
بسم الله الرحمن الرحیم

دانشگاه شاهد

دانشکده فنی و مهندسی

پایان نامه دوره کارشناسی ارشد مهندسی فناوری اطلاعات

مطالعه و امکان‌سنجی بهره‌گیری از تکنولوژی کارت هوشمند جاوا در رای‌گیری الکترونیکی و مباحث امنیتی مربوطه

نفیسه محمدی شکیبا

استاد راهنما:

جناب آقای دکتر دوستاری

دی ۱۳۹۰

مورد حمایت موسسه تحقیقات ارتباطات و فناوری اطلاعات

دانشگاه شاهد

دانشکده فنی و مهندسی

صورت جلسه هیئت داوران رساله کارشناسی ارشد

جلسه دفاعیه پروژه کارشناسی ارشد مربوط به آقای/خانم **نفیسه محمدی شکیبا** به شماره دانشجویی۸۸۷۵۲۸۴۰۰در رشته **مهندسی فناوری اطلاعات** با عنوان "**مطالعه و امکانسنجی بهره گیری از تکنولوژی کارت هوشمند جاوا در رای گیری الکترونیکی و مباحث امنیتی مربوطه**" به ارزش **۶ واحد** در روز **۹۰/۱۰/۲۸** در دانشکده فنی و مهندسی با حضور افراد ذیل تشکیل شد، نتیجه به قرار زیر است :

☑ پروژه نامبرده با نمره ۱۹/۵ قابل قبول می‌باشد.

☐ پروژه نامبرده مردود می‌باشد.

☐ پروژه نامبرده به شرط انجام اصلاحات جزیی قابل قبول می‌باشد. نمرهٔ دانشجو متعاقباً اعلام می‌شود.

☐ نام استاد راهنمای اول دکتر دوستار	دانشگاه : شاهد	امضاء	سهم استاد (به درصد):	۵۰٪
☐ نام استاد راهنمای دوم	دانشگاه :	امضاء	سهم استاد (به درصد):	
☐ نام استاد مشاور اول دکتر مردانی	دانشگاه :	امضاء	سهم استاد (به درصد):	۵۰٪
☐ نام استاد مشاور دوم	دانشگاه :	امضاء	سهم استاد (به درصد):	
☐ نام داور اول دکتر حاج سیدجوادی	دانشگاه : شاهد	امضاء		
☐ نام داور دوم دکتر یزدیان ورجانی	دانشگاه : تربیت مدرس	امضاء		
☐ نام داور سوم	دانشگاه :	امضاء		
☐ نام داور چهارم	دانشگاه :	امضاء		
☐ نام نماینده معاونت پژوهشی ناصر حضورزاده		امضاء		

تذکر:تعیین سهم اساتید در صورت وجود بیش از یک استاد راهنما و مشاور ضروری است.

شماره: تاریخ:	**اظهار نامه دانشجو**	

اینجانب *نفیسه محمدی شکیبا* دانشجوی کارشناسی ارشد رشته *مهندسی فناوری اطلاعات* گرایش *فناوری اطلاعات* دانشکده *فنی-مهندسی* دانشگاه شاهد، گواهی می دهم که پایان نامه/ رساله تدوین شده حاضر با عنوان؛ " *مطالعه و امکان‌سنجی بهره‌گیری از تکنولوژی کارت هوشمند جاوا در رای‌گیری الکترونیکی و مباحث امنیتی مربوطه* " به راهنمایی استاد محترم جناب آقای دکتر محمد علی دوستاری، توسط شخص اینجانب انجام و صحت و اصالت مطالب تدوین شده در آن، مورد تأیید است و چنان چه هر زمان، دانشگاه کسب اطلاع کند که گزارش پایان نامه/ رساله حاضر صحت و اصالت لازم را نداشته، دانشگاه حق دارد، مدرک تحصیلی اینجانب را مسترد و ابطال نماید هم چنین اعلام می دارد در صورت بهره گیری از منابع مختلف شامل؛ گزارش های تحقیقاتی، رساله، پایان نامه، کتاب، مقالات تخصصی و غیره، به منبع مورد استفاده و پدید آورنده آن به طور دقیق ارجاع داده شده و نیز مطالب مندرج در پایان نامه/ رساله حاضر تاکنون برای دریافت هیچ نوع مدرک یا امتیازی توسط اینجانب و یا سایر افراد به هیچ کجا ارایه نشده است. در تدوین متن پایان نامه/ رساله حاضر، چارچوب (فرمت) مصوب تدوین گزارش های پژوهشی تحصیلات تکمیلی دانشگاه شاهد به طور کامل مراعات شده و نهایتاً این که، کلیه حقوق مادی ناشی از گزارش پایان نامه/ رساله حاضر، متعلق به دانشگاه شاهد می باشد.

