بهبود امنیتی پروتکل FOO با بهره گیری از تکنولوژی جاوا کارت ۳ ومفهوم JIF

مصطفی محمدپورفرد[۱]، محمد علی دوستاری[۲]،نفیسه محمدی شکیبا[۳]، محمد باقر غزنوی قوشچی[۴]

[۱] دانشجوی کارشناسی ارشد فناوری اطلاعات،دانشگاه شاهد ،تهران
m.mohamadpour@shahed.ac.ir

[۳] استادیار، دانشگاه شاهد، تهران
doostari@shahed.ac.ir

[۲] کارشناس ارشد فناوری اطلاعات،دانشگاه شاهد،تهران
shakiba@shahed.ac.ir

[۴] استادیار، دانشگاه شاهد، تهران
ghaznavi@shahed.ac.ir

چکیده

امروزه، رای‌گیری اینترنتی به دلیل سرعت، شمارش اتوماتیک، کاهش هزینه وقابلیت خطای کم بسیار مورد توجه قرار گرفته است. در حالیکه از سال ۱۹۸۰ پروتکل های رای‌گیری الکترونیکی زیادی توسعه داده شده اند، مجموعه ویژگی‌های امنیتی که پروتکل باید به آنها نائل شود تکامل پیدا کرده است. در این مقاله روشی برای رای‌گیری امن اینترنتی با بهبود پروتکل رای‌گیریFOO و هم چنین استفاده از جاوا کارت ۳ ارائه شده که در آن بااستفاده از مفاهیم تسهیم راز ورمزنگاری به پروتکل FOO ویژگی‌هایی نظیر جلوگیری از خرید و فروش ،جلوگیری از تبانی، جلوگیری از شمارش آراء قبل ازاتمام انتخابات و چند مورد دیگر اضافه شدهاست.

در این مقاله علاوه بر استفاده ازتکنولوژی جاوا کارت ۳ در قالب یک وب سرو امن مبتنی بر کارت هوشمند –که می‌تواند بعنوانجایگزینی برای بستر ناامن سمت رای‌دهنده در نظر گرفته شود– که تمامی نیازهای امنیتی بستر مورد استفاده رای‌دهنده را در بالاترین سطح ممکن تامین می‌نماید، با ذخیره سازی رای در جاواکارت ۳ و الگوبرداری از مفهوم زبان Java Information Flow (JIF)برای تضمین محرمانگی و یکپارچگی رای ذخیره شده،امکان پیگیری شکایت بعد از اتمام انتخابات نیز میسر می‌گردد.

کلمات کلیدی

انتخابات الکترونیکی، انتخابات اینترنتی، رمزنگاری ، تکنولوژی جاوا کارت ۳، JIF ، بی طرفی

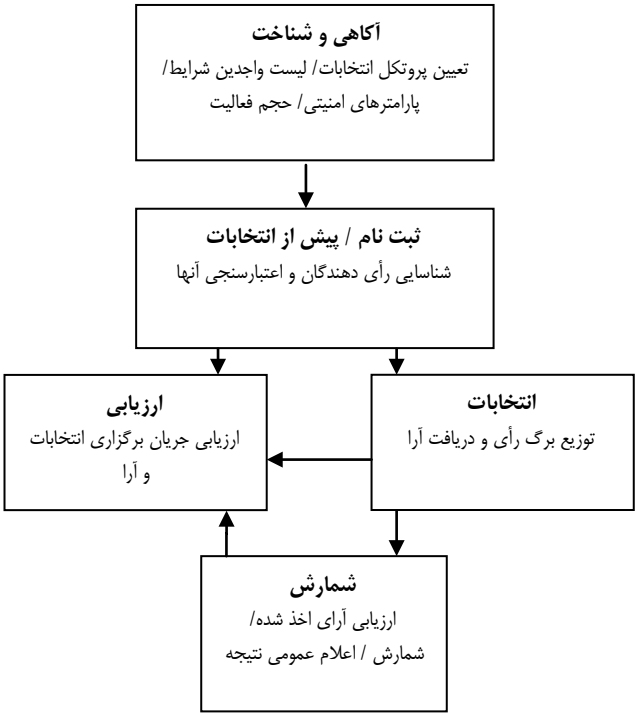
۱- مقدمه

در سال‌های اخیر، با توسعه زیرساخت‌های شبکه در سراسر دنیا سرویس‌های الکترونیکی، تعاملات شهروندان با نهادهای دولتی را آسانتر و در عین حال سرعت بخشیده است[19].رای‌گیری الکترونیکی یکی از جالب‌ترین سرویس ها در میان سرویس‌های الکترونیکی می‌باشد. رای‌گیری اینترنی که از رای‌گیری الکترونیکی مشتق شده است، شهروندان را قادر می‌سازد بدون نیاز به حضور فیزیکی در جایگاه‌های رای‌گیری درانتخابات شرکت کنند. پیاده‌سازی این موضوع مستلزم آماده‌سازی بسترهای لازم از جمله بکارگیری کارت هوشمند و نظایر آن است.

انتخابات به روش اینترنتی عموماً از مدل شکل(۱) تبعیت می‌کند و تنها با توجه به مسائل مختلف موجود در شرایط برگزاری و برگزار کننده، نحوه پیاده سازی آن متفاوت خواهد بود.

در مدل شکل(۱) پنج مرحله مجزا وجود دارد:

- آگاهی و شناخت: در این مرحله پروتکل‌ها تعریف شده، لیست واجدین شرایط شرکت در انتخابات استخراج گردیده و پارامترهای امنیتی و حجم فعالیت توسط مراجع قانونی مشخص می‌شود.
- ثبت نام: در این مرحله رأی‌دهندگان شناسایی و بوسیله مراجع قانونی اعتبار سنجی می‌شوند.
- برگزاری انتخابات: در این مرحله برگ رأی توزیع و واجدین شرایط رأی خود را ارائه می‌نمایند.
- ارزیابی: این مرحله همراه با مرحله قبل آغاز می‌شود و تا پایان انتخاب ادامه دارد در این مرحله سلامت برگزاری انتخابات کنترل می‌شود.
- شمارش: در این مرحله آرا صحت سنجی، شمارش و نتیجه اعلام می‌شود.



شکل (۱) : مدل کلی انتخابات الکترونیکی[11]

۱-۱- نیازمندی‌های امنیتی پروتکل‌های رای‌گیری الکترونیکی

اگرچه پروتکل های رای‌گیری الکترونیکی ویژگی‌های بسیار جالبی را ارائه می‌کند، اما ذات الکترونیکی بودن آنها، به هر حال نگرانی‌های امنیتی را مطرح می‌کند که باید مورد توجه قرار گرفته تا اعتبار انتخابات تضمین گردد. علیرغم این واقعیت که استاندارد مشخصی برای تعیین تمام پیش‌نیازهای امنیتی وجود ندارد،اکثر طرح‌های پیشنهادی در این زمینه بر نیازهای زیر تاکید دارند[5,12,18]:

یکپارچگی و صحت[1]: فقط آرای معتبر شمرده شوند. هم‌چنین تغییر، حذف و اضافه کردن رای ممکن نباشد.

