

نقد اخلاقی - تکنیکی رأی گیری الکترونیکی

دکتر فریا نصیری مفخم*، سیمین نقوی، یاسمن سرلتی

گروه مهندسی فناوری اطلاعات، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان

(تاریخ دریافت: 92/7/30، تاریخ پذیرش: 93/1/30)

چکیده

زمینه: همسو با جامعه اطلاعاتی، ایران نیز به سوی الکترونیکی شدن رأی گیری پیش می رود. رأی گیری الکترونیکی می تواند از جنبه های مختلفی همچون: ابعاد مهندسی، امنیتی، اخلاقی، حقوقی، اجتماعی، اقتصادی، سیاسی، روانشناختی، محیط زیست، و غیره، در به کارگیری تجهیزات و رویه های آن مورد مطالعه قرار گیرد. با فرض فراهم بودن تمام تجهیزات مربوطه، زیرساخت های شبکه ای لازم و پهنای باند کافی، بررسی میدانی نشان داده است که؛ با وجود کاهش هزینه ها، سادگی و شفافیت تعامل در این نوع مشارکت، موضوعات امنیت اطلاعات و قابلیت اعتماد، به عنوان عوامل راهکاری مهم بازدارنده در پذیرش و اقبال عمومی رأی گیری الکترونیکی مطرح بوده اند. این پژوهش با تحلیل تکنیکی، به این دو دسته نگرانی مطرح برای رأی دهنده، نامزد و مجری انتخابات الکترونیکی پاسخ می دهد. پاسخگویی و نقد سئوالات مطرح در این مقوله، با بررسی و تحلیل راهکارهای موجود امنیت اطلاعات انجام می شود.

نتیجه گیری: نتایج بررسی نشانگر آن است که؛ ویژگی های مثبت تکنیکی رأی گیری الکترونیکی از نظر امنیت اطلاعات و قابلیت اعتماد، گذار از رویکرد سنتی به الکترونیکی را یک ضرورت گریزناپذیر می نماید. به هر حال، زیرساخت شبکه ای و امنیتی از مهمترین پیش نیازهای تکنیکی انتخابات الکترونیکی است. لازم است پژوهش های آتی نیز ضمن برشمردن فواید متعدد رأی گیری الکترونیکی، به هم اندیشی و ارائه راه کار برای حل برخی مشکلات آن، رفع سایر موانع و تسهیل به کارگیری آن در کشور بپردازند.

کلیدواژگان: رأی گیری الکترونیکی، امنیت اطلاعات، قابلیت اعتماد

سرآغاز

رابطه دولت و شهروندان و روش ارائه خدمات دولتی را تغییر داده است. دولت الکترونیکی، باعث ایجاد تعاملی ساده، شفاف و ارزان بین دولت و شهروندان، شرکت های تجاری و دولت شده است. حرکت از دولت غیرالکترونیکی به دولت الکترونیکی موجب تحقق نوع الکترونیکی از دموکراسی می شود (1). از طریق دموکراسی الکترونیکی، فرآیندها و ساختارهای ارتباطات الکترونیکی بین دولت و شهروندان و مشارکت الکترونیکی مردم در فرآیندهای خط مشی گذاری و به بیانی، حاکمیت شهروند محور شکل می گیرد. از این رو، مشارکت الکترونیکی هدف نهایی و کلیدی رأی گیری الکترونیکی¹ نیز هست. در رأی گیری دستی، فرد باید مراحل را پشت سر بگذارد که

فرآیند رأی گیری، یک روش تصمیم گیری در میان گروه های مردم است. معروف ترین کاربرد رأی گیری در انتخاب دولت ها و مسئولین دولتی توسط افراد جامعه است. هر رأی، نشان دهنده نظر یک فرد در موافقت یا مخالفت با یک ایده، نامزد، یا حزب است. به بیانی دیگر، رأی گیری از مظاهر دموکراسی است که به معنی حکومت توسط مردم است. معمول ترین نوع آن، دموکراسی پارلمانی است که مردم با شرکت در انتخابات، نمایندگان خود در نوعی مجمع قانون گذاری را انتخاب می کنند. در این میان، ظهور فناوری های نوین اطلاعات و ارتباطات،

* نویسنده مسؤول: نشانی الکترونیکی: fnasiri@eng.ui.ac.ir

که، کمترین میزان اعتراض از طرف رأی‌دهنده، مجری و کاندیدا قابل طرح بوده و به بیانی، از سوی همگان قابل اعتماد باشد.