نام و نام خانوادگی دانشجو(دست نویس) :.....

امضاء دانشجو:

تاریخ:

این پروژه طبق قرارداد شماره ***۶۱۵۸/۵۰۰/ت*** مورخ ***۹۰/۰۴/۱۸*** تحت حمایت مادی و معنوی **موسسه تحقیقات ارتباطات و فناوری اطلاعات** صورت گرفته است.

تقدیم به

پدر و مادرعزیزم

و

آنان که ناتوان شدند تا ما به توانایی برسیم...

موهایشان سپید شد تا ماروسفید شویم...

و عاشقانه سوختند تا گرمابخش وجود ما و روشنگر راهمان باشند...

و به تمام آزاد مردانی که نیک می اندیشند و عقل و منطق را پیشه خود نموده و جز رضای الهی و پیشرفت و سعادت جامعه، هدفی ندارند.

دانشمندان، بزرگان و جوانمردانی که جان و مال خود را در حفظ و اعتلای این مرز و بوم فدا نموده و مینمایند .

تشکر و قدردانی

سپاس بی کران پروردگار یکتا را که هستی مان بخشید و به طریق علم و دانش رهنمونمان شد و به همنشینی رهروان علم و دانش مفتخرمان نمود و خوشه چینی از علم و معرفت را روزیمان ساخت و سلام و دورد بر محمّد و خاندان پاک او، طاهران معصوم، هم آنان که وجودمان وامدار وجودشان است؛ و نفرین پیوسته بر دشمنان ایشان تا روز رستاخیز...

بدون شک جایگاه و منزلت معلم، اجّل از آن است که در مقام قدردانی از زحمات بی شائبه ی او، با زبان قاصر و دست ناتوان، چیزی بنگاریم.

اما از آنجایی که تجلیل از معلم، سپاس از انسانی است که هدف و غایت آفرینش را تامین می کند و سلامت امانت هایی را که به دستش سپرده اند، تضمین؛ بر حسب وظیفه و از باب ***" من لم یشکر المنعم من المخلوقین لم یشکر اللّه عزّ و جلّ: "***

ازپدر و مادر عزیزم...این دو معلم بزرگوارم... که همواره بر کوتاهی و درشتی من، قلم عفو کشیده و کریمانه از کنار غفلت هایم گذشته اند و در تمام عرصه های زندگی یار و یاوری بی چشم داشت برای من بوده اند؛

از استاد با کمالات و شایسته؛ جناب آقای ***دکتر دوستاری*** *که در کمال سعه صدر، با حسن خلق و فروتنی، از هیچ کمکی در این عرصه بر من دریغ ننمودند و زحمت راهنمایی این رساله را بر عهده گرفتند؛*

از جناب ***آقای دکتر مردانی*** *که زحمت مشاوره این رساله را متقبل شدند*

و از استادان فرزانه و دلسوز؛ جناب آقایان ***دکتر یزدیان و دکتر حاج سید جوادی*** *که زحمت داوری این رساله را متقبل شدند؛ کمال تشکر و قدردانی را دارم.*

باشد که این خردترین، بخشی از زحمات آنان را سپاس گوید .