دموکراسی: فقط رای‌دهندگان واجد شرایط می‌توانند رای بدهند (یعنی رای‌دهندگان ثبت‌نام‌شده) واین رای‌دهندگان فقط یک بار می‌توانند رای بدهند.

رای دادن و رفتن: نیازی به مداخله رای‌دهنده در مرحله شمارش نباشد.

اثبات پذیری[2]: اثبات‌پذیری در دو قالب تعریف می شود: اثبات‌پذیری فردی و عمومی. در اثبات‌پذیری فردی، هر رای‌دهنده باید قادر باشد صحت و یکپارچگی فرآیند شمارش آرا را تصدیق کند. در حالت عمومی، همه شهروندان می‌توانند صحت کل انتخابات را بازبینی کنند.

گمنامی[3]: در کل فرآیند انتخابات لینکی میان رای و رای‌دهنده قابل ردیابی نباشد.

مقاوم در برابر تبانی: در صورتیکه بی‌طرفی در پروتکل تضمین نشده باشد، مراجع انتخاباتی با تبانی با یکدیگر می‌توانند نتایج انتخابات را دستکاری نمایند.

قابلیت نقل مکان: رای‌دهندگان می‌توانند از هر مکانی رای دهند.

۱-۲- فناوری جاوا کارت ۳

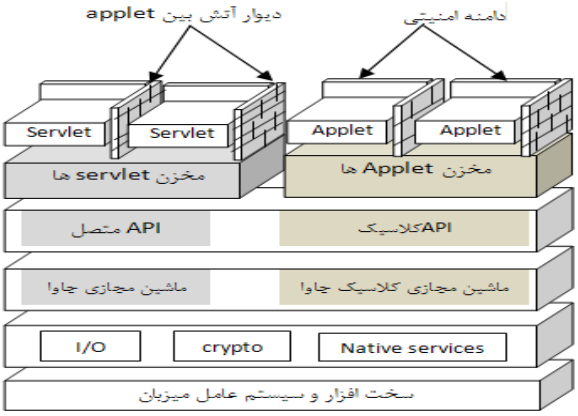
از کارت هوشمند در حوزه رای‌گیری الکترونیکی عموما در سه حوزه ذخیره امن داده، احراز هویت و امضای دیجیتال استفاده می‌شود[4]؛ حال آنکه کارت هوشمند دارای قابلیتهای بسیار بیشتری می‌باشد. یک کارت هوشمند جاوا کارت ۳ می‌تواند در قالب یک وب سرور امن عمل نماید.

فناوری جاوا کارت۳ جدیدترین نسخه فناوری می‌باشد که از پیشرفت‌های موجود در سخت‌افزار حافظه، واحدهای پردازشگر و قابلیتهای ارتباطاتی پیشرفته‌تری برای کار با کارت‌ها استفاده می‌نماید. این نسخه محدودیت نسخه‌های قبلی روی ماشین مجازی و محیط اجرایی را ندارد و مجموعه بیشتری از ویژگی‌های زبان جاوا را پشتیبانی می‌کند (مبتنی بر جاوا ۶ است). فناوری جاوا کارت۳ در قالب دو ویرایش کلاسیک و متصل ارائه شده‌است؛ ویرایش کلاسیک تکامل یافته جاوا کارت نسخه ۲.۲.۲می‌باشد که هدفش برنامه‌های کاربردی مبتنی بر APDU است و تنها یکسری الگوریتم‌های امنیتی جدیدی در آن افزوده شده است[16].

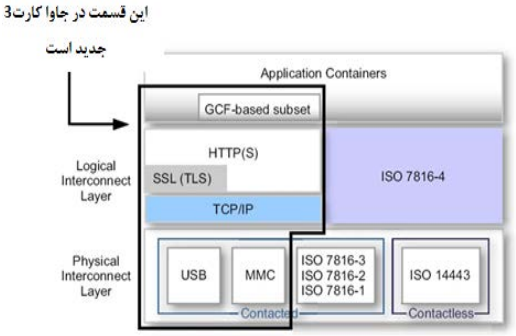
اما در ویرایش متصل یک ویژگی بسیار جدید و کاربردی افزوده شده است. در این ویرایش، یک کارت هوشمند مدرن جاوا کارت۳ می‌تواند بعنوان یک وب سرور، سرویس های امنیتی را برای شبکه فراهم و در خواست دسترسی به منابع شبکه را در بالاترین سطح امنیت تامین کند (شبکه گرا[4]). نوآوری این ویرایش servletهای جاوا هستند. اما در عین حال اجازه توسعه همزمان برنامه‌های کاربردی وب و برنامه‌های کاربردی قبلی کارت هوشمند را می‌دهد. برنامه های کاربردی وب- موجود در کانتینر وب-که روی کارت هستند، سرویس‌هایی را برای اعضای روی شبکه IP فراهم می‌کنند .آنها از طریق پروتکل‌های اینترنتی استاندارد مانندHTTP قابل دسترسی هستند؛ بنابراین براحتی می‌توانند با زیرساخت‌های سرویس‌های اینترنتی موجود مجتمع و یکپارچه شوند. با توجه به این بستر می‌توان داده‌ی بین سرویس گیرنده (مرورگر) و سرویس دهنده (کارت هوشمند) را با استفاده از استاندارد SSL امن کرد[16, 10].

معماری سطح بالای فناوری ویرایش متصل در شکل (۱) مشخص شده است. فناوری جاوا کارت ۳ درسمت کلاینت قادر است که در نقش یک کامپیوتر شخصی یا وب سرور عمل کند - که هم با پروتکل APDU کارمی‌کند و هم برای تعاملات پر سرعت از HTTP(s) استفاده می‌نماید و ویژگی‌های امنیتی کارت همچون مقاوم بودن در برابر مداخله[5] و نگهداری امن داده‌ها و کلیدها را به ارث ببرد[6]. ساختار پشته TCP/IP

پیاده‌سازی شده در جاوا کارت۳ در شکل (۲) آمده است. فناوری جاوا کارت ۳ در ویرایش متصل همچنین یکسری مکانیزم امنیتی برای امنیت ارتباطات در سطح برنامه کاربردی ارائه می‌دهد از جمله ایزوله کردن کد برنامه‌ها، کنترل دسترسی، تصدیق و اعطای مجوز روی کارت برای برنامه کلاینت، امنیت ارتباطات شبکه، مدیریت کلید، میزبانی امن برای برنامه‌های وب [6,16,17].



