوه برگزاری آن دقت و توجه خاصی را می‌طلبد، اما در سایر موارد می‌توان به‌راحتی انتخابات را به‌صورت الکترونیکی برگزار نمود، از جمله:

ـ انتخابات شغلی و حرفه‌ای در شرکت‌ها و سازمان‌های دولتی،
ـ انتخابات در گروه‌های تخصصی،
ـ انتخابات در دانشگاه‌ها،
ـ انتخابات در انجمن‌ها.

۳-۶ سیستم‌ها

سیستم‌های رأی‌گیری الکترونیکی براساس محل رأی‌دهی به دو گروه تقسیم می‌شوند:

۱. سیستم‌های ایستگاهی،[1]
۲. سیستم‌های رأی‌گیری از راه دور.[2]

در سیستم‌های ایستگاهی از دستگاهی به نام ماشین ثبت مستقیم[3] استفاده می‌شود. در این روش رأی‌دهندگان ناچارند که به حوزه‌های انتخاباتی مراجعه نمایند. ترمینال‌های رأی‌گیری دارای یک رابط کاربر گرافیکی بوده و تصویر کاندیداها را بر روی مانیتور نمایش می‌دهند. در نتیجه رأی‌دهنده می‌تواند گزینه مورد نظر را انتخاب نماید. پس از تأیید قطعی انتخاب توسط کاربر، رأی مربوطه ذخیره شده و به سایر آرا اضافه می‌گردد.

سیستم‌های انتخاباتی از راه دور، از امکانات فناوری‌های اطلاعات و ارتباطات استفاده می‌کنند. در این سیستم‌ها نیز رأی‌دهنده از یک رابط کاربر گرافیکی، مشابه ترمینال‌های رأی‌گیری برای انتخاب گزینه مورد نظر خود استفاده می‌کند، اگرچه رأی‌دهی از راه دور (از خانه با استفاده از رایانه‌های شخصی، با استفاده از رایانه‌های

---

1. Poll-site
2. Remotely
3. Direct Recording Electronic (DRE)

مستقر در سفارتخانه‌ها، بیمارستان‌ها و ...) انجام می‌گیرد.

هدف از به‌کارگیری سیستم‌های راه دور، انتقال اطلاعات دیجیتالی (آرا) به حوزه‌های ستادی از طریق شبکه‌های ارتباطی است تا رأی‌دهندگان ملزم به‌حضور در حوزه‌های انتخاباتی نباشند. انتخابات الکترونیکی از راه دور علاوه بر مزایای انتخابات الکترونیکی به روش ایستگاهی دارای مزایای ذیل نیز است:

- افزایش تعداد محل‌های رأی‌دهی بدون صرف هزینه (در این روش افزایش تعداد محل‌های رأی‌دهی، منجر به افزایش خطی هزینه انتخابات نمی‌شود)،
- استقلال جغرافیایی رأی‌دهندگان و در نتیجه سهولت دسترسی،
- تسهیل امکان مشارکت در انتخابات.

۳-۷ روش‌ها

الکترونیکی بودن انتخابات می‌تواند جنبه‌های مختلف داشته باشد، مانند شمارش الکترونیکی آرای کاغذی. اما آنچه که در اینجا مطرح می‌باشد، انجام کلیه فرایندهای انتخاباتی به‌صورت الکترونیکی است.

۳-۷-۱ باجه‌های مخصوص در حوزه انتخاباتی رأی‌دهنده

در این روش رأی‌دهنده ملزم به حضور در حوزه انتخاباتی مربوط به‌خود است. ضمناً اشخاص از تعرفه‌های کاغذی استفاده نموده و شمارش آرا به‌صورت اتوماتیک در داخل حوزه‌ها انجام می‌شود.

۳-۷-۲ باجه‌های مخصوص در هر حوزه انتخاباتی

لازم است که رأی‌دهنده به یکی از حوزه‌های انتخاباتی مراجعه نماید. در این روش، مشخصات رأی‌دهندگان توسط مسئولان حوزه مشخص شده و درصورت لزوم برای کنترل به حوزه مربوط به رأی‌دهنده ارسال می‌گردد.

۳-۷-۳ باجه‌های مخصوص در خارج از حوزه‌های انتخاباتی

در این روش ماشین‌های اتوماتیک رأی‌گیری در مکان‌های خاص مثل مراکز خرید،

ایستگاه‌ها، ادارات پست و ... در داخل باجه‌های خاصی قرار گرفته و افراد برای رأی‌دهی به این مکان‌ها مراجعه می‌کنند.

۳-۷-۴ رأی‌گیری از راه دور

در این روش از هر مکانی امکان رأی‌دهی وجود دارد و رأی‌دهنده می‌تواند از خانه، محل کار و یا هر نقطه دیگری رأی خود را ارسال نماید. فناوری‌های به‌کار گرفته شده در این روش بسیار متفاوتند:

- رأی‌دهی اینترنتی از طریق یک رایانه،
- رأی‌دهی به‌وسیله سرویس پیام کوتاه[1] از طریق تلفن همراه،
- رأی‌دهی به‌وسیله تلویزیون‌های محاوره‌ای.

۳-۸ مزایای به‌کارگیری

مزایای الکترونیکی نمودن انتخابات را از چندین نقطه‌نظر می‌توان مورد بررسی قرار داد:

۳-۸-۱ مزایای مدیریتی

۱. **بهبود فرایند پردازش آرا و تسریع در تجزیه و تحلیل نتایج**: به‌کارگیری انتخابات الکترونیکی، تجزیه و تحلیل و پردازش فرایند رأی‌گیری را بهبود می‌بخشد. به این معنی که بلافاصله پس از خاتمه انتخابات، نتایج حاصله در حوزه‌ها موجود بوده و نیازی به بسیج اشخاص و استفاده از افراد داوطلب برای شمارش آرا نیست.

۲. **کاهش تقلب و خطاهای مربوط به استفاده از تعرفه‌های کاغذی**: از جمله اشکالاتی که در استفاده از سیستم‌های سنتی وجود دارد، بلاتکلیفی در مورد نحوه برخورد با تعرفه‌های کاغذی پاره، تاشده یا علامت‌گذاری‌شده است. ازطرف دیگر، در این سیستم‌ها امکان نابودی آرای بعضی از صندوق‌ها و یا پرکردن صندوق با آرای تقلبی وجود دارد. با به‌کارگیری رأی‌گیری الکترونیکی این معضلات از بین می‌رود.

۳. **امکان شمارش آرای سفید**: رأی سفید رأیی است که در آن رأی‌دهنده هیچ‌یک از کاندیداها

---

1. Short Message Service (SMS)

را انتخاب نکرده است. در سیستم‌های سنتی، رأی سفید به‌عنوان رأی باطل تلقی شده و از سایر انواع آرای باطل قابل تفکیک نمی‌باشد، درحالی‌که در رأی‌گیری الکترونیکی این نوع آرا قابل شمارش بوده و می‌تواند از جنبه سیاسی بسیار حائز اهمیت باشد. البته نحوه برخورد با آرای سفید در انتخابات الکترونیکی به سیاست دولت بستگی دارد.

۲-۸-۳ مزایای مشارکتی

یکی از مباحث مطرح در انتخابات الکترونیکی، رشد میزان مشارکت در انتخابات می‌باشد. سه عامل مثبتی که در این‌گونه سیستم‌ها وجود دارد عبارت است از:

۱. امکان رأی‌دهی بدون نیاز به حضور در حوزه‌های انتخاباتی که شرکت در انتخابات را تسهیل کرده و سبب اجرای انتخابات مطابق سبک و سیاق زندگی امروزی می‌شود.

۲. امکان رأی‌دهی برای افرادی که خروج از خانه و حضور در حوزه‌ها آنها را دچار مشکل می‌کند، از جمله افراد پیر و معلول.

۳. تشویق جوانان به مشارکت در انتخابات؛ زیرا این قشر از طرفداران پروپا قرص فناوری‌های اطلاعات بوده و انتخابات الکترونیکی را روشی نوین و جالب توجه تلقی می‌کنند.

البته باید توجه داشت که در بسیاری از موارد، تعداد کم شرکت‌کنندگان به شرایط فیزیکی انتخابات بستگی ندارد، بلکه ناشی از طرز تفکر سیاسی، اجتماعی و شغلی افراد است. به همین دلیل و با توجه به تجربیات کشورهای مختلف در زمینه انتخابات الکترونیکی، نمی‌توان نتیجه گرفت که انتخابات الکترونیکی به‌طور قطع سبب افزایش میزان مشارکت مردم در انتخابات شده و یا اینکه هیچ‌گونه تأثیری بر آن ندارد.

۳-۸-۳ مزایای زندگی نوین شهری

۱. **نوگرایی در زندگی اجتماعی**: توانایی رأی‌دهی به‌صورت الکترونیکی، سمبل نوگرایی در زندگی اجتماعی است. کاربرانی که به‌طور فزاینده‌ای از جنبه‌های مختلف فناوری‌های اطلاعات در زندگی روزمره خود استفاده می‌کنند، تمایل دارند که درخصوص انتخابات نیز از فناوری‌های جدید استفاده کنند.

۲. **ظهور اشکال جدید مشارکت شهروندان**: رأی‌گیری الکترونیکی از راه دور به گروه‌های مختلف سیاسی امکان می‌دهد تا با یکدیگر به تبادل‌نظر بپردازند. به‌عبارت‌دیگر،

رأی‌دهی از راه دور شکل جدیدی از ابراز عقاید شهروندان محسوب می‌شود. بنابراین، می‌توان با استفاده از امکانات اینترنت، مباحثی را مطرح کرد، آنها را مورد نقد و تجزیه و تحلیل قرار داد و در نهایت رأی‌گیری الکترونیکی را برگزار نمود، که در این خصوص می‌توان از کنفرانس‌های مجازی نام برد.

۹-۳ چالش‌ها و ریسک‌های مرتبط

انتخابات الکترونیکی می‌تواند باعث بهبود فرایند انتخابات از جنبه‌های گوناگون شود. این فناوری امکان مشارکت فعالانه مردم (مشاوره الکترونیکی و مشارکت الکترونیکی) را در تصمیم‌گیری‌های دولتی فراهم نموده و باعث جلب اعتماد شهروندان می‌گردد. مشاوره الکترونیکی و رأی‌گیری الکترونیکی نمونه‌هایی از تحول دمکراسی در کشور محسوب می‌شوند.

البته انتخابات الکترونیکی عاری از مشکل نیست و به‌دلیل استفاده از سیستم‌های الکترونیکی چالش‌ها، ریسک‌ها و مشکلاتی را به همراه دارد.[۱] این چالش‌ها را می‌توان در سه گروه «قانونی، سیاسی-اجتماعی و فنی» دسته‌بندی نمود. چالش‌های قانونی به‌دلیل مغایرت قوانین موجود با برگزاری الکترونیکی انتخابات و لزوم تدوین قوانین جدید می‌باشد.[۲] چالش‌های سیاسی-اجتماعی ناشی از تأثیر فناوری‌های نوین ارتباطات و اطلاعات بر سیستم‌های انتخاباتی است.[۳] چالش‌های فنی هم مرتبط با محفوظ ماندن آرا، حفظ محرمانگی رأی‌دهنده و روش‌های امنیتی سیستم می‌باشد.

سیستم‌های رأی‌گیری الکترونیکی در مقایسه با سیستم‌های سنتی بسیار متفاوت‌اند و به‌دلیل این تفاوت‌ها، با چهار منبع ایجاد چالش مواجه خواهند بود:

- طبیعت دیجیتالی تعرفه‌ها،
- پیچیدگی سیستم‌های مورد استفاده،
- عدم شفافیت سیستم از دیدگاه رأی‌دهندگان و مسئولان انتخابات،
- وجود متخصصانی که به‌دلیل توانایی‌های علمی و فنی، قادرند به سیستم الکترونیکی نفوذ نمایند.

عوامل یادشده مهم‌ترین تهدیدات سیستم تلقی شده و منشأ حمله به سیستم از طرق

گوناگون به شمار می‌روند. به‌عنوان مثال، تجهیزات الکترونیکی به‌کار گرفته شده ممکن است دچار خرابی سخت‌افزاری شوند، نرم‌افزار مورد استفاده حاوی خطاهای برنامه‌نویسی عمدی یا غیرعمدی باشد و آرای دیجیتالی حذف و یا دستکاری شوند. همچنین ممکن است به محرمانگی رأی‌دهندگان نیز خدشه وارد شود. تمامی این چالش‌ها بسیار مهم است و می‌تواند سلامت انتخابات را تهدید نموده و یا اعتماد عمومی نسبت به فرایند دمکراسی را زیر سؤال ببرد.

آنچه مسلم است، اگر سیستم‌های رأی‌گیری الکترونیکی به شکل مطمئن محافظت نشوند، ریسک‌ها و مشکلات امنیتی بسیار زیادی را به‌دنبال خواهند داشت. این ریسک‌ها برحسب روش رأی‌گیری الکترونیکی با یکدیگر متفاوت بوده و برخی از ریسک‌های مشترک در تمامی سیستم‌های رأی‌گیری الکترونیکی به قرار زیر است:

۱-۹-۳ مشکلات امنیت سیستم

سیستم‌های رأی‌گیری الکترونیکی ممکن است به طرق مختلف مورد تهاجم قرار بگیرند، به‌خصوص زمانی که اطلاعات در یک نقطه متمرکز باشد. بدیهی است که رأی‌گیری سنتی و کاغذی نیز بدون تقلب نیست، اما استفاده از رایانه در فعالیت‌های انتخاباتی، در شرایط خاص و بدون توجه به نکات امنیتی می‌تواند سبب تقلب‌های بسیار گسترده شود. به همین دلیل لازم است که در حین بررسی بین این دو گروه از پیشامدها تفاوت قائل شویم:

۱. در هنگام اجرای رأی‌گیری الکترونیکی در مکان‌های ایزوله مانند باجه‌های انتخاباتی مستقر در حوزه‌ها، ریسک تقلب به همان حوزه محدود می‌شود که از آن جمله می‌توان از تغییر همه و یا بخشی از نرم‌افزار رأی‌گیری و یا تقلب در اعلام نتایج نام برد. این ریسک در حین برگزاری انتخابات، با کنترل سیستم مورد استفاده و کسب اطمینان از جامعیت آن تا حدودی کاهش می‌یابد.

۲. ریسک رأی‌گیری الکترونیکی در زمان انتقال نتایج انتخابات از طریق شبکه‌های رایانه‌ای به سرور مرکزی افزایش می‌یابد. همیشه افراد حرفه‌ای وجود دارند که با نفوذ در این شبکه‌ها می‌توانند در نتایج انتخابات دست برده و مطابق خواست خود آن را تغییر دهند. برخی از این حملات عبارت‌اند از:

ـ **حمله به سیستم‌های انتقال**: ایجاد خرابی در محیط فیزیکی انتقال (مانند بریدن کابل‌ها یا فیبر نوری)، ارسال بسته‌های اطلاعاتی زائد در شبکه به‌منظور کاهش سرعت سیستم و سرقت اطلاعات ردوبدل شده در شبکه.

ـ **حمله به سرورها**: ایجاد ترافیک در سرویس‌دهی سرور به‌وسیله فرستادن بسته‌های اطلاعاتی زائد، حمله ویروس‌ها و در اختیار گرفتن کامل راهبری سرورها.

ـ **حمله به حوزه‌های رأی‌گیری**: جعل هویت رأی‌دهندگان برای رأی‌دهی چندباره، تغییر مسیر سایت انتخاباتی به آدرس دیگر برای تصاحب پارامترهای وارد شده توسط رأی‌دهنده و انتشار ویروس در حوزه.

شایان ذکر است که درجه اهمیت این ریسک‌ها بسته به حساسیت انتخابات با یکدیگر متفاوت‌اند. به‌عبارت‌دیگر، سطوح امنیتی لازم برای انتخابات سیاسی با انتخابات شغلی کاملاً متفاوت است. ریسک‌های مطرح عبارت‌اند از:

۳-۹-۱-۱ امنیت رأی‌گیری و صحت آرا

ریسک سوءاستفاده از مفهوم «حق رأی» در سیستم‌های رأی‌گیری الکترونیکی بیش از سیستم‌های سنتی است. در انتخابات سنتی، در زمان انداختن برگه رأی در صندوق، هیچ واسطه‌ای بین انتخاب رأی‌دهنده و آنچه که روی تعرفه می‌نویسد وجود ندارد. بنابراین، عوامل فیزیکی نمی‌توانند سبب تغییر و یا جایگزینی آرا شوند. فرایند رأی‌دهی در این سیستم‌ها شفاف بوده و به‌راحتی توسط هر فرد قابل مشاهده است. اما در رأی‌گیری الکترونیکی، بین رأی‌دهنده و تعرفه‌اش یک سیستم رایانه‌ای مبهم و گنگ وجود دارد. احساس وجود یک جعبه سیاه که نمی‌تواند توسط رأی‌دهنده دیده شود، سبب بی‌اعتمادی به سیستم رأی‌گیری الکترونیکی می‌گردد. در سیستم‌های رأی‌گیری الکترونیکی امکان کشف ارتباط بین رأی و رأی‌دهنده وجود دارد، درحالی‌که این احتمال در سیستم‌های سنتی خیلی کم است.

۳-۹-۱-۲ رأی‌گیری در خارج از حوزه‌ها

الف) اعمال فشار به رأی‌دهندگان

در هنگام برگزاری رأی‌گیری الکترونیکی در حوزه‌های انتخاباتی، اعضای کمیته انتخابات

و نمایندگان احزاب و کاندیداها می‌توانند نظارت کاملی بر روند اجرای انتخابات داشته باشند. بنابراین، احتمال اعمال فشار به رأی‌دهندگان وجود نخواهد داشت. رأی‌دهی در داخل باجه‌های مخصوص نیز محرمانگی آرا را تضمین می‌کند. اما در سیستم‌های رأی‌گیری الکترونیکی در خارج از حوزه‌های انتخاباتی و بدون نظارت مسئولان، محرمانگی از ضمانت کمتری برخوردار است؛ زیرا رأی‌دهنده ممکن است تحت فشار افراد خاص مجبور به رأی‌دهی شود.

ب) احراز هویت رأی‌دهنده و تأیید آن

رأی‌گیری الکترونیکی در خارج از حوزه‌های انتخاباتی، تشخیص هویت رأی‌دهنده را مشکل می‌سازد؛ چرا که در این شرایط کنترل فیزیکی رأی‌دهندگان قابل اجرا نبوده و در نتیجه این فرایند از دید شهروندان از امنیت کافی برخوردار نیست.

۳-۱-۹-۳ نابرابری بین رأی‌دهندگان

استفاده از فناوری اطلاعات و ارتباطات مقدمه ایجاد نابرابری بین رأی‌دهندگان است؛ زیرا همه رأی‌دهندگان به این فناوری‌ها دسترسی نداشته و برخی در استفاده از آن از مهارت کافی برخوردار نیستند. از طرفی در بسیاری از کشورها، رأی‌گیری اینترنتی از جانب قشر جوان کشور و نیز گروه‌های تخصصی مورد استقبال فراوانی قرار گرفته است.

توجه به این نکته ضروری است که شکاف دیجیتالی[1] موجود، با گسترش استفاده از فناوری اطلاعات و ارتباطات و توسعه مهارت افراد کاهش می‌یابد. اعتراض به نابرابری رأی‌دهندگان زمانی وارد است که رأی‌گیری تنها به شیوه الکترونیکی انجام شود اما درصورت استفاده هم‌زمان از سایر روش‌های رأی‌گیری چنین اعتراضی وجود نخواهد داشت.

۳-۱۰ هزینه

یکی از مباحث بسیار مهم در مورد لزوم برگزاری انتخابات الکترونیکی، صرفه‌جویی درخصوص نیروی انسانی و تجهیزات مورد نیاز است. تخمین دقیق هزینه برگزاری

---

۱. به فاصله طبقاتی موجود بین اقشار جامعه در استفاده از فناوری اطلاعات و ارتباطات بازمی‌گردد.

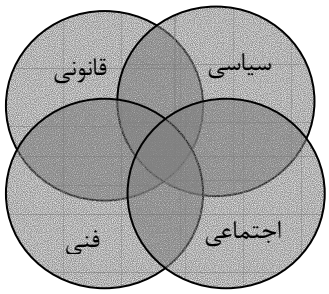
انتخابات الکترونیکی ممکن نیست. علاوه بر هزینه خرید تجهیزات سخت‌افزاری و نرم‌افزاری، هزینه نگهداری و استهلاک این تجهیزات نیز باید مدنظر قرار گیرد. ازطرف دیگر، هزینه‌های پنهان که سنجش کمّی آنها مشکل است نیز باید به سایر هزینه‌ها اضافه گردد. این هزینه‌ها شامل هزینه آموزش پرسنل حوزه‌های انتخاباتی، مدیران سیستم و نیز هزینه شبکه‌های ارتباطی است.

این هزینه برحسب روش‌های رأی‌گیری با یکدیگر متفاوت است. در رأی‌گیری اینترنتی بخشی از این هزینه به رأی‌دهندگان منتقل می‌شود؛ زیرا رأی‌دهنده از رایانه خود استفاده نموده و هزینه برقراری ارتباط را شخصاً می‌پردازد. استفاده از ماشین‌های رأی‌گیری خودکار هزینه زیادی را به‌دنبال دارد، اما این هزینه در طی چند دوره برگزاری انتخابات مستهلک می‌شود.

صرفه‌جویی‌های بالقوه (هزینه تعرفه‌های کاغذی و هزینه منابع انسانی، خصوصاً برای شمارش آرا)، تنها بخش کوچکی از کاهش هزینه بوده و قسمت عمده آن مربوط به هزینه تبلیغات نامزدها پیش از انتخابات است. بنابراین، دو عامل سبب کاهش هزینه انتخابات الکترونیکی نسبت به انتخابات سنتی می‌شود: اولاً انتخابات الکترونیکی از راه دور هزینه‌های مربوط به حوزه‌های انتخاباتی در روش رأی‌گیری سنتی را به‌شدت کاهش می‌دهد. ثانیاً کاندیداها می‌توانند تبلیغات انتخاباتی خود را به‌صورت الکترونیکی انجام دهند که خود منجر به کاهش شدید هزینه‌ها می‌گردد. البته تحقق موارد فوق مستلزم تجهیز منابع و آموزش رأی‌دهندگان خواهد بود.

۱۱-۳ ابعاد

تأکید بیشتر مطالعاتی که تاکنون در زمینه نگرش‌های مختلف رأی‌گیری الکترونیکی انجام شده، بر روی ابعاد فناوری و یا قوانین بوده است، اما در زمینه دمکراسی الکترونیکی علاوه بر دو بعد فنی و قانونی، ابعاد سیاسی و اجتماعی نیز مطرح می‌باشند. بنابراین لازم است که در ابتدا این چهار بعد از یکدیگر مجزا گردد: بعد سیاسی، بعد قانونی، بعد فنی و بعد اجتماعی. این ابعاد در شکل ۲-۳ نشان داده شده است.



شکل ۲-۳ ابعاد انتخابات الکترونیکی

بعد اجتماعی شامل موضوعات زیر است:

ـ سطح تحصیلات افراد،
ـ نوع شغل،
ـ میزان درآمد ماهانه،
ـ وضعیت تأهل،
ـ توزیع سنی جمعیت،
ـ دسترسی به رایانه و تلفن همراه،
ـ میزان استفاده از رایانه و اینترنت،
ـ میزان تراکنش‌های اینترنتی،
ـ سطح مشارکت سیاسی افراد،
ـ میزان گرایش عمومی به استفاده از فناوری‌های اطلاعات و ارتباطات،
ـ شکاف دیجیتالی موجود بین رأی‌دهندگان.

بعد قانونی شامل موضوعات زیر است:

ـ مدت‌زمان برگزاری انتخابات،
ـ رأی‌گیری از افراد خارج از کشور،
ـ نحوه ثبت‌نام کاندیداها و رأی‌دهندگان،
ـ نحوه فعالیت‌های انتخاباتی،
ـ نحوه و زمان شمارش آرا،
ـ آرای سفید و آرای باطل،

ـ تساوی در حق رأی و آزادی انتخاب،
ـ امکان رأی‌دهی برای تمام اقشار جامعه و جلوگیری از رأی‌دهی مجدد آنها،
ـ رعایت تساوی و عدالت در معرفی کاندیداها.

بعد سیاسی شامل موضوعات زیر است:

ـ نوع حکومت (سلطنت مشروطه، جمهوری و ...)،
ـ روش‌های برگزاری انتخابات،
ـ زمان و تعداد برگزاری هر یک از انتخابات،
ـ محل و تعداد حوزه‌های انتخاباتی،
ـ نهاد برگزارکننده و نهاد ناظر انتخابات الکترونیکی،
ـ هدف از برگزاری انتخابات الکترونیکی.

بعد فنی شامل موضوعات زیر است:

ـ فناوری سخت‌افزار،
ـ فناوری نرم‌افزار،
ـ خطوط مخابراتی،
ـ گمنامی رأی‌دهنده،
ـ محرمانگی آرا،
ـ صحت و جامعیت آرا،
ـ پهنای باند اینترنت،
ـ نحوه احراز هویت رأی‌دهندگان (امضای دیجیتالی، کارت شناسایی، کد شناسایی، رمز عبور و ...)،
ـ امنیت و قابلیت اطمینان سیستم،
ـ روش بازشماری آرا.

۱-۱۱-۳ اجتماعی

در این بعد، سطح مشارکت سیاسی افراد، میزان گرایش عمومی افراد به استفاده از فناوری‌های جدید و به‌خصوص رأی‌گیری الکترونیکی مورد بررسی قرار می‌گیرد. همچنین لازم است که اطلاعاتی در مورد میزان استفاده افراد از تلفن، تلفن همراه، رایانه‌های

شخصی، اینترنت، پهنای باند و در نهایت میزان تراکنش‌های اینترنتی به‌دست آوریم.

مطالعات اجتماعی کمک می‌کند که از نظریات شهروندان نیز مطلع شویم و این اطلاعات می‌تواند مرجعی برای مطالعات بعدی باشد. در بسیاری از کشورهای دنیا، پس از برگزاری انتخابات الکترونیکی پرسش‌نامه‌هایی را در اختیار شهروندان قرار می‌دهند. با جمع‌آوری نظرات رأی‌دهندگان می‌توان اطلاعات مفیدی درخصوص نحوه عملکرد فناوری استفاده شده در انتخابات و نقطه‌نظرات شهروندان در زمینه استفاده از فناوری‌های جدید به‌دست آورد. این پرسش‌نامه‌ها می‌تواند از طریق اینترنت و یا فرم‌های چاپی در اختیار افراد قرار بگیرد. مطالعات اجتماعی را می‌توان در دو بعد انجام داد:

۱. **بعد اقتصادی-اجتماعی**: شامل متغیرهایی مانند سطح تحصیلات، موقعیت شغلی، سطح درآمد و ...،

۲. **بعد فنی-اجتماعی**: شامل متغیرهایی مانند دارا بودن رایانه، تلفن همراه، میزان استفاده از اینترنت و... برای آگاهی از سطح سواد اطلاعاتی رأی‌دهندگان.

در بسیاری از کشورهای دنیا، یکی از عوامل مؤثر در پذیرش یا رد استفاده از فناوری‌های جدید، نحوه توزیع جمعیت براساس گروه‌های سنی است. به‌عبارت‌دیگر، در کشورهایی با جمعیت جوان این پدیده با مخالفت زیادی روبه‌رو نیست. سطح تحصیلات، میزان درآمد ماهانه و وضعیت تأهل نیز از جمله عواملی هستند که ارتباط مستقیمی با میزان گرایش افراد به استفاده از فناوری‌های جدید اطلاعات و ارتباطات دارند، به‌طوری‌که صاحبان درآمدهای بالا از رایانه در راستای اهداف شغلی استفاده می‌کنند و صاحبان درآمدهای پایین به تفریح با آن پرداخته و تنها از پست الکترونیک بهره می‌گیرند.

برزیل و هند، دو کشوری هستند که همیشه برگزاری انتخابات در آنها با مشکلات جدی همراه بوده است. ابعاد جغرافیایی، فساد در فرایندهای دمکراتیک، فقر گسترده و بی‌سوادی از جمله چالش‌های مهمی است که این دو کشور با آن مواجه‌اند. اما باوجود این، هردو کشور در حال حاضر در انتخابات از تعرفه‌های الکترونیکی استفاده می‌کنند. به‌عنوان مثال، در برزیل انتخابات با استفاده از مانیتورهای تماسی انجام می‌گیرد و استفاده از این روش مدرن بسیاری از مشکلات مطرح را از بین برده است. با طراحی این مانیتورها که تأکید عمده آن بر استفاده از عناصر گرافیکی مانند تصویر کاندیداهاست، به افراد بی‌سواد نیز فرصت استفاده مؤثر از حق رأیشان داده شده است. ازطرف دیگر، شمارش رایانه‌ای آرا

در این کشورها معضل تبانی در شمارش آرا را تا حد چشمگیری کاهش داده است.

۲-۱۱-۳ قانونی

قبل از تجزیه و تحلیل سیستم‌های مختلف رأی‌گیری الکترونیکی، باید ببینیم که آیا لازم است که ساختار سیستم‌های انتخاباتی جاری را تغییر داده و همگام با آخرین فناوری‌های موجود حرکت کرد؟ چنین ابزارهایی می‌تواند فرایندهای دمکراتیک را غنی‌تر سازد، اما آیا می‌تواند نظام انتخاباتی را از جهات مختلف بهبود بخشد؟ خوش‌بینی ذاتی نسبت به عملکرد فناوری‌های جدید نمی‌تواند پاسخ مثبت و مناسبی برای این سؤال باشد. درواقع قانون انتخابات تنها درصورتی می‌تواند تغییر کند که بتوان ثابت نمود ابزارهای جدید روند انتخابات را تسهیل کرده و ضمن افزایش صحت و دقت، میزان مشارکت عمومی را نیز افزایش می‌دهد.

نوع نظام قانونی هر کشور، عنصر اساسی این بعد را تشکیل می‌دهد. قانون انتخابات در هر کشور مبنای انتخاب راه‌حل‌های فنی برای برگزاری انتخابات الکترونیکی است، یعنی روشی که از طریق آن می‌توان رأی‌گیری الکترونیکی را برگزار نمود.

تغییر قانون انتخابات ــ درصورت برگزاری آن به‌صورت الکترونیکی ـــ بستگی به نوع و گستردگی انتخابات سیاسی دارد. از جمله مواد قانونی که نیاز به اصلاح و بازنگری خواهد داشت، می‌توان این موارد را نام برد: مدت‌زمان برگزاری انتخابات، نحوه احراز هویت افراد، رأی‌گیری از افرادی که در خارج از کشور زندگی می‌کنند، حوزه‌های اخذ رأی، نحوه ثبت‌نام کاندیداها و رأی‌دهندگان، نحوه فعالیت‌های انتخاباتی کاندیداها، نحوه و زمان شمارش آرا و بسیاری از موارد دیگر.

طبق قانون انتخابات سنتی، آرای سفید، تعرفه‌های کاغذی خط خورده، ناخوانا و تعرفه‌هایی که در آنها به‌جای نام یک نفر نام چند نفر درج شده، به‌عنوان رأی باطل تلقی می‌گردد. اما در رأی‌گیری الکترونیکی مکانیزم‌هایی وجود دارد که از طریق آن می‌توان این‌گونه خطاها را به حداقل ممکن کاهش داد. ذکر این نکته ضروری است که در انتخابات سنتی رأی‌دهنده می‌تواند با انگیزه‌های مختلف ــ عمداً و آگاهانه ــ یک رأی باطل و یا سفید را در صندوق رأی بیندازد. بنابراین، اگر این امکان طبق قانون در انتخابات سنتی به

شهروندان داده می‌شود، نباید در انتخابات الکترونیکی نادیده گرفته شود. در نتیجه، این عامل نیز در قانون انتخابات الکترونیکی باید مدنظر قرار گرفته و در روی صفحه نمایش مانیتور در کنار سایر گزینه‌ها، گزینه‌ای تحت‌عنوان رأی سفید درنظر گرفته شود.

یکی دیگر از ابعاد حائز اهمیت قانون انتخابات، تساوی حق رأی افراد است. در سیستم‌های رأی‌گیری الکترونیکی نیز برای رعایت این اصل باید موارد ذیل مدنظر قرار گیرد:

۱. امکان رأی‌دهی برای همه اقشار جامعه و جلوگیری از رأی‌دهی مجدد رأی‌دهندگان،

۲. رعایت تساوی و عدالت در معرفی کاندیداها،

۳. از بین بردن شکاف دیجیتالی موجود در بین رأی‌دهندگان.

امروزه پروتکل‌های مختلفی طراحی شده که مانع از رأی‌دهی چندباره افراد می‌گردد. ازطرف دیگر، در سیستم‌های رأی‌گیری الکترونیکی نمایش کاندیداها در روی فرم‌های الکترونیکی باید کاملاً بی‌طرفانه و با رعایت اعتدال صورت پذیرد. برخی از مشخصه‌های فیزیکی صفحه نمایش (مثل محل قرار گرفتن تصویر، رنگ، اندازه و ...) می‌تواند روی انتخاب رأی‌دهندگان تأثیر گذارده و به قانون رعایت مساوات در معرفی کاندیداها خدشه وارد کند. بنابراین، زمانی که تعداد کاندیداها زیاد بوده و نمی‌توان تصویر آنها را در روی یک صفحه نشان داد چه باید کرد؟ آیا می‌توان تصاویر آنها را در صفحات متوالی قرار داد؟ آیا این روش، اصل برابری و تساوی را نقض نمی‌کند؟ درواقع حتی اگر اکثریت جامعه از سواد اطلاعاتی بالا برخوردار بوده و بتوانند کاندیدای مورد نظر خود را با مرور صفحات انتخاب کنند، باز هم ازنظر روانی کاندیداها ترجیح می‌دهند که در صفحات نخست معرفی گردند. یکی از راه‌حل‌های پیشنهادی این است که هر صفحه نمایش شامل اسامی و یا تصویر کاندیداهای احزاب مختلف باشد. به‌این‌ترتیب رأی‌دهنده ناچار است که تمامی صفحات را مرور نماید.

۳-۱۱-۳ سیاسی

در این زمینه لازم است که اطلاعات کافی در موارد زیر حاصل شود:

۱. نوع حکومت کشور (سلطنت مشروطه، جمهوری و ...)،

۲. روش‌های برگزاری انتخابات، زمان و تعداد دفعات برگزاری هر یک از انتخابات (تعداد رأی‌دهندگان واجد شرایط، حوزه‌های انتخاباتی و ایستگاه‌های رأی‌گیری)،

۳. نقطه‌نظر بسیار مهم دیگر، نگرش دولتمردان به رأی‌گیری الکترونیکی است. اینکه آیا در فرایند سیاست‌گذاری درنظر گرفته شده است یا خیر؟ هدف از این سیاست چه بوده است؟ و آیا سازمانی رسمی برای برگزاری رأی‌گیری الکترونیکی درنظر گرفته شده است؟

۴-۱۱-۳ فنی

در این بُعد، فناوری سخت‌افزار، سرورهای رأی‌گیری، کارت‌های شناسایی ملی، امضای دیجیتالی، خطوط مخابراتی و ... مورد بررسی قرار می‌گیرد. موضوعات مطرح در بُعد فنی تنها در انتخابات اینترنتی از راه دور از اهمیت ویژه‌ای برخوردار است و در شرایطی که رأی‌دهندگان از ماشین‌های رأی‌گیری مستقر در حوزه‌های انتخاباتی استفاده می‌کنند، چندان تأثیرگذار نمی‌باشد.

پی‌نوشت‌ها

1. R. Mercuri, P.G. Neumann, *Verification for Electronic Balloting Systems, Secure Electronic Voting,* (Ed. Gritzalis, D.A.), Kluwer, Boston, pp. 31– 42, 2003.
2. B. Watt, Ibid.
3. L. Mitrou, D. Gritzalis, S. Katsikas, G. Quirchmayr, *Electronic Voting: Constitutional and Legal Requirements, and Their Technical Implications, Secure Electronic Voting,* (Ed. Gritzalis, D.A.), Kluwer, Boston, pp. 43-60, 2003.

فصل چهارم

روش‌های تحقق انتخابات الکترونیکی در برخی کشورها

به‌منظور نیل به راهکارهای مناسب برای پیاده‌سازی انتخابات الکترونیکی در یک کشور، لازم است که تجربیات سایر کشورها در این خصوص مورد ارزیابی قرار گرفته و ضمن بررسی چالش‌های پیش رو و راهکارهای ارائه شده در این کشورها، مدل مناسبی برای کشورمان تدوین گردد.

۱-۴ اسپانیا

در این قسمت به بررسی انتخابات الکترونیکی در کشور اسپانیا همراه با بررسی عملکرد ترمینال‌های رأی‌گیری و مشکلات و راه‌حل‌های ارائه شده در این خصوص می‌پردازیم.

۱-۱-۴ تجزیه و تحلیل عملکرد ترمینال‌های رأی‌گیری

در کشور اسپانیا ترمینال‌های رأی‌گیری با ثبت مستقیم، برای ثبت و ذخیره آرای الکترونیکی طراحی شده است. مزیت عمده این ترمینال‌ها آن است که مانع خطای غیرعمدی کاربران شده و امکان مشارکت افراد معلول را افزایش می‌دهد. این ویژگی به همراه سایر ویژگی‌ها سبب گسترش استفاده از این روش در حوزه‌های انتخاباتی شده است.[۱]

استفاده از ترمینال‌های رأی‌گیری در کشورهایی مانند آمریکا، هلند و برزیل با استقبال فراوانی مواجه شده است. در پی اشکالاتی که در انتخابات ریاست‌جمهوری آمریکا در سال ۲۰۰۰ ــ در اثر خطاهای کارت‌های پانچ و دستگاه‌های اسکن نوری ــ به‌وقوع پیوست، استفاده از این ترمینال‌ها به‌شدت مورد توجه دست‌اندرکاران قرار گرفت. در حال حاضر تقریباً یک‌سوم جمعیت آمریکا در انتخابات از ترمینال‌های رأی‌گیری استفاده می‌کنند، درحالی‌که در هلند و برزیل این آمار به‌ترتیب در حدود ۹۵ درصد و

۱۰۰ درصد می‌باشد. استفاده از این ترمینال‌ها بسیاری از مشکلات سیستم‌های قبلی را مرتفع نموده است؛ چرا که:

اولاً ترمینال‌های رأی‌گیری مانع از هدررفتن آرایی است که به‌دلیل خطاهای غیرعمد باطل اعلام می‌شوند.