چکیده

از آنجاییکه در پروتکل‌های رای‌گیری اینترنتی، رای‌دهندگان می‌توانند از هر ترمینالی رای بدهند، پروتکل و متصدیان انتخاباتی نمی‌توانند هیچ کنترلی بر روی امنیت این ترمینال‌ها -که عموماً رایانه‌ها و لپ‌تاپ‌های آلوده‌ای هستند و با اتصال به اینترنت به‌سادگی آلوده می‌شوند- داشته باشند. پروتکل‌های متعددی نیز که در حوزه رای‌گیری اینترنتی معرفی میشوند تنها به تامین امنیت دادههای مبادله شده بین واحدهای درگیر، در زیر ساخت ناامن اینترنت تمرکز می‌نمایند و دو منبع تهدید عمده را نادیده میگیرند: ۱) بستر (رایانه) نا امن سمت رایدهنده و ۲) بستر (سرور) نا امن سمت متصدیان انتخاباتی. تمرکز این پژوهش به امن سازی سمت رای‌دهنده معطوف شده است.

طبق همایشی که در سال ۲۰۰۷ در انجمن اقتصاد جهانی واقع در شهر Davos برگزار شد، Vint Cerf یکی از پیشکسوتان اینترنت ادعا نمود که حدود یک چهارم از رایانه های شخصی که در دنیا به اینترنت وصل می‌شوند، توسط مجرمان رایانه ای کنترل می‌شوند. بنابراین این رایانه ها، زمانی که میخواهند در رای‌گیری اینترنتی شرکت کنند می‌توانند بسادگی و بی آنکه خود رای‌دهنده و حتی مراجع قانونی رای متوجه شوند، محتوای رای را تغییر داده و بدین‌ترتیب حتی اگر تمامی ویژگی‌های دیگر یک سیستم رای‌گیری الکترونیکی اعم از محرمانگی، صحت و گمنامی که باید در مراحل بعد تامین شود هم بطور کامل فراهم شود، باز هم امنیت کل پروتکل رای‌گیری به مخاطره افتاده است. برای تامین امنیت سیستم‌های کلاینت تنها وجود آنتی‌ویروس کافی نیست و می‌بایست روش‌هایی باشند که امنیت را در سطح سیستم‌عامل پیاده‌سازی کنند تا اجازه نصب و اجرای هیچ برنامه‌ی بدون گواهینامه امنیتی را به کاربر ندهند.

در این پژوهش، راهکاری مبتنی بر تکنولوژی جاوا کارت ۳ برای امن سازی سمت کلاینت (رای‌دهنده) پیشنهاد می‌شود. در این راه‌حل، رایانه‌ی ناامن سمت رای‌دهنده با یک کارت هوشمند جاواکارت ۳ که مجهز به یک کارت‌خوان امن مجتمع شده با صفحه کلید و صفحه نمایش امن و یک اینترفیس اتصال به شبکه می‌باشد، جایگزین می‌شود. این ساختار جدید می‌تواند مستقیما و بدون نیاز به هیچ میان‌افزار و دستگاه میانی، به شبکه متصل شود و با وجود پشته TCP/IP پیاده‌سازی شده در جاواکارت ۳، این کارت می‌تواند در نقش یک وب‌سرور یا وب‌کلاینت امن عمل نموده، درخواست های HTTP را از اعضای دیگر موجود درشبکه دریافت، پردازش و پاسخ‌های HTTP مناسب را تولید نماید.

