

اللَّهُمَّ صَلِّ عَلَى مُحَمَّدٍ



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**

نویسنده: محمدی شکیبا

استاد راهنما:

جناب آقای دکتر دوستاری

دی ۱۳۹۰

مورد حمایت موسسه تحقیقات ارتباطات و فناوری اطلاعات



صورت جلسه هیئت داوران رساله کارشناسی ارشد

جلسه دفاعیه پروژه کارشناسی ارشد مربوط به آقای/خانم نفیسه محمدی شکبیا به شماره دانشجویی ۸۸۷۵۲۸۴۰۰ در 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 ۱۹۸۵ قابل قبول می باشد. *نمره دست دوم* *دکتر محمدحسین محمدزاده*

پروژه نامبرده مردود می باشد.

پروژه نامبرده به شرط انجام اصلاحات جزئی قابل قبول می باشد. نمره دانشجو متعاقباً اعلام می شود.

<i>۸۵۰</i>	امضاء	دانشگاه : شاه‌شاه	<input type="checkbox"/> نام استاد راهنمای اول <i>دکتر دوسان</i>
	امضاء	دانشگاه :	<input type="checkbox"/> نام استاد راهنمای دوم
<i>۸۵۰</i>	امضاء	دانشگاه :	<input type="checkbox"/> نام استاد مشاور اول <i>دکتر مردانی</i>
	امضاء	دانشگاه :	<input type="checkbox"/> نام استاد مشاور دوم
	امضاء	دانشگاه : شاه‌شاه	<input type="checkbox"/> نام داور اول <i>دکتر حاج سرجوادی</i>
	امضاء	دانشگاه : <i>پرسه مدرس</i>	<input type="checkbox"/> نام داور دوم <i>دکتر زینال رحمانی</i>
	امضاء	دانشگاه :	<input type="checkbox"/> نام داور سوم
	امضاء	دانشگاه :	<input type="checkbox"/> نام داور چهارم
	امضاء		<input type="checkbox"/> نام نماینده معاونت پژوهشی <i>دکتر محمدحسین محمدزاده</i>

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



اظهار نامه دانشجو

شماره:

تاریخ:

اینجانب نفیسه محمدی شکبیا دانشجوی کارشناسی ارشد رشته مهندسی فناوری اطلاعات گرایش فناوری اطلاعات دانشکده فنی-مهندسی دانشگاه شاهد، گواهی می‌دهم 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 چنانچه 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 می‌دارد در صورت بهره‌گیری از منابع مختلف شامل؛ گزارش‌های 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 هیچ‌کجا ارایه نشده است. در تدوین متن پایان نامه / رساله حاضر، چارچوب (فرمت) مصوب تدوین گزارش‌های 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 می‌باشد.

نام و نام خانوادگی دانشجو (دست نویس):

امضاء دانشجو:

تاریخ:

این پروژه طبق قرارداد شماره ۶۱۵۱/۵۰۰/ت مورخ ۹۰/۰۴/۱۸ تحت حمایت مادی و معنوی موسسه تحقیقات ارتباطات و فناوری اطلاعات صورت گرفته است.

تقدیم به

پدر و مادر عزیزم

و

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

موهایشان سپید شد تا ما روسفید 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 مورد بر محمد 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، اجل 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 الله عزّ و جلّ:** "

از پدر 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 یابوری 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 آقای 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 به سادگی 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 بدین ترتیب 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 مستقیماً 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 در شبکه 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 می‌شود که برای تضمین هر یک از این ویژگی‌ها راه‌کارهای امنیتی را پیشنهاد می‌دهد. این پروتکل هم‌چنین می‌تواند برای تضمین امنیت سمت رای‌دهنده از ایده جاوا کارت ۳ بعنوان جایگزینی امن برای ترمینال‌های رای‌گیری استفاده نماید.

کلید واژه:

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

د	فهرست اشکال
و	فهرست جداول
۱	فصل ۱- مقدمه
۱-۱	۱-۱- پیشگفتار
۲-۱	۲-۱- رلز مندی ها و ویژگیهای سیستمهای رای گوی الکترونیکی
۳-۱	۳-۱- مشکلات امریتی (چالش ها) سیستمهای رای گوی الکترونیکی و اینترنتی
۴-۱	۴-۱- هدف از طرح و الگوی ارائه شده در این پژوهش
۵-۱	۵-۱- نوآوری تحقیق
۶-۱	۶-۱- ساختار پژوهش
۷-۱	۷-۱- نتیجه ی نهایی
۱۱	فصل ۲- مروری بر مباحث امریتی و عملیاتی انواع پروتکل های رای گوی الکترونیکی
۱-۲	۱-۲- مقدمه
۲-۲	۲-۲- فازهای عملیاتی در رای گوی الکترونیکی
۳-۲	۳-۲- انواع اولیه سیستمهای رای گوی الکترونیکی
۴-۲	۴-۲- گردآوری از پروتکل های ارائه شده در حوزه رای گوی الکترونیکی
۱-۴-۲	۱-۴-۲- پروتکل های مبتنی بر امضای کور
۱-۱-۴-۲	۱-۱-۴-۲- ساختار امضای کور
۲-۱-۴-۲	۲-۱-۴-۲- پروتکل FOO - سال ۱۹۹۲
۳-۱-۴-۲	۳-۱-۴-۲- پروتکل پیشنهادی [۲] - سال ۲۰۰۱
۴-۱-۴-۲	۴-۱-۴-۲- پروتکل EVOx و EVOX-MA و REVS
۵-۱-۴-۲	۵-۱-۴-۲- سیستم رای گوی اینترنتی امن و گمنام [۳] - سال ۲۰۰۴
۶-۱-۴-۲	۶-۱-۴-۲- پروتکل رای گوی اینترنتی گمنام ضد اجبار با قابلیت توزیع رسد های چند گانه [۴] - سال ۲۰۰۸
۲-۴-۲	۲-۴-۲- پروتکل های مبتنی بر شبکه های مختلط
۱-۲-۴-۲	۱-۲-۴-۲- ساختار شبکه های مختلط
۲-۲-۴-۲	۲-۲-۴-۲- سیستم رای گوی اینترنتی SecVote
۳-۴-۲	۳-۴-۲- پروتکل های مبتنی بر رمزنگاری همومورفیک
۱-۳-۴-۲	۱-۳-۴-۲- ساختار رمزنگاری همومورفیک
۵-۲	۵-۲- مباحث امریتی حوزه رای گوی الکترونیکی
۱-۵-۲	۱-۵-۲- آسویبذی های سیستمهای رای گوی الکترونیکی
۲-۵-۲	۲-۵-۲- ریسک سیستمهای رای گوی الکترونیکی
۳-۵-۲	۳-۵-۲- آنالیز ریسک امریتی
۶-۲	۶-۲- مقایسه رای گوی اینترنتی با تجارت الکترونیکی
۱-۶-۲	۱-۶-۲- پروژه های رای گوی اینترنتی

۲۷ نتیجه‌گویی	۷-۲
۲۸ فصل ۳ - معرفی تکنولوژی جاواکارت ۳	۳
۲۸ ۱-۳- مقدمه	۱-۳-۱
۲۸ ۲-۳- سیستم‌عامل کارت هوشمند	۲-۳-۱
۲۸ ۱-۲-۳- سیستم‌عامل های مبتنی بر فایلی	۱-۲-۳-۱
۳۰ ۲-۲-۳- سیستم‌عامل های چندکاربردی	۲-۲-۳-۲
۳۲ ۳-۳- تکنولوژی و مباحث امریتی جاواکارت ها	۳-۳-۱
۳۳ ۱-۳-۳- معماری جاواکارت	۱-۳-۳-۱
۳۴ ۲-۳-۳- ویژگی‌های زبانی جاواکارت	۲-۳-۳-۱
۳۵ ۳-۳-۳- ماشین مجازی جاواکارت (JCVM)	۳-۳-۳-۱
۳۸ 3-3-4- محیط اجرایی جاواکارت (JCRE)	۳-۳-۳-۲
۴۰ ۵-۳-۳- API های جاواکارت	۵-۳-۳-۱
۴۱ ۶-۳-۳- مفاهیم و نوآوری جاواکارت	۶-۳-۳-۱
۴۳ ۷-۳-۳- نگرانی‌ها و آسیب‌پذیری‌های جاواکارت	۷-۳-۳-۱
۴۴ ۸-۳-۳- مزایای جاواکارت	۸-۳-۳-۱
۴۴ ۴-۳- تکنولوژی پلتفرم جاواکارت ۳	۴-۳-۱
۴۵ ۱-۴-۳- مقایسه جاواکارت ۲ و ۳	۱-۴-۳-۱
۴۸ ۲-۴-۳- ویژگی‌های تکنولوژی جاواکارت ۳	۲-۴-۳-۱
۴۹ ۱-۲-۴-۳- پلتفرم جاواکارت ۳، معماری و ویژگی کلاسریک	۱-۲-۴-۳-۱
۴۹ ۲-۲-۴-۳- پلتفرم جاواکارت ۳، معماری و ویژگی متصل	۲-۲-۴-۳-۱
۵۰ ۳-۲-۴-۳- برنامه کاربردی وب (Servlet) در جاواکارت ۳	۳-۲-۴-۳-۱
۵۲ ۳-۴-۳- مکانیزم های امریتی جاواکارت ۳	۳-۴-۳-۱
۵۲ ۴-۴-۳- نوآوری فناوری جاواکارت ۳	۴-۴-۳-۱
۵۴ ۵-۳- کاربردهای جاواکارت	۵-۳-۱
۵۹ ۶-۳- نتیجه‌گویی	۶-۳-۱
۶۰ فصل ۴ - راه‌کارهای تضمین امریت سیستم‌های کلانیت	۴
۶۰ ۱-۴- مقدمه	۱-۴-۱
۶۱ ۲-۴- مسئله ۱- تعامل امن کارت‌خوان با کلانیت (کارت)-معرفی چارچوب FINREAD	۲-۴-۱
۶۳ ۳-۴- مسئله ۳- روش پیشنهادی برای ایجاد پلتفرم امن	۳-۴-۱
۶۴ ۱-۳-۴- استفاده از TPM بعنوان پلتفرم رای‌گویی سمت رای‌دهنده	۱-۳-۴-۱
۶۶ ۲-۳-۴- استفاده از پلتفرم جاواکارت ۳ و ویژگی متصل بعنوان یک بستر رای‌گویی کامل	۲-۳-۴-۱
۶۶ ۱-۲-۳-۴- بررسی مدل‌های استفاده از جاواکارت ۳ برای تضمین امریت سمت کلانیت	۱-۲-۳-۴-۱
۶۹ ۴-۴- نتیجه‌گویی	۴-۴-۱
۷۰ فصل ۵ - معرفی یک پروتکل رای‌گویی اینترنتی جدید بر اساس زی‌ساخت جاواکارت ۳	۵
۷۰ ۱-۵- مقدمه	۱-۵-۱