رأی‌گیری الکترونیکی

به‌کارگیری خدمات رأی‌گیری الکترونیکی در فضای فناوری اطلاعات نه تنها مستلزم رعایت اخلاق و حقوقی است که همچون؛ سایر علوم و علوم مهندسی برای آن برقرار است، بلکه، لازم است تمهیداتی فراهم باشد که امکان جرائم از طریق این بستر سایبری به پایین‌ترین مقدار برسد تا مورد اقبال عمومی واقع شود. براساس یافته‌های محققان و صاحب‌نظران، سه عامل ادراک مفید بودن³، سازگاری⁴، و قابلیت اعتماد⁵ رأی‌گیری الکترونیکی، در پذیرش آن مؤثر است (7-10). از سوی دیگر، از میان ویژگی‌های یک سیستم خوب رأی‌گیری الکترونیکی، دقت⁶، حفظ حریم شخصی⁷، و قابلیت تصدیق و تأیید⁸، مواردی هستند که باعث ایجاد دغدغه‌های تکنیکی برای پذیرش این فناوری می‌شوند (11). لازم به ذکر است که؛ در بررسی پیش‌نیازهای انتخابات الکترونیکی در ایران نیز؛ شفافیت⁹، پاسخگویی¹⁰، فرصت مساوی¹¹، آزادی¹² و حریم شخصی، قابلیت اعتماد، تشخیص هویت¹³، امنیت شبکه و اطلاعات¹⁴، و مدیریت الکترونیکی¹⁵ به عنوان عوامل مؤثر در استقرار رأی‌گیری شناخته شده‌اند که از بُعد تکنیکی مطرح هستند (2). این پژوهش در قالب پرسش‌هایی از دید سه طرف اصلی یعنی رأی‌دهنده، مجری و نامزد در انتخابات الکترونیکی به این دغدغه‌ها می‌پردازد.

رأی‌گیری الکترونیکی از دید رأی‌دهنده

رأی‌دهنده از یک سو می‌خواهد که هویت و رأی او محفوظ بماند و از سوی دیگر مایل است که مشارکت او مخدوش نشده و به حساب بیاید (12و13). نیازهای حقوقی، اخلاقی، اجتماعی و

می‌تواند موجب هدر رفتن زمان و انرژی بسیاری گردد. فرد رأی‌دهنده باید با در دست داشتن مدارک لازم و انتظار در صفوف ثبت تأیید مدارک، رأی خود را نوشته و به صندوق بیندازد. رأی‌گیری الکترونیکی می‌تواند به سه صورت ایستگاهی، اینترنتی و سرویس پیام کوتاه انجام شود (2). هم اکنون، در شعبه‌هایی منتخب از استان‌های کشور، نوع ایستگاهی از رأی‌گیری الکترونیکی به انجام رسیده است. مجری پس از دریافت مدارک لازم از رأی‌دهنده، یک کارت الکترونیکی در اختیار وی قرار می‌دهد. سپس رأی‌دهنده با مراجعه به دستگاه و وارد نمودن کارت، کد نامزد مورد نظر خود را وارد می‌نماید. دستگاه چهره نامزد انتخابی وی را نمایش می‌دهد تا شخص از درستی انتخاب خود مطمئن شود. در انتهای فرآیند، برگه چاپ‌شده رأی در اختیار شخص رأی‌دهنده قرار می‌گیرد که در آن، کد انتخاب‌شده قابل ملاحظه است. در پایان، رأی‌دهنده کارت الکترونیکی را به ناظر تحویل داده و کارت شناسایی خود را دریافت می‌نماید. در رأی‌گیری اینترنتی یا از طریق پیام کوتاه، فرد واجد شرایط با وارد کردن کد شناسایی نامزد مورد نظر در سایت اینترنتی رأی‌گیری یا ارسال آن به صورت پیام کوتاه به نظام خدمت‌گزار² رأی‌گیری مشارکت می‌کند (2و3).

رأی‌گیری به روش سنتی که برای اولین بار در ایالت ویکتوریای استرالیا در 1856 انجام شد تا امروز تحولات بسیاری را پشت سر گذاشته و به صورت الکترونیکی یا توسط تجهیزات الکترونیکی در آمریکا، هند، بلژیک، برزیل، انگلستان، فرانسه، و استرالیا برگزار می‌شود (4). در ایران نیز اولین تلاش‌ها سال 1372 آغاز شد و پس از پیگیری در سال‌های 1378، 1380 و 1386، این تلاش‌ها هنوز به بهره‌برداری نرسیده و نافرجام مانده است (5). با کاهش نقش عامل انسانی در نظام رأی‌گیری الکترونیکی، ثبت، ذخیره و پردازش داده‌های انتخابات از طریق فناوری‌های خودکار و الکترونیکی باعث صرفه‌جویی در هزینه‌ها، تسهیل مشارکت مردم و بهبود کیفیت خدمات دولت می‌شود. ولی به هر حال، نگرانی‌های امنیتی به عنوان عاملی بازدارنده در پذیرش رأی‌گیری الکترونیکی مطرح بوده است (2و6). برای برگزاری یک رأی‌گیری مناسب، باید از سه جنبه به رأی‌گیری نگاه کرد و تمهیدات لازم را فراهم نمود. به طوری

امنیتی یک رأی‌دهنده در اعتماد به رأی‌گیری الکترونیکی در قالب سؤالات زیر قابل طرح است.

سؤال 1: آیا رأی فرد مخدوش شده است؟ در مخالفت با رأی‌گیری الکترونیکی اولین ایرادی که وارد می‌شود، مشکلاتی است که احتمال دارد در نرم‌افزارها و سخت‌افزارهای مربوطه وجود داشته باشد. چون مهم‌ترین نگرانی در مورد انتخابات الکترونیکی، امکان دست‌کاری رأی‌ها است. در فرآیند الکترونیکی می‌توان با تهیه نسخه پشتیبان ضریب اطمینان سیستم و نتایج را بالاتر برد. ولی این احتمال هست که نسخه پشتیبان فرایند رأی‌گیری معدوم شود. به هر حال، صندوق‌های رأی سنتی هم ممکن است در یک حادثه از دست بروند و حتی ممکن است در شمارش دستی آرا هم دچار مشکل شوند و برای بازشماری آراء وقت و انرژی بسیاری صرف شود. با این حال، در روش الکترونیکی ممکن است توسط یک رخنه‌گر¹⁶ تغییری در رأی فرد رأی‌دهنده اعمال گردد و سپس رأی تغییر یافته به نام فرد رأی‌دهنده ثبت شود. ولی در روش سنتی نیز ممکن است یک یا چند صندوق رأی در یک یا چند حوزه با صندوق(های) از قبل پُر شده‌ای جا به جا گردد. پس معایب نظام سنتی در این خصوص، کمتر از روش الکترونیکی نیست. چون، در روش الکترونیکی فرد می‌تواند پس از پایان رأی‌گیری، رأی خود را ببیند و از مخدوش نشدن آن اطمینان حاصل کند (14).