علاوه بر این، در این پژوهش یک پروتکل رای‌گیری اینترنتی به نام J-FUCI طراحی و پیشنهاد گردیده است که به تضمین سه ویژگی کلیدی بی‌طرفی، مقاومت در برابر خرید و فروش رای و مقاومت در برابر تبانی واحدهای انتخاباتی می‌پردازد. این ویژگی‌ها مسائلی امنیتی-اجتماعی هستند که در کمتر پروتکلی بدانها پرداخته شده است. در این پژوهش پروتکل کاملی طراحی می شود که برای تضمین هر یک از این ویژگی‌ها راه‌کارهای امنیتی را پیشنهاد می‌دهد. این پروتکل هم‌چنین می‌تواند برای تضمین امنیت سمت رای‌دهده از ایده جاوا کارت۳ بعنوان جایگزینی امن برای ترمینال‌های رای‌گیری استفاده نماید.

کلید واژه:

رایگیری الکترونیکی (اینترنتی)، خرید و فروش رای، بیطرفی، تبانی، تکنولوژی جاواکارت ۳، امضای کور

فهرست مطالب

عنوان صفحه

فهرست اشکال

عنوان صفحه

فهرست جداول

عنوان صفحه

فصل ۱ مقدمه

۱ ۱ پیشگفتار

رای‌گیری الکترونیک که به معنای اخذ رای یا شمارش آراء به صورت الکترونیکی است از دهه ی ۶۰ میلادی آغاز شد و امروزه انواع مختلفی از آن در انتخابات مختلف کشورها، مورد استفاده قرار میگیرد. در ایران هم این موضوع از سال ۱۳۷۸ مورد توجه قرار گرفت. تا کنون در این حوزه سیستم‌های مینیمم بسیاری برای رای‌گیری الکترونیکی پیادهسازی شده‌اند. امروزه کشورهای زیادی تلاش میکنند که از ماشینهای رای - گیری الکترونیک استفاده کنند. در این زمینه کشور استونی پیشتاز این عرصه بوده است و در حال حاضر، رای‌گیری الکترونیکی بصورت ایدهآل تنها در این کشور انجام می‌شود. سیستم رایگیری الکترونیکی دارای مزایای بسیاری می‌باشد، هم‌چون: نتایج صحیح و سریع و جدول بندی[1] شده، هزینههای کمتر، دسترسی راحتتر، ریسک انسانی کمتر و درجهی دقت بالاتر.

با وجود تنوع بسیار در روش‌ها ی رایگیری، به طور کلی میتوان راههای مورد استفاده برای اخذ رای، توسط رایدهندگان را به سه دستهی کلی تقسیم کرد:

- رایگیری ایستگاهی: فرد رایدهنده برای اخذ رای باید به ایستگاه های رایگیری مراجعه کند و از ماشینهای رایگیری کیوسکی استفاده کند.
- رایگیری الکترونیک از راه دور [2]: این روش شامل رای از طریق تلفن همراه، تلفنهای با قابلیت سیستم تون، تلویزیونهای کابلی یا راههای دیگر میشود. رایگیری الکترونیک اینترنتی مبتنی بر وب هم می - تواند در این دسته قرار بگیرد.
- رایگیری اینترنتی [3]

انتخابات الکترونیکی از نظر پیادهسازی در جامعه دارای چند شکل کلی است که هرکدام دارای مزایا و آسیبهایی است. شکل اول متصور برای انتخابات الکترونیکی عبارتست از مکانیزه نمودن شعب اخذ رای و نصب سیستم‌های اتوماسیون در آنها است. در این مدل روش دریافت رای همچنان به صورت کاغذی بوده و در شعب اخذ رای انجام می‌شود. اما ثبت آرا در پایگاه داده صورت گرفته و شمارش و تجمیع آرا به صورت رایانهای می‌باشد. در این شرایط مزایایی مانند دقت بیشتر در شمارش و سرعت بیشتر در اعلام نتایج انتخابات به دست میآید. شکل دیگر انتخابات الکترونیکی ، الکترونیکی نمودن عملیات اخذ رای است. در این روش هر کدام از شهروندان جامعه برای رایدادن دارای کارت هوشمند خاص خود هستند که کلید منحصر به فرد آنها درون آن وجود دارد. در این مدل کل عملیات اخذ رای الکترونیکی است و نیاز به اسناد کاغذی وجود ندارد. در این روال، از رای داده شده توسط شهروند، بوسیله کلید خصوصی وی که بر روی کارت هوشمند او وجود

[1] Tabulated
[1] Remote electronic voting
[3] i-voting

دارد، امضای دیجیتالی تولید می‌شود. بدین‌ترتیب رای اخذ شده غیر قابل جعل بوده و قابل پیگیری قضایی است.