شکل (۱):معماری فناوری ویرایش متصل جاواکارت۳[16]



شکل (۲):پشتهTCP/IPویرایشمتصلجاواکارت۳[10]

۳-۱ مفهوم JIF[۶]

در این مقاله به بهبود پروتکل FOO باتاکید بر استفاده از کارت هوشمند جاوا کارت ۳ و مفهموم JIF در آن، به عنوان بستری امن برای ارتباطاتا و امکان پیگیری شکایت پس از اتمام انتخابات پرداخته شده است.

JIFیک زبان برنامه نویسی امنیتی است که در آن زبان جاوا، برای کنترل جریان اطلاعات و کنترل دستیابی توسعه داده شده است. هدف اصلی جلوگیری از استفاده شدن نامناسب از اطلاعات محرمانه و/یا نامطمئن می باشد. JIF به دو موجودیت بی‌اعتماد به یکدیگر (بی‌اعتمادی دوطرفه) اجازه می‌دهدکه اطلاعات طبقه بندی شده را به اشتراک بگذارند [2,9].

JIFزبان جاوا را با اضافه کردن برچسب،که بیانگر محدویت روی اینکه چگونه اطلاعات ممکن است استفاده شود، توسعه می‌دهد. برای مثال اعلان متغیر زیر نه تنها اعلان می‌کند x ،از نوع داده Int است، بلکه نشان می‌دهد اطلاعات موجود در x توسط یک سیاست[۷] امنیتی کنترل می‌شود:

```
Int {Alice→Bob} x;
```

در این مورد،سیاست امنیتی که برای تامین محرمانگی می‌باشد به این موضوع اشاره می‌کند که اطلاعات موجود در x توسط شخص Alice کنترل می شود و Alice اجازه می‌دهد این اطلاعات توسط شخص Bob دیده شود.

سیاست محرمانگی[۸] سیاستی است که در آن خواننده[۹] به فرد مالک[۱۰] سیاست امنیتی اجازه می‌دهد تا تعیین کند کدام اشخاص اجازه خواندن یک قطعه اطلاعات مشخص را دارند که اصطلاحا خواننده نامیده می‌شوند و هم چنین افرادی که اجازه نوشتن دارند به‌عنوان نویسنده شناخته می‌شوند. یک سیاست خواننده به شکل نوشتاری $o \rightarrow r$ است،که در آن شخص o مالک سیاست امنیتی و شخص r خواننده تعیین شده است و o به r اجازه مشاهده اطلاعات خود را داده است.

سیاست یکپارچگی[۱۱] نیز سیاستی است که در آن نویسنده[۱۲] به مالک سیاست اجازه می‌دهد که تعیین کند کدام اشخاص اجازه نوشتن یک قطعه اطلاعات معلوم را دارند. یک سیاست نویسنده به شکل $o \leftarrow w$ است که در آن شخص o مالک سیاست و شخص w نویسنده تعیین شده است و o به w اجازه نوشتن اطلاعات خود را می دهد[2,9].

۲-پروتکل FOO

پروتکل‌های مختلفی به منظور تحقق انتخابات الکترونیکی طراحی و پیاده سازی شده است. از آن جمله می‌توان به پروتکل-های FOO[1]،EVOX[15]، EVOX-MA، REVS[19]، Helios[3]اشاره نمود. هر یک از این پروتکل‌ها از عناصر و اجزا مختلف با روابطی مشخص تشکیل شده‌اند. اما همگی سعی دارند تا یک انتخابات الکترونیکی را با حفظ تمام اصول انتخابات و در محیط امن پیاده سازی نمایند.

پروتکل FOO سه عامل اصلی دارد:

- رای‌دهنده(Voter)
- ارزیاب (Validator)
- برگزار کننده(Tallier)

برای درک هر چه بهتر این پروتکل علائم بکار رفته را به ترتیب زیر تعریف می نماییم:

- V (Validator): ارزیاب
- T (Tallier):برگزار کننده
- P (Pollster): رای‌دهنده
- Id: شناسه رای‌دهنده
- b (Ballot): برگ رای
- (e,d): کلید عمومی و خصوصی رای‌دهنده
- (ev, dv): کلید عمومی و خصوصی ارزیاب
- R: فاکتور کورکنندگی
- BB (Bulletin Board): تابلو اعلانات عمومی

فازهای پروتکل FOO[1] به شرح زیر خلاصه می‌شوند. لازم به ذکر است که در پروتکل FOOراجع به نحوه پیاده سازی و ثبت نام رای‌دهندگان مجاز در فاز ثبت‌نام توضیحی داده نشده است و تنها فرض شده است که رای‌دهندگان پیش از انتخابات ثبت‌نام می‌شوند. بدین ترتیب تنها سه فاز رای‌گیری، جمع‌آوری و شمارش آرا در ذیل بیان می‌گردد.

فاز پیش از انتخابات: همچون اکثر پروتکل‌ها در این پروتکل نیز، رأی‌دهندگان در یک مرحله قبل از برگزاری انتخابات، در انتخابات ثبت‌نام کرده و زوج کلید مخصوص انتخابات دریافت می‌نمایند. کلید خصوصی رای‌دهنده تا زمان اتمام انتخابات محرمانه نزد وی می‌ماند. در این پروتکل محدودیتی و یا توضیحی راجع به محل ذخیره کلیدهای رمزنگاری و هم چونین ماژولی که می‌خواهد از این کلیدها استفاده نماید، وجود ندارد.

فاز رای‌گیری: در زمان برگزاری انتخابات رأی‌دهنده، رأیِ خود را با کلید عمومیِ خود، رمز(b^e=B) و کور کرده ($B*R^{ev}$) و پس از امضا با کلید خصوصی ویژه‌ی انتخابات خود، آن را برای سنجش اعتبار به ارزیاب تحویل می‌دهد.

$P \rightarrow V:$ $((B*R^{ev})+ Id)^d$

ارزیاب علاوه بر کنترل امضا، بررسی می‌کند آیا رای‌دهنده در لیست رأی‌دهندگان مجاز وجود دارد یا خیر، در صورت تایید رأی را امضا کرده و به رای‌دهنده عودت می دهد (ارزیاب فقط کلید عمومی رای‌دهنده را می داند).

$V \rightarrow P:$ $(B*R^{ev})^{dv}$

سپس رای‌دهنده رای را از حالت کور خارج نموده و بدین ترتیب به امضای رای خود توسط ارزیاب دست می یابد.

$(B*R^{ev})^{dv}/R=B^{dv}$

فاز جمع آوری آرا: در این فاز، رای‌دهندگان آرا رمز شده و امضا شده‌ی خود توسط ارزیاب را از طریق یک کانال گمنام‌گر به برگزار کننده تحویل می‌دهند.