در انتخابات سنتی، از طریق شماره‌های شناسایی که کنار برگه آراء هست، امکان وجود تقلب، قابل پیگیری است. در انتخابات الکترونیکی، می‌توان با استفاده از الگوریتم‌های درهم‌ساز¹⁷، مطمئن شد که رأی‌دهنده، همان رأی را فرستاده است و همچنین، می‌توان از امضای دیجیتالی¹⁸ و رمزنگاری کلید عمومی استفاده کرد تا امنیت و محرمانگی اطلاعات حفظ شود (15).

بنابراین، با استفاده از پروتکل‌های امن می‌توان از امنیت در انتخابات الکترونیکی مطمئن شد و برای رسیدن به این هدف، زیرساخت نباید ضعیف باشد.

مخدوش شدن رأی الکترونیکی می‌تواند به دلیل تقلب از طریق دزدی رأی و حمله‌های تزریق کد توسط ماشین رأی‌گیری صورت گیرد (16). برای نمونه: یک ماشین رأی‌گیری (AcuuVote Ts) در مقابل حمله‌هایی که رأی‌هایی از یک نامزد دزدیده شده و به دیگری داده شود آسیب‌پذیر است. این حمله‌ها بدون این‌که شواهدی از کلاهبرداری در ثبت‌های سیستم¹⁹ پیدا شود انجام می‌گردد. برای جلوگیری از کشف حمله، تعداد رأی‌هایی که از یک کاندید به دیگری داده می‌شود طوری تنظیم می‌شود که کل رأی‌های داده شده ثابت مانده و بازرسین متوجه نشوند. حمله‌هایی که فقط رأی‌هایی را اضافه کرده یا از تعداد آن‌ها می‌کاهند قابل پیگیری هستند. این ماشین دو رکورد از هر رأی به صورت رمز شده نگه می‌دارد که یکی از آن‌ها در حافظه داخلی و دیگری در حافظه جانبی است. ولی رمزنگاری برای حمله‌های دزدی رأی مناسب نیست چون کلید کدگذاری²⁰ در حافظه ماشین رأی‌گیری ذخیره شده است و بدافزار²¹ به راحتی به آن دسترسی می‌یابد. بدافزاری که روی ماشین اجرا می‌شود هر دو کپی اضافه رکورد را تغییر می‌دهد. از آنجا که ماشین رأی‌گیری نیز لاگ‌های متعدد و شمارنده‌های گوناگونی نگه می‌دارد که نشان‌دهنده استفاده متعدد از ماشین هستند، یک حمله دزدی موفق باید این رکوردها را به نحوی تغییر دهد که با تاریخچه ساخته شده در ماشین سازگار باشد. برخی از این حمله‌ها از طریق تزریق کد است و سپس حمله‌کننده نرم‌افزار مخرب خود را روی یک یا تعدادی ماشین رأی‌گیری نصب می‌کند. اگر او بتواند حتی یک دسترسی به ماشین پیدا کند، می‌تواند از حمله‌های شناخته شده برای نصب دستی نرم‌افزار استفاده کرده یا ویروسی نصب کرده که به دیگر ماشین‌ها منتشر شود و به او اجازه خرابکاری گسترده بدهد. به جای نصب مستقیم کد مخرب روی هر ماشین به صورت جداگانه، حمله‌کننده می‌تواند ویروسی ایجاد کند که روی یک ماشین نصب شود و از یک ماشین رأی‌گیری به ماشین دیگری منتقل شود و به این ترتیب، تعداد زیادی از ماشین‌ها را آلوده

کند. ویروس می‌تواند به نحوی نوشته شود که برنامه‌های مخرب دیگری مانند: سرقت رأی یا منع خدمت²² را روی هر ماشین آلوده نصب کند (14 و 11). هدف حمله‌های منع خدمت که مربوط به سؤال‌های 4 و 11 نیز می‌شود، غیر قابل دسترس کردن ماشین‌های رأی‌گیری در روز رأی‌گیری یا محدود کردن دسترسی افراد مسئول به رأی‌ها پس از رأی‌گیری است. در بیشتر موارد، پیش از رأی‌گیری می‌توان حدس زد که رأی‌دهندگان در بعضی از حوزه‌ها به نسبت خاصی به یک نامزد یا حزب رأی می‌دهند. حمله‌های منع خدمت می‌توانند به طوری طراحی که با افزایش بارکاری پردازش ماشین، مانع ارائه خدمات از طرف آن ماشین‌ها گردند و باعث شوند که نتایج انتخابات تحریف شده یا به نفع یک حزب خاص باشد.