شکل دیگر، انتخابات الکترونیکی در محیط مجازی است به این صورت که شهروندان با مراجعه به درگاه وب (وب سایت) خاصی طبق پروتکلی خاص و با توجه به مباحث امنیتی مطرح در این زمینه و باز هم بوسیله کارت هوشمند اقدام به ثبت رای خود می‌نمایند. بدین‌ترتیب رایگیری به صورت کاملا متمرکز انجام خواهد شد و شمارش آرا بسیار سریع و حتی قابل شمارش لحظهای است. برای این منظور دیگر نیاز به شعب اخذ رای نیز نمی‌باشد و شهروندان می‌توانند بوسیله رایانه شخصی خود، لپتاپ و حتی گوشی تلفن همراه بوسیله پیامک اقدام به ثبت رای نمایند. از مشکلات این روش بحث تامین امنیت آن و میزان دسترسی و درصد استفاده افراد جامعه از رایانه (ضریب نفوذ) می‌باشد.

در این فصل ابتدا به نیازمندیها و ویژگی‌های امنیتی سیستم‌های رای‌گیری الکترونیکی پرداخته می شود. در ادامه، اهداف و مراحل پیاده سازی پژوهش بیان شده و خلاصه ای از آنچه که در این پروژه انجام شده است را مرور میکنیم. در انتها عناوین و خلاصهای از محتوای فصول بعد را به اختصار بیان می‌نماییم.

۱ ۲ نیازمندیها و ویژگیهای سیستم‌های رای‌گیری الکترونیکی

هر چند که تا بحال در حوزه رایگیری الکترونیکی تعریف [1] ثابتی برای یک سیستم ایدهآل بیان نشده و سیستم‌ها هر کدام ویژگیهای خاص خود را تامین می‌نمایند، اما ویژگیهای متنوعی برای سنجش سیستم‌های رایگیری الکترونیک بیان شده است که بخشی از آنها بصورت زیر دسته بندی می‌شوند[۱-۶]

۱. کارکرد[2]: در طی زمان رایگیری تمامی محاسبات باید در طول مدت منطقی انجام گیرد و رایدهنده مجبور نباشد که تا رایدادن سایر رایدهندگان منتظر بماند.

۲. عملی بودن به این مفهوم که تخصص و تجهیزات اضافی برای رایدادن موردنیاز نباشد.

۳. کارآمدی: محاسبات در یک زمان منطقی انجام گیرند.

۴. قابلیت حرکت[3]: محدودیتی روی مکان رای دادن برای رایدهندگان وجود نداشته باشد.

۵. پایایی[4]

۶. قابلیت ثبت وقایع

۷. در دسترس پذیی لازم: یعنی سیستم هرگز به حالت ناشناخته وارد نشود و یک مکانیزم پشتیبانگیری برای بازیابی سیستم در صورت خرابیهای سختافزاری وجود داشته باشد .

۸. دموکراسی: تنها کاربران مجاز و تنها یک رای معتبر به ازای هر کدام شمارش شود.

۹. مخفی بودن(حریم خصوصی)

۱۰. عدم قابلیت ردیابی: هیچ رایدهندهای نمی‌تواند اثبات کند که به یک شخص خاص رای داده است.

---

[1] Definition
[2] Functionality
[3] Mobility
[4] Durability

۱۱. دموکراسی: نمی‌توان تمام رایدهندگان را مجبور کرد تا انتخاب مشخصی داشته باشند.