ثانیاً ترمینال‌های رأی‌گیری سبب سهولت دسترسی افراد معلول از جمله افراد نابینا می‌شود. این افراد می‌توانند بدون نیاز به کمک دیگران با استفاده از یک «گوشی» که به ترمینال متصل است، آرای خود را ارسال کرده و تأییدیه آن را دریافت نمایند.

در نهایت، فرایند شمارش آرا با استفاده از ترمینال‌های رأی‌گیری سریع‌تر و دقیق‌تر صورت می‌گیرد؛ زیرا رأی‌های الکترونیکی مستقیماً پردازش شده و نیازی به خواندن آرا به‌صورت فیزیکی (مثلاً با استفاده از اسکنرهای نوری) نیست.

باوجود تمامی این مزایا، اتفاقاتی که در سالیان گذشته در نتیجه استفاده از این دستگاه‌ها حاصل شده، اعتمادپذیری و دقت این دستگاه‌ها را زیر سؤال برده است. به‌دلیل انتقادات وارده به ناکافی بودن مکانیزم‌های تأیید هویت رأی‌دهنده، تأیید صحت آرا و پیچیدگی ترمینال‌های رأی‌گیری، مقتضی است راه‌حل‌هایی برای افزایش قابلیت اعتماد این ترمینال‌ها ارائه گردد.

تحقیقات و پژوهش‌های انجام شده درخصوص نقایص امنیتی این سیستم‌ها، سبب ایجاد نگرانی در بین دست‌اندرکاران انتخابات شده است. علاوه بر این، عدم شفافیت عملیات رأی‌گیری، سبب افزایش شک وتردید درخصوص امنیت و صحت این‌گونه سیستم‌ها شده است. در اینجا برخی از انتقادات وارده به ترمینال‌های رأی‌گیری را مورد بررسی قرار می‌دهیم:

یکی از بارزترین انتقادات وارده، مربوط به عدم شفافیت فرایند رأی‌گیری ازنظر رأی‌دهندگان است. در یک سیستم رأی‌گیری سنتی که از تعرفه کاغذی استفاده می‌کند، رأی‌دهندگان مطمئن‌اند که آرایشان به صندوق ریخته شده است، چون خودشان تعرفه‌ها را نوشته و در صندوق می‌اندازند. البته توجه به این نکته ضروری است که هیچ تضمینی وجود ندارد که آرا در کمال صحت شمارش شود. در نتیجه، رأی‌دهندگان ناچارند به سلامت ناظران انتخابات اعتماد کنند.

اما در سیستم‌های رأی‌گیری که از ترمینال‌های رأی‌گیری استفاده می‌کنند، رأی‌دهندگان نمی‌توانند به‌صورت چشمی ثبت و ذخیره آرای خود را کنترل کنند؛ زیرا فرایند رأی‌دهی به‌صورت الکترونیکی انجام می‌شود. بنابراین، مکانیزمی لازم است تا با استفاده از آن بتوان این اعتماد را در رأی‌دهندگان به‌وجود آورد.

انتقاد بعدی مربوط به محدودیت‌های موجود در قابلیت ردیابی فرایندهای مختلف سیستم می‌باشد. در بسیاری از موارد به‌دلیل استفاده از روش‌های ماهرانه برنامه‌نویسی امکان ردیابی کدهای برنامه وجود ندارد. در نتیجه، رأی‌دهندگان نسبت به عملیاتی که در پشت پرده اتفاق می‌افتد کاملاً بدگمان خواهند بود.

ازطرف دیگر، در این سیستم‌ها امکان بازشماری آرا، مستقل از نتایج ترمینال‌های رأی‌گیری وجود ندارد. این نقطه‌ضعف سبب ایجاد اعتماد کورکورانه در بین رأی‌دهندگان خواهد شد.

انتقاد دیگر درخصوص پیچیدگی فرایند تأیید انتخابات به‌وسیله مسئولان مربوطه است. ترمینال‌های رأی‌گیری، دستگاه‌های پیچیده‌ای‌اند که کلیه عملیات مربوط به انتخابات در داخل آنها انجام می‌شود، از جمله پیکربندی، نمایش گزینه‌های انتخابی بر روی صفحه نمایش، انتخاب و تأیید گزینه‌های مورد نظر، رأی‌دهی و شمارش آرا. این پیچیدگی سبب ایجاد ناهنجاری و بی‌نظمی‌های مخفی در داخل ترمینال‌ها شده و شناسایی و ردیابی کدهای برنامه را مشکل می‌کند.

بنابراین، لازم است صحت و جامعیت عملکرد سیستم حتی پس از ردیابی فرایندهای آن همچنان دست‌نخورده باقی بماند.

امکان تغییرات در دقایق نهایی (که از مزایای سیستم است)، فرایند انتخابات را مشکل‌تر می‌سازد؛ زیرا صحت این تغییرات باید به‌سرعت مورد بررسی قرار گیرد.

معیارهای امنیتی به‌کارگرفته شده در این سیستم‌ها یکی دیگر از نقاط ضعف این سیستم می‌باشد. در بسیاری از موارد این معیارها کافی نبوده و امنیت فرایند انتخابات را تضمین نمی‌کند.

۲-۱-۴ راه‌حل‌های امنیتی ارائه شده و نقایص آنها

با توجه به انتقادات مطرح شده، متخصصان و محققان روش‌هایی را برای تضمین امنیت

لازم در ترمینال‌های رأی‌گیری ارائه نموده‌اند. اولین راه‌حل ارائه شده، نگهداری رکوردهای چاپی به موازات رأی‌گیری الکترونیکی است. هدف از ارائه این راه‌حل، ثبت رأی پس از تأیید رأی‌دهندگان توسط خود آنها و چاپ فیزیکی یک رکورد به‌عنوان رسید می‌باشد. در این روش گزینه‌های انتخابی در روی صفحه نمایش ترمینال‌های رأی‌گیری نمایش داده شده و پس از انتخاب رأی‌دهنده، گزینه انتخابی بر روی کاغذ چاپ می‌گردد. بنابراین، رأی‌دهندگان می‌توانند گزینه‌های چاپ شده را با گزینه‌های انتخابی خود بر روی صفحه نمایش مطابقت دهند. درصورت تأیید، رأی به‌صورت الکترونیکی ذخیره شده و نسخه چاپی آن نیز در صندوق فیزیکی انتخابات ریخته می‌شود. در خاتمه انتخابات، صحت نتایج آرای الکترونیکی ذخیره شده در ترمینال‌های رأی‌گیری را می‌توان با بازشماری رسیدهای چاپی موجود در صندوق‌های رأی کنترل نمود.

اگرچه راه‌حل ارائه شده به رأی‌دهندگان امکان می‌دهد که صحت آرای خود را تأیید کنند، اما مشکلاتی را نیز به‌دنبال دارد. در این روش امکان تأیید رأی برای افراد نابینا وجود ندارد. ازطرف دیگر، درصورت مشاهده مغایرت در تعداد رسیدهای کاغذی و آرای الکترونیکی، نمی‌توان تعیین کرد که اشکال مربوط به کدام قسمت می‌باشد. به‌عبارت دیگر، نمی‌توان به‌طور یقین اعلام نمود که نتایج صحیح مربوط به صندوق حاوی رسیدهای کاغذی است یا مربوط به آرای الکترونیکی و یا هیچ‌یک از آنها. محتاطانه نیست که همیشه فرض را بر صحت تعداد آرای کاغذی بگذاریم؛ زیرا در این روش نیز امکان تقلب در آرا وجود دارد.

دومین راه‌حل به تقلید از سیستم‌های سنتی، استفاده از یک حافظه قابل حمل[1] (مانند کارت‌های هوشمند) می‌باشد، به‌طوری‌که گزینه انتخابی فرد رأی‌دهنده پس از رأی‌دهی در این کارت ذخیره می‌گردد. به‌دلیل امکان شمارش موازی آرا، پس از رأی‌دهی، این کارت‌ها توسط فرد رأی‌دهنده در صندوق ریخته می‌شود. در این روش از یک ترمینال اضافی استفاده می‌شود. در نتیجه، دو فرایند مختلف، یعنی فرایند انتخاب گزینه و فرایند رأی‌دهی از هم جدا می‌شود. در این طرح برخلاف طرح قبلی، امکان تأیید رأی توسط افراد نابینا نیز وجود دارد. علاوه بر آن، معماری این طرح به‌گونه‌ای

1. Removable Card

است که ردیابی کلی سیستم را آسان می‌کند.

علی‌رغم مزایای گفته شده، این سیستم عاری از عیب نیست. به‌عنوان مثال، استفاده از حافظه متحرک می‌تواند امکان فروش آرا و نیز اعمال فشار به رأی‌دهندگان را فراهم کند؛ زیرا رأی‌دهنده می‌تواند محتوای حافظه را قبل از رأی دادن به دیگران نشان دهد. به‌علاوه، سیستم همچنان با مشکلات سیستم‌های سنتی از جمله دستکاری آرای فیزیکی مواجه بوده و قابلیت تشخیص عامل ایجاد مغایرت در هنگام شمارش موازی آرا را ندارد.

راه‌حل نهایی، مبتنی‌بر استفاده از ابزارهای رمزنویسی برای تأیید آراست. مزیت اصلی استفاده از پروتکل‌های رمزنگاری، این است که نه تنها به رأی‌دهنده امکان تأیید صحت رأیش را می‌دهد، بلکه می‌توان مطمئن شد که رأی مربوطه در فرایند شمارش شرکت داشته است و یا خیر. این روش به لحاظ تئوری، محرمانگی و جامعیت فرایندهای الکترونیکی را تضمین می‌کند، اما در عمل، تا حدود زیادی امنیت آن به امنیت سیستم (امنیت ترمینال‌های رأی‌گیری) بستگی دارد.

ازطرف دیگر، عملیاتی کردن این طرح در برخی از موارد بسیار مشکل است؛ زیرا برای ایجاد و تأیید رسیدهای چاپی، تجهیزات پیچیده‌ای مورد نیاز می‌باشد. به‌دلیل مشکلات یادشده، این روش برای انتخابات عمومی گسترده چندان مناسب نیست.

به‌عبارتی، راه‌حل‌های ارائه شده از نقطه‌نظر تئوری بدون عیب و نقص به‌نظر می‌رسند، اما در عمل با مشکلات عدیده‌ای مواجه‌اند. در ادامه، راه‌حل جدیدی ارائه می‌شود که به‌طور چشمگیری پیچیدگی ردیابی فرایندها در ترمینال‌های رأی‌گیری را کاهش داده و به رأی‌دهندگان امکان می‌دهد که بتوانند قبل از ثبت، آرای خود را تأیید کنند. طرح پیشنهادی معیارهای امنیتی لازم را برای تضمین محرمانگی، صحت و جامعیت آرا به‌کار می‌گیرد.

۳-۱-۴ طرح رمزنگاری با استفاده از سیستم تأیید[۱]

همان‌طورکه در قسمت‌های قبل توضیح داده شد، در یک انتخابات مبتنی‌بر ترمینال‌های رأی‌گیری، رأی‌دهندگان گزینه‌های خود را انتخاب، تأیید و سپس در همان ترمینال

---

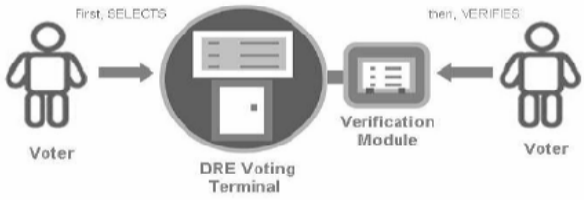
۱. Verification Module در ادامه به اختصار ماجول VM نوشته می‌شود.

رأی نهـایی خـود را ثبـت مـی‌کننـد. آرای داده شـده تـا پایـان مرحلـه شـمارش آرا در ترمینال‌ها ذخیره می‌شوند. در این حالت، هیچ نسخه دومی از آرا وجود ندارد. در نتیجـه جامعیت و صحت انتخابات به صحت عملکرد ترمینال‌ها بستگی خواهد داشت.

یـک گـروه تحقیـق و توسـعه در کشـور اسـپانیا[1] بـرای رفـع نـواقص موجـود در ترمینال‌های رأی‌گیری، طرحی را ارائه نمـوده‌انـد. اجـرای ایـن طـرح بـه رأی‌دهنـدگان اطمینان می‌دهد که رأی آنهـا بـه‌صـورت صـحیح ثبـت شـده و در نهایـت یـک فراینـد دمکراتیک امن و سالم را تضمین می‌کند.

طرح پیشنهادی برمبنای استفاده از یک سیستم سخت‌افزاری به نام «ماجول[2] تأیید» و یک پروتکل رمزنگاری تهیه شده است. ماجول تأیید، سخت‌افزار ساده‌ای دارد شامل یک صفحه نمایش، یک خروجی صدا و دو دکمه فشاری (دکمه تأیید و دکمه انصراف).

ماجول تأیید به رأی‌دهنده امکان می‌دهد تا قبل از ثبت نهایی، رأی خـود را تأییـد کند. همچنین این دستگاه شامل یـک حافظـه داخلـی بـرای ذخیـره آرای تأییـد شـده می‌باشد. از دیگر امکانات این دستگاه، توانایی رمزنگاری به‌منظور حفاظت از آرای تأییـد شده و حفظ امنیت فرایندهای الکترونیکی است. ماجول تأییـد بـه ترمینـال رأی‌گیـری متصل است و به رأی‌دهنده امکان تأیید رأیش را می‌دهد. پروتکل رمزنگـاری موجـود در این ماجول، رأی‌ها را در مقابل دست‌کاری و تغییرات بعدی محافظـت مـی‌کنـد. فراینـد رأی‌دهی مطابق شکل ۱-۴ می‌باشد:



شکل ۱-۴ فرایند رأی‌گیری در ترمینال رأی‌گیری

1. Scytl Group

۲. ماجول: در سخت افزار، قطعه مستقلی است که می‌تواند عمل کاملی را برای سیستم انجام دهد و می‌تـوان آن‌را با قطعات دیگری که عملکرد مشـابه دارنـد، تعـویض کـرد. در برنامـه‌نویسـی، مجموعـه‌ای از توابـع و سـاختمان داده‌هاست که کار مشخصی را انجام می‌دهد.

در ابتدا رأی‌دهنده با ترمینال رأی‌گیری ارتباط برقرار نموده و پس از مشاهده گزینه‌های مختلف روی صفحه نمایش، گزینه مورد نظر را انتخاب می‌کند. این انتخاب از ترمینال رأی‌گیری به ماجول تأیید فرستاده می‌شود. سپس رأی‌دهنده به‌صورت چشمی و یا به‌وسیله «هدستی» که به خروجی صدا در ماجول تأیید متصل است، رأی خود را تأیید می‌کند. درواقع کنترل می‌کند که گزینه انتخاب شده در ترمینال رأی‌گیری با اطلاعات منتقل شده به ماجول تأیید مطابقت دارد یا نه. در صورت تطابق، رأی‌دهنده به کمک دکمه تأیید انتخاب خود را تأیید می‌کند، در غیر این صورت، با فشردن کلید انصراف، فرایند رأی‌دهی مجددا از ترمینال رأی‌گیری آغاز می‌گردد.

در صورت تأیید رأی، رأی داده شده توسط تکنیک‌های رمزنگاری به‌صورت کد درمی‌آید. پس از خاتمه مهلت انتخابات، آرای موجود در ترمینال رأی‌گیری به مرکز شمارش آرا منتقل می‌شود (در بسیاری از موارد عمل شمارش آرا نیز در این ترمینال انجام می‌شود).

استفاده از ماجول تأیید بدون نیاز به بررسی صحت عملکرد ترمینال‌های رأی‌گیری، صحت نتایج را تضمین می‌کند. در نتیجه، نیازی به ردیابی و کنترل تمامی سیستم‌های درگیر در انتخابات نیست. ردیابی و کنترل ماجول تأیید (که یک دستگاه ساده است) برای کنترل کل سیستم کافی است. ازآنجاکه فرایندهای انجام شده در ماجول تأیید بسیار ساده‌تر از فرایندهای مربوط به ترمینال رأی‌گیری می‌باشد، در مجموع، ردیابی فرایندها، نظارت و تأیید آنها نیز ساده‌تر خواهد بود. به‌علاوه، در هنگام اجرای انتخابات، رأی‌دهندگان نقش نظارتی مهمی را ایفا می‌کنند؛ زیرا در حین رأی‌دهی می‌توانند صحت عملکرد ترمینال را تأیید کنند. این ویژگی سبب افزایش اعتماد رأی‌دهندگان به سیستم انتخاباتی می‌شود.

پروتکل رمزنگاری به‌کار رفته در ماجول تأیید، محرمانگی و جامعیت آرا را تضمین می‌کند. فرایند حفاظت آرا، پس از تأیید رأی توسط رأی‌دهنده، در ماجول تأیید انجام می‌شود که شامل امضای دیجیتالی آرا به‌وسیله کلیدهای اختصاصی می‌باشد.

مدیریت این کلیدهای اختصاصی به‌عهده اعضای شورای انتخابات در هر حوزه می‌باشد. به‌علاوه، رمزگشایی کلید اختصاصی، مستلزم گشودن پاکت‌های دیجیتالی

توسط اعضای شوراست.

پاکت‌ها با امضای دیجیتالی، از ماجول تأیید به ترمینال رأی‌گیری فرستاده شده و یک نسخه از آن در ماجول باقی می‌ماند. وجود این نسخه، امکان شمارش موازی آرا را فراهم می‌کند.

باز کردن پاکت‌های الکترونیکی، به‌وسیله یک فرایند پیچیده توسط اعضای شورا صورت می‌گیرد. استفاده از روش‌های پیچیده، محرمانگی آرای خوانده شده را تضمین کرده و مانع از کشف ارتباط بین آرا و توالی آنها می‌شود.

۴-۱-۴ معماری طرح جدید

همان‌طورکه گفته شد، راه‌حل پیشنهادی عمدتاً برمبنای اضافه کردن یک سخت‌افزار ساده و ایمن به هر ترمینال رأی‌گیری می‌باشد. این سخت‌افزار که ماجول تأیید نامیده می‌شود، آرای تأیید شده را رمز نموده و امضای دیجیتالی را به آن اضافه می‌کند. در ضمن، یک نسخه از آرا در این ماجول نگهداری می‌شود.

علاوه بر این ماجول، دو ماجول دیگر برای پیکربندی ماجول تأیید و بازیابی آرای داده شده مورد نیاز می‌باشد. این دو ماجول، ماجول پیکربندی[1] و ماجول بازگشا[2] نامیده می‌شوند و می‌توانند به تنهایی برای یک حوزه انتخاباتی، گروهی از حوزه‌ها و یا حتی در سراسر حوزه‌های انتخاباتی مورد استفاده قرار گیرند.

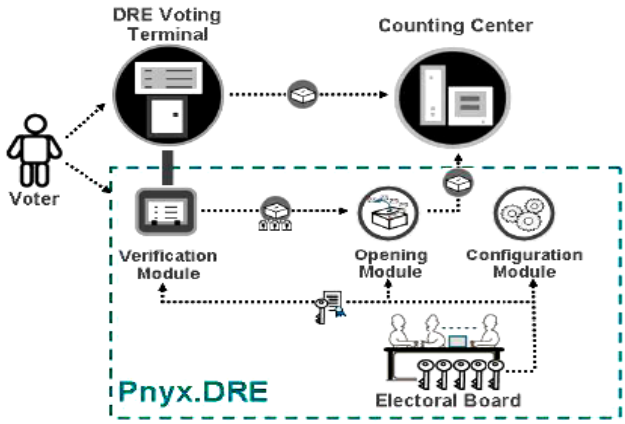
پارامترهای مورد نیاز برای پیکربندی (تنظیمات اولیه) سیستم‌های درگیر در انتخابات در ماجول پیکربندی تعریف می‌شود. ماجول بازگشا برای بازیابی آرای رمزشده و کنترل صحت و دقت نتایج به‌کار می‌رود. ازنظر فیزیکی این دو ماجول می‌توانند دو دستگاه کاملاً مستقل باشند، اما به‌دلیل سادگی معماری طرح، بهتر است در کنار هم و در یک سیستم نصب گردند. شکل ۲-۴ نحوه هم‌بندی ماجول‌های مختلف و ارتباط آنها را با یکدیگر نشان می‌دهد.

ماجول پیکربندی، پارامترهای مورد نیاز برای پروتکل‌های رمزنگاری را ایجاد می‌کند. یکی از مهم‌ترین پارامترهای امنیتی فرایند رأی‌گیری الکترونیکی، کلید اختصاصی

---

1. Configuration Module
2. Opening Module

انتخابات است، که برای باز کردن پاکت‌های دیجیتالی حاوی آرا به‌کار می‌رود.



شکل ۲-۴ معماری کلی طرح

بخش‌های مختلف کلید اختصاصی به‌وسیله یک برنامه رمزنگاری مخفی در اختیار اعضای شورای انتخابات قرار می‌گیرد. به‌عبارت دیگر، کلید اختصاصی تنها در اختیار یک فرد نیست. ماجول پیکربندی به‌جز یک رایانه استاندارد، به سخت‌افزار خاصی نیاز ندارد. به‌منظور حفظ امنیت سیستم انتخاباتی لازم است که این ماجول از سایر بخش‌های سیستم جدا بوده و تنها به عملیات رمزنگاری اختصاص یابد. این ماجول کاملاً مستقل بوده و هیچ ارتباطی با سایر شبکه‌های ارتباطی ندارد.

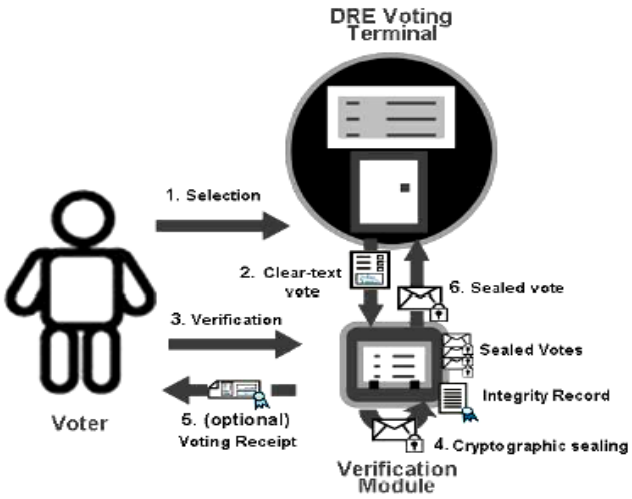
ماجول بازگشا پس از خاتمه انتخابات، آرای رمزشده توسط ماجول تأیید را بازخوانی می‌کند. به‌دلیل توزیع بخش‌های مختلف کلید اصلی بین اعضای شورای انتخابات و استفاده از پروتکل‌های پیچیده برای استخراج نتایج، محرمانگی رأی‌دهندگان کاملاً محفوظ می‌ماند، به‌طوری که نمی‌توان هیچ‌گونه ارتباطی بین آرا و ترتیب رأی‌دهندگان کشف نمود.

ماجول بازگشا نیز مشابه ماجول پیکربندی به سخت‌افزار خاصی نیاز ندارد. تنها به منظور حفظ امنیت سیستم، باید مستقل از سایر شبکه‌های ارتباطی قرار بگیرد. به‌این‌ترتیب با قرار دادن این دو ماجول در یک سیستم مجزا، امنیت در این طرح به

حداکثر ممکن می‌رسد. ماجول تأیید از طریق پورت «یو‌اس‌بی» و یا پورت سریال به ترمینال رأی‌گیری متصل می‌شود.

۵-۱-۴ مراحل رأی‌گیری

قبل از آغاز فرایند رأی‌گیری (شکل ۳-۴)، تنظیمات اولیه ماجول تأیید مورد بررسی قرار می‌گیرد تا از صحت اطلاعات و مقداردهی اولیه آنها طبق مقررات، اطمینان حاصل گردد (به‌طور مثال همه رکوردها خالی باشند). پس از انجام این کنترل، ماجول تأیید به ترمینال رأی‌گیری متصل می‌شود.



شکل ۳-۴ مراحل فرایند رأی‌دهی در ترمینال رأی‌گیری

رأی‌دهنده فرایند رأی‌دهی را در ترمینال رأی‌گیری آغاز می‌کند. به‌این‌ترتیب که ابتدا گزینه‌های مورد نظر خود را در ترمینال رأی‌گیری انتخاب می‌نماید. این گزینه‌ها به ماجول تأیید فرستاده می‌شود. گزینه‌های انتخاب شده در روی یک صفحه نمایش در ماجول تأیید نشان داده می‌شود (در بعضی از مواقع از طریق یک «هدست» متصل به خروجی صدا شنیده می‌شود). در نتیجه، رأی‌دهنده می‌تواند گزینه انتخابی خود را در

ترمینال رأی‌گیری با رکورد ارسالی به ماجول تأیید کنترل کند. در این مرحله رأی‌دهنده می‌تواند هرگونه خطایی را کشف نموده و از صحت ارسال رأیش به صندوق الکترونیکی اطمینان حاصل کند.

اگر رأی‌دهنده گزینه‌های نشان داده شده را تأیید نکند، می‌تواند با فشردن دکمه «لغو» عملیات را لغو نموده و مجدداً فرایند رأی‌دهی را از ترمینال رأی‌گیری آغاز کند. اگر مشکل همچنان باقی بود، نشان‌دهنده وجود خطا در ترمینال رأی‌گیری است که می‌بایست به اطلاع مسئولان حوزه‌ها برسد.

اگر رأی‌دهنده گزینه‌های نشان داده شده را تأیید کند، رأی به‌وسیله کلید عمومی انتخابات رمزگذاری می‌شود و از طریق یک پاکت دیجیتالی مهروموم شده ارسال می‌گردد. بازخوانی رمز پاکت‌های دیجیتالی تنها به‌کمک کلیدهای اختصاصی امکان‌پذیر است. کلید اختصاصی در مرحله پیکربندی ایجاد شده، به بخش‌های مختلف تقسیم و هر بخش آن در اختیار یکی از اعضای شورای انتخابات قرار می‌گیرد و پس از توزیع، کلید اولیه از بین می‌رود.

پس از تأیید رأی، پاکت دیجیتالی حاوی رأی به‌وسیله کلید اختصاصی ماجول تأیید، امضای دیجیتالی می‌شود. از این لحظه به بعد، این امضای دیجیتالی محرمانگی و جامعیت آرا را تضمین می‌کند. کلیدهای اختصاصی به‌کارگرفته شده در امضاهای دیجیتالی، توسط مسئولان انتخابات مدیریت شده و در مرحله پیکربندی در ماجول تأیید قرار می‌گیرند.

در مرحله بعد، رأی رمزشده با امضای دیجیتالی به ترمینال رأی‌گیری برگشته و در ترمینال رأی‌گیری ذخیره می‌گردد. به‌منظور کنترل صحت نتایج آرا، هم‌زمان با شمارش آرای دیجیتالی موجود در ترمینال رأی‌گیری، نسخه موجود در ماجول تأیید نیز مورد شمارش قرار می‌گیرد.

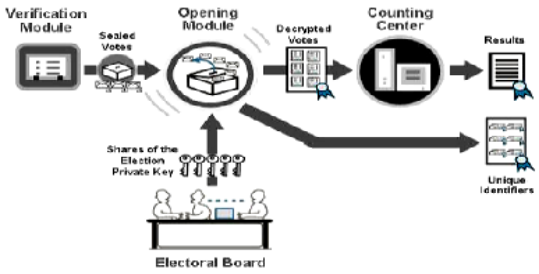
از دیگر امکانات ماجول تأیید، چاپ رسید برای رأی‌دهندگان است. هر رسید حاوی یک شناسه منحصربه‌فرد تصادفی است که به‌وسیله ماجول تأیید ایجاد، به همراه رأی امضای دیجیتالی شده و در پاکت دیجیتالی قرار می‌گیرد. به‌این‌ترتیب، امکان چاپ رسیدهای جعلی و نیز شکایات قلابی منتفی می‌شود.

رسیدهای چاپی به رأی‌دهندگان اطمینان می‌دهد که رأیشان در هنگام شمارش آرا حضور داشته است؛ زیرا پس از بازشدن پاکت‌های دیجیتالی توسط ماجول بازگشا، لیستی از شناسه‌های موجود در پاکت‌ها به‌صورت لیست چاپ شده و در حوزه‌ها نصب می‌گردد. بنابراین، رأی‌دهنده ضمن انطباق شناسه موجود در رسید چاپی خود و شناسه‌های موجود در این لیست‌ها می‌تواند از صحت انتخابات اطمینان حاصل نماید.

پس از پایان انتخابات، ماجول تأیید رأی‌دهی را متوقف نموده و پس از امضای دیجیتالی صندوق‌های دیجیتالی حاوی آرا، آنها را جهت رمزگشایی به ماجول بازگشا ارسال می‌کند.

۶-۱-۴ شمارش آرا

فرایند شمارش با استفاده از صندوق‌های الکترونیکی موجود در ترمینال رأی‌گیری انجام می‌شود. در ابتدا پاکت‌های دیجیتالی با استفاده از کلیدهای اختصاصی که در اختیار اعضای شورای انتخابات است، رمزگشایی می‌گردد. هم‌زمان با رمزگشایی پاکت‌های دیجیتالی، ترتیب آرا نیز به‌صورت تصادفی تغییر می‌کند (به‌طور مثال از طریق مخلوط شدن آرا)، تا محرمانگی آرا به‌صورت تمام و کمال تضمین گردد. همان‌طور که قبلاً بیان شد، کلید اختصاصی به‌صورت بخش‌های مجزا در اختیار اعضای شورای انتخابات قرار می‌گیرد. بنابراین، حضور کلیه اعضای شورا برای بازسازی مجدد کلید اختصاصی در هنگام رمزگشایی و شمارش آرا ضروری است. فرایند شمارش آرا در شکل ۴-۴ نشان داده شده است.



شکل ۴-۴ فرایند شمارش آرا در ترمینال رأی‌گیری

۴-۱-۷ فرایند ردیابی و نظارت

فرایند ردیابی،[1] نظارت و کنترل در طرح پیشنهادی، مبتنی‌بر تأیید صحت عملکرد دستگاه‌های فیزیکی و منطقی استفاده شده در انتخابات از جمله ترمینال‌های رأی‌گیری، کنترل بخش‌های مختلف شبکه‌های ارتباطی و رویه‌های اجرایی است. در این طرح، فرایند ردیابی بر روی سه جزء جداگانه به‌خصوص بر روی ماجول تأیید انجام می‌پذیرد.

ماجول تأیید به رأی‌دهندگان امکان می‌دهد که گزینه انتخابی خود در ترمینال رأی‌گیری را قبل از ثبت و ذخیره، تأیید نمایند. به این‌معنی که کنترل صحت عملکرد ترمینال رأی‌گیری توسط خود رأی‌دهنده انجام می‌شود.

هزینه و زمان ردیابی سیستم در این طرح نسبت به طرح‌های پیشین، کاهش بسیاری یافته است؛ زیرا فرایند ردیابی بر روی ماجول تأیید که بسیار ساده‌تر از ترمینال رأی‌گیری است تمرکز دارد.

۴-۱-۸ مزایای طرح جدید

برخی از قابلیت‌های این روش عبارت‌اند از:

۴-۱-۸-۱ قابلیت تأیید توسط رأی‌دهنده

رأی‌دهندگان می‌توانند قبل از رأی‌دهی، گزینه انتخابی خود را با استفاده از ماجول تأیید، تأیید نمایند. این ماجول یک ابزار بسیار مطمئن و قابل اعتماد است که ردیابی و کنترل آن بسیار آسان می‌باشد. علاوه بر این، به کمک رسیدهای چاپی، رأی‌دهندگان می‌توانند مطمئن شوند که آرایشان شمارش گردیده است. ضمناً افراد نابینا بدون نیاز به کمک دیگران می‌توانند گزینه مورد نظر خود را انتخاب و آن را تأیید نمایند.

۴-۱-۸-۲ سهولت ردیابی

در این سیستم، ردیابی سیستم محدود به ردیابی ماجول تأیید بوده و نیازی به ردیابی نرم‌افزارهای پیچیده ترمینال رأی‌گیری نیست. این مسئله هزینه و ریسک‌های مربوطه را

---

1. Audit

کاهش داده و فرایند اعتبارسنجی سیستم‌های رأی‌گیری را آسان می‌کند.

۴-۱-۸-۳ حفاظت از جامعیت آرا

پس از تأیید گزینه انتخابی توسط رأی‌دهنده، این رأی توسط ماجول تأیید امضای دیجیتالی شده و در نتیجه از تغییر و دستکاری رأی در مراحل بعدی جلوگیری می‌شود.

۴-۱-۸-۴ محرمانگی آرا

رمزنگاری آرا به‌وسیله کلید اختصاصی که بخش‌های مختلف آن بین اعضای شورای انتخابات توزیع شده است و همچنین استفاده از ترکیب بخش‌های مختلف کلید اختصاصی در هنگام رمزگشایی آرا، مانع از کشف ارتباط بین رأی و رأی‌دهنده مربوطه می‌شود.

۴-۱-۸-۵ افزونگی و امکان شمارش موازی آرا

با استفاده از آرای ذخیره شده در ماجول تأیید می‌توان عمل شمارش موازی آرا را مستقل از ترمینال‌های رأی‌گیری انجام داد.

۴-۱-۸-۶ افزایش اعتماد رأی‌دهندگان

اجرای عملیات اعتبارسنجی که در خارج از ترمینال رأی‌گیری و توسط ماجول تأیید انجام می‌شود، سبب افزایش اعتماد رأی‌دهندگان به فرایند انتخابات می‌گردد.

۴-۲ استونی

از ابتدای قرن حاضر، در کشور استونی، موضوع رأی‌گیری الکترونیکی به‌طور جدی در سطوح مختلف مورد بررسی قرار گرفته است، به‌طوری که در حال حاضر انتخابات شوراهای محلی، همه‌پرسی‌ها و انتخابات پارلمان اروپا به‌صورت الکترونیکی برگزار می‌شود.

احراز هویت رأی‌دهندگان با استفاده از کارت‌های شناسایی و امضای دیجیتالی میسر است. در ژانویه ۲۰۰۴، ۳۵۰۰۰۰ کارت شناسایی در اختیار مردم قرار گرفته و انتظار می‌رود که این آمار در پایان سال ۲۰۰۵ به ۸۰۰۰۰۰ کارت رسیده باشد. در نتیجه، اکثریت افراد واجد شرایط در این کشور، دارای کارت‌های شناسایی الکترونیکی هستند.

۴-۲-۱ حوزه سیستم‌های رأی‌گیری الکترونیکی

سیستم رأی‌گیری الکترونیکی بخش کوچکی از فرایند انتخابات است. از نقطه‌نظر تکنیکی، این فرایند از اجزای زیر تشکیل شده است:

- اعلام برگزاری انتخابات،
- ثبت‌نام از کاندیداها،
- آماده‌سازی حوزه‌های انتخاباتی،
- رأی‌گیری (که یکی از زیرمجموعه‌های آن رأی‌گیری الکترونیکی است)،
- شمارش آرا،
- نظارت، رسیدگی به شکایات و پشتیبانی از سایر فعالیت‌های مرتبط با انتخابات.

در کشور استونی، اجرای رأی‌گیری الکترونیکی در طی چندین مرحله صورت می‌گیرد:

۱. فهرست رأی‌دهندگان واجد شرایط تهیه شده و در چارچوب مناسب نگهداری می‌شود.

۲. فهرست کاندیداها تهیه شده و در چارچوب مناسب نگهداری می‌شود.

۳. رأی‌های الکترونیکی به‌صورت جداگانه شمارش شده و در پایان انتخابات به سایر آرا اضافه می‌گردد.

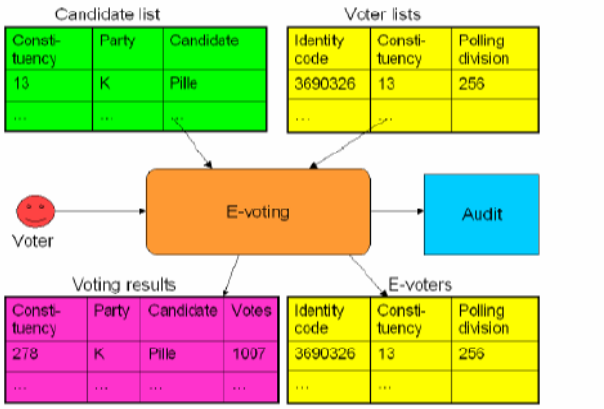
به‌عبارت دیگر، ورودی‌های سیستم رأی‌گیری الکترونیکی عبارت‌اند از:

- فهرست رأی‌دهندگان،
- فهرست کاندیداها،
- آرای رأی‌دهندگان.

خروجی‌های سیستم نیز عبارت‌اند از:

- خلاصه نتایج انتخابات الکترونیکی،
- فهرست رأی‌دهندگانی که از رأی‌گیری الکترونیکی استفاده کرده‌اند.

شکل ۵-۴ محدوده سیستم رأی‌گیری الکترونیکی و پارامترهای ورودی و خروجی آن را نشان می‌دهد:



شکل ۵-۴ حوزه رأی‌گیری الکترونیکی: ورودی‌ها و خروجی‌ها

۴-۲-۲ اصول اساسی رأی‌گیری الکترونیکی

قاعده کلی در رأی‌گیری الکترونیکی این است که باید مشابه رأی‌گیری‌های سنتی منطبق با اصول قانون مصوب انتخابات باشد. رأی‌گیری الکترونیکی باید محرمانه باشد، تنها افراد واجد شرایط مجاز به شرکت در انتخابات باشند و هر رأی‌دهنده باید بتواند ثابت کند که به چه کسی رأی داده است. طبق قانون انتخابات استونی، رأی‌گیری الکترونیکی از شش تا چهار روز مانده به انتخابات صورت می‌گیرد.