خوشبختانه، استفاده از تکنولوژی و راهکارهای مناسب، ریسک‌ها و خطرات انتخابات الکترونیکی را کاهش می‌دهد. با استفاده از کدهای کپچا²³ می‌توان مانع حملات منع خدمت و تزریق کد شد. همچنین، در سال‌های اخیر، پروتکل‌های انتخابات الکترونیکی مبتنی بر تابلوی اعلانات²⁴ ابداع شده‌اند که با استفاده از آنها، رأی‌دهنده می‌تواند مراحل مختلفی را که رأی وی از مرحله‌ی تولید تا مرحله‌ی شمارش طی می‌کند بررسی نموده و از مخدوش نشدن آن اطمینان حاصل نماید. از سوی دیگر، استفاده از ابزارها و برنامه‌های جلوگیری از نفوذ و تشخیص نفوذ از یک سو و برنامه‌های ضد بدافزار از سوی دیگر اطمینان بیشتری از سلامت عملکرد ماشین‌های رأی‌گیری به همراه خواهد داشت.

سؤال 2: آیا رأی فرد به حساب آمده و غیر قابل ردگیری است؟ در هر سیستم رأی‌گیری باید محرمانگی حفظ شود. افراد در سیستم رأی معمولی، آراء خودشان را بی‌نام در صندوق می‌ریزند و بدین صورت محرمانگی نیز حفظ می‌شود. این نگرانی در هر دو نوع سنتی و الکترونیکی وجود دارد که رأی فرد با هویت او مطابقت داده شود و احتمال ردگیری یا انتقام وجود داشته باشد.

از آنجا که لازم است برگه رأی ممه‌ور به امضای معتبر برگزارکننده باشند ولی محتوای آنها محرمانه باشد، در رأی‌گیری الکترونیکی از امضای کور²⁵ به منظور حفظ حریم خصوصی رأی‌دهنده استفاده می‌شود (15). این امضا به فرد اجازه می‌دهد که از فرد دیگری بخواهد که پیامی را بدون دانستن محتوای آن امضا نماید. به این طریق، فرد رأی‌دهنده از به حساب آمدن رأی خود اطمینان می‌یابد و همچنین، به دلیل محفوظ ماندن محتوا می‌داند رأی او غیر قابل ردگیری است و مراجع قانونی مسئول تأیید واجد شرایط بودن رأی‌دهنده، نمی‌توانند به محتوای رأی پی ببرند. درحالی‌که، با توجه به شماره‌ی سربرگ‌ها، آراء در رأی‌گیری سنتی قابل ردگیری است و فرد پس از انداختن رأی خود در صندوق رأی نمی‌تواند اطمینان حاصل کند که رأی او مخدوش نشده یا صندوقی که رأی فرد در آن است با صندوق دیگری جابه‌جا نشده است (17-19).

سؤال 3: آیا در صورت تمایل، رأی‌دهنده می‌تواند رأی خود را پس از پایان رأی‌گیری ببیند؟ در رأی‌گیری الکترونیکی فهرستی که توسط نظام‌های خدمتگزار و در نهایت، خدمتگزار شمارش منتشر می‌شود، به رأی‌دهندگان این امکان را می‌دهد که درستی شمارش را بررسی کنند. این فهرست به گونه‌ای است که هر فرد می‌تواند با جست‌وجوی رسید خود در لیست منتشر شده، رأیی که به نام او ثبت شده را بررسی کند و همچنین، سایر آراء را البته بدون اطلاع از نام رأی‌دهنده مشاهده و سلامت نتیجه را بررسی کند. در حالی‌که، در رأی‌گیری سنتی این امکان برای فرد وجود ندارد (20).

سؤال 4: آیا حق رأی فرد تا آخرین لحظه رأی‌گیری محفوظ است؟ در رأی‌گیری به روش سنتی امکان اتمام تعرفه‌ها در برخی شعب وجود دارد و ممکن است فرد نتواند تا لحظات آخر به دلیل وجود مشکل مذکور از حق رأی خود استفاده کند. اما، در رأی‌گیری الکترونیکی با فرض وجود زیرساخت مناسب (مورد بحث در سؤال 1؛ برای نمونه با جلوگیری از حملات)، حق رأی تا آخرین لحظه محفوظ است. بایستی تا وقتی که مهر زمانی²⁶

رای فرد از زمان اتمام رأی گیری کمتر است، فرد حق رأی دادن داشته باشد. از آنجا که تمام شهرهای کشور دارای یک محدوده زمانی²⁷ هستند، این مورد به سادگی قابل کنترل است.

سؤال 5: آیا فرد می تواند از هر جا و در هر زمان رأی بدهد؟ از آنجا که در نوع ایستگاهی رأی گیری الکترونیکی نیز لازم است برای رأی دادن به ایستگاهها مراجعه شود، به نظر می رسد که مزیتی نسبت به رأی گیری دستی ندارد. ولی با نگاهی کلان تر به مساله مشخص می شود که این روش باعث شده است که محدودیت مکانی حذف شود و برای نمونه، در انتخابات مجلس بتوان به فرد مورد نظر خود که برای حوزه دیگری نامزد شده است رأی داد. در صورتی که رأی گیری از نوع اینترنتی باشد، فرد با حضور در هر مکانی و زمانی امکان رأی دادن دارد و انتخابات الکترونیکی می تواند باعث صرفه جویی در زمان افراد شود (14).