$P \rightarrow T:$ B^{dv}

برگزارکننده پس از بررسی صحت امضا ارزیاب، آرای رمز شده و امضا شده را در لیستی قرار می‌دهد. این لیست پس از اتمام رای‌گیری در معرض دید همگان قرار می‌گیرد. پس از انتشار این لیست، هر رای‌دهنده، صحت رای منتشر شد ه(بعد از اتمام انتخابات) در لیست را ارزیابی نموده و در صورت تایید، کلید رمزگشایی ویژه انتخابات خود را از طریق یک کانال گمنام‌گر به برگزار کننده تحویل می‌دهد.

وقتی انتخابات به پایان رسید برگزارکننده آرای رمز شده، کلید رمزگشایی و نتیجه را منتشر می نماید. لازم به ذکر است که برگزارکننده برای انتشار آرا از یک تابلو اعلانات عمومی استفاده می‌نماید.

با توجه به ساختار پروتکل FOO، مزایا و معایب این پروتکل به شرح ذیل بیان می‌گردد:

پروتکل FOO دارای مزایای زیر می‌باشد:

- سادگی پیاده‌سازی
- تعداد کم اعضای درگیر در پروتکل
- عدم نیاز به پروتکل‌ها و امکانات رمزنگاری پیچیده و دانش تخصصی
- امکان بازرسی فردی و اجتماعی به دلیل استفاده از تابلو اعلانات عمومی
- امکان بررسی صحت انتخابات از طریق تابلو اعلانات عمومی
- تضمین گمنامی در فاز جمع‌آوری و شمارش به دلیل بهره‌گیری از کانال‌های گمنام‌گر
- امکان تبانی ارزیاب و برگزارکننده برای نقض گمنامی رای‌دهنده وجود ندارد. ارزیاب کلید عمومی ویژه انتخابات رای‌دهنده و رای کور شده را دارد، حال آنکه برگزارکننده کلید خصوصی و رای را دارد. لینک بین این دو تنها در اختیار رای‌دهنده می‌باشد.

پروتکل FOO دارای نقاط ضعف اساسی زیر است:

- از آنجاییکه در این پروتکل راجع به نحوه ثبت‌نام رای‌دهندگان مجاز حرفی به میان نیامده است، راجع به تضمین یا عدم تضمین امکان تبانی ثبت‌نام‌گر و ارزیاب برای نقض گمنامی رای‌دهنده نمی‌توان اظهارنظر قطعی کرد. در فاز رای‌گیری بیان شده است که هر رای‌دهنده با استفاده از Id، خود را به ارزیاب معرفی می‌نماید و ارزیاب هم لیستی از Id هایی که هنوز رای نداده‌اند را در اختیار دارد. اما آیا ارزیاب با تبانی با واحد ثبت‌نام‌گر نمی‌تواند به هویت واقعی رای‌هنده دست یابد.
- امکان خرید و فروش رای به دلیل نشان دادن سه مولفه b,B,d در تابلو اعلانات عمومی[1].
- امکان آگاهی از نتیجه انتخابات (به طور نسبی) قبل از اتمام زمان مجاز انتخابات توسط برگزار کننده، وجود دارد.
- امکان پیگیری شکایت پس از انتخابات وجود ندارد. چرا که محتوای واقعی رای در دست رای‌دهنده نبوده و تنها یک رسید در اختیار وی می‌باشد.
- ارزیاب یا مرجع شناسایی آرا به دلیل در دست داشتن لیست رای‌دهندگان مجاز قادر است که به جای رای دهندگان واجد شرایط اما غایب، آرایی (با تولید یک جفت کلید) را معرفی نماید(نقض دموکراسی).
- نقض ویژگی رای دادن و رفتن (رای‌دهنده در مرحله شمارش آرا به خاطر ارائه کلید خصوصی خود دخالت دارد)

این نقاط ضعف باعث شده علی‌رغم نقاط قوت زیاد این پروتکل در مقابل سایر پروتکل‌ها، تمایلی به استفاده از آن در انتخابات اینترنتی وجود نداشته باشد.

در این مقاله با اعمال تغییراتی در اطلاعات تبادل شده، نحوه رمزنگاری پروتکل FOO و استفاده از تکنولوژی جدید و کار آمد جاوا کارت ۳ و هم چنین مفهوم JIF، این پروتکل به گونه‌ای بهبود می‌یابد که با حفظ تمام اصول انتخابات و امنیت پیشین پروتکل FOO برای هریک از معیاب بیان شده، راه حلی ارائه می‌شود.

۳-پروتکل بهبود یافته FOO

دراین پروتکل بااستفاده از تسهیم راز و استفاده از مفاهیم زیر ساخت کلید عمومی (PKI) از دستکاری نتایج انتخابات، خرید و فروش رای و شمارش آرای زودتر از اتمام انتخابات جلوگیری می شود.

همانطور که اشاره شده در پروتکل FOO هیچ اشاره ای به محل ذخیره سازی کلید خصوصی و عمومی نشده است (در فاز پیش از انتخابات). واضح است که امنیت سیستم کلید عمومی/کلید خصوصی کاملا به مخفی نگه داشتن کلید خصوصی وابسته است. یک کلید خصوصی می‌تواند در کامپیوتر کاربران ذخیره شود و با اسم عبور حفاظت شود، که اشکال اساسی این مورد آن است که امنیت کلید خصوصی کاملا به امنیت کامپیوتر بستگی دارد. امن نبودن وآلوده بودن رایانه‌های سمت کلاینت به انواع برنامه ها و کدهای مخرب (یا شبکه Botnetو...) بزرگترین سد تامین امنیت کل پروتکل(فرآیند) رای‌گیری می‌باشد[8,13,14](در اکثر پروتکل‌های ارائه شده، یک فرض کاملا نادرست مبتنی بر امن بودن سیستم کلاینت در نظر گرفته شده است[12,19]).

یک جایگزین امن تر برای ذخیره سازی کلید خصوصی وعمومی و هم چنین جایگزینی به عنوان بستر ناامن (رایانه) رای‌دهنده، جاوا کارت ۳ (که در فاز پیش از انتخابات صادر شده) می باشد. در پروتکل بهبودیافته FOO هر شهروند با در دست داشتن یک کارت هوشمند مجهز به جاوا کارت ۳ در رای‌گیری شرکت می‌نماید. در این پروتکل فرض بر آن است که هر شهروند یک کارت هوشمند ملی از نوع جاواکارت ۳ دارد که با استفاده از این کارت می‌تواند به‌سادگی در انتخابات الکترونیکی و اینترنتی مشارکت نماید. درون کارت هر شهروند، یک سرولت رای‌گیری بارگذاری شده است که علاوه بر افزودن امکان رسیدگی به شکایات هر رای‌دهنده، می‌تواند در قالب تعاملات وب سرویسی با واحدهای درگیر در انتخابات تعامل و پیام‌هایی را مبتنی بر پروتکل HTTPS ردوبدل نماید. لازم به ذکر است که در این پروتکل تمامی ارتباطات انجام شده بین عوامل درگیر در پروتکل بااستفاده از پروتکل SSL انجام می گیرد.