۱. پیش از انتخابات، رأی‌دهندگان برای شرکت در انتخابات الکترونیکی یک شناسه امضای دیجیتال دریافت می‌کنند.

۲. رأی‌دهنده با ارائه امضای دیجیتال خود را به سیستم معرفی می‌کند.

۳. پس از تأیید هویت رأی‌دهنده، لیست کاندیداهای مربوط به حوزه انتخابی فرد رأی‌دهنده در روی صفحات وب کمیته انتخابات ملی نمایش داده می‌شود.

۴. رأی‌دهنده با استفاده از صفحات وب، کاندیدای مورد نظر خود را انتخاب و تأیید می‌کند.

قواعد زیر در انتخابات الکترونیکی تعریف شده است:

۴-۲-۲-۱ استفاده از کارت شناسایی الکترونیکی برای شناسایی رأی‌دهنده

این کارت‌ها تنها وسیله‌ای است که احراز هویت افراد را با حداکثر امنیت ممکن ساخته

و امکان امضای دیجیتالی را فراهم می‌نماید.

۴-۲-۲-۲ امکان رأی‌دهی مجدد

رأی‌دهنده می‌تواند بیش از یک‌بار رأی دهد. در این صورت رأی قبلی حذف خواهد شد. اگرچه طبق قانون انتخابات رأی‌دهی دوباره جرم تلقی می‌شود، اما مزیت این کار آن است که درصورتی‌که رأی‌دهنده‌ای تحت فشار رأی داده باشد، پس از خلاصی می‌تواند رأی خود را تغییر دهد. رأی‌دهی مجدد، رأی تکراری تلقی نمی‌شود؛ زیرا سیستم آخرین رأی را جایگزین می‌کند.

۴-۲-۲-۳ اولویت رأی‌دهی سنتی

اگر فردی قبل از موعد برگزاری انتخابات سنتی به‌صورت الکترونیکی رأی داده باشد، درصورتی‌که در روزهای رأی‌گیری مجدداً به یکی از صندوق‌ها مراجعه کرده و رأی بدهد، رأی الکترونیکی‌اش حذف می‌شود. در توجیه این اصل می‌توان گفت که اگر ــ به‌عنوان مثال ــ در انتخابات الکترونیکی مصالحه‌ای صورت گرفته باشد یا به دلایلی برخی از آرا باطل اعلام شود، امکان رأی‌دهی مجدد به‌روش سنتی وجود دارد.

همیشه دو گروه شرکت‌کننده در انتخابات وجود دارند: رأی‌دهنده و رأی‌گیرنده. در انتخابات الکترونیکی، این دو گروه رایانه شخصی رأی‌دهنده و سروری است که در کنترل کمیته انتخابات ملی است. رایانه‌های شخصی بنا به سلایق افراد متفاوت بوده و هیچ‌گونه کنترلی بر روی مشخصات آن نمی‌توان داشت، درحالی‌که سرورها توسط شورای انتخابات و متناسب با نیاز خریداری و نصب می‌گردد. درعین‌حال امکان بروز خطا و حمله به سرورها همچنان به قوت خود باقی است.

۴-۲-۳ مراحل رأی‌گیری

رأی‌گیری الکترونیکی شش تا چهار روز مانده به انتخابات صورت می‌گیرد. در این فرصتِ زمانی می‌توان فهرست کسانی را که در انتخابات الکترونیکی شرکت نموده‌اند، مشخص کرد. بنابراین، از رأی‌دهی مجدد آنها جلوگیری می‌شود.

طبق قانون انتخابات، درصورتی‌که فرد هم به‌صورت الکترونیکی و هم به‌صورت

سنتی رأی دهد، رأی الکترونیکی او باطل می‌شود، اما در مورد تعرفه‌های کاغذی، درصورتی‌که فرد با مراجعه به حوزه‌های انتخاباتی مربوط به‌خود رأی دهد، رأی او صحیح بوده و درصورتی‌که در حوزه‌های دیگر رأی دهد، رأی او باطل می‌گردد. برای رفع این محدودیت‌ها، راهکارهای زیر توسط متخصصان مربوطه ارائه شده است:

- فهرست الکترونیکی رأی‌دهندگان و کاندیداها باید یک هفته قبل از انتخابات تهیه و نهایی شود. البته فهرست رأی‌دهندگان به‌صورت پویا در روزهای رأی‌گیری تغییر می‌کند.
- به‌جای رأی‌گیری الکترونیکی ۲۴ ساعته، فاصله زمانی رأی‌دهی از ۸-۲۴ درنظر گرفته شود تا در فاصله زمانی ساعت ۲۴ شب تا ۸ صبح، سیستم‌ها کنترل گردد.
- پس از اتمام مهلت رأی‌گیری الکترونیکی، فهرست رأی‌دهندگان نهایی شود.
- آرای الکترونیکی مرتب شده و آرای مکرر و نیز آرای مربوط به شرکت‌کنندگان غیرواجد شرایط باطل اعلام گردد.
- فهرست کسانی که در انتخابات الکترونیکی شرکت کرده‌اند به حوزه‌های انتخاباتی ارسال گردد. این کار باید روز قبل از انتخابات سنتی به اتمام برسد. دریافت و پردازش به‌موقع فهرست رأی‌دهندگان، یکی از مهم‌ترین مراحل انتخابات محسوب می‌شود. اگر این اطلاعات به‌موقع در اختیار حوزه‌ها قرار نگیرد، منجر به رأی‌دهی چندباره افراد می‌گردد.
- در روز انتخابات، کسانی که قبلاً در رأی‌گیری الکترونیکی شرکت کرده‌اند، می‌توانند تا ساعت ۵ بعدازظهر مجدداً رأی خود را به صندوق بیندازند. در این صورت، رأی الکترونیکی آنها باطل شده و در پایان انتخابات فهرست اسامی این افراد به کمیته ملی انتخابات[1] فرستاده می‌شود. تا ساعت ۱۹ باید تمامی این لیست‌ها به کمیته فرستاده شده باشد.
- در ساعت ۲۰، صندوق‌های آرا باز شده و آرا شمارش می‌گردند و نتایج به سیستم اطلاعاتی انتخابات فرستاده می‌شود.

۴-۲-۴ سیستم رأی‌گیری

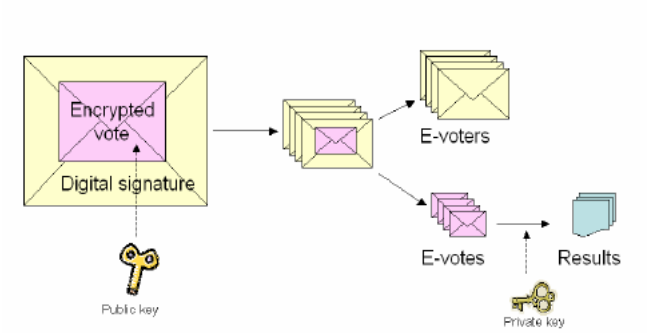
رأی‌گیری الکترونیکی مبتنی‌بر «روش پاکتی» بوده و مشابه رأی‌دهی با پاکت به شیوه

1. National Election Committe (NEC)

انتخابات سنتی است. در این روش رأی‌دهنده یک پاکت داخلی (که همان رأی رمزشده است) و یک پاکت خارجی (که امضای دیجیتالی است) را تولید می‌کند. مزایای سیستم پاکتی عبارت است از:

۱. سادگی و فهم آسان طرح و امکان اجرا به موازات سیستم سنتی،
۲. سادگی معماری سیستم (تعداد گروه‌های درگیر در این طرح حداقل است)،
۳. کاربرد کامل امضای دیجیتالی.

شکل ۶-۴ نمونه‌ای از روش پاکتی را نشان می‌دهد:

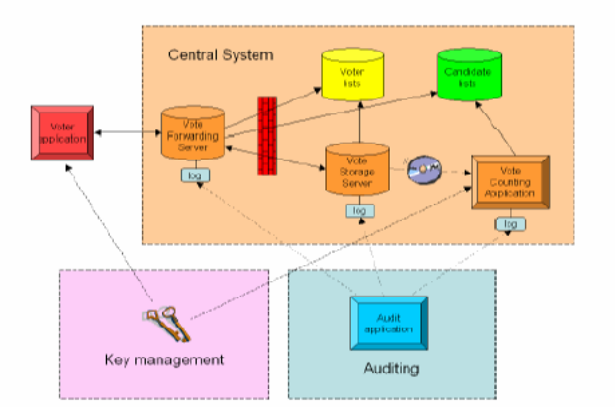


شکل ۶-۴ روش پاکتی

رأی‌دهنده رأی خود را با کلید عمومی سیستم رمز نموده و نتیجه را امضای دیجیتالی می‌کند. سپس آرای جمع‌آوری شده مرتب می‌شود و آرای باطل (آرای مکرر و آرای رأی‌دهندگان غیر واجد شرایط) جدا می‌گردد. سپس پاکت داخلی (رأی رمزشده) از پاکت خارجی (امضای دیجیتالی معرف رأی‌دهنده) جدا می‌شود. به‌این‌ترتیب، فهرست رأی‌دهندگان از پاکت‌های خارجی به‌دست می‌آید. پاکت‌های داخلی هم برای شمارش آرا به شمارنده فرستاده می‌شود. این شمارنده با استفاده از کلید اختصاصی که در اختیار دارد، آرا را بازگشایی و شمارش می‌کند و در نهایت، نتایج اعلام می‌گردد.

۴-۲-۵ معماری سیستم و گروه‌های شرکت‌کننده

در این قسمت اجزای سیستم معرفی شده و نحوه ارتباط و عملکرد آنها تشریح می‌گردد. شکل ۷-۴ معماری کلی سیستم را نشان می‌دهد:



شکل ۷-۴ معماری کلی سیستم

۴-۲-۵-۱ گروه‌های شرکت‌کننده

گروه‌های مختلف شرکت‌کننده در سیستم عبارت‌اند از:

۱. **رأی‌دهنده**: به کمک رایانه خود یک رأی الکترونیکی را رمز و امضای الکترونیکی نموده و به سیستم مرکزی ارسال می‌کند.

۲. **سیستم مرکزی**:[1] بخشی از سیستم که کنترل آن به عهده کمیته ملی انتخابات است و وظیفه‌اش دریافت و پردازش آراست.

۳. **مدیریت کلید**:[2] زوج کلیدهای مورد استفاده در سیستم را تولید و مدیریت می‌کند. کلید عمومی برای رمز نمودن آرا توسط رأی‌دهنده و کلید خصوصی برای بازگشایی آرا توسط شمارنده مورد استفاده قرار می‌گیرد.

۴. **نظارت و کنترل**:[3] به شکایات واصله رسیدگی می‌کند و این کار به کمک «فایل‌های ثبت وقایع»[4] که توسط سیستم مرکزی ارسال می‌گردد، انجام می‌شود.

۴-۲-۵-۲ اجزای سیستم

اجزای سیستم مرکزی عبارت‌اند از:

---

1. Central System
2. Key Management
3. Auditing
4. Log File

۱. **سرور انتقال‌دهنده رأی:**[1] هویت رأی‌دهنده را با استفاده از کارت شناسایی الکترونیکی تأیید نموده و کاندیداهای حوزه انتخاباتی رأی‌دهنده را به او نشان می‌دهد و رأی الکترونیکی رمزشده را دریافت می‌کند. رأی الکترونیکی بلافاصله به سرور ثبت رأی فرستاده شده و تأییدیه دریافت می‌گردد. سپس این تأییدیه برای رأی‌دهنده ارسال می‌گردد. فعالیت این بخش تا پایان مهلت انتخابات ادامه خواهد داشت.

۲. **سرور ذخیره‌سازی رأی:**[2] رأی‌های الکترونیکی را از سرور انتقال‌دهنده رأی دریافت و ذخیره می‌کند. پس از خاتمه انتخابات، آرای مکرر را حذف و آرای افراد غیرواجد شرایط را باطل می‌کند. در مرحله بعد، پاکت‌های داخلی و خارجی را جدا کرده و آنها را برای شمارش توسط شمارشگر آماده می‌سازد.

۳. **برنامه کاربردی شمارش آرا:**[3] از کلید خصوصی سیستم برای بازگشایی رمز آرا استفاده می‌کند و نتایج انتخابات را به‌صورت جدول اعلام می‌نماید.

۶-۲-۴ زیربرنامه‌های رأی‌گیری

این برنامه‌ها شامل موارد ذیل است:

۱-۶-۲-۴ مدیریت کلید

زیربرنامه‌های مدیریت کلید یکی از مهم‌ترین بخش‌های سیستم محسوب می‌شود که حفظ محرمانگی و گمنامی به آن وابسته است. ابزار اصلی تضمین امنیت رأی‌گیری در سیستم، رمزنگاری نامتقارن است. یک زوج کلید تولید شده، کلید عمومی برای رمز نمودن رأی توسط رأی‌دهنده و کلید خصوصی برای رمزگشایی رأی توسط شمارشگر استفاده می‌گردد. این نکته بسیار حائز اهمیت است که کلید خصوصی تنها در مرحله شمارش آرا توسط برنامه شمارش آرا مورد استفاده قرار می‌گیرد. پس از پایان مهلت ارسال شکایات، کلید خصوصی از بین می‌رود. محرمانگی رأی‌دهندگان با دو خطر عمده مواجه است:

اولاً گروه‌های حاضر در سیستم و یا خارج از آن ممکن است به کلید خصوصی

---

1. Vote Forwarding Server (VFS)
2. Vote Storage Server (VSS)
3. Vote Counting Application (VCA)

سیستم دسترسی پیدا کنند. اگرچه این کلید به‌صورت جداگانه در سیستم نگهداری می‌شود، اما خطر همچنان به قوت خود باقی است.

ثانیاً اطلاعات از اجزای مختلف سیستم (سرورهای مختلف، رأی‌دهنده) و کانال‌های انتقال اطلاعات عبور کرده و در نتیجه خطر افشای آرا افزایش می‌یابد. بنابراین، برای حفظ امنیت اطلاعات، تأکید عمده بر مدیریت کلید است.

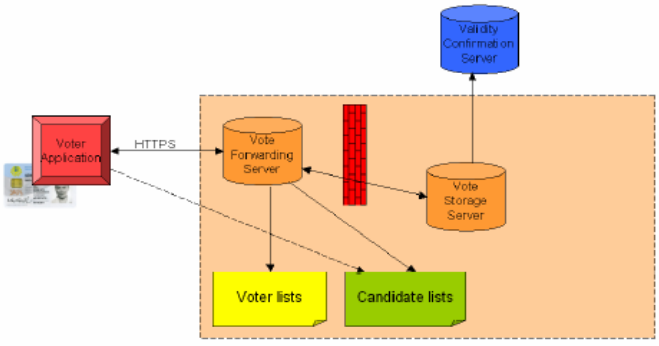
کلید خصوصی هم در معرض دو خطر قرار دارد:

۱. گروه‌هایی که کلید خصوصی را در اختیار دارند، می‌توانند تعیین کنند که هر فرد به نفع چه کسی رأی داده است. بنابراین، محرمانگی رأی‌دهنده نقض می‌گردد.

۲. کلید خصوصی ممکن است مفقود، خراب و یا حذف شود. در نتیجه، امکان رمزگشایی آرا از بین خواهد رفت و این یک خطر جدی است. بنابراین، باید به‌صورت هم‌زمان یک زوج کلید در سیستم مورد استفاده قرار گیرد.

۲-۶-۲-۴ رأی‌گیری و ذخیره‌سازی آرا

رأی‌گیری از روز دوشنبه تا چهارشنبه هفته انتخابات صورت می‌پذیرد. پس از پایان انتخابات، ارتباط سیستم مرکزی با دنیای خارج قطع می‌شود. رأی‌گیری تراکنشی بین رأی‌دهنده و سرور انتقال رأی است. اجزای شرکت‌کننده در رأی‌گیری در شکل ۸-۴ نشان داده شده است.



شکل ۸-۴ اجزای شرکت‌کننده در فرایند انتخابات

برنامه کاربردی رأی‌دهنده در محیط وب کار می‌کند. به‌علاوه، صفحات وب و برنامه‌های کوچک جاوا در مرورگر رأی‌دهنده بارگذاری شده و به کاربر امکان می‌دهد که بتواند رأی خود را رمز و دارای امضای دیجیتالی کند. ضمناً این برنامه اطلاعات کافی در مورد کاندیداها را در اختیار رأی‌دهندگان قرار می‌دهد.

اساساً سرور انتقال رأی، یک سرور وب با برنامه‌های مخصوص به‌خود است، این سرور تنها عنصر سیستم مرکزی می‌باشد که مستقیماً از طریق اینترنت قابل دستیابی است. بقیه اجزای سیستم مرکزی در پشت یک دیوار آتش[۱] داخلی محفوظ بوده و دسترسی به آنها تنها از طریق این سرور امکان‌پذیر است.

در طول مدت برگزاری انتخابات الکترونیکی، پایگاه اطلاعاتی حاوی اسامی رأی‌دهندگان تغییر می‌کند. پس از پایان انتخابات این فایل نیز نهایی و بسته می‌شود. همان‌طورکه در شکل ۸-۴ مشاهده می‌گردد، از یک سرور برای تأیید هویت رأی‌دهندگان استفاده می‌شود.[۲] این سرور بخشی از سیستم مرکزی نیست. مراحل رأی‌گیری بدین قرار است:

۱. رأی‌دهنده از طریق پروتکل امن اتصال به شبکه جهانی[۳] به سرور انتقال رأی دسترسی پیدا کرده و هویت خویش را با استفاده از کارت شناسایی الکترونیکی اعلام می‌کند.

۲. سرور انتقال رأی با استفاده از اطلاعات موجود در پایگاه اطلاعاتی افراد واجد شرایط، هویت رأی‌دهنده را بررسی کرده و حوزه انتخاباتی او را مشخص می‌نماید. اگر رأی‌دهنده واجد شرایط نباشد، پیغامی برای او ارسال شده و مستقیماً برای بررسی وضعیت خود به سروری که اطلاعات جمعیتی را نگه می‌دارد وصل می‌شود.

۳. سرور انتقال رأی با استفاده از اطلاعات موجود در سرور ذخیره‌ساز آرا، کنترل می‌کند که فرد قبلاً رأی داده است یا نه. درصورتی‌که پاسخ مثبت باشد، پیغامی برای فرد فرستاده می‌شود.

---

۱. Firewall: سیستم امنیتی برای محافظت از شبکه سازمانی در مقابل تهدیدهای خارجی.

2. Validity Confirmation Server (VCS)

۳. Hyper Text Transfer Protocol Secure (HTTPS): همان پروتکل HTTP، ولی به‌صورت امن است. پروتکل HTTP، زبان مشترک ارتباطی بین سرویس‌دهنده و سرویس‌گیرنده وب است. درواقع، مرورگر صدای خود را با استفاده از این پروتکل به گوش سرویس‌دهنده وب رسانده و از وی درخواست یک صفحه وب می‌نماید.

۴. سرور انتقال رأی فهرست کاندیداهای مربوط به حوزه انتخابی رأی‌دهنده را مشخص می‌نماید.

۵. رأی‌دهنده کاندیدای مورد نظر خود را انتخاب کرده و شماره مربوط به وی را در گروه مربوطه وارد می‌نماید.

۶. برنامه کاربردی از رأی‌دهنده در مورد تأیید انتخاب او سؤال می‌کند.

۷. برنامه کاربردی، انتخاب کاربر و یک عدد تصادفی را با کلید عمومی برنامه شمارش آرا رمز می‌کند. سپس رأی‌دهنده پیغام رمز را به‌صورت دیجیتالی امضا می‌کند.

۸. برنامه کاربردی، این پاکت دیجیتالی را به سرور انتقال رأی می‌فرستد. این سرور صحت اطلاعات ارسالی را کنترل می‌کند تا مشخص شود که شخص تأیید هویت شده دارای امضای دیجیتالی هست یا نه.

۹. سرور انتقال رأی اطلاعات دریافتی را به سرور ذخیره‌ساز آرا می‌فرستد. این سرور به سرور تأیید اعتبار دسترسی داشته و صحت امضای دیجیتالی را کنترل می‌کند.

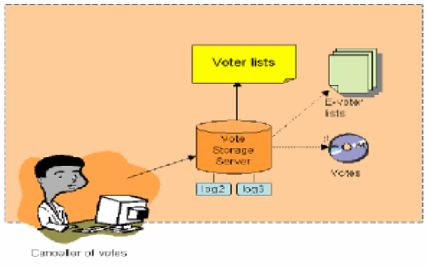
۱۰. درصورت تأیید، سرور ذخیره‌ساز آرا به سرور انتقال رأی تأییدیه دریافت رأی را ارسال می‌کند. در این مرحله به رأی‌دهنده نیز پیغام مناسب فرستاده می‌شود. اطلاعات مربوط به آرای پذیرفته شده در فایل log1 نگهداری می‌شود.

۱۱. رأی‌دهنده ممکن است چندین‌بار رأی دهد. تمامی این آرا از طریق سرور انتقال رأی به سرور ذخیره‌ساز آرا فرستاده می‌شود.

۱۲. پس از پایان مهلت انتخابات الکترونیکی، سرور انتقال رأی همه ارتباطات را قطع می‌نماید.

۳-۶-۲-۴ لغو آرا و مرتب‌سازی آنها

سرور ذخیره‌ساز آرا، مؤلفه اساسی در سیستم است که عمل لغو آرا و یا ذخیره‌سازی آنها را انجام می‌دهد. در نتیجه پردازش‌های این سرور، آرای قابل قبول (شماره‌های رمز شده کاندیداها که امضای دیجیتالی رأی‌دهنده از آن برداشته شده است) و فهرست رأی‌دهندگانی که به‌صورت الکترونیکی رأی داده‌اند مشخص می‌گردد. این فرایند در شکل ۹-۴ نشان داده شده است:



شکل ۹-۴ فرایند لغو آرا و مرتب‌سازی آنها

پس از پایان انتخابات، آرای تکراری بلافاصله حذف شده و تنها آخرین رأی شمارش می‌گردد. تاریخ رأی نیز با تاریخ اعتبار امضای دیجیتالی کنترل می‌شود. رأی‌های باطل شده در فایلی (به نام log2) نگهداری می‌گردد. پس از باطل نمودن آرای تکراری، فهرست افرادی که به‌صورت الکترونیکی رأی داده‌اند (شامل نام و شماره شناسایی)، به‌صورت هم‌زمان به تمامی حوزه‌های انتخاباتی فرستاده می‌شود. در این مرحله حفظ جامعیت و اصالت اطلاعات و امنیت خطوط ارتباطی از اهمیت بسیار زیادی برخوردار است؛ زیرا در غیر این‌صورت، افراد خاطی می‌توانند (به‌صورت الکترونیکی و سنتی) دو بار رأی دهند.

مرحله بعدی حذف آرای الکترونیکی در روز انتخابات اتفاق می‌افتد؛ زیرا افرادی که در انتخابات الکترونیکی شرکت کرده‌اند ممکن است دوباره در رأی‌گیری کاغذی شرکت کنند. در پایان روز انتخابات، فهرست این افراد به‌صورت یک سند با امضای دیجیتالی به کمیته بخش انتخاباتی فرستاده می‌شود. تمامی لیست‌های مربوط به لغو آرای الکترونیکی باید قبل از ساعت شش به کمیته بخش‌های انتخاباتی فرستاده شود. سپس کمیته‌ها این فهرست‌ها را به‌صورت دیجیتالی امضا نموده و آنها را قبل از ساعت هفت به کمیته ملی انتخابات می‌فرستند.

این کمیته فهرست یکپارچه‌ای از تمامی فهرست‌های دریافتی را ایجاد کرده و با امضای دیجیتالی برای سرور ذخیره‌ساز آرا می‌فرستد. این سرور امضای دیجیتالی را کنترل نموده و سپس آرای باطل را در فایل log2 ذخیره و آنها را از فهرست آرای قابل شمارش جدا می‌نماید. پس از اتمام مرحله حذف آرای باطل، پاکت‌های خارجی از

پاکت‌های داخلی جدا می‌شود. فرایند این مرحله به قرار ذیل است:

۱. پاکت‌ها برحسب حوزه‌های انتخاباتی مرتب می‌شود. کدهای شناسایی رأی‌دهندگان از امضای دیجیتالی آنها خوانده شده و با جستجو در پایگاه اطلاعاتی، واجد شرایط بودن آنها کنترل می‌گردد.

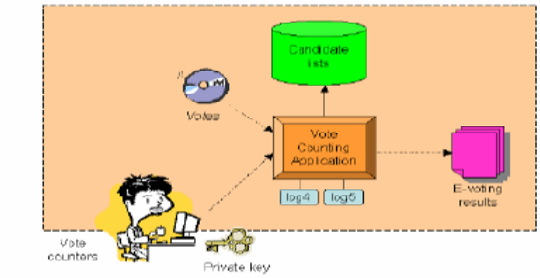
۲. پاکت‌های خارجی باز می‌شود، یعنی امضای دیجیتالی برداشته شده، اما رأیی که توسط کلید عمومی برنامه شمارش آرا رمز شده همچنان مخفی باقی می‌ماند.

۳. امضاهای دیجیتالی به‌صورت جداگانه ذخیره می‌گردد که معرف فهرست افرادی است که به‌صورت الکترونیکی رأی داده‌اند.

۴. آرا توسط یک رسانه ذخیره‌سازی خارجی مثل لوح فشرده (سی‌دی) به برنامه شمارش آرا ارسال می‌شوند. درضمن فرایند انتقال، صحت و جامعیت اطلاعات باید کاملاً حفظ گردد. آرایی که برای شمارش به برنامه شمارش آرا فرستاده می‌شود، در فایلی به نام log3 ذخیره می‌گردد.

۴-۶-۲-۴ شمارش آرا

شمارش آرا در سرور شمارنده آرا انجام می‌شود. این سرور باید به‌صورت هم‌زمان از اطلاعات سروری که حاوی فهرست کاندیداهاست استفاده نماید. ضروری است که فرایند شمارش آرا تکرارپذیر باشد؛ چرا که ممکن است سرور شمارنده دچار خرابی سخت‌افزاری شود. در این صورت، می‌توان عمل شمارش آرا را با استفاده از رایانه دیگر انجام داد. فرایند شمارش آرا در شکل ۱۰-۴ آمده است:



شکل ۱۰-۴ فرایند شمارش آرا

آرا به‌وسیله کلید خصوصی حوزه‌های انتخاباتی رمزگشایی می‌شوند و پس از رمزگشایی، کنترل می‌شود که آیا امکان رأی‌دهی به آن کاندیدا در آن حوزه انتخاباتی وجود دارد یا نه. اگر شماره کاندیدا در آن حوزه تأیید نشود، رأی باطل اعلام شده و در فایل log4 ذخیره می‌گردد. رأی‌های شمارش شده برحسب نام کاندیداها و حوزه‌های انتخاباتی مرتب شده و در فایل log5 ذخیره می‌گردد.

۵-۶-۲-۴ امکانات نظارت و کنترل

سیستم رأی‌گیری الکترونیکی طی مراحل مختلف چندین فایل ایجاد می‌کند:

Log 1: آرای دریافتی،

Log 2: آرای باطل شده،

Log 3: آرایی که باید شمارش شود،

Log 4: آرای نامعتبر (شماره کاندیدای نامعتبر)،

Log 5: آرای شمارش شده.

تمامی اطلاعات در این فایل‌ها به‌صورت رمز ذخیره می‌شود. جامعیت این فایل‌ها نیز به این شکل کنترل می‌شود که log1 برابر است با مجموع دو فایل log2, log3 و نیز log3 برابر است با مجموع دو فایل log4 و log5. همچنین با استفاده از یک برنامه تحت وب می‌توان این امکان را فراهم نمود که یک رأی‌دهنده بتواند با ارائه کد شناسایی خود، از وضعیت رأیش اطلاع حاصل نماید.

۴-۳ ایتالیا

بیشتر سیستم‌های رأی‌گیری الکترونیکی و پروژه‌های تحقیق و توسعه، تأکیدشان بر روی جنبه فنی قضیه است و راه‌حل‌های فنی انتخاب شده بسیار شبیه به هم می‌باشند.[۲و۳] واضح است که پیاده‌سازی و به‌کارگیری سیستم‌های مبتنی‌بر فناوری‌های اطلاعات و ارتباطات، می‌تواند باعث موفقیت و یا شکست سازمان‌ها گردد.[۴و۵] بنابراین، لازم است که در پروژه‌های رأی‌گیری الکترونیکی یک مرحله مطالعاتی برای بررسی عوامل موفقیت و شکست تجربیات سایر کشورها درنظر گرفته

شده و عقاید و توقعات کاربران نیز مورد مطالعه و بررسی قرار گیرد. یکی از این تجربیات مربوط به کشور ایتالیاست که در آن دو شهرداری، یک اتحادیه کارگری و دو شبکه اینترنتی برای آزمایش انتخابات الکترونیکی تعیین گردید.

۱-۳-۴ بررسی تجربیات

این طرح آزمایشی در پنج محیط مختلف به اجرا درآمد:

۱. **شهر ارسی**:[1] با ۱۶۵۰۰ نفر جمعیت در ۲۵ کیلومتری جنوب غربی پاریس،

۲. **ایالت کارپنتر**[2] **(شهر نیوهام)**: ناحیه مسکونی با حدود ۶۰۰ آپارتمان و جمعیتی متنوع با فرهنگ‌های گوناگون،

۳. **اتحادیه «سی جیل»**:[3] بزرگ‌ترین اتحادیه صنفی ایتالیا،

۴. **شبکه «آر سی ام»**:[4] شبکه شهری در میلان،

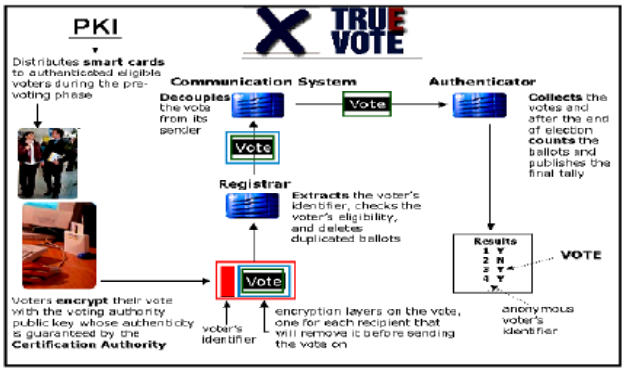
۵. **شبکه «او وای کا»**:[5] شبکه روستایی در مرز شرقی فنلاند که محیطی با مساحت ۴۵۰۰ کیلومترمربع و جمعیتی حدود ۲۰۰۰۰ نفر را پوشش می‌دهد.

۱-۱-۳-۴ دوره‌های رأی‌گیری

بین دسامبر ۲۰۰۲ و مارس ۲۰۰۳، هر یک از پنج سایت سازماندهی شده توانستند دو تا سه انتخابات را برگزار کنند که روی‌هم‌رفته ۱۴ تجربه عملی را به‌دنبال داشت. اولین و دومین دوره انتخابات در مورد موضوعات محلی بود. این موضوعات باید با دقت انتخاب می‌شد تا در افراد اشتیاق شرکت در انتخابات را فراهم کند. دوره سوم رأی‌گیری به‌صورت هم‌زمان در پنج سایت برگزار گردید. سازماندهی و مدیریت هم‌زمان این سایت‌ها ازنظر تکنیکی بسیار مهم بود. شکل۱۱-۴ مراحل انجام رأی‌گیری الکترونیکی در سیستم «رأی صحیح»[6] را نشان می‌دهد.

---

1. Orsay
2. Carpenter State
3. CGIL
4. RCM
5. OYK
6. True Vote



شکل ۱۱-۴ سیستم رأی‌گیری الکترونیکی «رأی صحیح»

در دوره‌های مختلف انتخابات، رأی به‌صورت انتخاب منفرد (بلی/ خیر) و یا انتخاب چندگانه بود. در دو انتخابات محلی که در شهر نیوهام برگزار گردید، وضعیت امنیت شهروندان به رأی گذاشته شد. در انتخابات مربوط به اتحادیه‌های کارگری «سی جیل»، سؤالاتی در مورد جنگ عراق، قوانین مهاجرت در کشور ایتالیا و نیز جایگاه سیاسی اتحادیه‌های کارگری مطرح گردید. در شهر ارسی، انتخابات در مورد جمع‌آوری نظرات شهروندان درخصوص توسعه محدوده استان و افزایش تعداد شهرداری‌ها بود. در شبکه شهری «آر سی ام»، وضعیت حمل‌ونقل عمومی در شهر میلان و تقدم اجرای عملیات شهرداری‌ها در طی کریسمس به رأی گذاشته شد. موضوع مطرح شده در شبکه «او وای کا»، مربوط به نحوه ارائه خدمات رفاهی و تمایل شهروندان به عضویت در ناتو بود. البته تمامی سایت‌ها به‌صورت هم‌زمان یک نظرسنجی راجع به مسئله ضرورت رفع وابستگی اروپا به نفت را اجرا نمودند.

۴-۳-۱-۲ ثبت‌نام از رأی‌دهندگان

در شهر ارسی یک دعوت‌نامه ازطرف شهرداری برای شرکت در انتخابات آزمایشی برای شهروندان ارسال گردید. اتحادیه کارگری «سی جیل»، گروه‌های مختلفی از اعضا و کارکنان خود را در این تجربه وارد نمود. تمام اعضای دو شبکه «آر سی ام» و «او وای کا» می‌توانستند در رأی‌گیری شرکت کنند.

رأی‌دهندگان واجد شرایط که دعوت‌نامه برایشان ارسال شده بود، یک کارت هوشمند که حاوی امضای دیجیتالی آنها بود، دریافت کردند. این افراد می‌توانستند از طریق باجه‌های رأی‌گیری و یا رایانه‌های شخصی (در منزل یا محیط کار) و یک دستگاه کارت‌خوان، آرای خود را ارسال نمایند. دستگاه کارت‌خوان به‌صورت رایگان در اختیار این افراد قرار می‌گرفت.

سخت‌افزار و نرم‌افزار مورد نیاز در باجه‌های رأی‌گیری توسط مسئولان انتخابات نصب می‌گردید، اما در مورد رایانه‌های شخصی، خود کاربران موظف به نصب و راه‌اندازی تجهیزات مورد نیاز بودند، که در بسیاری از موارد به‌دلیل عدم توانایی، برخی از کاربران واجد شرایط نتوانستند در انتخابات شرکت کنند. نتایج به‌دست آمده در جدول ۱-۴ نشان داده شده است:

جدول ۱-۴ نتایج به‌دست آمده از انتخابات شهر ارسی (ایتالیا)

دوره‌ها		ارسی	نیوهام	سی جیل	آر سی ام	او وای کا	جمع
اولین دوره ژانویه ۲۰۰۳	مدت‌زمان رأی‌گیری		۲ روز	۲ روز	۷ روز	* ۲۲ روز	
	تعداد ثبت‌نام‌کنندگان		۸۳	۳۲۶	۱۹۰	۳۱۰	۹۰۹
	تعداد رأی‌دهندگان		۷	۲۳۱	۱۳۰	۲۳۸	۶۰۶
	تعداد آرا		۶	۲۲۱	۱۲۵	۲۱۵	۵۷۷
	درصد آرا به ثبت‌نام‌کنندگان		۷	۶۸	۶۶	۶۹	۶۳
دومین دوره فوریه ۲۰۰۳	مدت‌زمان رأی‌گیری	۴ روز	۲ روز	۳ روز	۱۱ روز	۱۰ روز	
	تعداد ثبت‌نام‌کنندگان	۹۲۵	۹۶	۳۵۷	۳۰۳	۳۹۶	۲۰۷
							۷
	تعداد رأی‌دهندگان	--	--	۱۵۵	۲۰۷	۲۲۴	۵۸۶
	تعداد آرا	۶۲۸	۱۰	۱۴۵	۱۸۸	۲۱۰	۱۱۸
	درصد آرا به ثبت‌نام‌کنندگان	۶۸	۱۰	۴۱	۶۲	۵۳	۵۷
سومین دوره مارس ۲۰۰۳	مدت‌زمان رأی‌گیری	۴ روز	۲ روز	۱۲ روز	۱۲ روز	۱۲ روز	
	تعداد ثبت‌نام‌کنندگان	۹۲۵	۹۶	۳۵۷	۳۰۳	۳۹۶	۱۸۵
	تعداد رأی‌دهندگان	۴۷۷	۱۲	۱۳۷	۱۶۸	۱۹۷	۹۶۹
	تعداد آرا	۴۶۲	۱۲	۱۳۵	۱۵۸	۱۸۷	۹۵۴
	درصد آرا به ثبت‌نام‌کنندگان	۵۰	۱۳	۳۸	۵۲	۴۷	۵۱

* طولانی شدن زمان، به‌دلیل مشکلات فنی بوده است.

۴-۳-۱-۳ تنوع مکان‌های رأی‌دهی

در انتخابات ارسی، نیوهام و «سی جیل»، از باجه‌های مخصوصی به‌عنوان مکان‌های رأی‌دهی استفاده شد، درحالی‌که در دو شبکه «آر سی ام» و «او وای کا»، افراد با استفاده از رایانه‌های شخصی و اینترنت در انتخابات شرکت کردند. البته برای استفاده دانش‌آموزان دبیرستانی و افرادی که در نزدیکی ادارات زندگی می‌کردند نیز باجه‌های مخصوصی درنظر گرفته شده بود.

۴-۳-۱-۴ روش مطالعه تجربیات فوق

اولاً پس از برگزاری هر دوره از انتخابات، دست‌اندرکاران برای بررسی وضعیت رأی‌گیری، سؤالاتی را مطرح کرده و در اختیار شرکت‌کنندگان قرار دادند. ثانیاً کارشناسان مربوطه در روزهای رأی‌گیری به حوزه‌های انتخاباتی مراجعه کرده و عملکرد سیستم را از نزدیک مشاهده نمودند. ثالثاً سیستم رأی‌گیری الکترونیکی از سه جنبه مورد بررسی قرار گرفت. در بررسی اول، در هنگام ثبت‌نام افراد برای دریافت کارت هوشمند، اطلاعاتی از آنان درخصوص جنسیت، سن، شغل، سواد رایانه‌ای، میزان استفاده از رایانه اخذ گردید.