اما فرایند رأی دهی لحظه ای همیشه مطلوب نیست، پردازش سریع آراء وابسته به توانایی پردازش داده ای خدمتگزارهای دولت و فراهم کنندگان خدمات اینترنت است. اگر یک جمعیت بسیاری از رأی دهندگان بخواهند هم زمان رأی بدهند، توانایی محاسباتی نیاز به سیستمی دارد که بتواند این ترافیک را مدیریت کند. برگزاری رأی دهی در چند روز می تواند از این سربار جلوگیری کند. ولی این فرایند چند روزه رأی دهی می تواند باعث مبارزه سیاسی سختی شود (21).

به هر حال، رأی الکترونیکی با حذف محدودیت مکانی و هزینه ارسال ملزومات فیزیکی رأی گیری به کشورهای دیگر برای جمع آوری آراء هم وطنان، از این جهت برتری دارد. ولی لازم است هر رأی دهنده یک رایانه داشته و یا به تکنولوژی رأی دهی دسترسی داشته باشد. با توجه به ضریب نفوذ تلفن همراه و استفاده از پروتکل برنامه کاربردی بی سیم (وِپ)²⁸ دسترسی از همه جا برای رأی دهی امکان پذیر می شود.

رأی گیری الکترونیکی از دید مجری انتخابات

سلامت برگزاری رأی گیری الکترونیکی از دید مجری نیز اهمیت بسیاری دارد و در قالب پاسخگویی به سؤالات زیر می توان این نگرانی ها را مطرح نمود.

سؤال 1: آیا یک فرد می تواند بیشتر از یک بار رأی بدهد؟ در رأی گیری الکترونیکی، رأی دهنده تنها یک بار در هر یک از سیستم های خدمتگزار می تواند ثبت نام کند. در نتیجه، تنها یک رسید می تواند دریافت کند و با هر رسید هم تنها یک بار می توان رأی داد. پس از اتمام گشایش صندوق ها، آراء شمارش شده و فهرست حاوی هر رأی و رسید متناظر با آن منتشر می گردد. از آنجایی که تمامی سیستم های خدمتگزار در مرحله شمارش، لیست امضاهای خود را منتشر می کنند می توان با بررسی آن ها بروز تقلب را کشف نمود. البته، اگر همه خدمتگزارها با هم تبانی کرده باشند، تقلب صورت گرفته کشف نخواهد شد. همچنین، اگر از کارت استفاده شود، زمانی که رأی داده شد، کارت کاربر به صورت «رأی داده» نشان دار می شود و کارت برای رأی دهی دوباره نمی تواند استفاده شود. اما در رأی گیری سنتی، امکان تقلب و جعل شناسنامه و کارت شناسایی وجود دارد و یک فرد می تواند با مدارک جعلی در حوزه های مختلف در صورت متوجه نشدن مسئولین بیش از یک بار رأی دهد (19 و 20).

سؤال 2: آیا یک فرد می تواند در بیشتر از یک حوزه انتخابی رأی دهد؟ در صورت خرابی دستگاه و یا اگر تمام حوزه ها متصل نباشند، پایگاه داده های برون خط یک حوزه از حوزه دیگر خبر ندارد و ممکن است فردی بتواند بیش از یک رأی بدهد و از این رو، تقلب صورت بگیرد. ولی این نیز بستگی به شرایط نرم افزاری دارد و در مورد دستگاه های خودپرداز نیز مشکل از طریق پایگاه داده آنلاین حل شده است.

سؤال 3: آیا هویت رأی دهنده قابل تأیید است؟ از آنجایی که ممکن است فردی با کارت فرد دیگری رأی دهد، محرز است که با آن کارت رأی داده شده، ولی این نگرانی هست که نمی توان هویت رأی دهنده را تأیید کرد. به هر حال، در

رأی‌گیری الکترونیکی، رمزگذاری²⁹ این سری مشکلات را تا حد بسیاری حل کرده است. هویت‌شناسی فرد با استفاده از راهکارهای رمزگذاری و با استفاده از روش‌های زیست‌سنجی³⁰ قابل اثبات است.

از طریق امضاهای دیجیتالی که توسط گواهی‌های دیجیتالی³¹ یکتا و معتبر هستند، محرز می‌شود که یک فرد رأی داده است و هر فرد نیز با ارائه کلید خصوصی³² می‌تواند از رأی خودش آگاه شود. در راهکارهای زیست‌سنجی تشخیص هویت، به جای خواندن کدهای PIN، ورودی‌های زیست‌سنجی کارت‌خوان‌ها (از طریق تشخیص هویت اثر انگشت، اسکن رگ‌های شبکیه یا قرینه، تحلیل اندازه و مکان اجزای صورت، یا تشخیص ویژگی‌های خاص صدای کاربر، الگوی امضا کردن یا راه رفتن، یا حتی تحلیل سلول‌های DNA فرد در عرض چند ثانیه) برای تأیید اطلاعات رأی‌دهنده که روی کارت است استفاده نمی‌شود، بلکه به منظور تأیید اصالت خود کارت است. به عبارتی، سیستم رأی‌گیری در این زمینه تعاملی با مشخصات زیست‌سنجی رأی‌دهنده ندارد و این فرایند به تأیید خود کارت هوشمند کمک می‌کند. ترکیب دو یا چند تحلیل زیست‌سنجی می‌تواند در بهبود نتیجه و افزایش اعتماد سیستم مؤثر باشد. یک رخنه‌گر می‌تواند تعدادی از الگوهای زیست‌سنجی را با الگوهای دیگر جایگزین کند و باعث شود افرادی سودجو از کارت سایرین استفاده کرده و نتیجه انتخابات تغییر کند. نوع دیگری از حمله نیز وجود دارد که خود دولت با دسترسی مستقیم‌تری، الگوهای زیست‌سنجی ذخیره شده‌ی افراد را تغییر دهد (17 و 20). مقابله با این دو حمله مستلزم ایجاد انبار داده‌هایی³³ از الگوهای زیست‌سنجی رأی‌دهندگان باید امنیت بسیار بالا و توان پردازش بسیار سریع برای کشف متقلب از طریق مقایسه با آن داده‌ها است.