تغییر دیگری که در پروتکل بهبودیافته FOO انجام گرفته است، طراحی و افزودن فاز ثبت‌نام به مراحل پروتکل FOO است به گونه‌ای که امکان معرفی آرا و نقض گمنامی رای‌دهنده در اثر تبانی واحدهای انتخاباتی میسر نباشد.

هم چنین از آنجاییکه تامین محرمانگی و یکپارچگی رای ذخیره شده در کارت از موارد چالش برانگیز و مهم در تامین امنیت پروتکل ارائه شده است، در این پروتکل برای رسیدن به این هدف از مفهوم JIF و تابع "خوانندگان" و "نویسندگان" آن استفاده شده است.

برای درک هر چه بهتر این پروتکل علائم وعوامل جدید بکار رفته را به ترتیب زیر تعریف می نماییم:

- R(Registrant):واحدثبت‌نام‌کننده
- V(Validator):ارزیاب
- T(Tallier): برگزار کننده
- P(Pollster): رای‌دهنده
- Id:شناسه رای‌دهنده
- b(Ballot): برگه رای
- (e,d): کلید عمومی و خصوصی رای‌دهنده
- (er,dr): کلید عمومی و خصوصی ثبت‌نام‌کننده
- (ev, dv): کلید عمومی و خصوصی ارزیاب
- (et, dt):کلید عمومی و خصوصی برگزارکننده
- (ee,de): کلید عمومی و خصوصی انتخابات
- R:فاکتور کورکنندگی
- BB(Bulletin Board): تابلو اعلانات عمومی

کلید خصوصی انتخابات بین مراجع انتخابات و کاندیدها تسهیم راز شده است و بگونهای در یک HSMو در محلی امن نگهداری می‌شود که پیش از اتمام زمان انتخابات امکان افشای آن وجود ندارد.

ارتباطات انجام شده در این پروتکل به شکل زیر می‌باشد :

فاز ثبت‌نام: فاز شناسایی چند روز پیش از شروع انتخابات انجام می‌شود. در این فاز رای‌دهندگان به وب سایت ثبت‌نام‌کننده مراجعه می‌کنند تا بعنوان یک رادهنده مجاز شناسایی شوند. ثبت‌نام‌کننده درخواست خواندن اطلاعات هویتی شامل (نام، نام خانوادگی، سن و تابعیت) شهروندان را برای سرولت رای‌گیری کارت در قالب یک پیام HTTPS GET ارسال می‌نماید. این سرولت که در قالب یک وبسرور امن عمل‌می‌کند، داده های مذکور را آماده ساخته و در قالب یک پیام HTTPS POST برای ثبت‌نام‌کننده ارسال می‌نماید. بمنظور حفظ محرمانگی پیش از هر تعاملی میان وبسایت و کارت یک کانال SSL تشکیل شده و تمامی تعاملات در این کانال امن مبادله می‌گردند.

هم‌چنین برای جلوگیری از امکان تبانی واحد ثبت‌نام‌کننده با واحدهای دیگر انتخاباتی برای نقض گمنامی رادهنده، لازم است که در این مرحله شهروند، شناسه id که می‌تواند در قالب یک نام مستعار نیز در نظرگرفته شود را برای خویش انتخاب و پس از کورشدن این شناسه توسط سرولت رای‌گیری $Id*R^{er}$، این شناسه را برای امضا نزد ثبت‌نام‌کننده ارسال نماید. در صورت تایید اطلاعات هویتی رای‌دهنده و مجاز بودن وی به شرکت در انتخابات، ثبت‌نام‌کننده شناسه رای‌دهنده را امضا و برای وی ارسال می‌نماید.

$P \rightarrow R$: Identity Information + $Id*R^{er}$

$R \rightarrow P$: $(Id*R^{er})^{dr}$

رای‌دهنده با اعمال تابع عکس کورکنندگی به امضای شناسه خود توسط واحد ثبت‌نام گر دست می‌یابد. بدین ترتیب وی می‌تواند از این پس با استفاده از این شناسه، خود را به مراجع دیگر انتخاباتی معرفی نماید. بی‌آنکه هویت واقعی وی فاش شود.

فاز رای‌گیری: در این فاز، سرولت رای‌گیری، برگه رای را کور کرده $b*R^{ev}$ و به همراه شناسه و امضای شناسه خود توسط ثبت‌نام‌کننده و کلید خصوصی ویژه انتخابات خود، برای ارزیاب ارسال می‌نماید.

$P \rightarrow V$: $(Id^{dr})^{d}$, $(b*R^{ev})^{d}$

ارزیاب با بررسی امضاهای شناسه و تطبیق آن با محتوای شناسه، و با بررسی یکسان بودن امضای روی شناسه و امضای روی رای کور شده، مجاز بودن رای‌دهنده را تایید و رای کورشده را امضا می‌نماید.

شهروند با دریافت رای کور شده و امضا شده و اعمال تابع عکس کورکنندگی به امضای رای خود توسط ارزیاب می‌رسد.

$V \rightarrow P$: $(b*R^{ev})^{dv}$

فاز جمع آوری آرا: در این فاز، سرولت رای‌گیری محتوای امضا شده و رمز شده رای را با کلید عمومی انتخابات رمز کرده و بهمراه شناسه امضا شده و رمز شده را برای برگزارکننده ارسال می‌نماید.

$P \rightarrow T$: Id, $(Id^{dr})^{d}$, $(b^{dv})^{ee}$

برگزارکننده، با دریافت هر رای، محتوای دوبار امضا شده(امضای خود برگزار کننده و ارزیاب) و رمز شده رای به همراه Id،درون تابلو اعلانات عمومی نمایش می‌دهد. هم چنین بمنظور تایید دریافت رای، پیام دریافتی را امضا و بعنوان یک رسید درون کارت شهروند ذخیره (ذخیره سازی رای با استفاده از قابلیت های تکنولوژی جاوا کارت۳و قابلیت سرولت هامی باشد)مینماید.

$T \rightarrow P$: $((b^{dv})^{ee})^{dt}$

فاز شمارش: پس از اتمام فاز رای‌گیری، کلید خصوصی انتخابات با حضور کاندیدها و مراجع انتخاباتی افشا شده و آرا شمارش می‌شوند. پس از شمارش آرا، محتوای رمزگشایی شده هر رای، بعنوان یک ستون جدید به این تابلو(تابلو اعلانات) اضافه می‌گردد. بدین ترتیب هر شهروندی با تطابق تابلو اعلانات عمومی پیش از شمارش آرا و پس از شمارش آرا می‌تواند صحت

انتخابات را بررسی کند. تابلو اعلانات عمومی در فاز شمارش به دو صورت قابل پیاده‌سازی می‌باشد. در ادامه هریک از دو روش و مزایای هریک بیان می‌گردد:

۱. در روش اول، محتوای رمز شده و دوبار امضا شده رای به همراه محتوای رمزگشایی شده برای همگان قابل نمایش است و برای هر شهروند علاوه بر این اطلاعات، Id متناظر با رایش هم قابل مشاهده است. در این روش بدلیل نمایشId تنها به ازای هر شهروند، امکان ردیابی رای و مشاهده Id برای رشوه‌گر وجود ندارد و بدین ترتیب امکان خرید و فروش رای میسر نمی‌باشد. در واقع در این روش، به هر رای‌دهنده به اندازه‌ای اطلاعات داده می‌شود که بتوان تنها رای خود را ردیابی کند و امکان ردیابی رای وی توسط دیگران وجود نداشته باشد.