در بررسی دوم و پس از انتخابات، قابلیت استفاده سیستم، کیفیت سیستم از لحاظ محرمانگی و امنیت، نظر رأی‌دهندگان راجع به این نوع انتخابات و هویت رأی‌دهندگان مورد سؤال قرار گرفت و نهایتاً در بررسی سوم، سؤالاتی در مورد محل رأی‌دهی (خانه، محل کار، مدرسه و ...)، مزایا و مشکلات موجود به عمل آمد.

۴-۳-۲ یافته‌های مطالعه

۴-۳-۲-۱ اشتیاق شرکت در آزمایش فناوری‌های رأی‌گیری الکترونیکی

اشتیاق شرکت در این آزمایش در سازمان‌های مختلف متفاوت بود. در شهرهای اورسی و نیوهام که تجربیاتی در مورد انتخابات الکترونیکی داشتند، هدفشان بیشتر برگزاری سایر انواع انتخابات از جمله انتخابات سیاسی به شیوه الکترونیکی بود. اتحادیه کارگری «سی جیل» علاقه‌مند به استفاده از سیستم‌های رأی‌گیری الکترونیکی به‌عنوان یک ابزار ساده، امن و سریع بوده و اعتقاد داشت که از این طریق، امکان مشارکت سطوح پایین

جامعه در تصمیم‌گیری‌های مهم فراهم می‌گردد. هدف شبکه فرهنگی «آر سی ام»، افزایش سطح آگاهی دولت‌های محلی درخصوص فناوری‌های نوین اطلاعاتی و ارتباطی و افزایش همکاری و تشریک مساعی شهروندان و شهرداری‌ها بود.

۴-۳-۲-۲ پیامدهای سازمانی

خودارزیابی سازمان‌های درگیر در انتخابات الکترونیکی نتایج جالبی را به همراه داشت. مهم‌ترین مسئله، تأمین تجهیزات مورد نیاز انتخابات بود. فرایند ثبت‌نام، توزیع سخت‌افزار و نرم‌افزار، سازماندهی کارکنان پشتیبانی و پشتیبانی رأی‌دهندگان کاری پیچیده و مشکل بود که به عملکرد گروه‌های مختلف از جمله سازمان‌های برگزارکننده انتخابات، ادارات تشخیص هویت، شرکت‌های رایانه‌ای و خود رأی‌دهندگان بستگی داشت. تمامی این گروه‌ها می‌بایست با یکدیگر همکاری و تشریک مساعی داشته باشند.

یکی از مهم‌ترین مشکلات، مربوط به سازماندهی کاربران بود، به‌خصوص افرادی که می‌خواستند از خانه و از طریق اینترنت رأی خود را ارسال نمایند. ازطرف دیگر، در برخی موارد به‌دلیل مشکلات فنی سرور، پاره‌ای از آرا مورد شمارش قرار نمی‌گرفت.

۴-۳-۲-۳ تعداد شرکت‌کنندگان

در بسیاری از کشورها مشارکت افراد در فعالیت‌های سیاسی کاهش یافته که نتیجه آن کاهش چشمگیر تعداد شرکت‌کنندگان می‌باشد. طرفداران رأی‌گیری الکترونیکی معتقدند که استفاده از فناوری‌های جدید، رأی‌دهی را آسان‌تر نموده که این خود می‌تواند سبب افزایش تعداد شرکت‌کنندگان شود.

در بررسی‌های انجام‌گرفته، تمایل افراد پنج گروه تعریف شده برای شرکت در این آزمایش، بسیار متفاوت بود. همان‌طور که در جدول مشاهده می‌گردد، تعداد متقاضیان شرکت در انتخابات الکترونیکی در شهر اورسی بیش از سایر گروه‌ها بوده که دلیل آن را می‌توان در ارسال دعوت‌نامه توسط شهرداری‌ها برای ساکنان جستجو نمود. اعضای دو شبکه محلی تمایل زیادی برای شرکت در انتخابات داشتند، اما به‌دلیل مشکلات اجرایی (توزیع کارت‌خوان در بین رأی‌دهندگان) تعدادی از آنها نتوانستند در انتخابات شرکت کنند. مانع دیگر در این شبکه، نیاز به ثبت‌نام برای انتخابات بود، اگرچه افراد قبلاً به

عضویت این شبکه‌ها پذیرفته شده بودند، اما برای شرکت در انتخابات می‌بایست دوباره ثبت‌نام می‌کردند. ازطرفی محدودیت‌های سخت‌افزاری و نرم‌افزاری نیز سبب کاهش تعداد شرکت‌کنندگان در این آزمایش گردید.

با توجه به آمار به‌دست آمده، تعداد شرکت‌کنندگان در پنج گروه مختلف بسیار متفاوت بود. بنابراین، می‌توان نتیجه گرفت که تعداد شرکت‌کنندگان در انتخابات ـــ به‌جز استفاده از فناوری‌های جدید ـــ به عوامل دیگری نیز وابسته است که از آن جمله می‌توان به سواد رایانه‌ای و تمایل به مشارکت سیاسی افراد اشاره کرد. درواقع، اگرچه فناوری‌های جدید در ابتدا جاذبه زیادی دارد، اما مردم به‌سرعت با آن خو می‌گیرند.(۶)

از دیگر مشکلات مشاهده شده در این بررسی‌ها می‌توان از عدم توانایی کاربران در نصب سخت‌افزار و نرم‌افزارهای مورد نیاز نام برد. در طی دوره برگزاری انتخابات درخواست‌های زیادی از طرف رأی‌دهندگان خانگی در مورد نحوه نصب سخت‌افزار و نرم‌افزار دریافت شد. سهولت استفاده از برنامه‌های کاربردی رأی‌گیری، یکی از مهم‌ترین مسایلی است که در هنگام طراحی و پیاده‌سازی آنها باید مدنظر قرار بگیرد. بنابراین، اگر نمی‌خواهیم که فناوری مانعی در جهت پیشبرد اهدافمان شود، باید آن را به‌نحوی طراحی و پیاده سازیم که استفاده از آن نیاز به مهارت‌های خاص نداشته باشد.(۷) به‌عبارت دیگر، اگر استفاده از فناوری‌های نوین نتواند تعداد شرکت‌کنندگان در انتخابات را افزایش دهد، نباید با طراحی غلط به‌عنوان یک عامل منفی، سبب کاهش تعداد شرکت‌کنندگان شود.

یکی از مشخصه‌های رأی‌گیری الکترونیکی این است که می‌تواند بدون نیاز به هیچ‌گونه هزینه اضافی، در طی چند روز برگزار گردد. افزایش دوره زمانی رأی‌گیری می‌تواند سبب افزایش تعداد رأی‌دهندگان شود، اما این مطلب را نمی‌توان به‌عنوان یک قاعده کلی پذیرفت.

۴-۲-۳-۴ ارزیابی سیستم توسط رأی‌دهندگان

پس از برگزاری انتخابات، پرسش‌نامه‌هایی شامل ۶۰ پرسش برای ارزیابی سیستم در اختیار رأی‌دهندگان قرار گرفت. هفده متغیر جدید شناسایی شد که نه تای آن در جدول ۲-۴ آمده است. دو متغیر مربوط به استفاده از رایانه، سه متغیر مربوط به سطح اطمینان سیستم‌های رأی‌گیری الکترونیکی و چهار متغیر مربوط به معیارهای مختلف سنجش

سیستم «رأی صحیح» بود.

جدول ۲-۴ نتایج بررسی نظرات رأی‌دهندگان

ردیف	موضوع	بله (درصد)	خیر (درصد)	بی‌طرف (درصد)	مجموع
۱	استفاده روزانه از رایانه در خانه	۵۸	۴۲		۴۲۸
۲	استفاده روزانه از رایانه در محل کار یا مدرسه	۶۴	۳۶		۳۹۳
۳	اطمینان از امنیت سیستم (در مقابل تقلب و هکرها)	۴۳	۲۳	۳۴	۴۳۱
۴	اطمینان از محرمانگی سیستم	۸	۶۰	۳۲	۴۳۳
۵	اطمینان از قابلیت ردیابی و نظارت سیستم	۷۲	۷	۲۱	۲۷۹
۶	کار با سیستم آسان است	۹۲	۲	۶	۲۸۱
۷	سیستم سریع است	۸۰	۴	۱۶	۲۷۹
۸	نصب سیستم آسان است	۶۵	۱۱	۲۴	۲۶۰
۹	سیستم در هنگام مفقود شدن کارت آسیب‌پذیر است	۴۰	۲۷	۳۳	۲۸۰

پرسش‌نامه‌ها نشان داد که تعداد زیادی از کاربران (۴۳ درصد) به امنیت سیستم در قبال تقلب‌های داخلی و هکرهای خارجی اعتماد دارند، درحالی‌که ۲۳ درصد نظر منفی داشته و ۳۴ درصد نیز بی‌طرف بودند. سطح اطمینان افراد به حفظ محرمانگی آرا بسیار پایین بود. ۶۰ درصد افراد مطمئن به حفظ محرمانگی آرا نبوده و تنها ۸ درصد آن را رضایت‌بخش اعلام نمودند و ۳۲ درصد نیز نظر خاصی نداشتند. برای اطلاع از ارتباط موجود بین به‌کارگیری رایانه و سطح سواد افراد، سؤالاتی درخصوص میزان استفاده از رایانه مطرح شد و نتایج به‌دست آمده نسبتاً رضایت‌بخش بود.

در مرحله بعد این نکته مورد بررسی قرار گرفت که آیا هیچ ارتباطی بین پاسخ‌های داده شده و مشخصات رأی‌دهندگان وجود دارد یا نه؛ زیرا ممکن است فناوری جدید رأی‌گیری الکترونیکی برای بعضی از اقشار جامعه ساده‌تر و قابل استفاده‌تر باشد.

یکی از نتایج به‌دست آمده این بود که نظر افراد نسبت به برگزاری انتخابات الکترونیکی تا حدود زیادی به مشخصات آنها بستگی دارد. به‌طور مثال، در این بررسی‌ها زنان بیش از مردان نسبت به این شیوه انتخابات ابراز علاقه نموده بودند. افرادی که به‌طور دائم از رایانه و اینترنت استفاده می‌کردند، در نصب برنامه با مشکلات کمتری مواجه بودند.

پی‌نوشت‌ها

1. A. Riera, *SCYTL online World Security,* Barselona, Spain, 2004 [online]: Http://www.scytl.com

2. Anne-Marie & P. Van Den Besselaar. Internet Based Voting, TRUEVOTE Deliverable 2.1a, Amsterdam: Uva, 2002.

3. D. Bruschi, G. Poletti & E. Rosti, A Survey of E-Voting Protocols, TRUEVOTE Deliverable 2.0. Milano: University of Milano, 2002.

4. O. Anne-Marie & P. Van Den Besselaar, User Requirements for the TRUEVOTE Protocol, TRUEVOTE Deliverable 2.1b, Amsterdam: Uva, 2002 .

5. N. Barry, Hague & Brian Loader (eds.), Digital Democracy, London: Routledge, 2000.

6. C. Giovanni, C. Fiorella De, R. Laura, Community Networks and Access for all in the era of the Free Internet: Discover the Treasure of the Community, in L. Keeble & B.D. Loader (eds.), Community Informatics: Shaping Computer-Mediated Social Relations, London: Routledge, 2001.

7. T. Winograd. & F. Flores, *Understanding Computers and Cognition,* Norwood: Ablex, 2000.

فصل پنجم

پروتکل‌های معروف رأی‌گیری الکترونیکی

پیشرفت‌های اخیر در شبکه‌های ارتباطی و تکنیک‌های رمزنگاری، امکان جایگزینی سیستم‌های رأی‌گیری سنتی با سیستم‌های رأی‌گیری الکترونیکی را فراهم کرده است. تاکنون پروتکل‌های[1] مختلفی برای رأی‌گیری الکترونیکی ارائه شده، اما متأسفانه تعداد کمی از آنها در سیستم‌های عملیاتی به‌کار گرفته شده است.

محرمانگی و امنیت از ویژگی‌های ضروری یک سیستم رأی‌گیری الکترونیکی است، اما واضح نیست که با چه هزینه قابل قبولی می‌توان به این دو مشخصه دست یافت. در هنگام برگزاری انتخابات، تضمین امنیت و محرمانگی سیستم از منظر مدیر سیستم بسیار گران بوده و از دید کاربر بسیار پردردسر و پیچیده است. رأی‌گیری الکترونیکی (برخط) به کاربران امکان می‌دهد که بدون توجه به مکان فیزیکی حضورشان، با استفاده از امکانات شبکه‌های اینترنت در انتخابات شرکت نمایند.

یکی از مشخصه‌های سیستم‌های رأی‌گیری از راه دور، محرمانگی ذاتی آن‌هاست؛ زیرا رأی‌دهندگان می‌توانند بدون اینکه توسط افراد دیگر دیده شوند، در انتخابات شرکت نمایند. توجه به این نکته ضروری است که هنگام استفاده از سیستم‌های سنتی انتخابات، رسیدن به این مشخصه غیرممکن است.

سیستم رأی‌گیری برخط باید حاوی مکانیسم‌های امنیتی قدرتمند باشد که از طراحی نسبتاً پیچیده‌ای برخوردارند. در بیست سال گذشته، مطالعه مکانیزم‌های امنیتی در انتخابات الکترونیکی توجه زیادی را به‌خود معطوف داشته و منجر به ارائه پروتکل‌های رمزنگاری متنوعی شده است.[(۱)تا(۴)] این پروتکل‌ها باید از استانداردهای امنیتی انتخابات

---

۱. پروتکل به مجموعه قواعدی اطلاق می‌گردد که برای اجرای صحیح فرایندهای رأی‌گیری الکترونیکی به لحاظ فنی و امنیتی تنظیم گشته است.

تبعیت کند، از جمله دقت، قابلیت ردیابی، گمنامی رأی‌دهنده، محرمانگی رأی و آشکارسازی رأی‌دهی دوباره[۵و۶] پروتکل‌های رمزنگاری به دو گروه تقسیم می‌شوند:

۱. پروتکل‌های مبتنی‌بر توابع همسان،[۱]

۲. پروتکل‌های مبتنی‌بر امضاهای مخفی.[۲]

پروتکل‌های مبتنی‌بر توابع همسان، برای مخفی کردن محتوای تعرفه‌ها به‌منظورحفظ محرمانگی رأی، به طرح‌های پیچیده رمزنگاری نیاز دارد.[۷و۸] این پروتکل‌ها شامل دو مرحله‌اند: رمزنگاری و رأی‌گیری. نقطه‌ضعف بسیار مهم این پروتکل‌ها، پیچیدگی و هزینه بسیار زیاد آن است.

پروتکل امضاهای مخفی در سال ۱۹۸۳ توسط چاوم[۳] ارائه شد.[۹] این پروتکل هویت رأی‌دهنده را مخفی نگه می‌دارد، اما محتوای رأی توسط مسئولان قابل مشاهده خواهد بود. پروتکل مبتنی‌بر امضاهای مخفی شامل دو مرحله ثبت‌نام و رأی‌گیری است.

فوجیوکا[۴][۱۰] یک طرح عملیاتی مبتنی‌بر امضاهای مخفی ارائه کرده است. در این پروتکل، هر رأی‌دهنده رأی خود را با یک کلید مخفی امضا نموده، سپس از طریق یک کانال ارتباطی ناشناس به مرکز شمارش آرا می‌فرستد. یکی از معایب این پروتکل، پیچیدگی آن است؛ زیرا رأی‌گیری شامل دو مرحله است. در سال ۱۹۹۷ کرانور[۵] و کیترون[۶][۱۱] پروتکلی را ارائه کردند که برمبنای طرح فوجیوکا تهیه شده بود و «سنسوس»[۷] نامیده می‌شد. تفاوت اصلی این دو طرح در آن بود که در پروتکل «سنسوس» رأی‌گیری در یک مرحله و در پروتکل فوجیوکا، رأی‌گیری در دو مرحله اتفاق می‌افتاد.

یکی از معایب این طرح، افزایش ترافیک شبکه بود؛ زیرا رأی‌دهنده ناچار بود پیغام‌های متنی خود را دوبار ارسال کند. برعکس، در طرح ون‌ـشنگ،[۸][۱۲] ترافیک شبکه بسیار پایین بود؛ زیرا هر رأی‌دهنده تنها یک پیغام مخفی ارسال می‌کرد. اما این

---

1. Homomorphic Functions
2. Blind Signature
3. Chaum
4. Fujioka
5. Cranor
6. Cytron
7. Sensus
8. Wen-sheng

پروتکل نمی‌توانست از رأی‌دهی دوباره افراد ممانعت به عمل آورد.

در سال ۱۹۹۸، میو[1] و وارادهاراجان[2] [۱۳] دو طرح مطمئن برای رأی‌گیری الکترونیکی ارائه کردند. در این طرح‌ها، به گمنامی رأی‌دهنده توجه خاصی شده بود. این پروتکل‌ها قادر به شناسایی آرای تکراری نیز بودند. در سال ۱۹۹۹، کارو[3] و وانگ،[4] [۱۴] برای انتخابات الکترونیکی در مقیاس بزرگ طرحی را ارائه نمودند که از امضاهای مخفی استفاده نمی‌کرد. در این طرح برای اجرای تمام تراکنش‌ها، به‌جای استفاده از کانال‌های ارتباطی ناشناس، از پروتکل امن اتصال به شبکه جهانی استفاده گردید، اما این طرح مقرون به‌صرفه و کارا نبود؛ زیرا برای اجرایی کردن طرح، شش نفر مسئول درنظر گرفته شده بود.

در سال ۲۰۰۱، هامورتی[5] [۱۵] طرحی را ارائه نمود که در آن امکان گمنامی در اینترنت میسر شده بود. این پروتکل دارای سه مسئول اجرایی بود و احراز هویت رأی‌دهندگان با استفاده از گواهی‌نامه‌های دیجیتالی صورت می‌گرفت.

در سال ۲۰۰۳، جوکوئیم[6] و فریرا[7] [۱۶] سیستمی مبتنی‌بر زبان برنامه‌نویسی جاوا به نام «آر ای وی اس»[8] ارائه نمودند. پروتکل «آر ای وی اس» برمبنای طرح ارائه شده توسط دورتی[9] [۱۷] طراحی گردید که این طرح نیز خود نسخه اصلاح شده سیستم «ای واکس»[10] ترسیم شده توسط هرزبرگ[11] بود.[۱۸] در پروتکل «آر ای وی اس» رابطه زیر برقرار است که در آن t تعداد امضاها و nتعداد مدیران سیستم است: $t > n/2$

در سال ۲۰۰۳، چاین[12] و چانگ[13] [۱۹] یکی از نقاط ضعف طرح پیشنهادی میو و

---

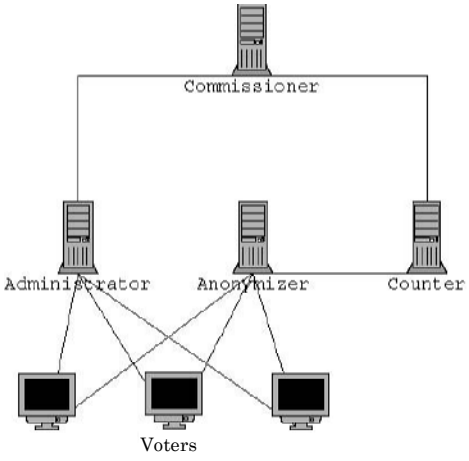
1. Mu
2. Varadharajan
3. Karo
4. Wang
5. Narasimhamurthi
6. Joaquim
7. Ferreira
8. REVS
9. DuRette
10. EVOX
11. Herschberg
12. Chien
13. Lin-hwang-chang

وارادهاراجان را به اثبات رساندند. این نقطه‌ضعف، عدم توانایی سیستم در تشخیص رأی‌دهی چندباره افراد بود. چانگ، پروتکل میو و وارادهاراجان را بهبود بخشیده و با ارائه طرحی امنیتی، امکان تقلب در استفاده از امضای دیجیتالی را منتفی ساخته است. این طرح پیشنهادی به هیچ کانال ارتباطی خاص نیاز ندارد.

در نهایت در سال ۲۰۰۵، زامورا[۱] (۲۰) دو اصلاحیه را به پروتکل چانگ اضافه کرد: اولاً طرح رمزنگاری با طرح الگوریتم امضای دیجیتالی[۲] جایگزین شد. ثانیاً دو مرحله رمزنگاری دیگر برای تضمین عملکرد مناسب به سیستم اضافه گردید.

۱-۵ پروتکل «ای واکس»

سیستم‌های رأی‌گیری الکترونیکی باید از امنیت بالایی برخوردار باشند و گمنامی رأی‌دهندگان و محرمانگی آرا در آن تضمین شود. مسئولان انتخابات درصددند از شرکت افراد غیرواجد شرایط در انتخابات ممانعت به عمل آورده و مانع از رأی‌دهی چندباره افراد واجد شرایط گردند. در نهایت، نتایج انتخابات باید صحیح و قابل بازبینی و کنترل توسط احزاب مربوطه باشد.



شکل ۱-۵ نمودار شبکه‌ای سیستم اولیه «ای واکس»

1. Garc´ıa-zamora
2. Digital Signature Algorithm (DSA)

در سال‌های اخیر پژوهشگران علوم رایانه، برای برگزاری انتخابات الکترونیکی سیستم‌های مختلفی را ارائه کرده‌اند. یکی از این سیستم‌ها، سیستم «ای واکس» است که توسط فوجیوکا، اکاموتو[1] و اهتا[2] پیشنهاد شده است.(۲۱) در این سیستم به‌جای استفاده از یک سرور اداره‌کننده، از چندین سرور مجزا استفاده گردیده است. در نتیجه، امکان جعل آرا به‌دلیل وابستگی سیستم به یک سرور کاملاً از بین رفته است. نمودار شبکه‌ای سیستم «ای واکس» در شکل ۱-۵ نشان داده شده است.

۱-۱-۵ مراحل پروتکل «ای واکس»

این پروتکل برمبنای پروتکل پیشنهادی توسط فوجیوکا، اکاموتو و اهتا[3] بوده و به پنج مرحله تقسیم می‌شود: آماده‌سازی، راهبری، گمنام‌سازی، گردآوری و شمارش آرا. جزئیات این مراحل به‌شرح ذیل است:

۱-۱-۱-۵ آماده‌سازی[4]

۱. رأی‌دهنده به‌منظور درخواست ارسال تعرفه به یک سرور راهبر[5] وصل می‌شود.
۲. سرور راهبر در ابتدا مشخص می‌کند که رأی‌دهنده به کدام تعرفه انتخاباتی می‌تواند دسترسی داشته باشد. سپس تعرفه مربوطه را ارسال می‌کند. این تعرفه توسط سرور به‌صورت دیجیتالی امضا می‌شود.
۳. رأی‌دهنده تعرفه را تکمیل کرده و آن را به‌صورت مخفی درمی‌آورد و پس از امضای دیجیتالی، مجدداً برای سرور ارسال می‌نماید.

۲-۱-۱-۵ راهبری[6]

۱. راهبر در ابتدا کنترل می‌کند که آیا فرد حق رأی دادن دارد یا نه. درصورتی‌که فرد

---

1. Okamoto
2. Ohta
3. FOO protocol
4. Preparation
5. Administrator
6. Management

واجد شرایط نباشد درخواستش رد می‌شود.
۲. راهبر کنترل می‌کند که فرد قبلاً رأی نداده باشد. درصورت وجود رأی، درخواست وی رد می‌گردد.
۳. راهبر امضای دیجیتالی رأی‌دهنده در روی تعرفه را کنترل می‌کند. درصورت معتبر بودن امضای فرد، راهبر تعرفه را به‌صورت دیجیتالی امضا نموده و به رأی‌دهنده برمی‌گرداند.

۳-۱-۱-۵ گمنام‌سازی[1]

۱. پس از انتخاب گزینه مورد نظر، رأی‌دهنده تعرفه را با کلید عمومی شمارنده رمز نموده و از طریق یک کانال ارتباطی امن به گمنام‌کننده می‌فرستد.
۲. گمنام‌کننده کلیه آرای مربوط به انتخابات را ذخیره می‌کند.
۳. گمنام‌کننده ترتیب تعرفه‌های ارسالی را به‌صورت تصادفی تغییر می‌دهد. ازآنجاکه ترتیب آرای ارسالی به شمارشگر با ترتیب دریافت آنها متفاوت است، شمارشگر نمی‌تواند هیچ‌گونه ارتباطی بین رأی‌دهنده و زمان دادن رأی کشف نماید.

۴-۱-۱-۵ گردآوری[2]

پس از خاتمه انتخابات، شمارنده آرا را از گمنام‌کننده دریافت می‌کند. روند زیر در مورد هر تعرفه اجرا می‌گردد:
۱. شمارنده صحت امضای دیجیتالی مدیر در روی تعرفه را کنترل می‌کند. اگر صحت امضا تأیید نشود، یک شکایت رسمی به مسئولان مربوطه ارسال شده و رأی شمارش نمی‌گردد.
۲. وجود امضای مدیر در روی تعرفه رأی کنترل می‌گردد. هدف از کنترل این امضا، ممانعت از شرکت افراد در انتخاباتی است که مجاز به شرکت در آن نیستند.
۳. در هنگام اخذ رأی، اطلاعات دیجیتالی رأی‌دهنده در یک بایت ذخیره می‌شود که

---

1. Anonymization
2. Collection

با استفاده از این بایت می‌توان رأی‌های تکراری را کشف نمود. سرور شمارنده این بایت‌ها را کنترل نموده و درصورت مشاهده بایت‌های مشابه، تنها یکی از آرا را شمارش می‌نماید.

۵-۱-۱-۵ شمارش[1]

۱. آرا پس از پشت‌سر گذاشتن مرحله قبل، به سرور شمارشگر ارسال می‌شوند.
۲. پس از شمارش تمامی آرای رسیده، شمارشگر نتایج انتخابات را اعلام می‌کند. مسئولان احزاب شرکت‌کننده در انتخابات می‌توانند صحت نتایج را کنترل نمایند.

۵-۱-۲ جعل آرا

در پروتکل اولیه «ای واکس»، تنها یک راهبر مسئولیت کنترل آرا و صدور مجوز رأی‌دهی را به‌عهده دارد. بنابراین، یک راهبر خاطی می‌تواند از این امکان سوءاستفاده کرده و آرای جعلی ایجاد نماید. درواقع، سرور شمارشگر آرای گمنامی را دریافت نموده و نمی‌تواند تشخیص دهد که آرای دریافتی مربوط به یک رأی‌دهنده واجد شرایط بوده و یا توسط راهبر جعل شده است. تنها در صورت فزونی تعداد آرای شمارش شده نسبت به تعداد رأی‌دهندگان ثبت‌نام شده، جعل آرا توسط راهبر محرز می‌گردد.

راهبر می‌تواند به‌راحتی آرا را جعل نماید، به‌طوری‌که احتمال شناسایی خطا و کشف جعل بسیار پایین است. راهبر در طول انتخابات تعدادی تعرفه انتخاباتی با امضای دیجیتالی تولید کرده، اما آن را بلافاصله در اختیار گمنام‌کننده قرار نمی‌دهد، بلکه در لحظات پایانی انتخابات، در ابتدا مشخص می‌کند که چه تعدادی از افراد در انتخابات ثبت‌نام نموده، اما در رأی‌گیری شرکت نکرده‌اند. سپس از طرف این رأی‌دهندگان تعرفه‌های مورد نظر خود را به گمنام‌کننده می‌فرستد. اگر رأی‌دهندگان در دقایق پایانی انتخابات تصمیم به رأی‌دهی بگیرند، راهبر به فرد اجازه شرکت نداده و ادعا می‌کند که وقت انتخابات به پایان رسیده است و یا به‌راحتی پاسخ می‌دهد که ایجاد ارتباط با سرور به‌دلیل شلوغی خط ممکن نمی‌باشد. به‌این‌ترتیب، نتیجه نهایی این سیستم، انتخاباتی است که در آن همیشه تعداد آرا کوچک‌تر یا مساوی تعداد ثبت‌نام‌کنندگان است. به‌عبارت دیگر، تقلب راهبر سیستم قابل کشف نمی‌باشد.

---

1. Counting

۳-۱-۵ راهبران چندگانه

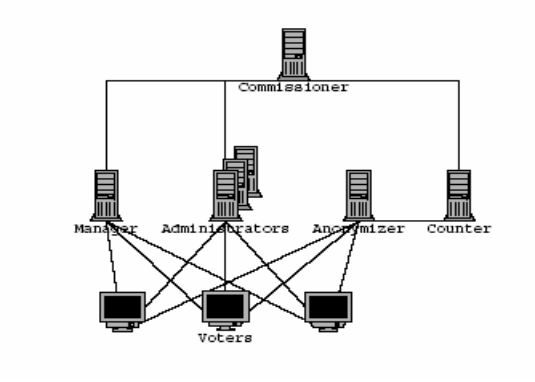
توزیع مسئولیت و بار کاری بین چندین راهبر دو فایده مهم دارد: اولاً امنیت کلی سیستم را افزایش می‌دهد؛ زیرا در این صورت یک راهبر قدرت جعل آرا را نخواهد داشت. ثانیاً در یک انتخابات با محدوده زمانی مشخص، یک راهبر تنها می‌تواند تعداد محدودی از تعرفه‌ها را به‌صورت دیجیتالی امضا نماید. بنابراین، با توزیع بار کاری، عملکرد سیستم بهبود می‌یابد.

همان‌طور که گفته شد، پروتکل «ای واکس» نسبت به جعل و تقلب بسیار آسیب‌پذیر است. در پروتکل اولیه که توسط فوجیوکو ارائه شد، این مشکل با ملزم کردن راهبر به انتشار فهرست رأی‌دهندگان مرتفع گردید. این فهرست حاوی اسامی افرادی بود که در رأی‌دهی شرکت کرده بودند. اگر افرادی برای شرکت در انتخابات الکترونیکی ثبت‌نام نموده اما در رأی‌گیری شرکت نکرده بودند، نامشان در این فهرست قید نمی‌شد. صحت این مکانیزم مستلزم بررسی و کنترل فهرست‌ها توسط رأی‌دهندگان بود. این کار ازنظر عملی چندان میسر نبود؛ زیرا هیچ تضمینی وجود نداشت افرادی که رأی نداده بودند، برای کنترل صحت انتخابات، لیست‌ها را کنترل نمایند. ممانعت از تقلب و جعل آرا باید بدون ایجاد مزاحمت و دردسر برای رأی‌دهندگان صورت پذیرد.

به‌منظور جلوگیری از جعل آرا توسط یک نفر راهبر مسئول، لازم است که تعرفه‌ها توسط چندین راهبر امضای الکترونیکی شود. به‌این‌ترتیب، هیچ راهبری نمی‌تواند از طرف یک رأی‌دهنده واجد شرایط و به‌جای او رأی دهد.

دو روش برای پیاده‌سازی راهبری چندگانه وجود دارد. قابل درک‌ترین راه‌حل این است که هر راهبر به‌صورت مستقل رأی را امضای الکترونیکی نماید. یک رأی درصورتی معتبر است که حاوی چندین امضا باشد. روش دیگر این است که آستانه‌ای برای تعداد امضاها درنظر گرفته شود.[۲۲] در این پروتکل‌ها یک امضای منفرد با استفاده از کلیدهای راهبران مختلف ایجاد می‌شود.

نمودار شبکه سیستم‌های «ای واکس» با مدیران چندتایی در شکل ۲-۵ نشان داده شده است.



شکل ۲-۵ مدیریت چندتایی در سیستم «ای واکس»

استفاده از چندین راهبر در سیستم، پیچیدگی‌های خاص خود را دارد. در زیر چندین پروتکل معرفی شده که به‌ظاهر معتبر به‌نظر می‌رسند، اما در عمل از امنیت کافی برخوردار نیستند.

۵-۱-۳-۱ پروتکل ساده[1]

این پروتکل ساده‌ترین شکل طرح امضاهای چندتایی است. سیستم شامل n راهبر بوده و برای تأیید تعرفه رأی، t امضا لازم است، به‌طوری‌که $t \leq n$. در این طرح درصورتی‌که $t \leq n/2$ باشد، احتمال رأی دادن تکراری افراد پیش می‌آید. در این حالت، زیرمجموعه‌های مستقلی از راهبران وجود خواهند داشت که می‌توانند تعرفه‌های مختلف را امضا کنند. بنابراین، رأی‌دهنده می‌تواند تعرفه خود را چندین بار به راهبران مختلف ارسال و تأیید آنها را دریافت نماید. ساده‌ترین راه‌حل برای رفع این مشکل این است که $t > n/2$ باشد. در این حالت، هیچ دو زیرمجموعه جدا از همی از راهبران تشکیل نخواهد شد.

۵-۱-۳-۲ پروتکل راهبران مرتبط[2]

برخی معتقدند درصورتی‌که راهبران بتوانند درخصوص تعرفه‌های امضا شده با یکدیگر

---

1. Simple Protocol
2. Communicating Administrator

ارتباط برقرار نمایند، امکان رأی‌دهی تکراری از بین خواهد رفت. در این صورت، راهبران باید بدانند که تعرفه مربوط به کیست و قبلاً توسط چه کسانی امضا شده است. اما اشکال این روش در این است که راهبر به هیچ طریقی نمی‌تواند تشخیص دهد که تعرفه قبلاً امضا شده است یا نه. این اطلاعات از دید راهبر مخفی می‌باشد. مخفی‌سازی تعرفه‌ها اطلاعات ثبت شده مربوط به آنها را تغییر می‌دهد. بنابراین، حتی تعرفه‌هایی با اطلاعات اولیه یکسان ممکن است درنظر راهبران متفاوت به‌نظر برسند.

۳-۳-۱-۵ پروتکل راهبران اداره شده[1]

یکی از راه‌حل‌های ارائه شده دیگر، استفاده از سرور مدیر است، به‌طوری که امضای این سرور برای تأیید رأی ضروری می‌باشد. در این پروتکل رأی‌دهنده باید $t < n$ امضا را به‌دست آورد. برای ممانعت از رأی‌دهی دوباره، مدیر فهرست راهبرانی را که تعرفه را امضا نموده‌اند، امضا می‌کند.

یکی از خطرات این پروتکل آن است که مدیر می‌تواند درخصوص رأی‌دهی چندباره با رأی‌دهندگان تبانی کند. بدتر اینکه مدیر با در دست داشتن کلید عمومی می‌تواند بدون اطلاع رأی‌دهنده، آرا را دستکاری نماید. زمانی که رأی‌دهنده برای به‌دست آوردن امضای مدیر، خود را به مدیر معرفی می‌کند، مدیر کد عبور رأی‌دهنده را در اختیار دارد. با استفاده از این کد رمز، کافی است که مدیر یک رأی جدید ساخته و آن را توسط راهبران مختلف که قبلاً برای این فرد رأیی را امضا نکرده‌اند، امضا نماید. پس از جمع‌آوری امضاهای کافی، مدیر می‌تواند فهرست راهبران را امضا کرده و آن را ارسال نماید.

تاکنون هیچ پروتکل مناسبی یافت نشده که به کمتر از $[n/2] + 1$ امضای راهبران نیاز داشته باشد. بنابراین، کاربران باید بدانند سیستم درصورتی امن خواهد بود که تعداد راهبرانی که تعرفه را امضا می‌کنند از نصف تعداد کل راهبران بیشتر باشد.

۴-۳-۱-۵ مراحل اجرایی پروتکل راهبران اداره شده

ایده اصلی پروتکل راهبران چندگانه مشابه پروتکل راهبری ساده است. این پروتکل نیز،

---

1. Managed Administrator

شامل پنج مرحله با تفاوت‌های ذیل می‌باشد:

۱. **آماده‌سازی**: در این پروتکل، تعرفه به‌جای راهبر توسط مدیر سیستم در اختیار افراد قرار می‌گیرد. این ایده تغییر قابل ملاحظه‌ای در امنیت سیستم ایجاد نمی‌کند، اما تنها مدیر است که به‌عنوان یک مسئول فعالیت‌های عمومی و مشترک توزیع تعرفه‌ها را انجام می‌دهد.

۲. **راهبری**: در این مرحله تعرفه‌ها به چندین راهبر فرستاده می‌شود. رأی‌دهنده برای دریافت امضای دیجیتالی، تعرفه مخفی خود را به تعداد معینی از راهبران ارسال می‌کند. این تعرفه‌ها در اصل با یکدیگر تفاوتی ندارند، اما به‌دلیل متفاوت بودن فاکتورهای مخفی‌سازی، از دید راهبران کاملاً متفاوت‌اند. تعرفه‌هایی که توسط رأی‌دهنده برای راهبران ارسال می‌شود، حاوی هیچ‌گونه اطلاعاتی در مورد راهبرانی که قبلاً تعرفه را امضا کرده‌اند، نیست. تنها رأی‌دهنده می‌داند که کدام‌یک از راهبران تعرفه او را امضا کرده‌اند. بنابراین، مجموعه امضاهای راهبران در یک تعرفه، نمی‌تواند محتوای رأی و هویت فرد رأی‌دهنده را افشا نماید. هر راهبر دقیقاً مانند یک راهبر واحد عمل می‌کند.

به‌منظور تکمیل عملیات راهبری یک مرحله نهایی به سیستم اضافه شده است. پس از امضای تعرفه توسط تعداد کافی از راهبران، رأی‌دهنده از مدیر سیستم درخواست امضای نهایی تعرفه را می‌کند. قبل از این مرحله، رأی‌دهنده فهرست راهبران را از دید مدیر سیستم مخفی می‌نماید. مدیر به ازای هر رأی‌دهنده یک فهرست را امضا می‌کند. وجود این امضا برای جلوگیری از رأی‌دهی مکرر رأی‌دهندگان ضروری است. مخفی کردن فهرست توسط رأی‌دهنده به این دلیل انجام می‌شود که مدیر نتواند با استفاده از فهرست راهبرانی که تعرفه را امضا کرده‌اند ارتباطی بین رأی و رأی‌دهنده پیدا کند.