سؤال 4: آیا می‌توان نتایج رأی‌گیری را تا قبل از اتمام آن متوجه شد؟ انتشار اخبار عمومی بدون درنگ از نتیجه رأی، نامطلوب است زیرا رأی کسانی که تا آن لحظه رأی داده‌اند بر روی

رأی‌گیری اثر خواهد گذاشت. در رأی‌گیری الکترونیکی نیز باید پس از پایان رأی‌گیری و با حضور مسئولان مربوطه، آراء شمارش و نتایج منتشر شود. برای شمارش آراء باید کلیدی خصوصی موجود باشد که می‌توان آن را به چندین قسمت تقسیم کرد و در اختیار مسئولین مختلف (مجریان انتخابات و ناظران نامزدها) قرار داد. در این صورت، با حضور تمام افراد و ارائه تمام اجزای کلید پس از پایان رأی‌گیری نتایج قابل گشایش و مشاهده است (15). درحالی‌که، در رأی‌گیری سنتی در مواقعی که بعضی از صندوق‌ها زودتر باز شوند قسمتی از نتایج می‌تواند قبل از اتمام رأی‌گیری منتشر شود (20).

سؤال 5: آیا افراد مختلف که مسئول هستند می‌توانند بر شمارش آراء نظارت کنند؟ همانگونه که در سؤال قبل اشاره گردید، در رأی‌گیری الکترونیکی با تقسیم کلید خصوصی به چند قسمت جهت شمارش آراء می‌توان کلید را در اختیار افرادی قرار داد که لازم است نظارت را انجام دهند. در حالی‌که، در رأی‌گیری سنتی ممکن است در صورت عدم حضور یکی از مسئولین شمارش صورت گیرد (20).

رأی‌گیری الکترونیکی از دید نامزد انتخابات

نه تنها سلامت انتخابات از دید مجری اهمیت دارد و برای رأی‌دهندگان باید قابل اعتماد باشد، بلکه سئوالاتی نیز از دید یک نامزد انتخاباتی به لحاظ اطلاع از نتایج درست مطرح است. سؤال 1: آیا نامزد انتخابات می‌تواند بر شمارش آراء ناظر باشد؟ همچون رأی‌گیری سنتی، در رأی‌گیری الکترونیکی نیز نامزد انتخابات مایل است که بر شمارش آراء نظارت داشته باشد. برای شمارش آراء باید کلید خصوصی موجود باشد. می‌توان کلید خصوصی را بین نمایندگان نامزدها تسهیم نمود. به‌طوری‌که، هیچ یک هیچ اطلاعاتی در مورد کلید به‌دست نیاورد. اما، اگر همه آنها (یا حداقل تعداد مشخصی از آنها) با هم مشارکت کنند، به کلید رمزگشایی دست یابند. پس از طریق تسهیم راز³⁴، نظارت آن‌ها بر صحت شمارش نیز فراهم است. ولی، این

نگرانی ممکن است مطرح شود که؛ چون کلید خصوصی نیز در دسترس کسانی است که باید آن را رمز کنند، پس رمزکنندگان کلید خصوصی می‌توانند به آراء دسترسی داشته باشند و تا حدودی امنیت آراء در خطر است (20). انواعی از تسهیم راز و به طور خاص با هدف تسهیم کلیدرمزگشایی در کاربرد رأی‌گیری الکترونیکی پیشنهاد شده است که نیاز به طرف سوم مورد اعتماد ندارد (22). بنابراین، از نظر فنی، امنیت آراء در خطر نیست و محرمانگی رأی اشخاص حفظ می‌شود.

سؤال 2: آیا نامزد انتخابات می‌تواند در شمارش آراء دخیل باشد؟ در رأی‌گیری الکترونیکی نیز همانند رأی‌گیری سنتی نظارت بر شمارش آراء می‌تواند وجود داشته باشد. این امکان توسط کلید خصوصی که به چندین قسمت تقسیم می‌شود صورت می‌گیرد. ممکن است با حضور تعداد کافی از قسمت‌های کلید خصوصی شمارش انجام شود. برای جلوگیری از ایجاد تبانی، باید در این نوع تقسیم‌بندی دقت لازم انجام شود که افراد ضروری به طور حتمی حضور داشته باشند و در صورت مفقود شدن قسمتی از کلید، با حضور و اطلاع مراتب بالا، شمارش صورت گرفته و آراء از دست نرود.

سؤال 3: آیا دیگران می‌توانند تعداد آراء نامزد انتخابات را حدس بزنند؟ با رعایت مسائل امنیتی هیچ کس قبل از شمارش آراء نمی‌تواند تعداد آراء نامزد انتخاباتی را در رأی‌گیری سنتی یا الکترونیکی حدس بزند. زیرا، در روش الکترونیکی بدون وجود تمامی قسمت‌های کلید خصوصی امکان مشاهده نتایج وجود ندارد و در روش سنتی نیز قبل از شمارش این امکان فراهم نمی‌شود.