۱۲. واجد شرایط بودن[1]

۱۳. غیر قابل استفاده دوباره[2]: تنها یک رای معتبر به ازای هر رای‌دهنده وجود دارد.

۱۴. گمنامی[3]:

- پیدا کردن لینکی میان رایدهنده و رای امکان پذیر نیست.

۱۵. دقت و صحت:

- حذف و افزودن آرا پس از پایان رایگیری امکانپذیر نباشد.
- رای معتبر شده نمی‌تواند تغییر کند.
- همه ی آرای معتبر شمرده می‌شوند.
- آرای نامعتبر شمرده نمی‌شوند.

۱۶. قابلیت رسیدگی و بازرسی: یکی از ویژگی‌های سیستم‌های رای‌گیری اثبات پذیری[4] است. با توجه به تعداد افراد درگیر و مجاز برای دسترسی به اطلاعات جمع‌آوری شده، برای اثبات پذیری (اطلاعات ممیزی)، اثبات‌پذیری به چند دسته تقسیم می‌شود:

- بازرسی عمومی[5]: هر کسی باید قادر باشد اعتبار کل فرآیند رایگیری را چک کند.
- بازرسی فردی[6]: هر رایدهنده اطلاعاتی داشته باشد که بتواند بررسی کند که رایش در شمارش نهایی درنظر گرفته شده است.

۱۷. انتخابات شفاف و بیطرف باشد. تشخیص نتیجه آرا حتی توسط مراجع ذیربط پیش از اتمام مهلت انتخاباتی میسر نباشد.

۱۸. سیستم قابل اعتماد باشد. یعنی حتی در صورت از بین رفتن ارتباطات اینترنتی و خراب شدن سیستم‌های رایگیری، هیچ رایی نباید از بین برود.

۱۹. انعطافپذیری: برای سناریوهای رایگیری متفاوت قابل تنظیم باشد.

۲۰. سادگی و راحتی: سیستم‌های رایگیری نباید نیاز به تخصص خاصی برای استفاده داشته باشند.

۲۱. رای‌دادن و رفتن[7]: پس از رای دادن رایدهنده نباید عمل دیگری انجام دهد.

۲۲. احراز هویت قوی و امن:

- پین یا کارت هوشمند (امضای دیجیتال): در سیستم رایگیری الکترونیکی در دست داشتن ID-card به تنهایی کافی نیست بلکه کاربر باید امضای دیجیتال هم داشته باشد. برای این کار باید

[1] Eligiblility
[2] Unreusability
[3] Anonymity
[4] Verifiability
[5] Public verifiability
[6] Individual verifiability
[7] Vote and go

نرم‌افزار بفرم یک ماژول رایگیری در اختیار افراد قرار گیرد تا روی رایانه خود نصب نمایند که استفاده از ID-card و امضای دیجیتال را امکان پذیر نماید. اما کارت‌خوان باید توسط خود افراد خریداری شود. بنابراین در اینجا پیچیدگی فرآیند نصب نرم افزار، نبود. دانش تحویل امضای دیجیتال از جمله موانع استفاده همه‌گیر از این سیستم می‌باشد.

- پسورد یکبار مصرف.
- اطلاعات بایومتریک (سیستم رایگیری الکترونیکی باید دارای یک حافظه بسیار امن برای نگهداری تمپلتهای بایومتریک باشد).

یک سیستم رایگیری اینترنتی علاوه بر موراد ذکر شده باید ویژگیهای زیر را هم داشته باشد:

۲۳. مقاوم در برابر تبانی: هیچ واحد انتخاباتی (همچون سرورهایی که در انتخابات شرکت دارند) و حتی مجموعهای از واحدهای انتخاباتی نباید بتوانند برای آرا توطئه بریزند و جلوی رایدادن رایدهندگان را بگیرند. این ویژگی را باید با اندازهگیری تعداد واحدهای متحد برای دخالت در انتخابات تعیین نمود.