۳. **گمنام‌سازی**: مرحله گمنام‌سازی دقیقاً برای حفظ محرمانگی رأی و رأی‌دهنده انجام می‌شود. به همین دلیل، این مشخصه در پروتکل جدید نیز بدون تغییر باقی مانده است.

۴. **گردآوری**: تعرفه، برای گذر از مرحله گردآوری به مرحله شمارش، باید دو آزمایش اضافی را پشت سر بگذارد. اولاً کنترل می‌شود که آیا تعرفه امضا شده به‌وسیله راهبران سیستم، توسط مدیر نیز امضای نهایی گردیده یا نه. ثانیاً آیا تعرفه حاوی تعداد کافی از امضای راهبران می‌باشد یا نه.

ترتیب انجام این کنترل‌ها هیچ‌گونه تأثیری بر امنیت انتخابات ندارد، اما به‌منظور حصول

کارایی بیشتر، کنترل وجود امضای مدیر قبل از کنترل امضاهای راهبران صورت می‌پذیرد؛ چرا که کنترل امضاها فرایندی پرهزینه است. بنابراین، تنها با کنترل امضای مدیر، ممکن است یک رأی باطل شده و از مرحله شمارش آرا حذف گردد و دیگر نیازی به کنترل امضاهای راهبران نباشد.

۵. **شمارش**: شمارش تعرفه‌ها در این پروتکل، مشابه پروتکل قبلی است، اما تعرفه‌هایی مورد شمارش قرار می‌گیرند که مرحله گردآوری را پشت سر گذاشته باشند. تمامی آرا در این مرحله قابل چاپ‌اند. ضعف عمده این پروتکل آن است که شمارنده می‌تواند از شمارش یک رأی امتناع کرده و قبل از چاپ فهرست داده‌های مربوطه، امضا را تغییر دهد. تنها رأی‌دهنده می‌تواند ثابت کند که رأیش شمرده شده یا نه. اما هدف این است که رأی‌دهنده تنها در یک مرحله درگیر فرایند انتخابات شود. یک راه‌حل بالقوه برای این مشکل، استفاده هم‌زمان از چندین شمارنده است. تنها در این صورت است که می‌توان ثابت کرد یک رأی توسط شمارنده‌ای دیگر از بین رفته است.

۲-۵ پروتکل «آر ای وی اس»

تاکنون پروتکل‌های مختلفی برای رأی‌گیری الکترونیکی ارائه شده، اما فقط تعداد کمی از آنها پیاده‌سازی گردیده است. اغلب این مدل‌ها روی مشخصه‌های پروتکل تأکید دارند و بسیاری از مسایل دنیای واقعی (مانند تحمل خرابی) را مدیریت نمی‌کنند.

سیستم «آر ای وی اس»[1] یک سیستم رأی‌گیری الکترونیکی قدرتمند است که برای محیط‌های گسترده و پرخطا مانند اینترنت طراحی شده است. هدف از ارائه سیستم «آر ای وی اس»، داشتن یک سیستم رأی‌گیری الکترونیکی است که بتواند مشخصه‌های سیستم‌های رأی‌گیری سنتی مانند دقت، دمکراسی، محرمانگی و تأییدپذیری را بهبود بخشد. علاوه بر آن، در سیستم «آر ای وی اس» خطاهای سناریوهای واقعی مانند خطای دستگاه و خطاهای خطوط مخابراتی که می‌تواند در اجرای پروتکل وقفه ایجاد نماید نیز مدنظر قرار گرفته است. این پروتکل در انتخابات الکترونیکی کشور پرتغال مورد استفاده قرار گرفت. قدرت «آر ای وی اس» در سه سطح است:

---

1. Robust Electronic Voting System (REVS)

۱. در هنگام بروز اشکال، فرایند رأی‌گیری متوقف شده و پس از رفع اشکال ادامه می‌یابد، بدون اینکه کوچک‌ترین خللی به اجرای پروتکل وارد آید.

۲. با استفاده از سرورهای تکراری[1] می‌توان میزان خطا را تا حد قابل قبولی کاهش داد.

۳. هیچ‌یک از سرورهای موجود در انتخابات نمی‌توانند به تنهایی و یا از طریق تبانی با دیگر سرورها به نتایج انتخابات خدشه‌ای وارد کنند.

در سالیان اخیر به‌منظور تسهیل روند انتخابات اقدامات گوناگونی انجام شده و به موازات انتخابات کاغذمحور از روش‌های جدید رأی‌دهی نیز استفاده گردیده است. به‌طور مثال می‌توان از صفحه‌های نمایش تماسی، پیام‌های کوتاه در تلفن همراه و استفاده از اینترنت نام برد.(۲۳)

سیستم‌های رأی‌گیری اینترنتی به چند دلیل از جذابیت بالایی برخوردارند:

۱. مردم به استفاده از رایانه برای انجام کارهایی مانند خرید، انجام عملیات بانکی از منزل یا محل کار و ... عادت کرده‌اند.

۲. به افراد امکان می‌دهد که بتوانند از هر جای دنیا در انتخابات شرکت کنند.

۳. هم‌زمان با اجرای فرایند رأی‌دهی، می‌توان صحت برگزاری انتخابات را کنترل نمود.

رای‌گیری از طریق اینترنت مسایل و مشکلات زیادی را به همراه دارد که مانع از استفاده گسترده این رسانه برای برگزاری انتخابات شده است.(۲۴)تا(۲۷) این مشکلات به سه گروه اساسی تقسیم می‌شوند:

۱. مشکلات مربوط به امنیت سیستم و میزان تحمل خرابی، که به معماری فعلی اینترنت برمی‌گردد. سرویس‌های مهمی همچون «دی ان اس»[2] می‌تواند دستکاری شود، اطلاعات در حین انتقال ممکن است تغییر یابد و یا به سرورهای خاص هدایت گردد.(۲۸) همچنین ممکن است خطوط ارتباطی دچار قطعی و یا خرابی شوند.

۲. مشکلات مربوط به محیط اجرایی پروتکل‌های رأی‌گیری، که شامل موارد زیر است:

ـ دستگاه‌هایی که توسط رأی‌دهندگان مورد استفاده قرار می‌گیرند باید قابل اطمینان بوده و به‌عنوان یک دستیار قابل اعتماد عمل نماید، اما عملاً به‌دلیل استفاده رایانه‌های

---

1. Replication Server

۲. Domain Name System (DNS) یک سرویس در محیط شبکه اینترنت است که برای ترجمه اسامی رایانه‌ها به آدرس‌های ip به‌کار می‌رود.

شخصی و چندکاربره از سیستم‌عامل‌های متفاوت، این کار مشکل به‌نظر می‌رسد.

ـ سرورهایی که در فرایند رأی‌گیری شرکت می‌کنند نباید از کار بیفتند، نباید قابل دسترسی غیرمجاز باشند و نباید قادر به سوءاستفاده از پروتکل‌های رأی‌گیری باشند.

ـ پروتکل رأی‌گیری نباید به‌دلیل خرابی دستگاه‌ها و یا مشکلات ارتباطی از کار بیفتد.

۳. برخی از مشکلات دیگر مربوط به ایجاد خرابکاری در پروتکل‌های رأی‌گیری و یا انتخابات در حال اجراست. نوع دیگری از این حملات، اعمال فشار به رأی‌دهندگان است و زمانی اتفاق می‌افتد که رأی‌دهندگان بدون حضور کمیته منتخب انتخابات، رأی می‌دهند.

«آر ای وی اس» یک سیستم رأی‌گیری اینترنتی است که بسیاری از این مشکلات را مرتفع کرده است. این پروتکل برای پوشش تمامی خطاهای سخت‌افزاری و ارتباطی از تجهیزات مختلفی استفاده می‌نماید.

در این پروتکل پنج سرور وجود دارد: عامل مسئول یا سرپرست،[1] توزیع‌کننده تعرفه،[2] مدیر،[3] گمنام‌کننده،[4] شمارنده.[5] همچنین از یک ماجول برای تعامل رأی‌دهنده با سرورهای انتخابات استفاده می‌شود (مانند گرفتن تعرفه‌ها، امضا شدن آنها توسط رأی‌دهنده و سرورها و ارسال آنها و ...).

۱-۲-۵ سرور سرپرست

ناظر و عامل مسئول انتخابات است و شکایات واصله از طرف رأی‌دهندگان و سرورهای انتخابات را دریافت می‌کند. اگر این شکایات سبب ایجاد شک و سوءظن نسبت به صحت انتخابات شود، برای یافتن علت آن، بررسی‌های لازم صورت می‌گیرد. این سرور عامل مسئول آماده‌سازی انتخابات، تولید و نگهداری کلیدهای محرمانه انتخابات، تعیین نوع سؤالات تعرفه‌ها و پیکربندی انتخابات است.

---

1. Commissioner
2. Ballot Distributor
3. Administrator
4. Anonymizer
5. Counter

۵-۲-۲ سرور توزیع‌کننده تعرفه

این سرور مسئول توزیع تعرفه‌ها و اطلاعات تنظیم شده توسط ناظر انتخابات است. هزینه کلی این فرایند براساس روش تبادل اطلاعات تعیین می‌گردد. تمامی اطلاعاتی که توسط این توزیع‌کننده در اختیار رأی‌دهندگان قرار می‌گیرد باید توسط ناظری که همگی به آن اطمینان دارند، امضا شود. ممکن است در عمل چندین توزیع‌کننده وجود داشته باشد. تعدد توزیع‌کنندگان علاوه بر اینکه بار کاری هر توزیع‌کننده را کاهش می‌دهد، سبب افزایش کارایی در انتخابات با مقیاس بزرگ می‌شود.

۵-۲-۳ سرور مدیر

عاملی در انتخابات است که می‌تواند در مورد پذیرش و یا عدم پذیرش تعرفه‌ها تصمیم بگیرد. یک تعرفه درصورتی قابل پذیرش است که ــ اگر و فقط اگر ــ حاوی حداقل امضاهای لازم توسط مدیر باشد. اگر n تعداد کل مدیران باشد، یک رأی‌دهنده باید به اندازه $t > n/2$ امضای معتبر از مدیران مختلف دریافت نماید تا تعرفه‌اش قابل پذیرش گردد. بنابراین، غیرممکن است که رأی‌دهنده بتواند دو رأی تکراری ارسال نماید. یک رأی‌دهنده از کدهای رمز متفاوتی برای به‌دست آوردن امضای مدیران استفاده می‌کند بدین ترتیب، با دانستن یک کد رمز، مدیر نمی‌تواند هویت رأی‌دهنده را جعل نماید.

۵-۲-۴ گمنام‌کننده

این سرور گمنام ماندن دستگاه فرد رأی‌دهنده را تضمین کرده و مانع از کشف ارتباط بین تعرفه و دستگاهی می‌شود که تعرفه از طریق آن ارسال شده است. یک رأی‌دهنده می‌تواند به تعداد دلخواه از گمنام‌کننده‌های موجود در انتخابات استفاده کند. گمنام‌کننده مکان رأی‌دهنده را مخفی نگه داشته و با ایجاد یک تأخیر زمانی تصادفی، ترتیب تعرفه‌های ارسالی را قبل از رسیدن به سرور شمارنده تغییر می‌دهد. درواقع، گمنام‌کننده مانع از آن می‌شود که با تجزیه و تحلیل زمان ارسال تعرفه، بتوان به هویت رأی‌دهنده پی برد.

۵-۲-۵ شمارنده

سروری است که اعتبار تعرفه‌ها و تعداد امضاهای مورد نیاز در آن را کنترل می‌کند. در

مرحله بعد شمارنده، بیت تأیید را که در فاز امضای تعرفه‌ها توسط رأی‌دهنده ایجاد شده برداشته و شمارش را آغاز می‌نماید.

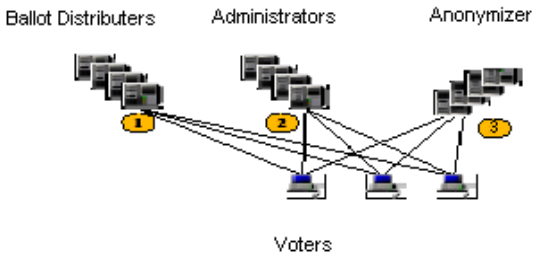
رأی‌دهنده رأی نهایی خود را از طریق گمنام‌کننده به شمارنده می‌فرستد. این تعرفه‌ها با کلید عمومی رمز می‌شوند. بنابراین، هیچ‌یک از این دو سرور نمی‌توانند در طول انتخابات از محتوای تعرفه‌ها آگاه گردند. تنها در پایان انتخابات و پس از آزادسازی کلید خصوصی است که سرورهای شمارنده می‌توانند نتایج انتخابات را تجزیه و تحلیل کنند.

در سیستم «آر ای وی اس» چندین سرور شمارنده وجود دارد که هریک از آنها توسط یک گمنام‌کننده مجزا قابل دسترسی است. رأی‌دهندگان می‌توانند آرایشان را به هر شمارنده و ــ یا به‌عبارت بهتر ــ به هر گمنام‌کننده‌ای بفرستند و حتی امکان ارسال یک رأی به چندین شمارنده هم وجود دارد. به این معنا که شمارنده‌های مختلف، در انتهای انتخابات مجموعه‌های متفاوتی از آرا را دریافت می‌کنند و حتی ممکن است حاوی آرای تکراری نیز باشند. یک شمارنده اصلی[1] پس از دریافت آرای شمارنده‌های مختلف، آرای تکراری را کنار گذاشته و نتیجه نهایی را اعلام می‌کند.

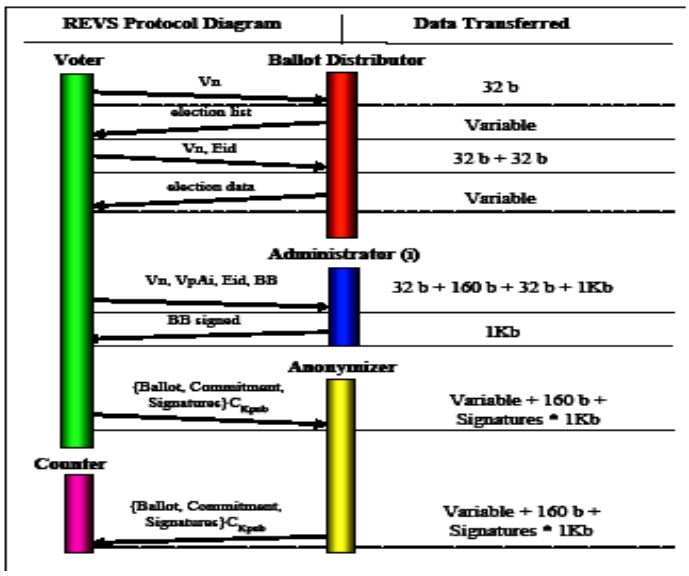
۶-۲-۵ روند اجرایی

پروتکل «آر ای وی اس» این امکان را فراهم می‌کند که بتوان کپی‌های متفاوتی از سرورهای درگیر در انتخابات داشت. تفاوت این پروتکل با پروتکل «ای واکس» در آن است که در این پروتکل با به‌کارگیری توزیع‌کننده تعرفه‌ها، تمامی عملیات منطقی در یک سرور مستقل انجام می‌شود. تنها محدودیت این پروتکل، تعداد امضاهای مورد نیاز برای تأیید اعتبار یک تعرفه است، یعنی $t> n/2$، که t تعداد امضاها و n تعداد مدیران می‌باشد. همان‌طور که در شکل ۳-۵ و ۴-۵ نشان داده شده، ازنظر رأی‌دهنده این پروتکل شامل سه مرحله است:

1. Master



شکل ۳-۵ پروتکل «آر ای وی اس»



V_n - Voter's Number

E_{id} - Election Identifications

V_p A_i -Voter's Password for Administrator i

BB - Blind Commited Ballot

{m}c_{kpub}-m Encrypted with Counter's Public Key

Election List - List of elections in which the voter can participate

Election Data-Ballot questions, elections configuration, Administration signing keys and election public key all signed key by the commissioner

شکل ۴-۵ جزئیات پروتکل «آر ای وی اس»

۵-۲-۶-۱ توزیع تعرفه‌ها

رأی‌دهنده با یک توزیع‌کننده تعرفه ارتباط برقرار کرده و برای شرکت در انتخابات مورد نظر یک تعرفه خالی دریافت می‌کند. توزیع‌کننده تعرفه، تعرفه درخواستی و کلید عمومی انتخابات را که توسط ناظر (سرپرست) امضا شده برای رأی‌دهنده می‌فرستد. این کار در دو مرحله اتفاق می‌افتد. در ابتدا رأی‌دهنده به سرور توزیع‌کننده تعرفه متصل شده و یک کد شناسایی برای دریافت فهرست انتخاباتی که او می‌تواند در آن شرکت کند، اخذ می‌کند. سپس رأی‌دهنده انتخابات مورد نظر را انتخاب کرده و از توزیع‌کننده درخواست تعرفه می‌نماید.

۵-۲-۶-۲ امضای تعرفه‌ها

پس از انتخاب کاندیدای مورد نظر در روی تعرفه، رأی‌دهنده یک رشته بیت تصادفی به تعرفه اضافه می‌کند و مجدداً آن را با یک عامل تصادفی به‌صورت مخفی درآورده و برای مدیر ارسال می‌نماید. مدیر پس از دریافت درخواست امضای تعرفه، در ابتدا کنترل می‌کند که آیا برای آن فرد رأی‌دهنده قبلاً تعرفه‌ای را امضا نموده است یا نه. اگر پاسخ منفی باشد، او تعرفه را امضا و امضا را ذخیره می‌کند و تعرفه امضا شده را نیز برای رأی‌دهنده ارسال می‌نماید.

پس از دریافت امضا، رأی‌دهنده با استفاده از کلید عمومی مدیر و عامل مخفی‌کننده‌اش، صحت تعرفه برگشتی را کنترل می‌کند. این فرایند برای جمع‌آوری کلیه امضاهای مورد نیاز (t) ادامه می‌یابد. باید توجه داشت که مدیران نمی‌توانند بین امضاهای خود و امضاهای رأی‌دهندگان ارتباطی برقرار نمایند.

۵-۲-۶-۳ ارسال تعرفه‌ها

در این مرحله رأی‌دهنده بسته اطلاعاتی رأی را با الحاق تعرفه رأی، به‌صورت دیجیتالی امضا کرده و آن را تأیید می‌نماید. وی می‌تواند این بسته اطلاعاتی را در یک وسیله ذخیره‌سازی امن، ذخیره کند. این مرحله اختیاری بوده و تضمینی برای اثبات دقت و صحت عملکرد سیستم است، اما محرمانگی رأی را خدشه‌دار می‌سازد. در مرحله بعد،

رأی‌دهنده بسته اطلاعاتی رمز شده را به گمنام‌کننده می‌فرستد. به‌منظور حصول اطمینان، رأی‌دهنده می‌تواند یک بسته اطلاعاتی را به چندین شمارنده ارسال کند.

پس از خاتمه انتخابات، ناظر کلید خصوصی انتخابات را منتشر می‌کند. سپس فرایند شمارش آرا به‌وسیله سرورهای شمارش و در طی مراحل زیر اجرا می‌گردد:

۱. رمزگشایی بسته‌های اطلاعاتی رسیده با استفاده از کلید خصوصی،

۲. کنترل تعداد امضاهای مورد نیاز (یعنی t)،

۳. حذف آرای تکراری،

۴. شمارش آرای باقیمانده،

۵. زمانی که از چندین شمارنده استفاده می‌شود، شمارنده اصلی همه آرای تأیید شده را دریافت می‌کند و آرای تکراری را مشخص نموده و نتایج نهایی را اعلام می‌کند.

در خاتمه، شمارنده‌ها محتوای بسته‌های اطلاعاتی دریافتی و مدیران تمامی تعرفه‌های امضا شده مخفی را چاپ می‌کنند. در نتیجه، رأی‌دهنده می‌تواند مطمئن شود که رأیش شمارش گردیده است. اگر رأی در نتایج اعلام شده حضور نداشته باشد، رأی‌دهنده می‌تواند با استفاده از بسته اطلاعاتی ذخیره شده ادعای ارسال صحیح رأیش را اثبات نماید. همچنین تعداد کل آرا و تعداد آرای تأیید شده نیز قابل تشخیص می‌باشد.

۵-۲-۷ شرایط اجرای پروتکل

پروتکل «آر ای وی اس» در محیط جاوا به‌کار می‌رود و با همه سیستم‌عامل‌ها قابل اجراست. برای رمزنگاری نیز از یک نرم‌افزار رمزنگاری[1] و در روی سرورها از یک پایگاه اطلاعاتی[2] استفاده می‌شود.

۵-۲-۷-۱ آماده‌سازی انتخابات

قبل از اجرای پروتکل «آر ای وی اس» لازم است که مقدماتی فراهم گردد. این مقدمات شامل تولید زوج کلیدها، ثبت‌نام از رأی‌دهندگان و پیکربندی سرورهاست. ثبت‌نام از رأی‌دهندگان شامل تعریف مشخصات آنها (کد کاربری) و جمع‌آوری کد رمز آنها برای مدیران است (این

---

1. logi.crypt
2. MYSQL

عمل بسیار مطمئن است؛ زیرا کدهای رمز به‌روشی مشابه یونیکس ذخیره می‌گردند).

پیکربندی سرورها شامل نصب آنها (ایجاد کلید خصوصی و عمومی) و مقداردهی اولیه پایگاه‌های اطلاعاتی با اطلاعات مربوط به انتخابات و رأی‌دهندگان است. نرم‌افزار رأی‌گیری در هنگام ثبت‌نام از رأی‌دهندگان در اختیار آنان قرار گرفته و یا از طریق تارنمای انتخابات بارگذاری می‌شود. همچنین این نرم‌افزار از طریق سرورهای توزیع‌کننده تعرفه‌ها قابل دریافت بوده و حاوی کلید عمومی ناظر نیز هست.

۸-۲-۵ امنیت سیستم

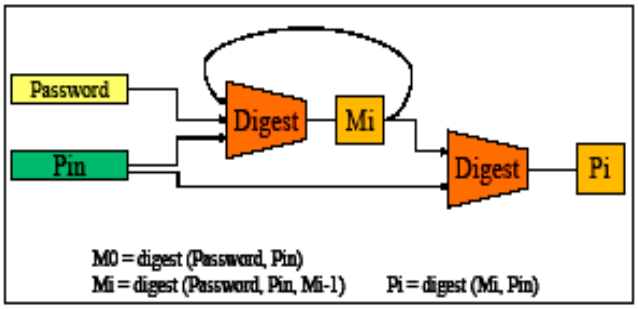
مدیریت سیستم «ای واکس»، قابلیت برگزاری هم‌زمان چندین انتخابات را دارد. در این حالت، تعرفه‌های خاص هر انتخابات بین رأی‌دهندگان واجد شرایط توزیع می‌شود، اما هیچ تضمینی برای جابه‌جایی تعرفه‌ها توسط رأی‌دهندگان و یا سرقت آنها وجود ندارد. در نتیجه این امکان وجود دارد که بعضی از افراد در انتخاباتی که واجد شرایط شرکت در آن نیستند، شرکت نمایند. در سیستم «آر ای وی اس»، مدیر هر انتخابات، یک زوج کلید نامتقارن دارد. اگر رأی‌دهندگان تعرفه‌ها را جابه‌جا کنند، امضاها با یکدیگر مطابقت نداشته و در نتیجه رأی باطل اعلام می‌گردد.

ماجول رأی‌دهنده هویت رأی‌دهنده را مشخص می‌کند و بسیار مهم است که رأی‌دهنده به آن اطمینان داشته باشد. در سیستم «آر ای وی اس» برای اطمینان از جامعیت رأی، این ماجول حاوی امضای الکترونیکی ناظر است. در هنگام به‌کارگیری یک برنامه کاربردی مطمئن، مواردی همچون هویت‌شناسی و امنیت ارتباطات باید به‌دقت مدنظر قرار بگیرد. در پروتکل «آر ای وی اس»، رأی‌دهنده در هنگام ایجاد ارتباط با سرور از کلید عمومی سرور برای شناسایی آن استفاده می‌کند.

برای شناسایی رأی‌دهندگان از روش ارائه کد کاربری و رمز عبور استفاده می‌شود. رأی‌دهنده به‌منظور ممانعت از جعل هویتش، در هنگام برقراری ارتباط با سرورهای مدیریتی مختلف، از رمزهای عبور مختلف استفاده می‌کند. اما به‌منظور حفظ مشخصه کاربرپسند[1] بودن مرحله هویت‌شناسی، نیازی نیست که کاربر تمامی این رمزها را به‌خاطر

1. User-friendly

بسپارد. به‌عبارت‌دیگر، برای ایجاد تمامی رمزهای مورد نیاز از یک الگوریتم خاص استفاده شده است. این الگوریتم از دو رمز استفاده می‌کند: یک رمز قوی (نه یک رمز معمولی، مانند یک رشته کاراکتر تصادفی) و یک پین‌کد فعال که باید توسط رأی‌دهنده به‌خاطر سپرده شود. روش تولید رمز عبور در شکل ۵-۵ نشان داده شده است:



شکل ۵-۵ تولید رمز عبور

این دو رمز عبور در ماجول رأی‌دهنده ایجاد شده و پس از آن به ازای هر مدیر یک رمز عبور تولید می‌شود.

M_0 =digest (password, pin)
M_i =digest (password, pin, m_{i-1})
P_i =digest (m_i, pin)

به‌دلیل اینکه این الگوریتم از توابع خلاصه‌ساز[۱] استفاده می‌کند، مدیر A_i رمز P_i را می‌داند، اما نمی‌تواند رمزهای Pj را محاسبه کند. برای افزایش امنیت سیستم دو رمز عبور اولیه توسط رأی‌دهنده انتخاب می‌شود. در مرحله ثبت‌نام، رأی‌دهنده برای احراز هویتش از رمزهای واقعی خود استفاده می‌کند. در روش دیگر می‌توان به رأی‌دهنده در ابتدا رمز عبور داد و سپس این امکان را برای او فراهم کرد که خودش رمزهای عبورش را تغییر دهد.

---

۱. تابعی است که پارامترهای ورودی با طول دلخواه را به یک پارامتر خروجی با طول معین تبدیل می‌کند و مزیتش این است که خروجی طول ثابت دارد. این مسئله در هنگام ذخیره‌سازی یا پردازش از اهمیت برخوردار است. دیگر اینکه پارامتر خروجی کوتاه‌تر از پارامتر ورودی است. بنابراین، پردازش و ذخیره‌سازی نیز سریع‌تر خواهد بود. از این تابع در پروتکل‌های رمزنگاری استفاده می‌شود (digest).

۹-۲-۵ ارزیابی عملکرد پروتکل «آر ای وی اس»

در این خصوص می‌توان به موارد ذیل اشاره کرد:

- شکستن الگوریتم‌های رمزنگاری استفاده شده بسیار پیچیده بوده و در این پروتکل از سه الگوریتم رمزنگاری استفاده شده است:

ـ الگوریتم «آر اس ای»[1] برای تولید و کنترل امضاهای مخفی و غیرمخفی و رمزگذاری بسته اطلاعاتی ارسالی،

ـ الگوریتم «تریپل دس»[2] برای رمزگذاری بسته اطلاعاتی،

ـ الگوریتم «اس اچ ای»[3] برای همه محاسبات مربوط به تابع خلاصه‌ساز.

- ارتباطات بسیار امن است. همه ارتباطات در «آر ای وی اس» از لایه امن[4] استفاده کرده و همه سرورها به‌وسیله کلید عمومی شناسایی می‌شوند.
- تمامی سرورها، رایانه‌ها و دروازه‌های ارتباطی در مقابل حملات ویروسی غیرقابل نفوذند.
- گمنامی به‌دقت تضمین شده و به‌درستی عمل می‌نماید.
- تعداد امضاهای مورد نیاز برابر است با $t>n/2$.
- رأی‌دهنده می‌تواند اطلاعات مورد نظر خود را در مراحل دوم و سوم پروتکل رأی‌گیری در یک وسیله ذخیره‌سازی امن ذخیره کند.
- ناظر تنها در خاتمه انتخابات است که می‌تواند کلید خصوصی را منتشر نماید.
- **دقت**: رأی نمی‌تواند تغییر یابد؛ زیرا این کار باعث از بین رفتن امضاهای مدیران و در نتیجه ابطال رأی می‌گردد. اگر رأی فرد در شمارش نهایی آرا ملحوظ نشده باشد، رأی‌دهنده می‌تواند ضمن کنترل فهرست آرای دریافتی که توسط شمارنده چاپ گردیده، از حذف رأی خود مطلع شود. حذف رأی در هنگام استفاده از چندین شمارنده بسیار مشکل‌تر است؛ چرا که باید رأی از پایگاه اطلاعاتی همه شمارنده‌ها حذف گردد. از آنجایی که امضاها به همراه

---

1. RSA Algorithm
2. Triple-DES
3. SHA Algorithm

۴. Secure Socket Layer (SSL): یک فناوری استاندارد برای تأمین ارتباطی امن مابین یک وب سرور و یک مرورگر اینترنت است. این ارتباط امن از تمامی اطلاعات ردوبدل شده محافظت می‌کند تا در حین انتقال به‌صورت محرمانه و دست‌نخورده باقی بماند.

آرا منتشر می‌شود، غیرممکن است که یک رأی نامعتبر در لیست نهایی وجود داشته باشد. بنابراین، جنبه‌های مختلف ویژگی «دقت» در این پروتکل لحاظ شده است.

- **دمکراسی**: هر رأی‌دهنده در هر انتخابات تنها می‌تواند یک‌بار رأی دهد؛ زیرا $t>n/2$ (رأی‌دهنده نمی‌تواند دو امضای معتبر به‌دست آورد). همه رأی‌دهندگان می‌توانند مادامی‌که t مدیر و یک گمنام‌کننده حضور دارند، رأی دهند، پس دمکراسی نیز تضمین می‌گردد.
- **محرمانگی**: با توجه به روش‌های رمزگذاری پیش‌گفته، بخش اول محرمانگی تضمین می‌شود. اما بخش دوم، مشابه بسیاری از پروتکل‌های رأی‌گیری، هنوز تکمیل نشده است؛ چرا که رأی‌دهنده می‌تواند گزینه انتخابی‌اش را آشکار سازد.
- **قابلیت اثبات**: هر رأی‌دهنده می‌تواند اطمینان حاصل کند که رأیش در هنگام شمارش آرا درنظر گرفته شده است. همچنین با مشاهده امضای دیجیتالی به همراه رأی در فهرست منتشر شده، مطمئن می‌شود که سایر آرا نیز معتبرند.
- **قابلیت دسترسی**: سیستم مادامی‌که حداقل سرورهای مورد نیاز در حال کار می‌باشند، قابل دسترس است. این حداقل عبارت است از یک سرور توزیع‌کننده تعرفه، t مدیر، یک زوج گمنام‌کننده / شمارنده.

«آر ای وی اس» یک سیستم رأی‌گیری الکترونیکی قدرتمند است که می‌تواند در محیط‌های پرخطا مانند اینترنت مورد استفاده قرار گیرد. این سیستم مبتنی‌بر امضاهای مخفی بوده و تمامی ویژگی‌های یک سیستم رأی‌گیری مطلوب را داراست.

مشخصه مهم دیگر سیستم «آر ای وی اس»، مستقل بودن از نوع تعرفه‌هاست، پس می‌تواند در انتخابات مختلف مورد استفاده قرار گیرد. این سیستم برای انتخابات با مقیاس بزرگ طراحی شده است. «آر ای وی اس» در محیط جاوا پیاده‌سازی شده و برای جلوگیری از ایجاد گلوگاه می‌توان از تکرار سرورها[1] استفاده کرد.

۳-۵ پروتکل «سلز»[2]

در این قسمت به معرفی یک سیستم رأی‌گیری الکترونیکی مطمئن برای انتخابات

---

1. Replication
2. Secure Electoral Electronic System (SELES)

برخط با مقیاس متوسط می‌پردازیم. این سیستم از یک پروتکل ارتباطی امن با نام «سلز» استفاده می‌کند که مانع تقلب و رأی‌دهی چندباره افراد می‌گردد. پروتکل «سلز» در ششمین کنفرانس بین‌المللی علوم رایانه که از تاریخ ۲۶-۳۰ سپتامبر ۲۰۰۵ در مکزیک برگزار شد، توسط فرانسیسکو رودرز[1] اسپانیایی ارائه گردید.

«سلز» حاوی تمامی استانداردهای سیستم‌های سنتی از جمله دقت، دمکراسی، محرمانگی، سهولت کاربرد، قابلیت انعطاف، قابلیت ردیابی و قابلیت کشف آرای تکراری است. این سیستم در یک شبکه اینترنت توزیع شده و ناهمگن مورد آزمایش قرار گرفته و شامل ایستگاه‌های کاری، رایانه‌های کیفی و رایانه‌های جیبی[2] است که از ارتباطات باسیم و یا بدون‌سیم استفاده کرده‌اند.

۱-۳-۵ مراحل پروتکل

این پروتکل شامل سه مرحله است: هویت‌شناسی، رأی‌گیری و شمارش آرا. در این پروتکل تعامل بین چهار موجودیت مدنظر است: رأی‌دهنده، سرور هویت‌شناسی، سرور رأی‌گیری و سرور شمارش آرا. ابزارهای رمزنگاری مورد استفاده در این پروتکل عبارت‌اند از: گواهی‌نامه دیجیتالی، امضاهای مخفی و نشان زمانی. علائم به‌کار گرفته شده برای توصیف این پروتکل هم عبارت‌اند از:

V: رأی‌دهنده،

AS: سرور هویت‌شناسی،

VS: سرور رأی‌گیری،

TCS: سرور شمارش آرا،

t: نشان زمانی،

q: پارامتر DSA، $2^{159}<q<2^{160}$،

L: در فاصله $0\leq L\leq 8$ قرار دارد و p در فاصله $2^{512\,64L}<p<2^{511+64L}$ به‌دست می‌آید،

---

1. Francisco Rodrez

۲. Personal Digital Assistant (PDA): رایانه کوچک سبک‌وزنی که برای انجام عملیات شخصی مانند تقویم، دفترچه یادداشت و ... طراحی شده است.

g: مولد Z^*_p،

a: کلید خصوصی DSA، به‌طوری‌که $1 \le a \le q-1$،

α: $g^{(p-1)/q} \bmod p$،

y: $\alpha^a \bmod p$،

cert: گواهی‌نامه دیجیتالی که به‌وسیله فرد صلاحیت‌دار داده می‌شود.

n_x, $\{e_x, d_x\}$ اطلاعات کلید برای کاربر x است، به‌طوری‌که $n_x = p1 * p2$ که p1 و p2 دو عدد بزرگ اول بوده و $e_x * d_x \bmod \varphi(n_x) = 1$. در ادامه، سه مرحله این پروتکل مورد بررسی قرار می‌گیرد.

۱-۱-۳-۵ هویت‌شناسی

هویت‌شناسی شامل سه مرحله است:

۱. رأی‌دهنده دو عامل مخفی b_1 و b_2 و دو عدد تصادفی k_1 و a را انتخاب می‌کند. با استفاده از این اعداد و پارامترهای دیگر، مقادیر z_2، z_1 و y به شکل زیر تولید می‌شود:

$y = \alpha^a \bmod p$

$z_1 = [(\alpha^a \bmod p).(b_1^{eAS})] \bmod n_{AS}$

$z_2 = [(\alpha^{k1} \bmod p).(b_2^{eAS})] \bmod n_{AS}$

سپس رأی‌دهنده اطلاعات زیر را برای شناسایی به سرور هویت‌شناسی می‌فرستند:

$\{V, AS, Cert_V, t, z_1, z_2, [(z_1 \,ll\, z_2 \,ll\, t)^{dV} \bmod n_V]\}$

۲. این سرور صحت امضای رأی‌دهنده، یعنی $[(z_1 \,ll\, z_2 \,ll\, t)^{dV} \bmod n_V]$ را با کلید عمومی که در $Cert_V$ قرار دارد مقایسه می‌کند. اگر امضا معتبر باشد، سرور هویت‌شناسی عدد تصادفی k_2 را انتخاب کرده و آن را در یک پایگاه داده به‌عنوان کد شناسایی ذخیره می‌نماید. بنابراین، مقدار k_2 باید برای هر فرد منحصربه‌فرد باشد. در مرحله بعد سرور هویت‌شناسی مقادیر زیر را ایجاد می‌کند:

$z_3 = (k^2 \,ll\, t)^{eV} \bmod n_V$

$z_4 = (z_1 \times AS)^{dAS} \bmod n_{AS} = [(\alpha^a \bmod p) \times AS]^{d}_{AS}\, b_1 \bmod n_{AS}$

$z_5 = (z_2 \times (\alpha^{k2} \bmod p) \times AS)^{\overset{d}{AS}} \bmod n_{AS}$

$= [(\alpha^{k1} \bmod p) \times (\alpha^{k2} \bmod p) \times AS]^{d}_{AS}\, b2 \bmod n_{AS}$

$z_6 = (z_2 \times (\alpha^{k2} \bmod p) \times AS)^{\overset{d}{AS}} \bmod n_{AS}$

در نهایت، سرور هویت‌شناسی پیغام پاسخ را برای رأی‌دهنده می‌فرستد. توجه به این نکته ضروری است که مقادیر z_4 و z_5 و z_6 جداگانه توسط کلید عمومی رأی‌دهنده رمز می‌شوند. علاوه بر این، یک نشان زمانی t به پیغام اضافه می‌گردد، به این دلیل که سه مقدار فوق نمی‌توانند به‌صورت هم‌زمان به رمز درآیند.