نتیجه‌گیری

بررسی انجام شده در این پژوهش نشان می‌دهد که؛ برخی از نگرانی‌ها در مورد رأی‌گیری الکترونیکی بسیار قابل تأمل و گاه فراتر از نگرانی‌های مطرح در نظام سنتی است. از دید

رأی‌دهنده، داشتن حق رأی و تا آخرین لحظه زمان رأی‌گیری، و غیرقابل ردگیری بودن و نیز مخدوش نشدن رأی او، نیاز اساسی است. به هر حال، از دید مجری انتخابات لازم است محرر شود که هر فرد فقط یک بار و فقط در یک حوزه رأی دهد، در عین اینکه هویت رأی‌دهنده قابل تأیید بوده و جعلی نباشد. نگرانی مجری، امکان نظارت بر سلامت برگزاری انتخابات، مخفی ماندن نتایج رأی‌گیری تا پیش از اتمام آن، و نیز امکان نظارت بر شمارش آراء توسط افراد مسئول است. افزون بر قابل حدس نبودن تعداد آراء نامزدها پیش از پایان انتخابات، نظارت و دخیل بودن نامزد در شمارش آراء برای او اهمیت دارد. پروتکل‌های امن با استفاده از امضاهای کور و دیجیتالی و نیز گواهی‌های دیجیتالی به خوبی به این نیازها پاسخ می‌دهد. این سازوکارهای امنیتی برای حفظ حریم شخصی و حفاظت از آرای افراد و نیز اطمینان از سلامت رأی‌گیری و شفاف بودن فرایند رأی‌گیری بیانگر برتری رأی‌گیری الکترونیکی به لحاظ امنیتی و اعتماد است. ولی بررسی تکنیکی نشان می‌دهد که این امر مستلزم فراهم‌بودن تمام تجهیزات مربوطه، زیرساخت‌های شبکه‌ای لازم و پهنای باند کافی است تا نظام به‌طور مؤثری از حملات امنیتی و سوءاستفاده‌های متقلبانه مصون باشد. جدول 1 این دو روش رأی‌گیری را به‌طور مختصر مقایسه می‌کند.

جدول 1: مقایسه رأی‌گیری سنتی و الکترونیکی

سؤال	سادگی و امکان پاسخگویی و رفع نگرانی توسط روش	رأی‌گیری الکترونیکی
آیا رأی فرد مخدوش شده است؟	بلی: پیگیری رأی توسط شماره‌های سربرگ	بلی: امکان پیگیری از طریق نسخه پشتیبان
آیا رأی فرد به حساب آمده و غیر قابل ردگیری است؟	تا حدی: قابل ردگیری بودن از شماره سربرگ‌ها	بلی: اطمینان از به حساب آمدن رأی و غیرقابل ردگیری بودن آن به کمک امضای کور
آیا در صورت تمایل، فرد می‌تواند رأی خود را پس از پایان رأی‌گیری ببیند؟	خیر: این امکان وجود ندارد	بلی: مشاهده رأی با استفاده از رسید رأی‌دهی
آیا حق رأی فرد تا آخرین لحظه رأی‌گیری محفوظ است؟	خیر: در صورت اتمام تعرفه‌ها این امکان وجود ندارد	بلی: وجود این امکان با فرض وجود زیرساخت‌ها
آیا فرد می‌تواند از هر جا و در هر زمان رأی بدهد؟	خیر: وجود محدودیت مکانی	بلی: حذف محدودیت‌ها در صورت اینترنتی بودن
آیا یک فرد می‌تواند بیشتر از یک بار رأی بدهد؟	تا حدی: امکان وجود تقلب	تا حدی: تقلب در صورت تباری سیستم‌های خدمت‌رار
آیا یک فرد می‌تواند در بیشتر از یک حوزه انتخابی رأی دهد؟	بلی: در صورت تقلب و رأی دادن با شناسنامه‌های مختلف	خیر: عدم وجود این امکان به کمک پایگاه داده‌های آنلاین
آیا هویت رأی دهنده قابل تأیید است؟	تأیدی: به کمک شناسنامه و کارت ملی که امکان تقلب هم وجود دارد	بلی: حل این مسئله به کمک مشخصات زیست‌سنجی
آیا می‌توان نتایج رأی‌گیری را تا قبل از اتمام آن متوجه شد؟	بلی: امکان افشای قسمتی از نتایج از طریق زودتر باز شدن بعضی از صندوق‌ها!	تا حدی: امکان شمارش زود هنگام توسط کلید خصوصی با حضور مسئولین
آیا افراد مختلف که مسئول هستند می‌توانند بر شمارش آراء نظارت کنند؟	تا حدی: شمارش در صورت عدم حضور بعضی از مسئولین نیز انجام می‌شود!	بلی: عدم امکان شمارش بدون حضور بعضی از مسئولین به دلیل تکه‌تکه بودن کلید خصوصی
آیا نامزد انتخابات می‌تواند بر شمارش آراء ناظر باشد؟	بلی: این امکان هست	بلی: با قرار دادن تکه‌ای از کلید در اختیار ناظر نامزدها
آیا نامزد انتخابات می‌تواند در شمارش آراء دخیل باشد؟	بلی: نظارت توسط ناظرین	بلی: نظارت ناظرین به کمک تکه‌های کلید خصوصی
آیا دیگران می‌توانند تعداد آراء یک نامزد را حدس بزنند؟	تأیدی: در صورت باز شدن صندوق‌ها	خیر: عدم امکان حدس آراء قبل از شمارش