۲. در روش دوم، محتوای رمز شده و دوبار امضا شده رای بهمراه محتوای رمزگشایی شده و Idدرون تابلو نشان داده می شود. در اینصورت پس از انتخابات، هر کسی می‌تواند وضعیت رای خود و دیگران را (با در دست داشتن شناسه‌های آنها) پیش و پس از شمارش آرا بررسی نماید. بدین ترتیب امکان خرید و فروش رای پس از فاز مشارش میسر خواهد بود. اما ازآنجاییکه پس از شمارش آرا، اساسا انگیزه ای برای خرید و فروش رای توسط رشوه‌گر وجود نخواهد داشت، در این روش نیز، امکان خرید و فروش رای ناچیز می‌باشد.

نکته مهمی که راجع به هر دو این روش‌ها وجود دارد این است که امکان خرید و فروش رای بسیار ناچیز می‌باشد چرا که پیش از شمارش آرا، امکان بررسی محتوای رای توسط شخصی غیر از رای‌دهنده، چه یکی از مراجع انتخاباتی باشد و چه رشوه گر باشد، وجود نخواهد داشت و بدین ترتیب انگیزه خرید و فروش رای از بین خواهد رفت. زمانیکه انتخابات به پایان رسید ،کلید خصوصی انتخابات که تسهیم راز شده، منتشر می شود و آرای رمز شده در تابلو اعلانات رمز گشایی می‌گردند و هررای‌دهنده می تواند درستی رای خود و کل انتخابات رابا مقایسهتابلواعلانات عمومی پیش و بعد از انتخابات با نتایج انتخابات بررسی کند.

در این مقاله با استفاده از مفهوم JIF, محرمانگی(خواندن) ویکپارچگی (نوشتن) رای ذخیره شده در کارت تامین گردیده است.در JIF برای محرمانگی ویکپارچگی اطلاعات به ترتیب تابع خوانندگان (مجموعه اشخاصی که مالک معتقد است باید به آنها اجازه خواندن اطلاعات بر اساس سیاست c داده شود) و نویسندگان (مجموعه اشخاصی که مالک اطلاعات معتقد است می‌توانند اطلاعات را بر اساس سیاست نویسنده c تحت تاثیر قرار دهند) تعریف می شود.

در پروتکل ارائه شده حق نوشتن به برگزار کننده داده شده است یعنی با الگوبرداریازJIF تابع نویسندگان به صورت زیر تعریف می‌شود:

Writers= {T} + {IP, Mac address, Digital Certificate}

یعنی حق نوشتن رای به آدرس IP،آدرس سخت‌افزاری وگواهینامه دیجیتالی (گواهینامه دیجیتالی برگزار کننده درجاوا کارت ۳ بارگذاری شده است که معادل سیاست c در JIF است) برگزارکننده داده می‌شود. هنگام نوشتن رای، اپلت و سرولت مورد نظر جاوا کارت ۳ با توجه به سناریو اشاره شده در بالا به بررسی موارد بالا پرداخته ودر صورت هم‌خوانی موارد تعریف شده در تابع نویسندگان با موارد ارائه شده توسط برگزارکننده،رای در سرولت رای‌گیری نوشته می‌شود.

حق خواندن که رای هم با تعریف تابع خوانندگان فقط به سازمان رسیدگی به شکایت (سرور سازمان) داده می‌شود که در صورت شکایت شهروندی بتواند رای از داخل کارت خوانده و بر اساس ادعای او به شکایتش رسیدگی کند:

Readers= {PR} + {IP, Mac address, Digital Certificate}

یعنی سازمانی(سرور سازمانی) حق خواندن رای را دارد که اطلاعات آن (IP, Mac address, Digital Certificate) با اطلاعات موجود در تابع خوانندگان مطابقت داشته باشد.

۴-تحلیل امنیتی پروتکل بهبود یافته FOO

گم نامی: در پروتکل بهبودیافتهFOO به دلیل استفاده از شناسه امضا شده توسط ثبت‌نام‌کننده در فاز رای‌گیری و جمع‌وآوری، امکان شناسایی رای‌دهنده حتی در صورت تبانی تمامی واحدهای درگیر در انتخابات اعم از ثبت‌نام‌کننده هم وجود نخواهد داشت، چرا که ثبت‌نام‌کننده تنها کورشده شناسه رای‌دهنده را داردو واحدهای دیگر امضا شده این شناسه لینک میان این دو اطلاعات، فاکتور کنندگی شناسه است که تنها در اختیار خود رای‌دهنده می‌باشد.تنها روش نقض گمنامی رای‌دهنده، ردیابی IP می‌باشد. در پروتکل بهبودیافته FOO برای جلوگیری امکان ردیابی IP به رای دهندگان پیشنهاد می‌شود که برای ارسال آرای خود به واحدهای انتخاباتی از شبکه های گمنام و یا پروکسی سرورهای عمومی استفاده نمایند.

دقت:در این پروتکل امکان تغییر رای وجود ندارد چراکه رای در تابلو اعلانات منتشر می شود.در صورت تغییر رای با توجه به ویژگیامکان پیگیری شکایت این پروتکل، فرد می‌تواند ادعا کند که رای رمز گشایی شده با رای داده شده یکسان نیست.

تبانی:همانگونه که در بحث گمنامی بیان شد تبانی عناصر دخیل در انتخابات نمی‌تواند مشخص کند چه کسی چه رایی داده است. در این پروتکل تنها رای‌دهنده است که رابطه بین اطلاعاتی که ثبت‌نام‌کننده دریافت کرده با اطلاعاتی که ارزیاب از رای‌دهنده دریافت می‌کند و اطلاعاتی که برگزار کننده از رای‌دهنده دریافت می‌کند را می‌داند.

از آنجاییکه در این پروتکل برخلاف پروتکل FOO، لیست اطلاعات تمامی شهروندان در دست ثبت‌نام‌کننده نبوده و این واحد با خواندن اطلاعات شهروندان از درون کارت آنها و بررسی امضای یک مرجع معتبر بر روی این اطلاعات ذخیره شده در کارت، به ازای هر شهروند، مجاز بودن وی را برای شرکت در انتخابات تشخیص می‌دهد و بدین ترتیب به دلیل عدم اطلاع از حضور یا عدم حضور شهروندان واجد شرایط، نمی تواند به جای آنها آرایی را معرفی نماید.