۳. رأی‌دهنده z_3 را رمزگشایی کرده و k_2 را به‌دست می‌آورد. علاوه بر این، رأی‌دهنده می‌تواند z_4 و z_5 و z_6 را با استفاده از عدد توانی d_v رمزگشایی نماید. سپس فاکتورهای مخفی برداشته شده و مقادیر s_1 و s_2 و s_3 تولید می‌شود.

$$s_1 = z_4 \times b_1^{-1} = [(\alpha^a \bmod p)\times AS]^{d_{AS}} \bmod n_{AS}$$
$$s_2 = z_5 \times b_2^{-1} = [(\alpha^{k1} \bmod p)\times(\alpha^{k2} \bmod p)\times AS]^{d_{AS}} \bmod n_{AS}$$
$$s_3 = z_6 \times b_2^{-2} = [(\alpha^{2k1} \bmod p)\times(\alpha^{k2} \bmod p)\times AS]^{d_{AS}} \bmod n_{AS}$$

۲-۱-۳-۵ رأی‌گیری

رأی‌گیری شامل سه مرحله است:

۱. در مرحله رأی‌گیری، رأی‌دهنده تعرفه m را با استفاده از الگوریتم امضای دیجیتالی و x_1, x_2 به‌عنوان کلید خصوصی امضا می‌کند. رأی‌دهنده می‌تواند این مقادیر را تولید کند؛ زیرا او قبلاً k_2 را رمزگشایی کرده است. باید توجه داشت که دو امضا در زوج‌های (r_1, s_4), (r_2, s_5) وجود دارد. به‌عبارت‌دیگر، بخش نخست امضاها، یعنی r_1 و r_2 می‌توانند از روش زیر به‌دست آیند:

$$x_1 = k_1 + k_2$$
$$x_2 = 2k_1 + k_2$$
$$r_1 = (\alpha^{x1} \bmod p) \bmod q$$
$$r_2 = (\alpha^{x2} \bmod p) \bmod q$$

بخش دوم امضا که s_5 و s_4 نامیده می‌شود، از طریق محاسبات زیر به‌دست می‌آید:

$$s_4 = x_1^{-1}(m + a r_1) \bmod q$$
$$s_5 = x_2^{-1}(m + a r_2) \bmod q$$

علاوه بر این، لازم است مقادیر L2 , L1 را محاسبه نماید:

$L1=[((\alpha^{k1} \bmod p) \bmod n_{AS}) \times ((\alpha^{k2} \bmod p) \bmod n_{AS})] \bmod n_{AS}$
$L2=[((\alpha^{k1} \bmod p)^{2} \bmod n_{AS}) \times ((\alpha^{k2} \bmod p) \bmod n_{AS})] \bmod n_{AS}$

در مرحله بعد دو مقدار pr1, pr2 از طریق روش زیر محاسبه می‌گردد:

$pr_1=[(r_1 \times n_{AS})+(l_1 \times q)] \bmod(n_{AS}. q)$
$pr_2=[(r_2 \times n_{AS})+(l_2 \times q)] \bmod(n_{AS}. q)$

در نهایت، تعرفه رأی به شکل زیر ایجاد می‌شود:

$Ticket = \{s_1, s_2, s_3, s_4, s_5, y, pr_1, pr_2, m\}$

۲. رأی‌دهنده این رأی را به سرور رأی‌گیری می‌فرستد. این سرور درمجموع پنج امضا را تأیید اعتبار می‌کند. سه معادله تأیید اعتبار به شکل زیر است:

$(AS \times y) \bmod n_{AS} = s_1^{\ e_{AS}} \bmod n_{AS}$
$(AS \times pr1. q^{-1} \bmod n_{AS} = s_2^{\ eAS} \bmod n_{AS}$
$(AS \times pr_2 . q^{-1} \bmod n_{AS} = s_3^{\ eAS} \bmod n_{AS}$

برای تأیید امضاهای دیجیتالی از رویه زیر استفاده می‌شود:

```
DSAverifier(r, s)
{
w = s^-1 mod q
u1 = w. m mod q
 u2 = r. w mod q
v = (α^u1 y^u2 mod p) mod q
 return v
}
```

سپس صحت امضاهای s1, s2 با معادله زیر کنترل می‌شود:

$r_1 = DSAverifier\ (r_1, s_4)$
$r_2 = DSAverifier\ (r_2, s_5)$

۳. اگر هر پنج امضا به‌درستی تأیید شود، سرور رأی‌گیری تعرفه فرستاده شده توسط رأی‌دهنده را به‌عنوان یک رأی معتبر ذخیره می‌کند.

پس از اتمام مدت رأی‌گیری، سرور رأی‌گیری همه تعرفه‌های دریافتی معتبر را از طریق شبکه‌های ارتباطی به سرور شمارش می‌فرستد.

۳-۱-۳-۵ مرحله شمارش آرا

سرور شمارش تعرفه‌های معتبر را از سرورهای رأی‌گیری دریافت کرده و تعرفه‌های یکسان را تشخیص می‌دهد و آنها را تنها یک‌بار مورد شمارش قرار می‌دهد. در این مرحله می‌توان رأی‌دهندگان خاطی را که ممکن است چندین بار رأی داده باشند، شناسایی کرد. رأی‌دهنده از کلید مشابه برای امضای آرای مختلف استفاده می‌کند. بنابراین، به‌راحتی می‌توان آرای تکراری را تشخیص داد. سرور شمارش حداقل دو تعرفه به شکل زیر دریافت می‌کند:

$B_1=\{s_1, s_2, s_3, s_4, s_5, y, pr_1, pr_2, m\}$

$B_2=\{s_1, s_2, s_3, s'_4, s'_5, y, pr_1, pr_2, m'\}$

این سرور هویت رأی‌دهنده را با استفاده از اطلاعاتی که از این دو تعرفه به‌دست می‌آید از طریق معادلات زیر مشخص می‌نماید:

$$x_1 = \frac{m'-m}{s_4'-s_4} \bmod q$$

$$x_2 = \frac{m'-m}{s_5'-s_5} \bmod q$$

$$k_1 = x_2 - x_1$$

$$k_2 = x_1 - k_1$$

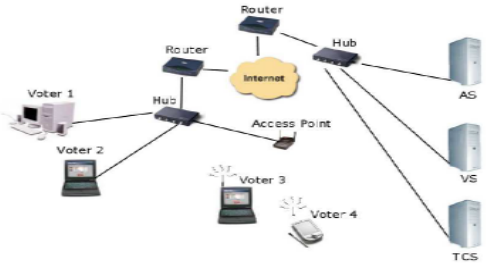
همان‌طور که قبلاً خاطرنشان گردید، تمامی مقادیر k_2 که به رأی‌دهندگان اختصاص یافته در بانک اطلاعاتی سرور هویت‌شناسی ذخیره می‌شود. بنابراین، سرور شمارش می‌تواند از سرور هویت‌شناسی نام رأی‌دهنده متناظر با مقدار محاسبه شده k_2 را درخواست نماید. به‌این‌ترتیب، هویت رأی‌دهنده خاطی مشخص می‌گردد.

۲-۳-۵ کاربرد پروتکل

پروتکل «سلز» برای انتخابات الکترونیکی با مقیاس متوسط (حدود چندین ده‌هزار رأی‌دهنده) طراحی و پیاده‌سازی شده است. محدودیت تعداد رأی‌دهندگان عمدتاً به وب سرور به‌کار گرفته شده بستگی دارد. این متدلوژی براساس الگوی مشتری کارگزار عمل نموده و به‌صورت هم‌زمان از چندین تکنیک و ابزار رمزنگاری استفاده می‌کند. در

نتیجه، صحت و دقت و امنیت پروتکل تضمین می‌شود.

در عمل، رأی‌دهنده با یک برنامه کاربردی سروکار دارد. این برنامه می‌تواند با محدوده گسترده‌ای از دستگاه‌ها از جمله رایانه و رایانه کیفی مورد استفاده قرار گیرد. رأی‌دهندگان واجد شرایط می‌توانند از طریق شبکه‌های اینترنتی باسیم یا بدون سیم در انتخابات شرکت کنند. معماری کلی سیستم «سلز» در شکل ۶-۵ نشان داده شده است:



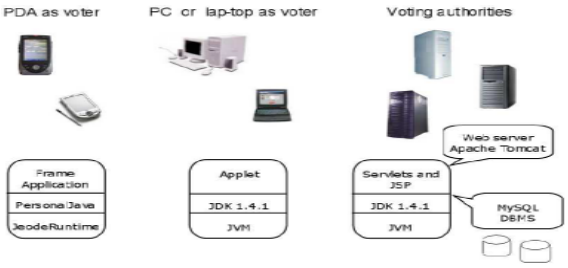
شکل ۶-۵ معماری کلی سیستم «سلز»

شرکت‌کنندگانی که از رایانه‌های قوی استفاده می‌کنند، می‌توانند بدون استفاده از برنامه‌های کاربردی محلی در انتخابات شرکت نمایند. ضمناً کاربران می‌توانند در هنگام ثبت‌نام برای شرکت در انتخابات الکترونیکی نرم‌افزارهای مربوطه را بارگذاری[1] کنند.

شکل ۷-۵ یک مدل لایه‌ای از بالا به پایین را برای هر یک از دستگاه‌های موجود در سیستم نشان می‌دهد. همان‌طورکه بیان شد، در پروتکل «سلز» سه سرور مسئول تعریف می‌شود: سرور هویت‌شناسی، سرور رأی‌گیری و سرور شمارش. علاوه بر این، یک مسئول صدور مجوز[2] نیز مورد نیاز است که در مرحله مقدماتی، زوج کلیدهای عمومی و خصوصی شرکت‌کنندگان را تولید می‌نماید. برای تمامی شرکت‌کنندگان در انتخابات (رأی‌دهندگان و مسئولان) یک زوج کلید عمومی و خصوصی (۱۰۲۴ بیتی) درنظر گرفته می‌شود. علاوه بر این، مسئول صدور مجوز، توزیع گواهی‌نامه‌های دیجیتالی متناظر با هر کلید عمومی را نیز به‌عهده دارد.

---

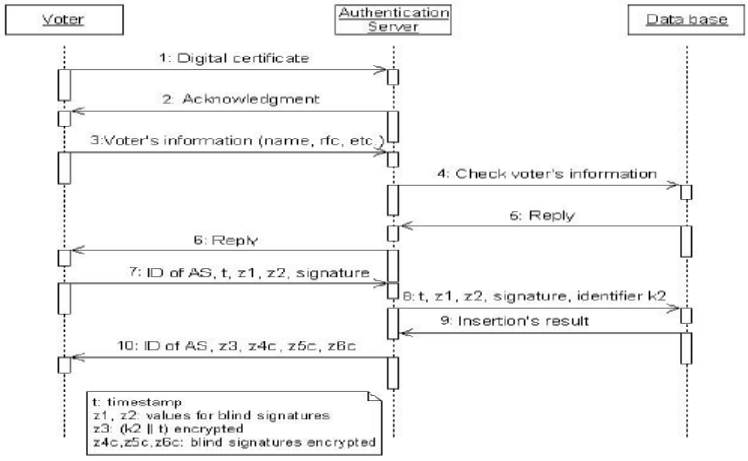
1. Download
2. Certificate Authority (CA)



شکل ۷-۵ مدل «سلز» لایه‌ای از بالا به پایین

۵-۳-۳ سرور هویت‌شناسی[1]

وظیفه این سرور احراز هویت کاربرانی است که برای شرکت در انتخابات ثبت‌نام کرده‌اند. ازنظر پروتکل «سلز» کاربر واجد شرایط کسی است که به‌طور صحیح در پایگاه اطلاعاتی انتخابات در سرور هویت‌شناسی ثبت‌نام نموده است. شکل ۸-۵ جریان داده بین رأی‌دهنده و سرور هویت‌شناسی را در مرحله احراز هویت نشان می‌دهد.



شکل ۸-۵ جریان داده بین رأی‌دهنده و سرور هویت‌شناسی

1. Authentication Server (AS)

سرور هویت‌شناسی مسئول دریافت گواهی‌نامه‌های دیجیتالی کاربران به همراه اطلاعات شخصی آنهاست. این سرور شناسه عمومی و امضای دریافتی را تأیید اعتبار می‌کند. مرحله بعدی، کنترل هویت رأی‌دهنده است، به‌عنوان مثال، اینکه آیا قبلاً یک امضای مخفی به کاربر اختصاص داده شده یا نه. اگر جواب مثبت باشد، سرور هویت‌شناسی شناسه منحصربه‌فرد رأی‌دهنده یعنی k_2 را از پایگاه اطلاعاتی بازیابی می‌کند. در غیر این صورت، اگر کاربر برای اولین‌بار با این سرور ارتباط برقرار کند، یک مقدار منحصربه‌فرد k_2 به او اختصاص یافته و در پایگاه اطلاعاتی ذخیره می‌گردد تا بتوان در آینده این کاربر را شناسایی نمود. سرور هویت‌شناسی امضاهای مخفی را به همراه k_2 و نشان زمانی رمز می‌نماید. این اطلاعات در یک پیغام خلاصه شده و بعدها برای رأی‌دهنده ارسال می‌گردد.

۴-۳-۵ سرور رأی‌گیری[1]

این سرور مسئول دریافت تعرفه شرکت‌کنندگان در انتخابات است. تعرفه‌های دریافتی باید حاوی موارد زیر باشند:

۱. گزینه انتخابی، یعنی نامزدی که توسط رأی‌دهنده انتخاب می‌شود.

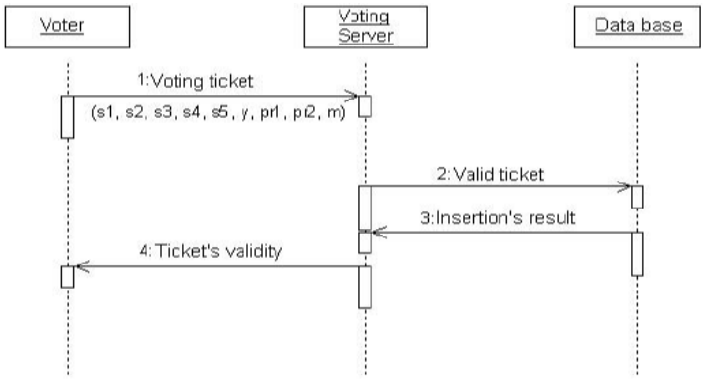
۲. پارامترهای عمومی، که برای تأیید دو امضای دیجیتالی رأی لازم است.

۳. پنج امضای متناظر با پروتکل امنیتی «سلز»، که سه تای آن امضاهای زوج کلیدهای عمومی و خصوصی[2] (امضای اول) و دو تای دیگر امضاهای دیجیتالی[3] (امضای دوم) نامیده می‌شوند.

شکل ۹-۵ جریان داده بین یک رأی‌دهنده و سرور رأی‌گیری را در مرحله رأی‌گیری نشان می‌دهد. سرور رأی‌گیری پس از دریافت تعرفه، کلید عمومی سرور هویت‌شناسی را که برای تأیید سه امضای اول لازم است، دریافت می‌کند. اگر همه امضاهای اول معتبر باشند، در آن صورت دو امضای دوم تأیید اعتبار می‌شوند. اگر هر پنج امضا معتبر باشد، یک پیغام پاسخ به‌صورت خودکار تولید شده و برای رأی‌دهنده ارسال می‌شود. اما حتی اگر یکی از پنج امضا معتبر نباشد، رأی‌دهنده پیغامی مبتنی‌بر عدم پذیرش رأیش دریافت می‌کند.

---

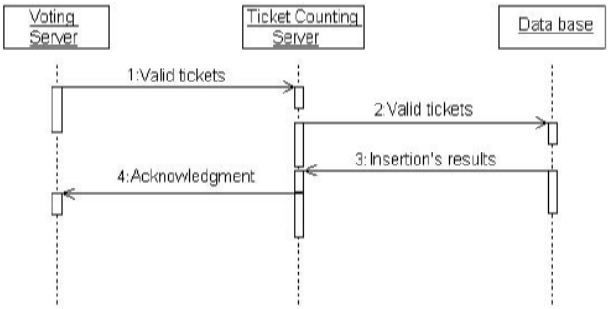
1. Voting Server (VS)
2. RSA
3. Digital Signiture Algoritm (DSA)



شکل ۹-۵ جریان داده بین رأی‌دهنده و سرور رأی‌گیری

۵-۳-۵ سرور شمارش[1]

این سرور همه تعرفه‌های ثبت شده را که حاوی پنج امضای دیجیتالی بوده و مرحله تأیید اعتبار را پشت سر گذاشته‌اند، دریافت می‌کند. شکل ۱۰-۵ جریان داده بین سرور رأی‌گیری و سرور شمارش را نشان می‌دهد. بدیهی است که وظیفه اصلی سرور شمارش، شمارش صحیح آراست.

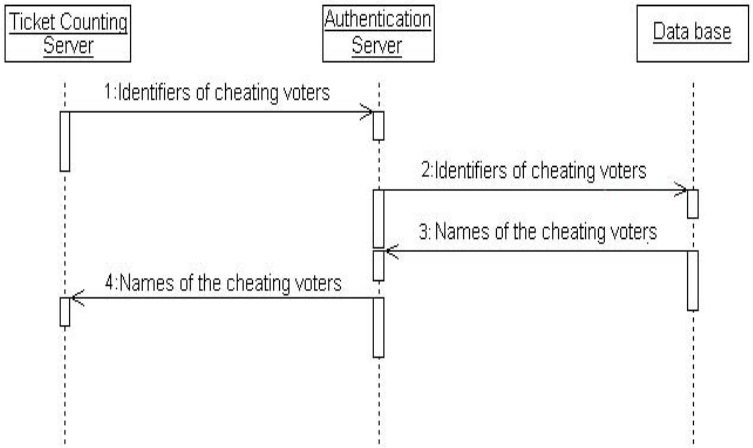


شکل ۱۰-۵ جریان داده بین سرور شمارش و سرور رأی‌گیری

برای این منظور، سرور شمارش در ابتدا همه تعرفه‌های دریافتی را در پایگاه

1. Ticket Counting Server (TCS)

اطلاعاتی خود ذخیره می‌کند و سپس تعرفه‌های مشابه را شناسایی می‌نماید؛ زیرا در مرحله شمارش نهایی، این تعرفه‌ها باید تنها یک‌بار شمارش گردند. رویه آشکارسازی آرای مکرری که ممکن است توسط افراد خاطی ارسال شود، همان روشی است که قبلاً مورد بررسی قرار گرفت. سرور شمارش در هنگام مواجهه با آرای مشکوک، شناسه‌های این آرا را به سرور هویت‌شناسی گزارش می‌کند و این سرور با استفاده از شناسه‌ها، هویت رأی‌دهنده خاطی را کشف می‌نماید. جریان داده بین سرور شمارش و سرور هویت‌شناسی در شکل ۱۱-۵ نشان داده شده است.



شکل ۱۱-۵ جریان داده بین سرور شمارش و سرور هویت‌شناسی

تنها پس از تجزیه و تحلیل تعرفه‌های دریافتی است که سرور شمارش، شمارش آرا را آغاز می‌کند. در نهایت، به‌منظور شفاف‌سازی عملکرد سیستم، سرور شمارش فهرست دقیقی از اطلاعات تعرفه‌های معتبر و نامعتبر را که طی فرایند رأی‌گیری دریافت شده، چاپ می‌نماید.

۶-۳-۵ رأی‌دهنده

هر فرد به‌منظور شرکت در رأی‌گیری، باید دو مرحله را پشت سر بگذارد:

۵-۳-۶-۱ مرحله هویت‌شناسی

در این مرحله رأی‌دهنده گواهی‌نامه دیجیتالی و اطلاعات شخصی خود را به سرور هویت‌شناسی می‌فرستد. برای این منظور، رأی‌دهنده در ابتدا کلید عمومی این سرور را به‌دست آورده و متنی را که باید توسط این سرور امضای مخفی شود، آماده و امضا می‌کند. سرور هویت‌شناسی مقدار k_2 را که شناسه منحصربه‌فرد رأی‌دهنده است، ایجاد می‌نماید که حاوی سه امضای مخفی دیجیتالی است. رأی‌دهنده می‌تواند عامل مخفی‌کننده را برداشته و پارامترهای موجود در پیغام را ذخیره نماید.

۵-۳-۶-۲ مرحله رأی‌گیری

در شروع این مرحله، شرکت‌کننده نامزد مورد نظر خود را انتخاب می‌کند. سپس تعرفه را با استفاده از سیستم رمزنگاری، به‌صورت دیجیتالی امضا نموده و آن را به سرور رأی‌گیری می‌فرستد. این سرور اعتبار تعرفه را کنترل کرده و درصورت تأیید، یک پیام تأیید برای رأی‌دهنده می‌فرستد. در غیر این صورت، رأی‌دهنده یک پیغام خطا دریافت می‌کند. اگر همه‌چیز درست پیش برود، رأی‌دهنده تعرفه را به همراه پارامترهای مرتبط ذخیره می‌کند. وقتی نتایج نهایی انتخابات منتشر شود، تمامی رأی‌دهندگان واجد شرایط می‌توانند مطمئن شوند که آرایشان شمارش گردیده است.

۵-۳-۷ ارزیابی پروتکل

این پروتکل دارای مشخصات زیر است:

۱. **دقت**: در این پروتکل تنها آرای معتبر مورد شمارش قرار می‌گیرند؛ زیرا سرور رأی‌گیری، آرای فرستاده شده توسط سرور هویت‌شناسی را که حاوی سه امضای دیجیتالی نباشد نمی‌پذیرد. همچنین این پروتکل حاوی رویه‌ای است که می‌تواند آرای معتبری را که توسط یک رأی‌دهنده و به‌صورت تکراری ارسال می‌شود، کشف نماید.

۲. **دمکراسی**: این مشخصه نیز قابل تحقق است، زیرا سرور هویت‌شناسی هویت رأی‌دهنده را شناسایی کرده و مشخصات لازم فرد را برای شرکت در انتخابات کنترل می‌نماید.

۳. **محرمانگی**: وجود امضاهای مخفی مانع کشف ارتباط بین رأی و رأی‌دهنده می‌شود.

۴. **تأیید**: از آنجایی‌که هر تعرفه حاوی پنج امضای دیجیتالی است، رأی‌دهنده در هنگام انتشار نتایج می‌تواند از شمارش رأیش اطمینان حاصل کند؛ زیرا سرور شمارش، علاوه بر اعلام نتایج نهایی انتخابات، کلیه تعرفه‌های دریافتی معتبر را منتشر می‌نماید.

۵. **سهولت**: رأی‌دهندگان می‌توانند فرایند رأی‌دهی را در یک زمان کوتاه، در یک مرحله و با حداقل تجهیزات به پایان برسانند.

۶. **قابلیت انعطاف**: سیستم قابل انعطاف است؛ زیرا مبتنی‌بر امضاهای مخفی بوده و در آن امکان استفاده از اشکال مختلف تعرفه‌ها وجود دارد.

۷. **قابلیت کشف آرای تکراری رأی‌دهندگان**: این سیستم علاوه بر توانایی کشف آرای تکراری، توانایی اعلام هویت رأی‌دهنده خاطی را نیز داراست.

۵-۴ مقایسه پروتکل‌ها

جدول ۱-۵ مقایسه میان چندین پروتکل معروف رأی‌گیری الکترونیکی را نشان می‌دهد. مشخصه‌هایی که مورد بررسی قرار گرفته‌اند به‌ترتیب عبارت‌اند از: دقت، دمکراسی، محرمانگی، تأیید، سهولت، انعطاف‌پذیری و آشکارسازی آرای تکراری.

جدول ۱-۵ مقایسه پروتکل های مختلف رأی‌گیری الکترونیکی

پروتکل	دقت	دمکراسی	محرمانگی	قابلیت تأیید	سهولت	قابلیت انعطاف	تشخیص آرای تکراری
شوماخر[۲۹]	√	√	√	√	√	×	×
فوجیوکا[۳۰]	√	√	√	√	×	√	×
سنسوس[۳۱]	√	√	√	√	√	√	×
کارو[۳۲]	√	√	√	√	√	√	×
آر ای وی اس[۳۳]	√	√	√	√	√	√	×
سلز[۳۴]	√	√	√	√	√	√	√

جدول ۲-۵ پروتکل‌های مختلف فهرست شده در جدول ۱-۵ را برحسب تعداد کل زوج کلیدها، تعداد کدهای رمز و نیز تعداد مسئولان مورد نیاز با یکدیگر مقایسه

می‌کند. علاوه بر این، تعداد دفعاتی که تعرفه در حین فرایند رأی‌دهی در شبکه جابه‌جا می‌شود نیز مورد بررسی قرار گرفته است.

جدول ۲-۵ مقایسه برخی از ویژگی‌های دیگر پروتکل‌ها

طرح	جابه‌جایی	مسئولان	کد رمز	کلیدها
سنسوس[۳۵]	3N	3	1	1 + N
کارو[۳۶]	3N	6	0	1 + KN
آر ای وی اس[۳۷]	2N	3 + i	T	2 + IN
سلز[۳۸]	N	3	1	1 + 2N

در این جدول، N تعداد آرای فرستاده شده در یک انتخابات است. در مورد پروتکل «آر ای وی اس»، t مقداری بزرگ‌تر از i/2 است که در آن i تعداد مسئولان انتخابات می‌باشد. در مورد پروتکل کارو،[1] k تعداد زوج کلیدهایی است که مسئول شمارش آرا تعیین می‌کند.

تعداد و بزرگی پیغام‌های مبادله شده در مرحله هویت‌شناسی و رأی‌گیری در پروتکل «سلز» در جدول ۳-۵ خلاصه شده است.

جدول ۳-۵ بزرگی تقریبی پیام‌ها

ردیف	مرحله	پیام اول	پیام دوم
۱	**هویت‌شناسی**	کیلوبایت ۱۹,۵	کیلوبایت ۴,۵
۲	**رأی‌گیری**	کیلوبایت ۶,۷	--

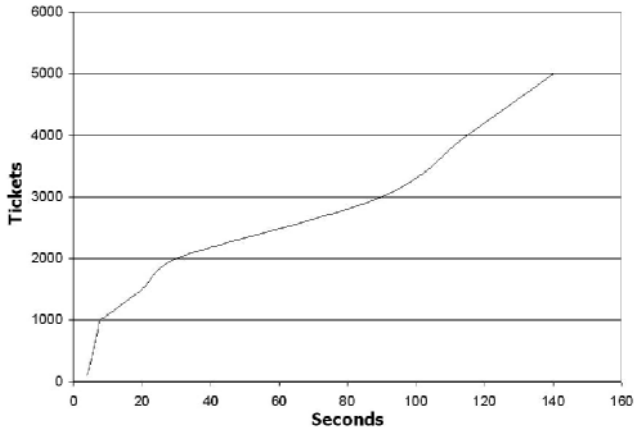
در جدول ۴-۵ خلاصه‌ای از تعداد عملیات انجام شده در مراحل مختلف پروتکل «سلز» نشان داده شده است.

1. Karro

جدول ۴-۵ فعالیت‌های رمزنگاری

ردیف	مرحله	رأی‌دهنده	سرور هویت‌شناسی	سرور رأی‌گیری
۱	**هویت‌شناسی**	۱ امضای زوج کلیدهای عمومی و خصوصی ۲ رمزگذاری زوج کلیدها	۱ تأیید اعتبار زوج کلیدها ۴ رمزگذاری زوج کلیدها ۳ امضای مخفی	
۲	**رأی‌گیری**	۴ رمزگشایی زوج کلیدها ۲ امضای دیجیتالی		۳ تأیید اعتبار زوج کلیدها ۲ تأیید اعتبار امضای دیجیتالی
جمع کل		**۹ فعالیت**	**۸ فعالیت**	**۵ فعالیت**

شکل ۱۲-۵ زمان مورد نیاز برای تأیید اعتبار و شمارش آرای دریافتی را نشان می‌دهد.



شکل ۱۲-۵ زمان محاسبه نتایج آرا در مرحله رأی‌گیری

تجربه نشان داده است که این پروتکل می‌تواند در کمتر از ۱۶۰ ثانیه نتایج انتخاباتی با حدود ۵۰۰۰ رأی را اعلام کند.

۵-۵ استفاده از کارت‌های هوشمند در انتخابات الکترونیکی

در سالیان اخیر بسیاری از دولت‌ها در فرایندهای مدیریتی از برنامه‌های کاربردی تحت اینترنت استفاده کرده‌اند. دامنه این کاربردها از فرم‌های الکترونیکی ساده تا برنامه‌های پیچیده تحت وب مانند اظهارنامه‌های مالیاتی را دربرمی‌گیرد.

امروزه از فناوری‌های اطلاعات و ارتباطات در زمینه‌های مختلف تجاری و مدیریتی استفاده می‌شود، اما پرسشی که در اینجا مطرح است این است که آیا می‌توان از اینترنت برای رأی‌گیری نیز استفاده نمود؟ اگر چنین است، اصول طراحی و پیاده‌سازی چنین سیستمی چیست؟ همان‌طوری که قبلاً بیان شد:

- دولت الکترونیکی مجموعه فرایندهایی است که خدمات دولتی را به‌صورت الکترونیک به شهروندان ارائه می‌دهد.
- دمکراسی الکترونیکی شامل استفاده از فناوری اطلاعات و ارتباطات برای پشتیبانی مشارکت شهروندان در تصمیم‌گیری‌های دمکراتیک مانند انتخابات، رفراندوم‌ها و مرحله تبلیغات پیش از آنهاست.
- انتخابات الکترونیکی زیرمجموعه‌ای از دمکراسی الکترونیکی است که باید فرایند گمنامی را (که موضوع اصلی این فصل است) تضمین نماید.
- در این قسمت الزامات سیستم‌های رأی‌گیری الکترونیکی را مورد بررسی قرار داده و سپس الگوریتم سیستم انتخابات الکترونیکی شهر وین در کشور اتریش را ارائه می‌نماییم.

۵-۵-۱ هویت‌شناسی در مقابل گمنامی

چگونه یک فرد می‌تواند پس از شناسایی توسط سیستم رأی‌گیری و تأیید هویت، همچنان به‌عنوان یک فرد گمنام در سیستم رأی دهد؟ تمامی پروتکل‌های رأی‌گیری ناچارند به این سوال اساسی پاسخ گویند.

سیستم‌های رأی‌گیری الکترونیکی را که از اینترنت استفاده می‌کنند، می‌توان به سیستم‌های رأی‌گیری پستی، که سال‌هاست در اروپا مورد استفاده قرار می‌گیرند، تشبیه کرد. در سیستم رأی‌گیری پستی، رأی‌دهنده قبل از تاریخ برگزاری انتخابات، ثبت‌نام نموده و در یک چارچوب زمانی مشخص رأیش را از هر مکان دلخواه ارسال می‌کند.

سیستم رأی‌گیری الکترونیکی از بسیاری از جهات شبیه سیستم‌های رأی‌گیری پستی است. دو عنصر اساسی در سیستم‌های رأی‌گیری الکترونیکی وجود دارد:[۳۹]

۱. فرایند ثبت‌نام که طی آن رأی‌دهنده به‌صورت کاملاً شفاف تعیین هویت می‌شود.

۲. فرایند رأی‌دهی که طی آن رأی‌دهنده گمنام است.

۲-۵-۵ احراز هویت

سیستم‌های احراز هویت به سه گروه مختلف تقسیم می‌شوند: سیستم‌های مبتنی‌بر پین، سیستم‌های مبتنی‌بر اعداد تراکنشی و سیستم‌هایی که از کارت‌های هوشمند برای احراز هویت استفاده می‌کنند.

۱-۲-۵-۵ سیستم‌های مبتنی‌بر پین‌کد[۱]

رأی‌دهنده یک کاربر تعیین هویت شده در اینترنت است. بنابراین، پس از برقراری ارتباط با سیستم،[۲] می‌تواند صفحه مربوط به تعرفه انتخاباتی را تکمیل و ارسال نماید. در این شرایط ارتباط بین مرورگر و سرورهای رأی‌گیری توسط استانداردهای رأی‌گیری محافظت می‌شود. در این سیستم‌ها هیچ‌گونه تضمینی برای حفظ گمنامی وجود ندارد. کاربرد این سیستم‌ها در انتخاباتی است که در آنها گمنامی از اهمیت چندانی برخوردار نیست (مانند انجمن‌ها، شوراهای دانش‌آموزی، انتخابات اعضای هیئت علمی دانشگاه‌ها و ...). مزایای این سیستم عبارت است از: کاهش چشمگیر هزینه انتخابات و امکان مشارکت آسان افرادی که در خارج از کشور زندگی می‌کنند.

۲-۲-۵-۵ سیستم‌های مبتنی‌بر اعداد تراکنشی[۳]

در این سیستم‌ها یک سری اعداد تراکنشی یا دادوستدی ایجاد شده و انتخابات با استفاده از این اعداد در یک مرورگر وب انجام می‌گردد. ارتباط بین رأی‌دهنده و مرورگر وب محافظت شده و کلید رمزنگاری به‌وسیله یک مرکز ایجاد اعتماد[۴] تولید می‌شود.[۴۰و۴۱]

---

۱. Pin-based: در این روش از یک عدد منحصربه‌فرد به نام پین‌کد برای شناسایی رأی‌دهنده استفاده می‌شود.

2. Login

3. Tan-based: Transaction Number

4. Trust Center

پس از اخذ رأی، رأی‌دهنده به‌عنوان رسید، یک عدد تصادفی دریافت می‌کند و در خاتمه انتخابات، با کنترل این عدد می‌تواند از شمارش رأیش اطمینان حاصل نماید.

سیستم election.com مثالی از این‌گونه سیستم‌هاست که در انتخابات شورای دانش‌آموزی در وین در سال ۲۰۰۲ مورد استفاده قرار گرفت.[۴۲] در این سیستم رأی‌دهندگان می‌توانستند با استفاده از یک مرورگر وب و با وارد کردن شماره تراکنشی خود در رأی‌گیری شرکت نمایند. در این سیستم‌ها نیز تضمینی برای گمنامی رأی‌دهندگان وجود ندارد.

۳-۲-۵-۵ سیستم‌های مبتنی‌بر کارت‌های هوشمند

اگرچه سیستم مبتنی‌بر پین‌کد و سیستم مبتنی‌بر اعداد تراکنشی کاربرد بسیار ساده‌ای داشته و در سطح گسترده‌ای مورد استفاده قرار می‌گیرند، اما به‌دلیل عدم محرمانگی، مناسب انتخابات دمکراتیک نیستند. درواقع، این دو سیستم در مواردی که گمنامی اهمیت چندانی ندارد، کاربرد دارند. در سیستم‌هایی که از کارت‌های هوشمند برای امضای دیجیتالی استفاده می‌کنند، برای حفظ امنیت اطلاعات، از روش‌های مختلف رمزنگاری استفاده می‌شود که در ادامه به تشریح برخی از آنها می‌پردازیم.

۳-۵-۵ سیستم‌های یک‌مرحله‌ای

الگوریتمی که در سال ۱۹۹۳ توسط فوجیوکا، اکاموتو و اهتا ارائه شد، مبنای طراحی بسیاری از سیستم‌ها قرار گرفت (به‌عنوان مثال [۴۳]و[۴۴]). در ابتدا به‌شرح برخی از کلمات اختصاری استفاده شده در آن می‌پردازیم:

BS: تعرفه رأی،

B: سرور صندوق رأی،

R: سرور ثبت نام،

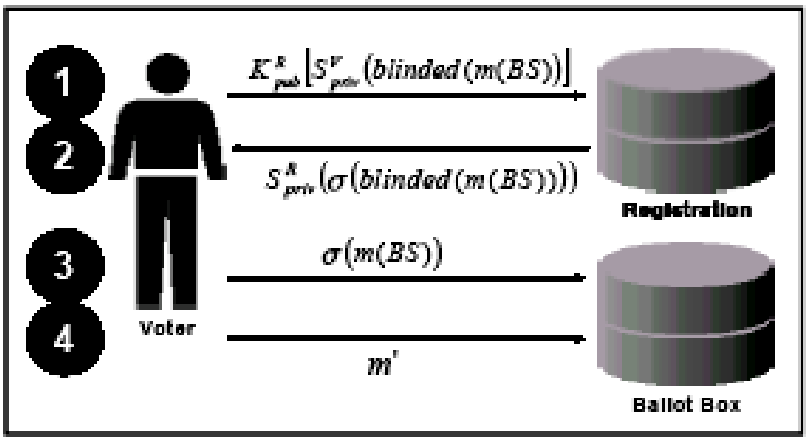
V: رأی‌دهنده،

m , m': کلید رمز متقارن،

$S^{(V,R,B)}_{(priv,pub)}$: کلید دوتایی امضا برای رأی‌دهنده، سرور ثبت‌نام و سرور صندوق رأی،

$K^{(V,R,B)}_{(priv,pub)}$: کلید دوتایی برای رمزنگاری.

شکل ۱۳-۵ را درنظر بگیرید که در آن رأی‌دهنده تعرفه رأی را پر می‌کند و این تعرفه با کلید متقارن رمز می‌شود ((m(BS) در مرحله بعد، این تعرفه به‌صورت مخفی درمی‌آید blinded(m(BS)).



شکل ۱۳-۵ مدل یک‌مرحله‌ای

این بسته توسط رأی‌دهنده امضای الکترونیکی و سپس با کلید عمومی K^R_{pub} رمز شده و به سرور ثبت‌نام فرستاده می‌شود.

$$K^R_{Pub}\left[S^V_{\Pr iv}(blinded(m(BS))\right]$$

سرور ثبت‌نام کلید عمومی رأی‌دهنده را باز کرده و هویت او را شناسایی می‌کند. بنابراین، مشخص می‌شود که آیا متقاضی حق رأی دارد یا نه. اگر جواب مثبت باشد، سرور ثبت‌نام $blinded(m(BS))$ را امضا کرده و داده $\sigma(blinded(m(BS))$ را با کلید اختصاصی خود یعنی $S^R_{\Pr iv}$ رمز می‌نماید. سپس پیغام $S^R_{\Pr iv}(\sigma(blinded\ (m(BS))))$ از طرف سرور ثبت‌نام به‌عنوان مجوز رأی برای رأی‌دهنده فرستاده می‌شود.

رأی‌دهنده می‌تواند به‌وسیله کلید عمومی رمزنگاری که در اختیار اوست این پیغام را رمزگشایی کند. رأی‌دهنده در ابتدا صحت امضای دیجیتالی $S^R_{\Pr iv}$ را به کمک مرکز

ایجاد اعتماد تأیید نموده و سپس لایه مخفی‌ساز را برمی‌دارد. در این مرحله، دو مقدار $m(BS), \sigma(m(BS))$ که توسط سرور ثبت‌نام تأیید شده در اختیار او قرار دارد.