۲۴. در دسترسپذیری: سیستم تا زمانیکه انتخابات تمام نشده، باید در دسترس باشد.

۲۵. قابلیت شروع دوباره: تا زمانیکه مهلت انتخابات تمام نشده، سیستم باید به کاربرانی که فرآیند رای-گیریشان متوقف شده اجازه ادامه یا شروع دوباره را بدهد.

۲۶. امن‌سازی رایانه سمت رای‌دهنده برای اطمینان از معتمد بود بستر رای‌دهنده.

۱ ۳ -مشکلات امنیتی(چالش ها) سیستم‌های رایگیری الکترونیکی و اینترنتی

در این قسمت، مشکلات سیستم‌های رای‌گیری الکترونیکی و اینترنتی بیان می‌شود:

الف: رای‌گیری الکترونیکی

چالشهای مطرح شده در رایگیری الکترونیکی، عموما به شرح زیر میباشند [۷-۹]:

- محدودیت تعداد تولیدکنندگان نرمافزار
- تعرض هکرها
- تقلب در رایگیری از طریق رایانه
- کلاهبرداری از رای
- برنامههای نادرست نصب شده بر روی رایانه های موجود در ایستگاه های رای‌گیری
- عدم عملکرد درست رایانه های موجود در ایستگاه های رای‌گیری

ب: رای‌گیری اینترنتی

پروتکل‌های ارائه شده برای کاربردهای رایگیری اینترنتی علاوه بر اینکه باید نیازمندیها و مشکلات موجود در حوزه رایگیری الکترونیکی را آدرسدهی کنند، به دلیل تعامل با زیرساخت ناامنی چون اینترنت،

یکسری تهدیدات و آسیبپذیریهای جدید را نیز باید مدنظر قرار داده و راهحلهایی برای هر یک ارائه دهند. از جمله مشکلات معمول برای اکثر پروتکل‌های رایگیری اینترنتی می‌توان به موارد زیراشاره نمود:

- حملات عدم سرویس‌دهی[1]: در این حالت هکرها می‌توانند با ازدیاد بار از طریق ارسال درخواستهای اطلاعاتی، جلوی رایگیری رایدهندگان را بگیرند. مثلا در حالتیکه از تصدیق مبتنی بر بایومتریک استفاده میکنیم، حمله عدم سرویسدهی توزیع‌شده [2] به سرورهای حاوی تمپلیت های بایومتریک پیش از رایگیری و در حین آن بسیار خطر زاست.
- هک کردن سرورها به منظور تغییر، کپی و تخریب داده‌های ذخیره شده و نرمافزارهایی که تمامیت آرا را از بین میبرند.
- عدم مقیاسپذیری سیستم که به دست تولیدکننده و طراح سیستم تعیین می‌شود هم یکی از مشکلات این رده می‌باشد .
- خراب شدن سرورها بدون نقض امنیت و کارکرد کل سیستم[3]، در سیستم‌های رایگیری الکترونیکی قابل جبران نیست. اگر سیستم بایومتریک بعنوان متدی برای کنترل دسترسی استفاده شود، در صورت عدم کارکرد درست می‌توان با روش‌ها ی سنتی آن را دور زد[4] اما این کار در رایگیری الکترونیکی امکانپذیر نمی‌باشد در اینصورت حملاتی هم‌چون DDOS می‌توانند اثرات بسیار مخربی را بر جای بگذراند.
- چگونگی تصدیق هویت امن رایدهندگان بطوریکه امنیت مورد انتظار را ارائه و سربار هزینهای بالایی نداشته باشد.
- اطمینان از محرمانگی و گمنامی رایدهنده
- افزودن قابلیت بازرسی فردی به سیستم: یعنی طراحی یک سیستم قابل اعتماد بطوریکه کاربر مطمئن است که رایی که در سیستم ثبت می‌شود، همانیست که او انتخاب کرده است. برای این مسئله دو راهحل ارائه می‌شود:
  - **راه حل ۱:** تولید رسید برای هر رایدهنده. در فصل های بعد خواهیم گفت که تولید رسید اگرچه امکان بازرسی فردی سیستم را فراهم می‌کند اما از آن طرف امکان خرید و فروش رای را هم بسیار بالا میبرد. در رایگیری الکترونیکی قابلیت بازرسی ویژگی است که در مقابل مخفیانه بودن رای قرار می‌گیرد. به این مفهوم که از یک طرف رایدهنده می‌خواهد بتواند کل فرآیند رایگیری بالاخص درستی رای خود را در شمارش نهایی بازرسی کند و از طرف دیگر اگر اطلاعات زیادی در این خصوص در اختیار رایدهنده قرار گیرد وی می‌تواند از این اطلاعات برای خرید و فروش رای استفاده کند. بنابراین اطلاعاتی که در این