اثبات پذیری، پیگیری شکایت و دموکراسی: رای‌دهنده به راحتی به کمک اطلاعات مندرج در تابلو اعلانات می‌تواند از سلامت رای خود آگاهی یابد و یا اثبات کند چه رایی صادر کرده بوده است.

تابلو اعلانات در این پروتکل به‌گونه‌ای طراحی و پیاده‌سازی شده است که پیش از انتخابات تمامی آرای رمز شده به همراه شناسه متناظر با هر رای را به همگان نشان خواهد داد. بدین ترتیب به هر رای‌دهنده این امکان را می‌دهد که بتواند از سلامت انتخابات مطمئن باشد. رای‌دهندگان با مشاهده

آرای رمز شده خود در تابلو اعلانات عمومی مطمئن خواهند شد که آرای آنها به سلامت توسط شمارش گر جمع‌آوری شده است. وجود تابلو اعلانات عمومی، از مخدوش شدن، سوزانده شدن و جایگزین شدن آرا توسط برگزارکننده و یا هر حمله‌گر دیگری جلوگیری می‌نماید.

پس از شمارش آرا، تابلواعلانات عمومی پاک شده و آرای رمزشده به همراه مقادیر رمزگشایی شده را به همگان نشان می‌دهد. هم‌چنین هر شهروند قادر است که علاوه بر این اطلاعات، شناسه وزمان رای‌گیری خود را نیز مشاهده نماید. بدین ترتیب هر شهروند می‌تواند با در دست داشتن کلید خصوصی انتخابات، محتوای تابلو اعلانات عمومی را پیش و پس از شمارش با هم مقایسه و بدین ترتیب صحت انتخابات را برررسی نماید.

پس از شمارش آرا، ممکن است محتوای رمزگشایی شده برخی از آرا، غیر معتبر باشد. بنابراین درون تابلو اعلانات عمومی، به ازای این آرا، حالت غیر معتبر نمایش داده می‌شود. برگزارکننده، می‌تواند شناسه این افراد را درون تابلو اعلانات عمومی برای رسیدگی به دلیل عدم اعتبار آرای آنها منتشر نموده و از آنها درخواست مراجعه نماید. بدین ترتیب یکسری از شکایات بدین صورت و به سادگی قابل ردیابی خواهد بود. علاوه بر این هر شهروند پس از انتخابات می‌تواند با در دست داشتن کارت خود به مرجع رسیدگی به شکایت مراجعه نماید. در این صورت محتوای دوبار امضا شده و رمز شده رای وی که توسط برگزارکننده درون کارت او در فاز جمع‌آوری ذخیره شده بود، از کارت خوانده شده و محتوای مندرج درون تابلو اعلانات عمومی تطبیق داده می‌شود و بدین ترتیب به شکایت وی رسیدگی خواهد شد.

هم چنین لازم به ذکر است که هر چند تابلو اعلانات عمومی صرفا در قالب یک پرتال پیاده‌سازی می‌شود و پردازش خاصی انجام نمی‌دهد، اما اعتبار یک رای‌گیری از دید رای‌دهندگان به صحت و دقت این تابلو می باشد[7]. لذا حفظ محرمانگی (برای جلوگیری از خرید و فروش رای)، صحت (برای جلوگیری از دستکاری در آرا) و در دسترس بودن این در کسب اعتماد رای‌دهندگان بسیار تاثیرگذار بوده. بدین ترتیب همانطور که بیان شد، محرمانگی این تابلو از طریق محدود کردن حق خواندن هر رسید به هر رای‌دهنده تضمین می‌شود. هم چنین برای تضمین صحت، لازم به ذکر است که تنها برگزارکننده و آن هم پیش از انتخابات می‌تواند در این تابلو، آرا را اضافه نماید. دستکاری این تابلو توسط هیچ مرجع دیگری امکان‌پذیر نمی‌باشد.

جلوگیری از خریدوفروش: برای جلوگیری از امکان خرید و فروش رای، مکانیزمی باید مورد استفاده قرار گیرد که پس از شمارش آرا، میزان اطلاعاتی که به هر رای‌دهنده تحویل داده می‌شود تنها به اندازه‌ای باشد که وی را متقاعد نماید که رایش بدرستی شمارش شده است و نه به میزانی که برای متقاعد ساختن دیگران از جمله رشوه دهنده بتوان از آن استفاده نمود.

در پروتکل بهبودیافته FOO، تابلو اعلانات عمومی پس از شمارش آرا، شناسه رای را به همگان نشان نداده (روش اول نمایش تابلو اعانات) و تنها هر رای‌دهنده با در دست داشتن کارتی که شناسه و رای دوبار امضا شده و رمز شده داخل آن ذخیره شده، می‌تواند شناسه رای خود را مشاهده نماید. از آنجاییکه نوشتن شناسه و محتوای دوبار امضا شده و رمز شده رای داخل کارت هر شهروند تنها توسط برگزارکننده قابل انجام است (با استفاده از مفهوم JIF)، لذا رشوه‌دهنده یا حمله‌گر قادر به ذخیره رسیدهای رشوه‌گیرندگان داخل کارت خود نبوده و بدین ترتیب برای خرید هر رای، پس از شمارش آرا، رشوه‌دهنده باید کارت رای‌دهنده و پین آن را در اختیار داشته باشد که این با اصول حفظ محرمانگی کارت به نوعی در تناقض است.

هم چنین در این پروتکل پیش از شمارش آرا شناسه و رای دوبار امضا شده و رمز شده درون تابلو اعلانات عمومی نمایش داده می‌شود، رشوه دهنده حتی با در دست داشتن شناسه رای‌دهنده امکان بررسی محتوای رای را نخواهد داشت چرا که رای توسط کلید عمومی انتخابات رمز شده است و کلید خصوصی انتخابات نیز بین واحدهای انتخاباتی و کاندیداها به گونه‌ای تسهیم راز شده است که امکان بازیابی و افشای آن پیش از انتخابات وجود ندارد. بدین ترتیب امکان خریدو فروش رای پیش از شمارش آرا وجود ندارد، بنابراین خرید و فروش در حالت منطقی خودش که پیش از انتخابات است، قابل انجام نیست. در واقع این روش انگیزه خریدار و فروشنده را تحت الشعاع قرار می‌دهد.

بی طرفی[13]**:** در این پروتکل کلیه آرا توسط کلید عمومی انتخابات رمز شده است و کلید خصوصی به نوعی میان مراجع انتخاباتی و کاندیداها تسهیم راز می‌شوندکه امکان رمزگشایی و شمارش زود هنگام آرا پیش از پایان انتخابات وجود ندارد.