تعرفه تأیید شده $m(BS)$ توسط رأی‌دهنده به سرور صندوق رأی ارسال می‌شود. در پروتکل‌های اولیه، پس از پایان انتخابات، تعرفه‌های رمز شده به‌صورت فهرست منتشر می‌شد. در این صورت، رأی‌دهنده پس از تأیید حضور تعرفه رمز شده مربوط به‌خود، کلید رمزگشایی m' را برای سرور صندوق رأی می‌فرستد. سرور از این کلید برای رمزگشایی تعرفه رأی و شمارش آرا استفاده می‌کند. پس از خاتمه شمارش آرا، کلیدها و تعرفه‌های رأی به‌صورت فهرست در اختیار همگان قرار می‌گیرد؛ بنابراین، رأی‌دهندگان می‌توانند صحت انتخابات و عدم دستکاری آرا را کنترل نمایند.

این الگوریتم به اشکال گوناگون مورد استفاده قرار می‌گیرد، اما یک مشکل اساسی در همه آنها وجود دارد؛ این الگوریتم یک الگوریتم یک‌مرحله‌ای است، به‌عبارتی احراز هویت و رأی‌دهی در یک مرحله اتفاق می‌افتد. بنابراین، درصورت تبانی مدیران سرور ثبت‌نام و سرور صندوق رأی، محرمانگی آرا نقض شده و ممکن است ازطرف افرادی که در انتخابات شرکت نکرده‌اند هم رأی داده شود.

این پروتکل در سطح کاربران از امنیت بالایی برخوردار است، اما افراد متخصص به کمک برخی از برنامه‌ها مانند جاوا می‌توانند آدرس اینترنتی تعرفه‌های رمز شده را به‌دست آورده و به جای دیگران رأی دهند. بنابراین، درصورتی‌که ثبت‌نام و رأی‌دهی در یک مرحله اتفاق بیفتد هیچ تضمینی برای حفظ گمنامی و محرمانگی وجود نخواهد داشت.

۵-۵-۴ طرح پروتکل دومرحله‌ای

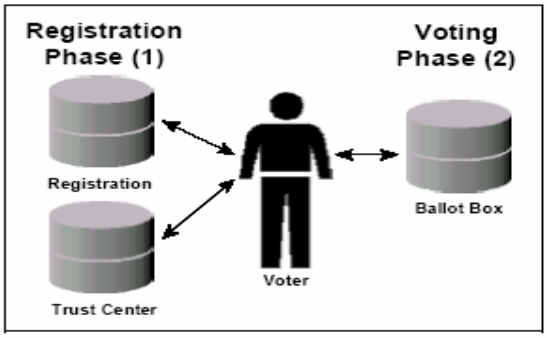
این طرح فرم تکمیل شده الگوریتم قبلی[۴۵] است. در این طرح، ثبت‌نام و رأی‌دهی در دو مرحله جداگانه انجام می‌شود.

۵-۵-۴-۱ مرحله ثبت‌نام

در این مرحله هویت رأی‌دهنده کنترل شده و رأی‌دهنده یک توکن[1] (بسته اطلاعاتی)

1. Token

مخفی و رمز شده را دریافت می‌کند.



شکل ۱۴-۵ طرح دو مرحله‌ای و گروه‌های شرکت‌کننده

رأی‌دهندگان می‌توانند در محدوده زمانی مشخصی قبل از انتخابات ثبت‌نام کنند. ازآنجاکه پس از ثبت‌نام تعرفه در اختیار رأی‌دهنده قرار نمی‌گیرد، بنابراین، فرایند ثبت‌نام و احراز هویت رأی‌دهندگان حتی پیش از کامل شدن فهرست نهایی کاندیداها نیز قابل اجراست. در ابتدا رأی‌دهنده یک توکن تصادفی مخفی دریافت می‌کند. سپس متنی به آن اضافه شده و به‌وسیله کلید اختصاصی رأی‌دهنده، امضای الکترونیکی می‌شود.

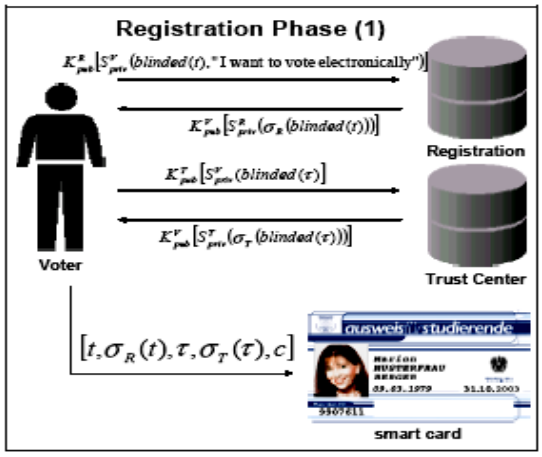
$$S^{V}_{\Pr iv}(blinded(t),"I\ want\ \ to\ voteelecorinically")$$

در مرحله بعد، این متن به‌وسیله کلید عمومی سرور ثبت‌نام به‌صورت رمز درمی‌آید:

$$K^{R}_{Pub}\left[S^{V}_{\Pr iv}(blinded(t),"\text{I want to voteelecorinically}")\right]$$

در این مرحله سرور ثبت‌نام با کنترل امضای الکترونیکی هویت رأی‌دهنده را تأیید و یا رد می‌کند. درصورت تأیید، سرور یک توکن جدید به نام t تولید کرده وآن را به‌صورت مخفی و رمز شده درمی‌آورد و در نتیجه توکن t به‌صورت $\sigma_R(blinded(t))$ درمی‌آید. در اینجا همان مکانیزم قبلی مورد استفاده قرار گرفته است.[۴۶] اما از آنجایی‌که تنها یک توکن به‌جای تعرفه امضا می‌شود، پس پیغام ارسالی کوتاه‌تر بوده و ذخیره‌سازی آن در یک رسانه امن راحت‌تر خواهد بود.

سرور ثبت‌نام توکن $\sigma_R(t)$ را ذخیره می‌کند. اگر توکن امضا شده از بین برود و رأی‌دهنده مجدداً درخواست توکن نماید، سرور ثبت‌نام یک نسخه از توکن ذخیره شده را در اختیار وی قرار می‌دهد. در نتیجه، از ایجاد توکن‌های اضافی جلوگیری به عمل می‌آید.



شکل ۱۵-۵ مرحله ثبت‌نام رأی‌دهندگان

در بسیاری از موارد، رأی‌دهندگان موظف به حضور در حوزه‌های انتخاباتی خاص مثلاً حوزه C هستند. بنابراین، قبل از انتخابات کد حوزه در اختیار رأی‌دهنده قرار می‌گیرد. رأی‌دهنده در پایان مرحله ثبت‌نام دو توکن در اختیار دارد که یکی مربوط به تأیید هویت و دیگری مربوط به اطلاعات حوزه انتخاباتی اوست. هر دو توکن برای رأی‌دهی در روز انتخابات لازم است.

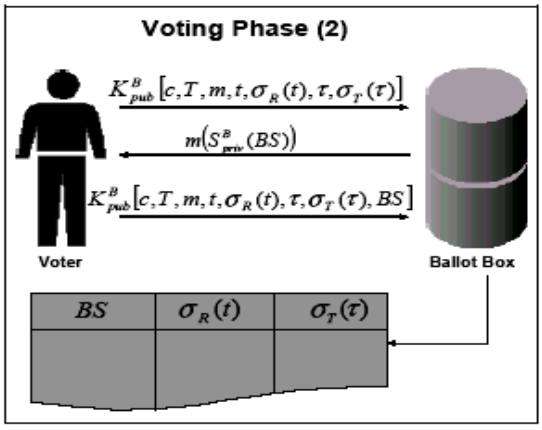
۲-۴-۵-۵ رأی‌دهی

رأی‌دهنده در روز انتخابات برای دریافت تعرفه الکترونیکی، توکن‌ها را به سرور صندوق رأی می‌فرستد. در این مرحله، نیازی به امضای الکترونیکی رأی‌دهنده نیست و تنها ابزار احراز هویت وی همان دو توکنی است که در مرحله ثبت‌نام دریافت نموده است. رأی‌دهنده برای حفظ امنیت ارتباط، کلیدهای m , m' را ایجاد می‌کند. وی همچنین

شناسه T مربوط به مرکز ایجاد اعتماد را به توکن اضافه می‌نماید. این شناسه برای تشخیص هویت رأی‌دهنده و یا خواندن کلید عمومی رمزنگاری به‌کار نمی‌رود، بلکه مرکز ایجاد اعتماد از آن برای تشخیص امضاهای مخفی استفاده می‌کند.

پیغام $[c,T,m,t,\sigma_R(t),\tau,\sigma_T(\tau)]$ به‌وسیله کلید عمومی سرور صندوق رأی یعنی $K^B_{\mu b}$ رمزشده و به این سرور فرستاده می‌شود. پس از رمزگشایی، سرور صندوق رأی امضاهای $\sigma_R(t) and \sigma_\tau(\tau)$ را خوانده و درصورت تأیید توکن‌ها یک تعرفه خالی را که توسط کلید متقارن به رمز درآورده شده است، برای رأی‌دهنده می‌فرستد. رأی‌دهنده تعرفه را دریافت کرده و آن را با کلید 'm رمزگشایی و سپس تکمیل می‌نماید.

این تعرفه با توکن‌های c,T ترکیب شده و دوباره با کلید عمومی سرور صندوق رأی رمز و ارسال می‌گردد. پس از تأیید اعتبار توکن‌ها، سرور صندوق رأی تعرفه و سایر اطلاعات دریافتی از رأی‌دهنده را ذخیره می‌کند.



شکل ۱۶-۵ مرحله رأی‌دهی

۳-۴-۵-۵ محیط ذخیره‌سازی

از آنجایی‌که این الگوریتم از پروتکل دومرحله‌ای استفاده می‌کند، لازم است که توکن به‌صورت موقت در یک محیط امن و محرمانه ذخیره شود. سه راه برای ذخیره کردن این توکن وجود دارد:

الف) استفاده از کارت هوشمند برای امضای دیجیتالی

احتمال از دست‌رفتن اطلاعات ذخیره شده در روی این کارت‌ها نسبت به سایر محیط‌های ذخیره‌سازی، بسیار کمتر است. از طرفی، به‌دلیل استفاده از پین‌کد، احتمال دسترسی افراد غیرمجاز نیز منتفی می‌باشد، اما این روش دارای دو مشکل اساسی است:

اولاً برای نوشتن توکن، امکان دسترسی به بعضی از قسمت‌های کارت هوشمند لازم است. بنابراین، کارت‌ها باید متناسب با این فرایند ذخیره‌سازی طراحی شوند. برنامه‌های کاربردی نیز که از کارت هوشمند استفاده می‌نمایند می‌توانند به نام و سایر مشخصات پرسنلی افراد که در روی کارت ذخیره شده دسترسی پیدا کنند. از طرفی، هر کارت هوشمند یک کد شناسایی دارد که در سرتاسر جهان منحصربه‌فرد است. این کد در هنگام تولید کارت مقداردهی شده و در آن ذخیره می‌گردد. بنابراین، درصورت استفاده از کارت در هر کجای دنیا امکان ردیابی آن وجود خواهد داشت.

ثانیاً ازآنجاکه توکن انتخابات در فاصله زمانی بین ثبت‌نام و رأی‌گیری در کارت وجود دارد، اشخاص ثالث می‌توانند با استفاده از برنامه‌های مختلف، به اطلاعات کارت دسترسی پیدا کنند در نتیجه پس از رأی‌گیری، آرا قابل ردیابی بوده و به‌این‌ترتیب تضمینی برای گمنامی و محرمانگی وجود نخواهد داشت.

بنابراین، کارت‌های هوشمند با امضای دیجیتالی درصورتی برای ذخیره‌سازی توکن‌ها قابل استفاده خواهند بود که طراحی مجددی بر روی آنها صورت گیرد، به‌نحوی‌که دارنده کارت بتواند در مواقع مختلف، تعیین کند که کدام داده‌ها از روی کارت قابل خواندن باشند.

ب) استفاده از محیط‌های ذخیره‌سازی مشابه کیف الکترونیکی

در این روش رأی‌دهنده از یک فلاپی و یا یک حافظه «یو اس بی»[1] برای ذخیره توکن انتخابات استفاده می‌کند که تا زمان برگزاری انتخابات بدون استفاده باقی می‌ماند. نقطه‌ضعف این روش، قابلیت اطمینان پایین دستگاه ذخیره‌سازی است، به‌خصوص

---

۱. Universal Serial Bus (USB) رابطی در رایانه‌های جدید است که امکان اتصال تجهیزات جانبی مثل چاپگر، اسکنر، دوربین‌های وب و ... را فراهم می‌کند.

فلاپی که در مقابل خطاهای خواندن و نوشتن بسیار آسیب‌پذیر بوده و حفاظت اطلاعات در آن به‌صورت دستی و با استفاده از کد عبور انجام می‌شود. از طرفی، اطلاعات ذخیره شده در این دستگاه‌ها را می‌توان به تعداد نامحدود تکثیر نمود.

ج) استفاده از کارت‌های هوشمند جداگانه

در این روش از دو کارت هوشمند استفاده می‌شود. کارت اول برای امضای دیجیتالی و تعیین هویت رأی‌دهنده در هنگام ثبت‌نام و کارت دوم پس از تأیید هویت رأی‌دهنده برای ذخیره‌سازی توکن انتخابات. در روز انتخابات فقط از کارت دوم برای شناسایی استفاده می‌شود. بنابراین، محرمانگی و گمنامی رأی‌دهنده حفظ می‌گردد. این کارت‌ها توسط کارت‌خوان‌های چندمنظوره قابل خواندن بوده و در نتیجه نیازی به سخت‌افزار اضافه نیست.

پی‌نوشت‌ها

1. D. Chaum, *Blind Signatures for Untraceable Payments, Advances in Cryptology,* CRYPTO 82, pp. 199-203, 1999.
2. L. Cranor, R. K. Cytron, Sensus, A Security-conscious Electronic Polling System for the Internet, Proceedings of the Hawaii International Conference on System Sciences, Vol. 3, pp. 561-570, Wailea, Hawaii, 2000.
3. B. Durette, Multiple Administrators for Electronic Voting, Master Thesis, Massachussetts Institute of Technology, 2001.
4. A. Fujioka, T. Okamoto, Y. Ohta, A Practical Secret Voting Scheme for Large Scale Elections, Advances In Cryptology-AUSCRYPT '92, Vol. 718, (Lecture Notes in Computer Science. Springer-verlag, Berlin) pp. 244-251, 2001.
5. Y. Varadharajan, Anonymous Secure E-Voting Over A Network, Proceedins of the 14th Annual Computer Security Applications Conference, (IEEE Computer Society,): pp. 293-299, 1998.
6. C. Garcia-zamora, F. Rodr´Iguez and D. Arroyo, "An Efficient and Effective E-Voting Protocol for online Elections, Technical Report CINVESTAV-IPN, 17 Pages, 2005. [online]: http://delta.cs.cinvestav.mx/francisco/repository/repository.html .
7. R. Kenneth, A Cryptographic Scheme for Computerized General Elections, Advances in Cryptology, CRYPTO'91, Vol. 576, (Lecture Notes in Computer Science. Springer-Verlag, Berlin), pp. 405-419, 2000.
8. H. Nurmi, A. Salomaa and L. Santean, Secret Ballot Elections in Computer Networks, Computers and Security 36 (10), pp. 553-560, 2000.
9. D. Chaum, Ibid.

10. A. Fujioka, T. Okamoto, Y. Ohta, Ibid.

11. L. Cranor, R.K. Cytron, Ibid.

12. K. Jared, W. Jie, Towards A Practical, Secure, and Very Large Scale Online Election, Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC'99), (Scottsdale, AZ. Diciembre), pp. 161-169, 2000.

13. B. Schoenmakers. A Simple Publicly Verifiable Secret Sharing Scheme and its Application to the Electronic Voting, Advances in Cryptology, CRYPTO'99, Vol. 1666, (Lecture Notes in Computer Science,) pp. 148-164, 1999.

14. L. Iuon-chung, H. Min-shiang, C. Chin-chen, Security Enhancement for Anonymous Secure E-voting Over A Network, Computer Standards & Interfaces, Vol. 25, No. 2, pp. 131-139, 2003.

15. C. Garcia-Zamora, F. Rodr´Iguez and D. Arroyo, Ibid.

16. E. A. Fisch, G. B. White, Secure Computers and Networks-analysis, Design, and Implementation, Boca Raton: CRC Press, 2000.

17. B. Durette, Ibid.

18. M. Herschberg, Secure Electronic Voting Over the Word Wide Web, Master Thesis, Massachussetts Institute of Technology, 1997.

19. Y. Varadharajan, Ibid.

20. C. Garcia-zamora, F. Rodr´Iguez and D. Arroyo, Ibid.

21. M. Herschberg, Ibid.

22. G. Rosario, J. Stanis Law, K. Hugo and R. Tal, Robust Threshold DSS Signatures, In Ueli Maurer, Editor, Advances in Cryptology, pp. 354-371. Springer-verlag,1999.

23. A. Monteiro, Electronic Voting Systems, FCT, Lisbon University, TR-01-X. (In Portuguese) 2001.

24. D. Baltimore, C. Vest. What is, What It Could Be, Caltech-MIT Voting Technology Project , 2001 [Online]: http://www.vote.caltech.edu/reports/index.htm.

25. L. Cranor, Voting after Florida: No Easy Answers, 2001 [online]: http://lorrie.cranor.org.

26. R. Rivest, Electronic Voting, Proc. of Financial Cryptography, Grand Cayman, Cayman Islands, 2001.

27. A. Rubin, Security Considerations for Remote Electronic Voting Over the Internet, in Comm. Of ACM, 45(12), 2002.

28. A. Lioy, et al, DNS Security, Proc. of TERENA Networking Conference. Lisbon, Portugal, pp. 22-25, 2000.

29. B. Schoenmakers, Ibid.

30. A. Fujioka, T. Okamoto, Y. Ohta, Ibid.

31. L. Cranor, R.K. Cytron, Ibid.

32. K. Jared, W. Jie, Ibid.

33. R. Joaquim, Y. Uquete, Z. Andr´e, P. Ferreira, REVS-A Robust Electronic Voting System, Proceedings of IADIS International Conference E-Society 2003, (Lisbon, Portugal), pp. 95-103, 2003.

34. C. P. Garcia-zamora, F. Rodriguez-henriquez, D. Ortiz-Arroyo, SELES: An E-voting System For Medium Scale online Elections, In Proceedings Of IEEE's ENC-2005, Mexican International Conference on Computer Science, Puebla Pue., Mexico September 26th-30th, 2005.

35. L. Cranor, R. K. Cytron, Ibid.

36. K. Jared, W. Jie, Ibid.

37. R. Joaquim, Y. Uquete, Z. Andr´e, P. Ferreira, Ibid.

38. C. P. Garcia-zamora, F. Rodriguez-henriquez, D. Ortiz-Arroyo, Ibid.

39. H. Nurmi, A. Salomaa and L. Santean, Ibid.

40. J. Feghhi, P. Williams, Digital Signatures-Aplied Internet Security, Addisson-wesley, 2000.

41. E. A. Fisch, G. B. White, Ibid.

42. EU Student Vote, 2002, [online]: http://www.Eusv.org.

43. Sensus E-voting System, 2002, [online]: http://lorrie.cranor.org/voting/sensus

44. Forschungsgruppe Internetwahlen, 2002, [online]: http://www.internetwahlen.de .

45. A. Prosser, R. Müller-Török, Electronic Voting Via the Internet, Presented at International Conference on Enterprise Information Systems ICEIS2001, Setùbal, 2001.

46. M. Herschberg, Ibid.

فصل ششم

ارزیابی انتخابات الکترونیکی در برخی کشورها

رأی‌گیری بیـان واضـحی از دمکراسـی اسـت کـه در همـه جوامـع از جملـه انجمـن‌هـا، شرکت‌ها، گروه‌های شغلی و البته در سطح سیاسی وجود دارد. علاوه بر منافع مـدیریتی موجـود در انتخابـات الکترونیکـی، نکـاتی در مـورد سـادگی و سـهولت روش بـرای رأی‌دهندگان نیز مطرح است. معرفی رأی‌گیری الکترونیکی، پرسش‌هـای متنـوعی را در بین گروه‌های مختلف مطرح نموده است که از جمله آنها می‌تـوان بـه مـواردی همچـون امنیت رأی، حفظ محرمانگی، صحت انتخابـات، اهمیـت عوامـل اقتصـادی ایـن شـیوه و فرهنگ ملیت‌های مختلف اشاره کرد.

با مدنظر قرار دادن برداشت‌های مختلف از رأی‌گیری، در ابتدا باید پرسـید کـه آیـا در کشور ما گرایش عمومی برای اجرای انتخابات الکترونیکی وجود دارد یـا نـه؟ اگرچـه رأی‌گیری الکترونیکی برای برخی از انتخابات ادواری قابل اجراست، اما تجزیـه و تحلیـل و نقد هزینه‌های مورد نیاز، منافع و ریسک‌های مربوطه آن از اهمیـت خاصـی برخـوردار است.

رأی‌گیری فرایندی رسمی است که پایه و اساس تعلـق بـه یـک جامعـه سیاسـی را تشکیل می‌دهد. بنابراین، انجام هرگونه تغییری در ایـن فراینـد بایـد بسـیار معقولانـه و سنجیده باشد تا سبب بی‌اعتمادی در رأی‌دهندگان نشود. در قسمت‌های بعد نمونه‌هایی از رأی‌گیری الکترونیکی در کشورهای مختلف جهان ارائه می‌شود.[1]

۱-۶ انتخابات سیاسی (سراسری)

درخصوص انتخابات سیاسی (سراسری) که به‌صورت الکترونیکی برگزار شده، می‌توان بـه موارد ذیل اشاره کرد.

۱-۱-۶ شهر نانسی فرانسه

در جریان رأی‌گیری در این شهر روش باجه‌های رأی‌گیری در حوزه‌های انتخاباتی با تکیه بر دو روش زیر استفاده شد:

۱. رأی‌گیری شبکه‌ای در حوزه‌های انتخاباتی (انتخابات ریاست‌جمهوری در ۲۱ آوریل و ۵ می ۲۰۰۲)،

۲. رأی‌گیری با استفاده از کارت‌های هوشمند، حاوی اثر انگشت رأی‌دهندگان (انتخابات مجلس شورا در ژوئن ۲۰۰۲).

البته در ابتدا این تمایل وجود داشت که انتخابات در شهر نانسی به‌صورت الکترونیکی و از راه دور انجام شود، اما شورای ملی فناوری اطلاعات فرانسه به دلایل ذیل مخالف آن بود:

۱. با ارسال کد شناسایی و رمز عبور از طریق پست معمولی به محل زندگی افراد، هریک از افراد ساکن در آن می‌توانند از این کارت‌ها سوءاستفاده نموده و به‌جای دیگران رأی دهند.

۲. رأی‌دهی از محل سکونت صحت و امنیت آرا را تضمین نمی‌کند؛ زیرا رأی‌دهنده ممکن است تحت فشار و نفوذ دیگران باشد.

۳. مکانیسم‌های فنی نمی‌تواند گمنامی رأی‌دهنده را تضمین نماید.

در انتخابات شهر نانسی کلیه رأی‌دهندگان موظف به حضور در حوزه‌های انتخاباتی بودند. نتایج حاصل از این تجربه عبارت بود از:

۱. میزان مشارکت افراد در انتخابات با استفاده از هر دو روش یادشده بسیار قابل ملاحظه بود.

۲. با نظرسنجی انجام شده، ۶۶ درصد شرکت‌کنندگان از این شیوه برگزاری انتخابات کاملاً راضی بوده، اما ۵۰ درصد آنها به سیستم‌های رایانه‌ای اطمینان کامل نداشتند.

۳. شناسایی کارت‌های هوشمند به‌دلیل وجود خراش و یا بریدگی در روی انگشت نشانه، با مشکلاتی مواجه شده و در نتیجه باعث عدم تشخیص هویت رأی‌دهنده می‌گردید.

۴. مدت زیادی برای برداشتن اثر انگشت افراد و آماده‌سازی کارت‌های هوشمند لازم بود، درحالی‌که سرعت در انتخابات الکترونیکی یکی از مباحث بسیار مهم محسوب می‌شود.

۵. در حالت استفاده از شبکه‌های رایانه‌ای برای انتخابات، این احتمال وجود دارد که برخی از سیستم‌ها هک شده و در نتیجه آرای گروهی از رأی‌دهندگان از دور خارج شود.

۶-۱-۲ ناحیه بریتانیایی شمال فرانسه

در جریان این رأی‌گیری در مارس ۲۰۰۱، از روش باجه‌های رأی‌گیری در حوزه‌های انتخاباتی و اینترنت استفاده شد. نتایج مثبت حاصل از این تجربه عبارت بود از اینکه مشارکت در انتخابات قابل ملاحظه بود، هیچ محدودیتی در استفاده از اینترنت وجود نداشت و همه گروه‌های سنی به یک روش مشابه در انتخابات شرکت کردند. نتایج منفی هم عبارت بود از اینکه عملیات رأی‌گیری بسیار کند بود؛ زیرا با مشکلاتی همچون تعداد کم مراکز رأی‌گیری مواجه بوده و از طرفی به‌دلیل کم‌بودن پهنای باند، مشکلاتی در ترافیک شبکه به‌وجود آمد.

۶-۱-۳ شورای‌عالی فرانسویان خارج از کشور[1]

این سیستم رأی‌گیری از راه دور ــ بدون نیاز به مراجعه به حوزه‌های رأی‌گیری و با استفاده از پست الکترونیک ــ در ۲۸ مارس ۲۰۰۳ برای فرانسویانی استفاده شد که در خارج از کشور زندگی می‌کردند. این انتخابات تنها انتخاباتی بود که افراد می‌توانستند از طریق پست الکترونیک رأی دهند. نتایج حاصل از این تجربه در مورد فرانسویان ساکن در ایالات متحده آمریکا عبارت بود از:

۱. نفوذ و گستردگی فراوان استفاده از شبکه اینترنت در آمریکا،

۲. بالا بودن فرهنگ استفاده از اینترنت در میان فرانسویان ساکن آمریکا،

۳. کم بودن میزان مشارکت افراد در انتخابات.

نتیجه مثبت حاصل از این تجربه عبارت بود از اینکه میزان مشارکت در انتخابات نسبت به انتخابات سال ۱۹۹۷، ۲/۵ درصد افزایش یافت. این نتیجه می‌تواند به‌عنوان یک موفقیت نسبی تلقی شود؛[2] زیرا هنگام برگزاری همین انتخابات برای فرانسویان ساکن در

---

1. Supreme Council of French Abroad (SCFA)

۲. بیش از ۶۱۰۰۰ نفر در انتخابات ثبت‌نام نموده و ۸۸۰۰ نفر (۱۴/۴۷ درصد) رأی دادند. در این انتخابات ۶۰/۶ درصد با استفاده از اینترنت، ۳۳/۸۴ درصد با استفاده از پست و ۵/۶ درصد به ۱۱ حوزه رأی‌گیری مراجعه کردند.

کانادا، که در آن از روش رأی‌گیری سنتی استفاده شد، میزان مشارکت رأی‌دهندگان از ۲۱/۱ درصد در سال ۱۹۹۷ به ۱۴/۷ درصد در سال ۲۰۰۲ کاهش یافت. همچنین کارکنان حوزه‌های رأی‌گیری توانستند مدیریت صندوق‌های الکترونیکی و رمزگشایی آرا را بدون نیاز به هیچ‌گونه آموزش خاصی انجام دهند.

نتایج منفی حاصل از این تجربه عبارت بود از اینکه برای ذخیره‌سازی آرا یک سرویس‌دهنده بسیار قوی مورد نیاز بود. درواقع، اطلاعات ذخیره شده در بانک‌های اطلاعاتی باید در سرورهای محرمانه‌ای ذخیره می‌گردید، همان‌طور که در رأی‌گیری سنتی، مستندات در دپارتمان‌های اداری ذخیره می‌شود.

۴-۱-۶ سایر کشورها

الف) بزریل

برزیل در استفاده از انتخابات الکترونیکی بسیار پیشرفته است. در انتخابات اکتبر سال ۲۰۰۰، ۱۰۹ میلیون نفر از طریق این روش رأی دادند. اجرای انتخابات به‌صورت الکترونیکی، میزان تقلب در انتخابات و زمان شمارش آرا را تا حد چشمگیری کاهش داد. ازطرف دیگر، افراد بی‌سواد که حدود ۲۰ درصد جمعیت را تشکیل می‌دادند، توانستند به‌راحتی در انتخابات شرکت نمایند.

در جریان انتخابات، تأثیر استفاده از ماشین‌های رأی‌گیری در کاهش میزان تقلب بسیار گسترده‌تر از میزان تأثیر آن بر افزایش میزان مشارکت شهروندان بود. ازطرفی، ماشین‌های رأی‌گیری امکان برگزاری چندین انتخابات به‌صورت هم‌زمان را ـــ که در برزیل رایج است ـــ فراهم می‌کند.

ب) بلژیک

اولین رأی‌گیری الکترونیکی در کشور بلژیک در سال ۱۹۹۴ انجام شد. هزینه بسیار بالای این انتخابات مانع از انتخاب این روش به‌عنوان روش اصلی برای برگزاری انتخابات در این کشور گردید.

روش به‌کار رفته، استفاده از ماشین‌های رأی‌گیری بود که در آن رأی‌دهنده از یک کارت مغناطیسی برای احراز هویت خویش استفاده کرده و با استفاده از یک قلم نوری کاندیدای مورد نظر خود را از روی صفحه نمایش انتخاب می‌کرد.

ج) انگلستان

تنها کشوری است که در سال‌های اخیر مطالعات بسیار گسترده‌ای را در مورد رأی‌گیری از راه دور انجام داده و طی چند سال گذشته از این روش برای بسیاری از انتخابات ادواری خود استفاده کرده است.

تجربیات انگلستان شامل تمامی انواع روش‌های رأی‌گیری الکترونیکی از جمله رأی‌گیری با استفاده از باجه‌های انتخاباتی در داخل حوزه‌ها، باجه‌های رأی‌گیری در خارج از حوزه‌ها (مانند ایستگاه‌ها یا مراکز خرید)، رأی‌گیری از راه دور (مانند استفاده از سیستم پیام کوتاه) و یا از طریق اینترنت با استفاده از رایانه‌های شخصی و یا تلویزیون‌های محاوره‌ای بوده است.

اگرچه نتایج انتخابات در سال ۲۰۰۳ ازنظر تکنیکی بسیار رضایت‌بخش بود، اما این روش نتوانست سبب جلب مشارکت بیشتر افراد برای شرکت در انتخابات شود؛ زیرا عوامل دیگری همچون مدت‌زمان برگزاری انتخابات، میزان تبلیغات انجام شده درخصوص کاندیداها و میزان آشنایی افراد با این شیوه رأی‌دهی، از جمله عوامل تأثیرگذار بر میزان مشارکت افراد بود.

۶-۲ انتخابات محلی

در این قسمت به برخی از موارد رأی‌گیری الکترونیکی در انتخابات محلی اشاره می‌شود.

۶-۲-۱ شهر «ایسی لس مولینکس»[1]

در جریان رأی‌گیری برای انتخاب اعضای شورای محلی در این شهر در نوامبر ۲۰۰۲، از روش رأی‌گیری اینترنتی بدون نیاز به مراجعه رأی‌دهندگان به حوزه‌ها استفاده شد. این تجربه نشان داد که اجرای رأی‌گیری الکترونیکی بدون نیاز به مراجعه رأی‌دهندگان به حوزه‌ها هم میسر است.

محدودیت‌ها و یافته‌های این تجربه عبارت بود از اینکه میزان مشارکت افراد در انتخابات بسیار پایین بود، که این مسئله به پیچیدگی کدهای انتخاباتی و بروز مشکلات

1. Issy-les-moulineaux

فنی بازمی‌گشت. در جریان این انتخابات ۱۴۴۹ نفر برای شرکت در انتخابات ثبت‌نام کردند، ۹۳۹ نفر کد شناسایی محرمانه دریافت نموده و تنها ۸۶۰ نفر توانستند رأی دهند.

ازطرف دیگر، سرعت پایین بارگذاری نرم‌افزار رأی‌گیری، ناسازگار بودن سیستم‌های رأی‌گیری با رایانه‌های مکینتاش و تنوع تجهیزات رایانه‌ای موجود در منازل، مشکلات فنی زیادی را به همراه داشت.

نظر کلی شورای فناوری اطلاعات فرانسه در مورد برگزاری انتخابات به‌صورت الکترونیکی، منفی بود و به‌کارگیری این روش را تنها در مورد انتخابات کم‌اهمیت مجاز دانست.

۶-۲-۲ شهر ارسی

در جریان انتخابات این شهر، از روش رأی‌گیری در باجه‌های مستقر در حوزه‌های انتخاباتی با استفاده از کارت‌های هوشمند یا گواهی‌نامه‌های دیجیتالی استفاده شد. رأی‌گیری در دو مرحله و در روزهای چهارشنبه تا شنبه انجام گرفت. در مرحله اول (۲۶ فوریه تا مارس سال ۲۰۰۳)، شرکت‌کنندگان می‌بایست نظر خود را درخصوص «گسترش محدوده شهر» اعلام می‌کردند. در مرحله دوم (۱۹ تا ۲۲ مارس ۲۰۰۳) نظرات شهروندان در مورد مشکل کمبود نفت در اروپا و راه‌حل‌های مبارزه با این کمبود جمع‌آوری گردید.

این انتخابات مردم را برای به‌کارگیری ابزارهای نو در زندگی عمومی تشویق کرد؛ زیرا روش پیشنهادی توانسته بود به‌نحو مطلوبی توجه افراد را به‌خود جلب نماید. ازسوی دیگر، محدودیت‌های این تجربه عبارت بود از: میزان مشارکت کم مردم در انتخابات و اینکه استفاده از کارت‌های هوشمند برای احراز هویت رأی‌دهندگان، هزینه زیادی را به‌دنبال داشت. علی‌رغم تمایل بسیار زیاد رأی‌دهندگان به استفاده از این نوع کارت‌ها، تنها برای ۹/۴ درصد افرادی که برای شرکت در انتخابات ثبت‌نام نموده بودند کارت شناسایی هوشمند صادر گردید.

۶-۳ انتخابات گروه‌های شغلی و انجمن‌ها

درخصوص این نوع از انتخابات، می‌توان به انتخابات الکترونیکی برای انتخاب اعضای کانون وکلا در انجمن وکلای دادگستری در فرانسه در ۲۵ و ۲۶ نوامبر ۲۰۰۲ اشاره کرد

که طی آن از روش باجه‌های رأی‌گیری مستقر در حوزه‌های انتخاباتی و رأی‌گیری اینترنتی استفاده شد. نتایج حاصل از این تجربه عبارت بود از:

۱. میزان مشارکت بالای افراد، که مشروعیت و صحت این روش را تأیید می‌نمود.

۲. عملیات سیستم بسیار ساده و روان بود و مشکلات فنی معدودی طی انتخابات رخ داد که آن هم به کمبود دانش استفاده از سیستم و یا مشکلات مربوط به ارتباط با تارنمای انتخابات بازمی‌گشت.

۳. برگزاری انتخابات شغلی می‌توانست بدون نیاز به حضور فیزیکی افراد، به‌صورت الکترونیکی برگزار شود.

۴. در این روش امکان رأی‌دهی مجدد افراد و نیز شرکت افراد غیرواجد شرایط وجود داشت. البته این اشکال با استفاده از سرویس‌دهنده‌های قوی قابل رفع بود.

۵. رأی‌گیری اینترنتی بیشتر مورد استقبال جوانان قرار گرفت.

۶. اگرچه انتخابات اینترنتی کاملاً امکان‌پذیر بود، اما به‌صورت کامل جایگزین انتخابات سنتی نگردید.

پی‌نوشت‌ها

1. *What is the Future of Electronic Voting in France, the Internet Rights Forum,* 2003, [online]: www.foruminternet.org.

فصل هفتم

استانداردهای انتخابات الکترونیکی

در ۳۰ سپتامبر سال ۲۰۰۴ شورای وزیران اروپا توصیه‌نامه Rec(2004)11 را که در مورد استانداردهای فنی، قانونی و عملیاتی رأی‌گیری الکترونیکی بود، تصویب نمود. این توصیه‌نامه نتیجه مطالعه یک گروه چندنفره از متخصصان (حقوق‌دانان، جامعه‌شناسان، سیاست‌مداران، شرکت‌های رایانه‌ای و ...) در زمینه‌های مختلف بوده و هدف از ارائه آن عبارت بود از:[1]

الف) بهبود روند انتخابات به موازات پیشرفت‌های جدید در جامعه و افزایش استفاده از فناوری‌های جدید اطلاعات و ارتباطات،

ب) کاهش زمان و هزینه برگزاری انتخابات،

ج) اعلام نتایج انتخابات با دقت، سرعت و قابلیت اطمینان بیشتر،

د) فراهم کردن امکان شرکت در انتخابات برای افراد معلول و کسانی که برای مراجعه به حوزه‌های رأی‌گیری با مشکل مواجه‌اند،

ه) ارائه خدمات بهتر به رأی‌دهندگان با ارائه روش‌های متفاوت رأی‌گیری،

و) افزایش تعداد رأی‌دهندگان با ایجاد کانال‌های اضافی رأی‌دهی.

تبعیت از استانداردهای مطرح در این توصیه‌نامه برای کشورهای عضو الزام‌آور است.

۱-۷ استانداردهای قانونی

۱-۱-۷ قاعده کلی

۱-۱-۱-۷ حق رأی عمومی

۱. در یک سیستم رأی‌گیری الکترونیکی، رابط کاربر باید ساده و قابل فهم باشد.

۲. شرایط مورد نیاز برای ثبت‌نام، نباید مانع از شرکت افراد در رأی‌گیری الکترونیکی شود.

۳. طراحی سیستم‌های رأی‌گیری الکترونیکی باید به‌نحوی باشد که به‌سادگی قابل استفاده بوده و برای افراد معلول و ناتوان نیز فرصت شرکت در انتخابات را فراهم کند.
۴. رأی‌گیری اینترنتی که در سراسر جهان قابل دسترسی است، تنها یک گزینه اختیاری و اضافی در رأی‌گیری است.