33. Data warehouse

انبار داده‌ها

34. Secret Sharing

تسهیم راز

واژه‌نامه

1. e-Voting رأی‌گیری الکترونیکی
2. Server خدمت‌گزار
3. Usability ادراک مفیدبودن
4. Compatibility سازگاری
5. Reliability قابلیت اعتماد
6. Accuracy دقت
7. Privacy حفظ حریم شخصی
8. Verifiability قابلیت تصدیق و تأیید
9. Transparency شفافیت
10. Responsibility پاسخگویی
11. Equality of voter influence فرصت مساوی رأی‌دهنده
12. Freedom آزادی
13. Ensuring the identity تشخیص هویت
14. Network & information security امنیت شبکه و اطلاعات
15. Electronic management مدیریت الکترونیکی
16. Hacker رخنه‌گر
17. Hash function تابع درهم‌ساز
18. Digital signature امضای دیجیتال
19. System logs ثبت‌های سیستم
20. Encoding کدگذاری
21. Malware بدافزار
22. DoS (Denial of Service) مانع از خدمت‌رسانی
23. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) کپچا
24. Bulletin board تابلوی اعلانات
25. Blind signature امضای کور
26. Time stamp مهر زمانی
27. Time zone محدوده زمانی
28. WAP (Wireless Application Protocol) پروتکل برنامه بی‌سیم
29. Encryption رمزگذاری
30. Biometric زیست‌سنجی
31. Digital certificate گواهی دیجیتالی
32. Private Key کلید خصوصی

منابع

1. Pieters W, Becker MJ. (2005). Ethics of e-voting: An essay on requirements and values in Internet elections. UK: Ethics of New Information Technology: Proceedings of the Sixth International Conference of Computer Ethics.
2. Rahnavard F, Kharestani N. (2005). Prerequisite of e-election in Iran. Journal of Managmnet knowledge; 78: 25-44. (In Persian).
3. Burmester M, Magkos E. (2003). Towards secure and practical e-elections in the new era: Secure electronic voting. US: Springer. P. 63-76
4. Fathian M, Taghavi MS. (2009). E- Voting. Tehran: Islamic Palement Research Center.(In Persian).
5. Capital. (2009). Vacacy of e-election in Iran. Available at: [http:// hamvatansalam. com/ news131691.htm](http://hamvatansalam.com/news131691.htm). Accessed: 11 Apr. 2014. (In Persian).
6. Robinson D, Halderman J (2012). Ethical issues in e-voting security analysis. Proceedings of international conference on Financial Cryptography and Data Security.
7. Bahadoripoor M. (2006). Note that in engeeneering ethics. Ethics in Science & Technology; 1(1): 1-11. (In Persian).
8. Khanifar H, Jandaghi GR, Bordbar H. (2012). Role of ethical climate to utilize information technologies. Ethics in Science & Technology; 7(4): 10-18. (In Persian).
9. Sadeghi Arani Z, Mirghafori SHA, Sabet Z. (2013). Ethical decision making in the cyberspace and demographic factors affecting: study of internet crimes in Yazd province. Ethics in Science & Technology; 8(1): 60-69. (In Persian).
10. Schaupp L, Carter L. (2005). E-voting from apathy to adoption. The Journal of Enterprise Information Management; 18 (5): 586- 601.
11. Cranor L, Cytron K. (1997). Sensus: A security-conscious electronic polling system for the Internet. IEEE Thirtieth Hawaii International Conference on System Sciences.
12. Shayo M, Harel A. (2012). Non-consequentialist voting. Journal of Economic Behavior & Organization; 81(1): 299-313.

18. Subariah I, Maznah K, Mazleena S, Shah Rizan A. (2003). Secure E-Voting With Blind Signature. 4th international conference on telecommunication technology.
19. Schneier B. (1996). Applied cryptography. Canada: Katherine Schowalter. P. 125-210.
20. Novotný M. (2009). Design and analysis of a practical e-voting protocol. The Future of Identity in the Information Society; 170-183.
21. Brennan J. (2012). the Ethics of Voting. USA: Princeton University Press.
22. Fouque P, Poupard G, Stern J. (2001). Sharing decryption in the context of voting or lotteries. FC'00 Proceedings of the 4th International Conference on Financial Cryptography.
13. Guerrero A. (2010). The Paradox of Voting and the Ethics of Political Representation. Philosophy & Public Affairs; 38(3): 272-306.
14. Littlewood B, Bryans JW, Ryan PYA, Strigini L. (2006). E-voting: Dependability Requirements and Design for Dependability. Proceedings of the First International Conference on Availability, Reliability and Security.
15. Sherif MH. (2003). Protocols for Secure Electronic Commerce. 2nd ed. USA: CRC Press.
16. ProCon (2013). Electronic Voting Machines and Related Voting Technology. Available at: <http://votingmachines.procon.org/view.resource.php?resourceID=000273>. Accessed: 11 Apr. 2014.
17. Ferreira P (2007). Traceable Electronic Voting [Dissertação de Doutoramento]. Lisboa: Instituto Superior Técnico-Universidade Técnica de Lisboa.