رای دادن و رفتن: در این پروتکل برخلاف پروتکل FOO نیازی به مشارکت شهروندان پس از پایان انتخابات وجود ندارد.

امنیت تبادل اطلاعات: در این پروتکل به دلیل بهره‌گیری از تکنولوژی جاوا کارت۳ وپروتکل SSL درون کارت، این اطمینان وجود دارد که بین کارت و تمامی واحدهای درگیر در هر فاز یک کانال SSL تاسیس می‌شود و بدین ترتیب امکان نقص محرمانگی و صحت در هیچ یک از مراحل انتخاباتی وجود نخواهد داشت چرا که امنیتی بصورت انتها به انتها تضمین شده است. هم چنین به خاطر استفاده از جاوا کارت برای ذخیره کلید خصوصی و عمومی رای‌دهنده، می‌توان از عدم افشا کلید خصوصی رای‌دهنده در حین تبادل اطلاعات مطمئن بود.

راحتی پیاده سازی: این پروتکل در اجرا به سادگی پروتکل FOO بوده و پیاده‌سازی آن بسیار ساده است. هم چنین به خاطر وجود جاوا کارت به عنوان بستر امن سمت رای‌دهنده، نگرانی‌های مربوط به ناامن بودن رایانه رای‌دهنده در آن وجود ندارد.

تهدیدواجبار[14]**:** در پروتکل‌های رای‌گیری اینترنتی با توجه به اینکه رای‌دهنده در هر مکانی می‌تواند رای دهد موضوع اجبار را نمی‌توان حذف کرد.

۵-نتیجه گیری

در این مقاله با بهره‌گیری از تکنولوژی جاوا کارت ۳ و مفهوم JIF، وتسهیم راز و مفاهیم PKI، ایرادات امنیتی پروتکل FOO برطرف شده و بدین ترتیب یک پروتکل بهبودیافته FOO معرفی گردیده است. در این پروتکل برای امن سازی بستر سمت رای‌دهنده از تکنولوژی جاواکارت ۳ استفاده می‌گردد. تکنولوژی جاوا کارت ۳ در ویرایش متصل قادر است که در نقش یک وب سرور امن عمل کرده و تمامی تعاملات شبکه ای با دیگر واحدهای انتخابات را از طریق فعالسازی پشته SSL درون کارت هوشند، بصورت انتها به انتها امن نماید. هم چنین با استفاده از مفهوم زبان JIF معایب امنیتی پروتکل FOO از جمله سادگی خرید و فروش آرا و معرفی آرا به جای رای‌دهندگان غایب در پروتکل بهبودیافته FOO حل شده و ویژگی‌های

جدیـدی از جملـه امکـان پیگیـری شـکایات رای‌دهنـدگان، امکـان تضـمین بی‌طرفی و دموگراسی با بهره‌گیـری از ایـن زبـان در ایـن پروتکـل تضـمین می‌شود.

با توجه به قابلیت های جاواکارت ۳انتظار می رود که ایـن کـارت جایگزین مناسبی برای رایانه های سمت کلاینت باشد. از این رو در نظر داریم با مطالعه و تحقیق بیشتر روی جاوا کارت ۳ شرایط را برای کـاربردی‌ترشـدن این کارت در رای‌گیری الکترونیکی را فراهم سازیم.

مراجع

[1] A. Fujioka, T. Okamoto and K. Ohta, *A practical secret voting scheme for large scale elections*, in: and e. J. Seberry and Y. Zheng, Advances in Cryptology – AUSCRYPT'92 (1992), pp. 244–251.

[2] A. C. Myers. JFlow: *Practical mostly-static information flow control*. In Proc. ACM Symp. on Principles of Programming Languages, pages 228–241, January 1999

[3] Ben Adida, *Helios: web-based open-audit voting*, Proceedings of the 17th conference on Security symposium, p.335-348, July 28-August 01, 2008, San Jose, CA

[4] C. H. Yang, Tu, S. Y., Yen , P. H., "*Implementation of an Electronic Voting System with Contactless IC Cards for Small-Scale Voting*," 2009, pp. 122-125.

[5] Fan, C.I. and W.Z. Sun, *An efficient multi-receipt mechanism for uncoercible anonymous electronic voting*. Mathematical and Computer Modelling, 2008. 48(9-10): p. 1611-1627.

[6] Guillaume Barbu, Humus Thiebeauld, and Vincent Guerin, *Attacks on Java Card 3.0 Combining Fault and Logical Attacks*, published in "Smart Card Research and Advanced Application. 9th IFIP WG 8.8/11.2 International Conference.CARDIS 2010, Passau : Germany (2010)"

[7] Hugo Jonker,Jun Pang, *Bulletin Boards in Voting Systems: Modeling and Measuring Privacy*,2011

SixthInternational Conference on Availability, Reliability and Security

[8] Heiberg, S., H. Lipmaa, and F. Van Laenen, *On e-vote integrity in the case of malicious voter computers*.Computer Security–ESORICS 2010, 2011: p. 373-388.

[9] http://www.cs.cornell.edu/jif/doc/jif-3.3.0/manual.html

[10] http://www.oracle.com/technetwork/articles/javase/javacard3-142122.html

[11] I. M. Rosner and G. Rosner, *"Electronic Voting Protocols and Schemes,"* The Hebrew University of Jerusalem, Israel, 2002.

[12] J. V. S. Mauw , E. P. de Vink, *Data Anonymity in the FOO Voting Scheme*, Electronic Notes in Theoretical Computer Science (ENTCS), 168, p.5-28, February, 2007 [doi>10.1016/j.entcs.2006.11.001]

[13] Joaquim, R., C. Ribeiro, and P. Ferreira, *Improving remote voting security with CodeVoting*.Towards Trustworthy Elections, 2010: p. 310-329.

[14] Lauer, T. W., *"The risk of e-voting,"* Electronic Journal of E-government, vol. 2, pp. 177-186, 2004.

[15] M. A. Herschberg, *Secure electronic voting over the world wide web,(1997)., et al*.

[16] SUN Microsystem IncTHE JAVA CARD™ 3 PLATFORM,White Paper,August 2008

[17] Sterckx, M., et al. *Efficient implementation of anonymous credentials on Java Card smart cards*. 2009: IEEE.

[18] Sodiya, A.S.,Adelani, D.I. ,*A Secure e-Voting Architecture ,Information Technology*: New Generations (ITNG), 2011 Eighth International Conference on

[19] Z. REVS—*A robust electronic voting system - Joaquim*, et al. - 2004

زیرنویس‌ها

[1]Accuracy
[2]Verifiability
[3]Anonymity
[4]Network-oriented
[5]Tamper -resistance
[6]Java Information Flow
[7]Policy
[8]Confidentiality
[9]Reader
[10]Owner
[11]Integrity
[12] Writers
[13]Fairness
[14]Coercion