۲-۱-۱-۷ حق رأی مساوی

۱. در همه انتخابات و همه‌پرسی‌ها، رأی‌دهنده تنها یک‌بار حق رأی دارد و درصورتی به وی اجازه رأی‌دهی داده می‌شود که قبلاً رأی خود را به‌صندوق نریخته باشد.
۲. سیستم رأی‌گیری الکترونیکی باید مانع از ارسال رأی، از بیش از یک کانال ارتباطی شود.
۳. هر رأیی که به صندوق الکترونیکی ریخته می‌شود، باید حتماً و فقط یک‌بار شمارش شود.
۴. درصورت استفاده از کانال‌های الکترونیکی و غیرالکترونیکی برای رأی‌دهی، وجود روش مطمئن و قابل اعتماد برای جمع‌آوری آرا و اعلام نتایج صحیح ضروری است.

۳-۱-۱-۷ آزادی در حق رأی

۱. سازمان برگزارکننده انتخابات الکترونیکی، باید امکان برگزاری انتخابات آزاد برای همه اقشار جامعه را فراهم کند.
۲. فرایند رأی‌گیری الکترونیکی باید به‌نحوی انجام شود که مانع از برملا شدن آرا گردد.
۳. در هریک از مراحل رأی‌گیری الکترونیکی، پیش از تأیید نهایی رأی توسط رأی‌دهنده، امکان تغییر گزینه انتخابی و یا انصراف از رأی‌دهی فراهم شود.
۴. سیستم رأی‌گیری الکترونیکی باید احتمال دستکاری و مخدوش نمودن آرا را از افراد خاطی سلب نماید.
۵. در سیستم‌های رأی‌گیری الکترونیکی، افراد باید بتوانند گزینه دلخواه خود را انتخاب کنند، حتی اگر این انتخاب، یک رأی سفید باشد.
۶. سیستم رأی‌گیری الکترونیکی باید به‌وضوح ثبت رأی افراد را در هنگام رأی‌دهی و پس از خاتمه انتخابات به آنان اثبات نماید.
۷. سیستم رأی‌گیری الکترونیکی، پس از تأیید و ثبت رأی، باید از تغییر آن توسط رأی‌دهنده ممانعت به عمل آورد.

۷-۱-۱-۴ محرمانگی رأی

۱. سیستم رأی‌گیری الکترونیکی باید طوری سازماندهی شود که در کلیه مراحل رأی‌گیری، هویت رأی‌دهندگان محفوظ مانده و از هر عاملی که محرمانگی آرا را به‌خطر می‌اندازد، جلوگیری کند.

۲. سیستم رأی‌گیری الکترونیکی باید محرمانه بودن آرا در صندوق‌های رأی الکترونیکی و نیز محرمانگی آرای شمارش شده را تضمین کرده و مانع از کشف ارتباط بین رأی و رأی‌دهنده شود.

۳. صندوق‌های رأی الکترونیکی باید طوری طراحی شوند که با توجه به تعداد مشخص آرا در آن‌ها، امکان کشف ارتباط بین آرا و رأی‌دهندگان خاص وجود نداشته باشد.

۴. به‌منظور ممانعت از خدشه‌دار شدن محرمانگی آرا توسط اطلاعات مورد نیاز برای پردازش الکترونیکی، طراحی معیارهای امنیتی قوی ضروری است.

۷-۱-۲ تضمین‌های آیین‌نامه‌ای

۷-۱-۲-۱ شفافیت

۱. مسئولان انتخابات باید مطمئن شوند که رأی‌دهندگان سیستم رأی‌گیری الکترونیکی را درک کرده و به آن اعتماد دارند.

۲. در مورد نحوه عملکرد سیستم رأی‌گیری الکترونیکی، باید اطلاعات کافی در اختیار عموم قرار گیرد.

۳. پیش از برگزاری انتخابات الکترونیکی واقعی، امکان تمرین و کار با این شیوه جدید انتخابات فراهم شود.

۴. ناظران می‌توانند در چارچوب قانون، بر انتخابات الکترونیکی نظارت و کنترل داشته باشند.

۷-۱-۲-۲ ممیزی آرا و قابلیت اثبات

۱. مؤلفه‌های سیستم رأی‌گیری الکترونیکی باید برای مسئولان مجاز انتخابات، آشکار و هویدا باشند تا در مواقع لزوم بتوانند عمل ممیزی و اعتبارسنجی را انجام دهند.

۲. در برخی مواقع ــ در حین اجرا و خصوصاً پس از انجام تغییرات در سیستم ـــ لازم است که صحت عملکرد سیستم توسط یک گروه مستقل که از طرف مسئولان انتخابات برگزیده می‌شوند، مورد بازبینی قرار گیرد.

۳. امکان بازشماری آرا ضروری است. سایر مشخصه‌های سیستم رأی‌گیری الکترونیکی که ممکن است بر صحت نتایج انتخابات تأثیر بگذارد، باید قابل اثبات و تأیید باشد.
۴. سیستم رأی‌گیری الکترونیکی باید توانایی برگزاری مجدد بخشی از انتخابات و یا کل آن را داشته باشد.

۳-۲-۱-۷ امنیت و قابلیت اطمینان

۱. مسئولان انتخابات باید از امنیت و صحت سیستم رأی‌گیری الکترونیکی اطمینان حاصل نمایند.
۲. در کلیه مراحل انتخابات، باید از دخالت افراد متقلب و غیرمجاز که بر عملکرد صحیح سیستم تأثیرگذارند، ممانعت به عمل آید.
۳. سیستم رأی‌گیری الکترونیکی باید درطی فرایند انتخابات از معیارهای حفاظتی و امنیتی کافی برخوردار بوده و مانع دستکاری، تخریب و نفوذ افراد خاطی گردد.
۴. قبل از برگزاری انتخابات الکترونیکی، مسئولان مجاز انتخابات باید کاملاً به صحت و دقت سیستم اطمینان کامل داشته و هیچ‌گونه شک و شبهه‌ای در این خصوص نداشته باشند.
۵. تنها افرادی که توسط دست‌اندرکاران انتخابات مجاز شناخته شده‌اند می‌توانند به سرورها و اطلاعات مربوط به انتخابات دسترسی داشته باشند. بدیهی است که برای داشتن چنین مجوزی لازم است که قوانینی تدوین شود. عملیات فنی باید توسط یک تیم حداقل دونفره اجرا گردد. ترکیب این تیم‌ها باید به‌صورت منظم تغییر یابد.
۶. پس از باز کردن صندوق‌های رأی الکترونیکی، هر فعالیت مجاز بر روی سیستم، باید در حضور یک تیم متشکل از حداقل دو نفر صورت پذیرد، حتی اگر این فعالیت ارائه یک گزارش باشد.
۷. سیستم رأی‌گیری الکترونیکی باید دسترس‌پذیری و جامعیت آرا را حفظ نماید. آرا تا پیش از آغاز شمارش، می‌بایست به‌صورت مخفی و محرمانه نگهداری شود. لازمه نگهداری آرا در محیط‌های کنترل شده خارجی این است که آرا با روش‌های خاص به‌صورت رمز درآیند.
۸. در انتخابات الکترونیکی، در یک مرحله از پیش تعیین شده، اطلاعات مربوط به هویت رأی‌دهندگان باید از رأی آنها جدا گردد.

۷-۲ استانداردهای عملیاتی

۷-۲-۱ اطلاعیه

۱. کلیه مراحل مورد نیاز برای برگزاری انتخابات الکترونیکی، (قبل از برگزاری، در حین برگزاری و پس از پایان انتخابات) باید به‌صورت کاملاً مشخص در یک جدول زمانی تعریف شود.

۲. انتخابات الکترونیکی نباید پیش از صدور اطلاعیه انتخابات برگزار گردد، به‌خصوص در مورد انتخابات الکترونیکی از راه دور، کلیه اطلاعات مورد نیاز باید در یک دوره زمانی مشخص و قبل از انتخابات در اختیار افراد قرار گیرد.

۳. رأی‌دهندگان باید قبل از شروع انتخابات، با یک بیان بسیار ساده و واضح، با نحوه عملکرد سیستم رأی‌گیری الکترونیکی و کلیه مراحل مورد نیاز برای شرکت در انتخابات و رأی‌دهی آشنا شوند.

۷-۲-۲ رأی‌دهندگان

۱. صورت اسامی رأی‌دهندگان باید به‌طور منظم به‌روز شود. رأی‌دهنده باید بتواند اطلاعات ذخیره شده مربوط به‌خود را کنترل کرده و درصورت نیاز اصلاح نماید.

۲. امکان ایجاد یک ثبات الکترونیکی و تولید یک مکانیزم برای ثبت‌نام برخط (آنلاین) ضروری است. درصورتی‌که برای شرکت افراد در انتخابات الکترونیکی برنامه‌های خاص مورد نیاز باشد، لازم است که این برنامه‌ها به‌صورت الکترونیکی و درصورت نیاز به‌صورت محاوره‌ای طراحی شود.

۳. درصورت تداخل زمان ثبت‌نام و رأی‌گیری، باید مکانیزم خاصی برای احراز هویت رأی‌دهندگان فراهم گردد.

۷-۲-۳ کاندیداها

۱. سیستم رأی‌گیری الکترونیکی باید امکان معرفی برخط کاندیداها را داشته باشد.

۲. فهرست اسامی کاندیداها که به‌صورت الکترونیکی تهیه و در دسترس عموم قرار گرفته، باید برای مقاصد دیگر از جمله شناساندن کاندیداها مورد استفاده قرار گیرد.

۷-۲-۴ رأی‌گیری

۱. درصورت برگزاری هم‌زمان رأی‌گیری الکترونیکی از راه دور و رأی‌گیری در حوزه‌های انتخاباتی، طراحی سیستم باید به‌نحوی باشد که مانع از رأی‌دهی دوباره افراد گردد.

۲. رأی‌گیری الکترونیکی از راه دور ممکن است پیش از برگزاری انتخابات در حوزه‌های انتخاباتی شروع شده و حتی خاتمه یابد، اما پس از اتمام مهلت رأی‌گیری در این حوزه‌ها، رأی‌گیری می‌بایست متوقف شود.

۳. در تمامی روش‌های رأی‌گیری الکترونیکی از جمله سیستم‌های راه دور، باید مکانیزم‌های هدایت و پشتیبانی کاربران تعبیه شده و به‌راحتی در دسترس عموم قرار گیرد.

۴. در سیستم رأی‌گیری الکترونیکی باید در نحوه معرفی تمامی کاندیداها و شناساندن آنها مساوات رعایت شود.

۵. تعرفه الکترونیکی نباید حاوی اطلاعات اضافی در مورد کاندیداها باشد. همچنین در این تعرفه‌ها باید از هر نوع پیغام تأثیرگذار بر انتخاب افراد، اجتناب گردد.

۶. اگر تصمیم بر این باشد که اطلاعاتی در مورد کاندیداها در تارنمای انتخابات الکترونیکی قرار بگیرد، این اطلاعات باید با رعایت اعتدال و تساوی ارائه شود.

۷. قبل از استفاده از سیستم رأی‌گیری الکترونیکی از راه دور، باید توجه رأی‌دهندگان را به این مطلب جلب نمود که ارائه رأیشان به‌وسیله ابزارهای الکترونیکی، به‌منزله شرکت آنها در یک انتخابات واقعی است. در انتخابات آزمایشی نیز رأی‌دهندگان باید بدانند که برای کسب آمادگی، در یک انتخابات غیرواقعی شرکت می‌نمایند.

۸. سیستم رأی‌گیری الکترونیکی از راه دور نباید هیچ‌گونه مدرکی دال بر گزینه انتخابی رأی‌دهنده به‌جا بگذارد.

۹. صفحه نمایش دستگاهی که رأی‌دهنده از آن برای ارسال رأی خود استفاده می‌کند نباید هیچ‌گونه اثر صوتی، تصویری و یا تماسی از رأی باقی بگذارد.

۷-۲-۵ نتایج آرا

۱. سیستم رأی‌گیری الکترونیکی نباید تعداد آرای کاندیداها را قبل از بستن صندوق‌های رأی الکترونیکی به آنان اعلام کرده و یا قبل از خاتمه مهلت انتخابات، نتایج آرا را در اختیار عموم قرار دهد.

۲. سیستم‌های رأی‌گیری الکترونیکی باید از هرگونه پردازش بر روی آرا که منجر به هویدا شدن گزینه‌های انتخابی رأی‌دهندگان می‌شود، ممانعت به عمل آورند.
۳. پس از خاتمه مهلت انتخابات، باید بلافاصله عمل رمزگشایی آرا آغاز گردد.
۴. نمایندگان مجاز کاندیداها می‌بایست در شمارش آرا حضور داشته باشند. همچنین کلیه ناظران انتخابات می‌توانند بر این کار نظارت نمایند.
۵. باید یک رکورد برای ذخیره‌سازی اطلاعات مربوط به شمارش آرای الکترونیکی درنظر گرفته شود که در آن اطلاعاتی همچون زمان شروع و خاتمه شمارش، مشخصات افراد درگیر در این فرایند و نتایج شمارش نگهداری گردد.
۶. آرای معیوب و ناقص باید به‌صورت جداگانه ذخیره شود.

۶-۲-۷ ارزیابی

۱. سیستم رأی‌گیری الکترونیکی باید قابل ارزیابی و بررسی دقیق باشد.
۲. برداشت‌ها و نتایج حاصل از ارزیابی باید در انتخابات بعدی مدنظر قرار گیرد.

۳-۷ الزامات فنی

۱-۳-۷ قابلیت دسترسی

۱. لازم است معیارهایی برای سنجش قابلیت استفاده نرم‌افزارها و سخت‌افزارهای سیستم رأی‌گیری الکترونیکی توسط رأی‌دهندگان درنظر گرفته شود. حتی درصورت نیاز، روش‌های مختلف رأی‌گیری در اختیار همگان قرار گیرد.
۲. کاربران باید در طراحی سیستم‌های رأی‌گیری الکترونیکی دخیل باشند، به‌خصوص برای شناسایی موانع و محدودیت‌ها و آزمایش سهولت کاربرد مراحل اصلی رأی‌گیری.
۳. در مواقع لزوم باید امکانات اضافی و کمک‌های شخصی در اختیار کاربران قرار گیرد. امکانات کاربران باید حتی‌الامکان با آنچه که در دستورالعمل‌های تنظیمی برای اجرای انتخابات الکترونیکی عنوان شده، مطابقت داشته باشد.
۴. توسعه فناوری‌های جدید باید با تفکر و تعمق بسیار صورت پذیرد، به‌نحوی‌که با فناوری‌های موجود سازگار بوده و مناسب افراد معلول طراحی گردد.
۵. کاندیداها باید به بهترین شکل به رأی‌دهندگان معرفی شوند.

۷-۳-۲ قابلیت استفاده

۱. برای اطمینان از صحت عملکرد بخش‌های فنی مختلف و نیز سرویس‌های سیستم رأی‌گیری الکترونیکی، لازم است استانداردهای وسیعی تعریف گردد.
۲. در حال حاضر استاندارد زبان «ای ام ال»،[1] استاندارد وسیعی است که می‌تواند در انتخابات الکترونیکی مورد استفاده قرار گیرد.
۳. در مورد برخی از انتخابات محلی و خاص می‌توان از زبان‌های استاندارد دیگر هم استفاده نمود، اما این زبان باید با نگارش کلی «ای ام ال» سازگار باشد.

۷-۳-۳ عملکرد سیستم‌ها

۱. مسئولان انتخابات باید فهرست تأییدشده نرم‌افزارهای مورد استفاده در انتخابات الکترونیکی را منتشر نمایند. البته به‌دلایل امنیتی، نرم‌افزارهای حفاظت اطلاعات از این قاعده مستثنا هستند. در این فهرست‌ها باید نام نرم‌افزار، شماره نسخه، تاریخ نصب و شرح مختصری از آن بیان گردد. رویه‌ای نیز باید برای به‌روزرسانی منظم این نرم‌افزارها و نرم‌افزارهای حفاظتی مدنظر قرار گیرد. همچنین در هر زمانی باید امکان کنترل وضعیت تجهیزات رأی‌گیری وجود داشته باشد.
۲. هر سیستم پشتیبانی باید با استانداردها و مقتضیات سیستم اصلی مطابقت داشته باشد.
۳. عملیات پشتیبان‌گیری از داده‌های سیستم باید دائماً و به‌طور منظم انجام گیرد تا خللی در روند اجرای انتخابات به‌وجود نیاید.
۴. مسئولان تجهیزات انتخابات، باید با اجرای فرایند خاصی، از عملکرد صحیح تجهیزات در طی روزهای انتخابات اطمینان حاصل نمایند.
۵. قبل از برگزاری انتخابات، تجهیزات مورد نیاز باید به‌دقت مورد بررسی قرار گرفته و عملکرد آنها توسط مسئولان انتخابات مورد تأیید قرار گیرد.
۶. کلیه عملیات فنی باید منوط به اجرای یک کنترل قانونی باشد. هر تغییر مهمی در تجهیزات کلیدی باید به اطلاع مسئولان برسد.
۷. کلید انتخابات الکترونیکی باید در محل مطمئنی نگهداری شود. این محل در طول دوره برگزاری انتخابات باید از دسترسی افراد محفوظ بماند.

---

1. Election Markup Language (EML)

۸. در هنگام بروز اتفاقاتی که جامعیت آرا را به‌خطر می‌اندازد، مسئولان تجهیزات باید به‌سرعت این مطلب را به اطلاع مسئولان انتخابات برسانند. درجه اهمیت اتفاقات باید قبلاً توسط مسئولان انتخابات مشخص گردد.

۷-۳-۴ امنیت

۷-۳-۴-۱ نیازهای کلی

۱. معیارهای فنی باید تضمین کند که هیچ داده‌ای در صورت خرابی و یا ایجاد اشکال در سیستم رأی‌گیری الکترونیکی به‌صورت کامل از بین نمی‌رود.
۲. سیستم‌های رأی‌گیری الکترونیکی باید گمنامی رأی‌دهنده را حفظ کنند. فهرست اسامی رأی‌دهندگان که به‌وسیله سیستم‌های رأی‌گیری الکترونیکی ثبت و یا مخابره می‌شود باید محرمانه باشد.
۳. سیستم رأی‌گیری الکترونیکی باید به‌منظور اطمینان از عملکرد صحیح اجزا، کنترل‌های منظمی را متناسب با مشخصات فنی آنها انجام دهد.
۴. سیستم رأی‌گیری الکترونیکی باید براساس هویت کاربر و نقش او در سیستم، دستیابی او به سرویس‌هایش را محدود نماید. احراز هویت کاربر قبل از هر عمل دیگری باید صورت پذیرد.
۵. سیستم رأی‌گیری الکترونیکی باید اصالت اطلاعات را حفظ نموده و مانع سوءاستفاده، دستکاری، تغییر و یا دسترسی به اطلاعات گردد. در محیط‌های غیرقابل کنترل، این عمل با استفاده از مکانیسم‌های رمزنگاری صورت می‌گیرد.
۶. رأی‌دهندگان و کاندیداها باید دارای مشخصه منحصربه‌فردی بوده، به‌نحوی‌که به‌راحتی از سایر افراد قابل تشخیص باشند.
۷. سیستم‌های رأی‌گیری الکترونیکی باید قابل ارزیابی و بررسی دقیق باشد. به همین دلیل، لازم است که عملیات انجام شده طی فرایند رأی‌گیری و نتایج حاصله برای بررسی‌های آتی در مکان‌های مخصوصی ذخیره شود.
۸. در سیستم رأی‌گیری الکترونیکی باید زمان وقوع رخدادها ثبت گردد.

۹. مسئولان انتخابات موظف‌اند از استانداردهای امنیتی که توسط گروه‌های مستقل مورد بررسی قرار گرفته، پیروی نمایند.

۲-۴-۳-۷ الزامات مرحله قبل از انتخابات

۱. اصالت و جامعیت فهرست رأی‌هندگان و کاندیداها باید حفظ شده و منابع اطلاعاتی مورد تأیید قرار بگیرد. محافظت از داده‌ها از اهمیت بالایی برخوردار است.
۲. اعلام نامزدی کاندیداها و تعیین صلاحیت آنها باید در محدوده زمانی مشخصی صورت پذیرد.
۳. این موضوع که ثبت‌نام از رأی‌دهندگان در مهلت مقرر انجام شده، باید قابل اثبات باشد.

۳-۴-۳-۷ الزامات مرحله رأی‌گیری

۱. جامعیت اطلاعات در حین انتقال از مرحله قبل از رأی‌گیری باید حفظ گردد (فهرست رأی‌دهندگان و کاندیداها).
۲. باید تضمین شود که سیستم رأی‌گیری الکترونیکی یک تعرفه قانونی را در اختیار رأی‌دهنده قرار می‌دهد. در مورد رأی‌گیری الکترونیکی از راه دور، رأی‌دهنده باید مطمئن شود که ارتباطش با سرور مرکزی برقرار شده و تعرفه معتبر و قانونی به او ارائه گردیده است.
۳. ارسال رأی الکترونیکی در مهلت مقرر باید قابل اثبات باشد.
۴. سیستم‌های مورد استفاده توسط رأی‌دهندگان باید در مقابل هر عاملی که می‌تواند سبب تغییر آرا گردد محافظت شود.
۵. هرگونه اثری از انتخاب رأی‌دهنده در روی صفحه نمایش، باید بلافاصله پس از رأی‌دهی از بین برود. در مورد رأی‌گیری الکترونیکی از راه دور، رأی‌دهنده باید بداند که چگونه می‌تواند در خاتمه اطلاعات اضافی را حذف نماید تا ردپایی از دستگاهی که از طریق آن رأی ارسال شده، باقی نماند.
۶. سیستم رأی‌گیری الکترونیکی باید در ابتدا از واجد شرایط بودن رأی‌دهنده اطمینان حاصل نماید. این سیستم باید هویت فرد را تأیید کرده و تعداد آرایی را که وی مجاز به ارسال آن می‌باشد، کنترل نماید. رأی داده شده باید در یک صندوق الکترونیکی ذخیره گردد.

۷. سیستم رأی‌گیری الکترونیکی باید تضمین کند که انتخاب رأی‌دهنده دقیقاً به‌صورت یک رأی به سیستم ارائه می‌شود و رأی پلمپ شده در صندوق الکترونیکی قرار می‌گیرد.
۸. پس از پایان مهلت قانونی رأی‌گیری الکترونیکی، هیچ رأی‌دهنده‌ای نمی‌تواند مجدداً به سیستم دسترسی پیدا کند. اما به‌دلیل احتمال وجود تأخیر در کانال‌های ارتباطی، امکان پذیرش آرای الکترونیکی توسط صندوق‌های الکترونیکی، تا مدت‌زمان معینی میسر است.

۷-۴-۳-۴ الزامات مراحل رأی‌گیری پستی

۱. جامعیت اطلاعات منتقل شده در حین مرحله رأی‌گیری (آرا، فهرست رأی‌دهندگان و فهرست کاندیداها) باید حفظ شود.
۲. در مرحله شمارش آرا، رأی‌ها باید به‌صورت دقیق شمارش گردند. شمارش آرا باید تکرارپذیر باشد.
۳. سیستم رأی‌گیری الکترونیکی باید جامعیت صندوق‌های الکترونیکی و نتایج حاصل از شمارش آرا را تا زمان مورد نیاز حفظ نماید.

۷-۴ استانداردهای نظارتی

۷-۴-۱ کلی

۱. سیستم نظارتی باید بخشی از سیستم رأی‌گیری الکترونیکی بوده و امکان نظارت فنی، منطقی و کاربردی درسطوح مختلف سیستم وجود داشته باشد.
۲. در یک سیستم رأی‌گیری الکترونیکی باید امکان نظارت از ابتدا تا انتها وجود داشته باشد، از جمله نظارت بر عملیات ثبت‌نام رأی‌دهندگان و تأیید اعتبار آنها.

۷-۴-۲ ذخیره اطلاعات

۱. سیستم نظارتی باید باز و گسترده باشد و به‌صورت دائم پیامدها و تهدیدات سیستم را گزارش نماید.
۲. سیستم نظارتی باید رخدادها، فعالیت‌ها و زمان وقوع آنها را ثبت کند.

۷-۴-۳ نظارت

۱. سیستم نظارتی باید توانایی نظارت دقیق بر انتخابات را داشته باشد تا اطمینان حاصل شود که رویه اجرای انتخابات و نتایج حاصله مطابق با قانون بوده است.
۲. باید از افشای اطلاعات نظارتی به افراد فاقد صلاحیت ممانعت به عمل آید.
۳. سیستم‌های نظارتی باید در هر شرایطی گمنامی رأی‌دهنده را حفظ نماید.

۷-۴-۴ قابلیت اثبات

۱. سیستم نظارتی باید قابلیت بازبینی و تأیید عملیات انجام شده در سیستم رأی‌گیری الکترونیکی، تأیید صحت نتایج و کشف تقلب متخلفان را داشته باشد. همچنین سیستم باید بتواند ثابت کند که آرای شمارش شده قبلاً تأیید شده‌اند و همه آرای تأیید شده نیز مورد شمارش قرار گرفته‌اند.
۲. سیستم نظارتی باید بتواند ثابت کند که انتخابات الکترونیکی از قانون و مقررات پیروی کرده است. در این صورت، می‌توان به صحت و دقت نتایج اطمینان داشت.

۷-۴-۵ سایر

۱. سیستم نظارتی باید در مقابل حملات احتمالی، تغییر و یا از بین رفتن داده‌ها محافظت گردد.
۲. باید اطمینان حاصل شود که طی فرایند نظارت، اطلاعات به‌دست آمده توسط ناظران انتخابات، محرمانه باقی می‌ماند.

پی‌نوشت‌ها

1. *Recommendation Rec(2004)11 of the Committee of Ministers to Member States on Legal,* Operational and Technical Standards for E-Voting 2004, [online]: http://wcd.coe.int.

فصل هشتم

نتیجه‌گیری

تأثیر سریع فناوری اطلاعات و ارتباطات بر تمامی جنبه‌های زندگی اجتماعی بشر همچنان ادامه دارد. این تأثیرات نه تنها در بخش‌های آموزش، اقتصاد و رسانه‌ها بلکه در بعد سیاسی نیز مشهود می‌باشد. از دیدگاه متخصصین علوم سیاسی، تحقق دمکراسی الکترونیکی نتیجه استفاده فناوری اطلاعات و ارتباطات در ساختار سیاسی حکومت‌هاست.

دمکراسی الکترونیکی رویکرد مهمی برای تحکیم پایه‌های دمکراسی در یک کشور است به نحوی که با جلب اعتماد مردم، آن‌ها را به مشارکت در فعالیت‌های سیاسی کشور ترغیب می‌نماید. یکی از بارزترین زیرسیستم‌های دمکراسی الکترونیکی، انتخابات الکترونیکی است که هدف از آن افزایش صحت و دقت در برگزاری انتخابات، حفظ محرمانگی رأی‌دهندگان، کاهش هزینه‌های اجرایی، تسریع در اعلام نتایج و نهایتاً مدیریت صحیح حوزه‌های انتخاباتی است. مدیریت انتخابات به کلیه فعالیت‌ها و عملیاتی باز می‌گردد که در راستای برگزاری صحیح انتخابات همزمان با به‌کارگیری روش‌های قانونی انجام می‌پذیرد. بدون شک استفاده از رأی‌گیری الکترونیکی می‌تواند موجبات ارتقاء و بهسازی روش‌های مدیریتی در نظام انتخاباتی را فراهم آورد.

ازسوی دیگر در سال‌های گذشته عدم موفقیت برخی از کشورها در برگزاری انتخابات الکترونیکی توجه متخصصین زیادی را به‌خود معطوف داشته است. بسیاری از مشکلات به‌دلیل نقایص موجود در تجهیزات انتخاباتی و سیستم‌های به کار گرفته شده، گزارش شده است. چنین معضلاتی سبب خدشه‌دار شدن اعتماد ملت‌ها به فرایند دمکراسی در کشور خواهد شد. به این دلیل بسیاری از دولت‌ها در سراسر جهان تصمیم گرفتند که مبالغی را جهت اصلاح و بهبود تجهیزات انتخابات و نیز به‌کارگیری روش‌های نوین مدیریت انتخابات سرمایه‌گذاری نمایند. در حال حاضر بسیاری از کشورهای عضو

اتحادیه اروپا، به گونه‌ای انتخابات الکترونیکی را تجربه کرده و استراتژی‌های لازم جهت پیاده‌سازی صحیح این نوع انتخابات را تدوین نموده‌اند.

انتخابات الکترونیکی می‌تواند علاوه بر مدرنیزه نمودن فرایند انتخابات، ضمن به کارگیری فناوری‌های نوین اطلاعات و ارتباطات، امکان مشارکت الکترونیکی افراد را فراهم نموده و سبب بهبود ارتباط و تعامل ملت و دولت گردد. از طرفی استفاده از تمامی مزایای انتخابات الکترونیکی مستلزم به کارگیری معیارهای امنیتی پیشرفته و افزایش اعتماد رأی‌دهندگان و مسئولین انتخابات به این سیستم می‌باشد. رأی‌گیری الکترونیکی از ضروریات قرن حاضر است. لذا برای استفاده از این فناوری نوین، لازم است عوامل مستقیم و غیرمستقیم به عنوان زیربنا در امر توسعه رأی‌گیری الکترونیکی مورد بررسی و مطالعه قرار گیرد. همچنین مسئولین و دست‌اندرکاران باید این امر مهم را شناخته و درک نمایند.

در کشور ما با ملاحظه سطح متوسط سواد اطلاعاتی رأی‌دهندگان، ناکارآمد بودن زیرساخت‌های ارتباطاتی و کم بودن پهنای باند اینترنت در شرایط فعلی، بهترین روش برای برگزاری انتخاات الکترونیکی در برنامه کوتاه‌مدت، استفاده از ماشین‌های رأی‌گیری مستقر در حوزه‌های انتخاباتی می‌باشد. البته لازم است تجربیات لازم در برگزاری این نوع از انتخابات در سطوح سازمانی، محلی و منطقه‌ای حاصل گردیده و با رفع نواقص موجود بستر لازم برای انتخابات الکترونیکی در سطوح ملی فراهم گردد.

با توجه به جمعیت جوان کشور و علاقه این گروه به استفاده از فناوری‌های نوین اطلاعات و ارتباطات، رأی‌گیری اینترنتی در صورت ایجاد بستر مناسب و مطمئن می‌تواند در اولویت بعدی قرار گیرد.

منابع و مآخذ

قاضی‌شریعت‌پناهی، ابوالفضل. بایسته‌های حقوق اساسی، انتشارات دانشگاه تهران، ۱۳۸۱.

سوابق اخذ و شمارش *آراء انتخابات در ایران*، گزارش اداره کل رایانه شورای نگهبان، آذر ۱۳۸۴.

گروه مهندسین مشاور معمار و شهرساز عمران آب و انرژی ره شهر، بخش تحقیق و توسعه، ۱۳۸۳.

فتحیان، محمد و حاتم مهدوی، *مبانی و مدیریت فناوری اطلاعات*، تهران، انتشارات دانشگاه علـم و صنعت، ۱۳۸۵.

Anne-Marie. O, & P. Van Den Besselaar, *User Requirements for the TRUEVOTE Protocol,* TRUEVOTE Deliverable 2.1b, Amsterdam: Uva, 2002 .

Anne-Marie. O, & P. Van Den Besselaar. Internet Based Voting, TRUEVOTE Deliverable 2.1a, Amsterdam: Uva, 2002.

Baltimore. D, C. Vest. What is, What It Could Be, Caltech-MIT Voting Technology Project , 2001 [online]: http://www.vote.caltech.edu/reports/index.html.

Barry. N, Hague & Brian Loader (eds.), Digital Democracy, London: Routledge, 2000.

Bruschi. D, G. Poletti & E. Rosti, A Survey of E-Voting Protocols, TRUEVOTE Deliverable 2.0. Milano: University of Milano, 2002.

Chaum. D, Blind Signatures for Untraceable Payments, Advances in Cryptology, CRYPTO 82, 1999.

Cranor. L, R. K. Cytron, Sensus, A Security-Conscious Electronic Polling System for the Internet, Proceedings of the Hawaii International Conference on System Sciences, Vol. 3, Wailea, Hawaii, 2000.

Cranor. L, Voting after Florida : No Easy Answers, 2001 [online]: http:// lorrie.cranor.org.

Durette. B, Multiple Administrators for Electronic Voting, Master Thesis, Massachussetts Institute of Technology, 2001.

EU Student Vote, 2002, [online]: http://www.Eusv.org.

Feghhi. J, P. Williams, Digital Signatures - Aplied Internet Security, Addisson-Wesley, 2000.

Fisch. E. A, G. B. White, Secure Computers and Networks - Analysis, Design, and Implementation, Boca Raton: CRC Press, 2000.

Forschungsgruppe Internetwahlen, 2002, [online]: http://www.internetwahlen.de .

Fujioka. A, T. Okamoto, Y. Ohta, A Practical Secret Voting Scheme for Large Scale Elections, Advances in Cryptology-AUSCRYPT '92, Vol. 718, (Lecture Notes in Computer Science. Springer-Verlag, Berlin), 2001.

Garcia-Zamora. C, F. Rodr´Iguez and D. Arroyo, "An Efficient and Effective E-Voting Protocol for online Elections, Technical Report CINVESTAV-IPN, 17 Pages, 2005. [online]: http://delta.cs.cinvestav.mx/francisco/repository/repository.html .

Garcia-Zamora. C. P, F. Rodriguez-Henriquez, D. Ortiz-Arroyo, SELES: An E-Voting System For Medium Scale online Elections, In Proceedings Of IEEE's ENC-2005, Mexican International Conference on Computer Science, Puebla Pue., Mexico September 26th-30th, 2005.

Giovanni. C, C. Fiorella De, R. Laura, Community Networks and Access for all in the era of the Free Internet: Discover the Treasure of the Community, in L. Keeble & B.D. Loader (eds.), Community Informatics: Shaping Computer-Mediated Social Relations, London: Routledge, 2001.

Hague. B, B. Loader, Digital Democracy. Discourse and Decision Making in the Digital Age, 1999.

Herschberg. M, Secure Electronic Voting Over the Word Wide Web, Master Thesis, Massachussetts Institute of Technology, 1997.

Iuon-Chung. L, H. Min-Shiang, C. Chin-Chen, Security Enhancement for Anonymous Secure E-Voting Over A Network, Computer Standards & Interfaces, Vol. 25, No. 2, 2003.

Jared. K, W. Jie, Towards A Practical, Secure, and Very Large Scale Online Election, Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC'99), (Scottsdale, AZ. Diciembre), 2000.

Joaquim. R, Y. Uquete, Z. Andr´e, P. Ferreira, REVS -A Robust Electronic Voting System, Proceedings of IADIS International Conference E-Society 2003, (Lisbon, Portugal), 2003.

Kenneth. R, A Cryptographic Scheme for Computerized General Elections, Advances in Cryptology, CRYPTO'91, Vol. 576, (Lecture Notes in Computer Science. Springer-Verlag, Berlin), 2000.

Lioy. A, et al, DNS Security, Proc. of TERENA Networking Conference. Lisbon, Portugal, 2000.

Mercuri. R, P.G. Neumann, Verification for Electronic Balloting Systems, Secure Electronic Voting, (Ed. Gritzalis, D.A.), Kluwer, Boston, 2003.

Mitrou. L, D. Gritzalis, S. Katsikas, G. Quirchmayr, Electronic Voting: Constitutional and Legal Requirements, and Their Technical Implications, Secure Electronic Voting, (Ed. Gritzalis, D.A.), Kluwer, Boston, 2003.

Monteiro. A, Electronic Voting Systems, FCT, Lisbon University, TR-01-X. (In Portuguese) 2001.

Nurmi. H, A. Salomaa and L. Santean, Secret Ballot Elections in Computer Networks, Computers and Security 36 (10), 2000.

Prosser. A, R. Müller-Török, Electronic Voting Via the Internet, Presented at International Conference on Enterprise Information Systems ICEIS2001, Setùbal, 2001.

Recommendation Rec(2004)11 of the Committee of Ministers to Member States on Legal, Operational and Technical Standards for E-Voting 2004, [online]: http://wcd.coe.int.

Riera. A, SCYTL online World Security, Barselona, Spain, 2004 [online]: http://www.scytl.com

Rivest. R, Electronic Voting, Proc. of Financial Cryptography, Grand Cayman, Cayman Islands, 2001.

Rosario. G, J. Stanis Law, K. Hugo and R. Tal, Robust Threshold DSS Signatures, In Ueli Maurer, Editor, Advances in Cryptology, Springer-Verlag, 1999.

Rubin. A, Security Considerations for Remote Electronic Voting Over the Internet, in Comm. of ACM, 45(12), 2002.

Schoenmakers. B, A Simple Publicly Verifiable Secret Sharing Scheme and its Application to the Electronic Voting, Advances in Cryptology, CRYPTO'99, Vol. 1666, (Lecture Notes in Computer Science), 1999.

Sensus E-Voting System, 2002, [online]: http://lorrie.cranor.org/voting/sensus

Taylor. J, E. Burt, Parliaments on the Web: Learning Through Innovation, [In:] Coleman, S. Taylor. C., Van De Donk, W. eds, Parliament in the Age of the Internet, Oxford University Press, Oxford, 1999.

Varadharajan. Y, Anonymous Secure E- Voting Over A Network, Proceedins of the 14th Annual Computer Security Applications Conference, (IEEE Computer Society), 1998.

Watson. R, S. Akselson, B. Evjemo, N. Aarsaether, Teledemocracy in Local Government, Association for Computer Machinery, Communications of ACM, 42(12), 1999.

Watt. B, Implementing Electronic Voting 2002, [online]: http://www.lcd.gov.uk/elections/e-voting/pdf/legal-report.pdf

What is the Future of Electronic Voting in France, the Internet Rights Forum, 2003, [online]: www.foruminternet.org.

Winograd. T, & F. Flores, *Understanding Computers and Cognition,* Norwood: Ablex, 2000.