[1] Denial of Servises(DOS)
[2] DDOS
[3] Fail safe
[4] Bypass

میان باید به رایدهنده تحویل داده شود، باید به اندازهای باشد که بتواند بصورت شخصی بازرسی کند که رایش شمرده شده باشد اما نباید برای متقاعد ساختن دیگران کافی باشد.

- **راه حل ۲:** استفاده از یک برد الکترونیکی عمومی [1] که تمامی آرای ذخیره شده در سرروهای شمارنده[2] در این برد نشان داده می‌شود.

در پروتکل‌های رایگیری اینترنتی و الکترونیکی معمولا از هردو روش در کنار هم استفاده می‌شود.

- مشکلات اجتماعی مانند دسترسی همگانی به اینترنت و قابلیت کار با کامپیوتر.
- آسیب‌پذیری سیستم عاملها: این سیستم‌ها روی یک سیستمعامل عمومی اجرا می‌شوند و اکثرا هم از ویندوز استفاده می‌کنند که اگر آخرین بروزرسانی های امنیتی را انجام نداده باشد، در صورت اتصال به اینترنت در مقابل ویروسها وکرمها بسیار آسیبپذیر است. این ویروسها وکرمها می‌توانند کاری کنند که رایها خراب و یا گم شوند و درصورتیکه ثبت کاغذی وجود نداشته باشد، ایجاد دوباره این آرا غیر ممکن می‌شود.
  - راه حل: مهاجرت به یک سیستمعامل باز
- آسیبپذیری های زیرساخت اینترنت
- سادگی خرید و فروش رای: بر طبق [۴] خرید و فروش رای[3] به چهار صورت بیان می‌شود:
  - نقاب زنی: در صورتی که متد تشخیص رایدهندگان ناکارآمد باشد، یک فرد بدخواه می‌تواند خود را به جای رایدهنده جا بزند.
  - انتخاب یک رشته مشخص: اجبارکننده می‌تواند به رایدهنده بگوید که از یک رشته بیتی مشخص برای ساختن رای خود استفاده کند، در اینصورت پس از پایان انتخابات و منتشر شدن آرا، اجبارکننده می‌تواند با توجه به این رشته رای را بررسی کند.
  - اثبات با استفاده رسید رایگیری. فرد بدخواه می‌تواند در روز انتخابات حضور داشته و رای افراد را مانیتور کند.
- آسیبپذیریها و آلوده بودن پلتفرم رایانههای شخصی سمت رایدهندگان : هرگز نمی‌توان مطمئن شد که تمامی این رایانههای شخصی از هر نوع کد آلودهای[4] پاک هستند.
- سادگی تبانی اعضای انتخاباتی برای نقض امنیت پروتکل رای‌گیری در سه قالب:
  - نقض گمنامی رای‌دهنده
  - معرفی آرا به جای رای‌دهندگان غیر مجاز
  - عدم سرویس‌دهی عمدی به رای‌دهندگان مجاز

[1] Bullitin Board
[2] Tallier
[3] Coercion and Bribery
[4] Malware