5-2- بخش زمینه های عدم اجبار، بی طرفی و تباری در رای گوی اختزنتی	۷۱
۱-۲-۵ تضمین عدم اجبار در رای گوی اختزنتی	۷۱
۲-۲-۵ تضمین بی طرفی در رای گوی اختزنتی	۷۴
۳-۲-۵ تضمین عدم امکان تباری در رای گوی اختزنتی	۷۴
۳-۵- جاواکارت ۳ - جایگزینی امن برای رامنه ناامن سمت رای دهنده	۷۷
۴-۵- معرفی ساختار و مراحل J-FUCI	۷۹
۱-۴-۵ ترسرم نمودارهای J-FUCI بفرم نمودارهای UML در نرم افزار Visual Paradigm	۸۲
۲-۴-۵ ملاحظات امریت	۸۵
۱-۲-۴-۵ پروتکل امضای کور قابل لئیک	۸۵
۳-۴-۵ فاز شناسایی رای دهندگان	۸۶
۴-۴-۵ فاز ثبت نام	۸۷
۵-۴-۵ فاز رای گوی	۸۸
۶-۴-۵ فاز جمع آوری	۸۹
۷-۴-۵ فاز شمارش آرا	۹۱
۵-۵- پیشنهاد نحوه بچاده سازی شمارشگر	۹۱
۶-۵- تضمین بی طرفی در پروتکل پیشنهادی	۹۲
۷-۵- ارزیابی امریتی پروتکل پیشنهادی	۹۵
۸-۵- مقایسه پروتکل J-FUCI با دیگر پروتکل ها	۱۰۱
۹-۵- نتیجه گوی	۱۰۲
فصل ۶ - نتیجه گوی	۱۰۴
۱-۶- نتیجه ی پژوهش	۱۰۴
۲-۶- پیشنهادات	۱۰۶
ضمیمه أ - مقدمه ای مفاهیم کارت هوشمند	۱۰۸
ضمیمه ب - تکنولوژی جاواکارت	۱۱۴
ضمیمه ج - پروتکل J-FUCI و بچاده سازی آن	۱۲۱
فصل ۷ - مراجع	۱۲۶
۱-۷- مراجع فارسی	۱۲۶
۲-۷- مراجع انگلیسی	۱۲۶
واژه نامه فارسی به انگلیسی	۱۳۰
واژه نامه انگلیسی به فارسی	۱۳۴

فهرست اشکال

عنوان صفحه

- شکل ۱: مدل کلری انتخابات الکترونیکی ۱۲
- شکل ۲: ساختار شبکه مختلط رمزگشایی ۱۷
- شکل ۳: معماری و ارتباطات سیستم SecVote ۱۸
- شکل ۴: نگاه شمانتیکی به رای‌گیری آنلاین با استفاده از رمزنگاری همومورفیک ۲۰
- شکل ۵: روی رای‌گیری سننچی ۲۱
- شکل ۶: روی رای‌گیری الکترونیکی ۲۳
- شکل ۷: ابعاد امریتی سیستم‌های رای‌گیری ۲۶
- شکل ۸: ساختار سیستم فایلی ISO 7816-4 ۲۹
- شکل ۹: معماری نرم‌افزای جاواکارت ۳۱
- شکل ۱۰: ساختار سیستم عامل MULTOS ۳۲
- شکل ۱۱: ماشین مجازی جاواکارت ۳۵
- شکل ۱۲: روی کامل تبدیلی یک کد جاوا به یک Applet ۳۷
- شکل ۱۳: روی تبدیلی یک بسته شامل چندلی فایلی کلاس به یک فایلی cap ۳۷
- شکل ۱۴: نصاب جاواکارت و برنامه نصب خارج کارت ۳۸
- شکل ۱۵: معماری سیستم کارت در جاواکارت ۳۹
- شکل ۱۶: ارتباطات APDU I/O ۴۰
- شکل ۱۷: دی‌گرام توالی که تقابل مکن برنامه کاربردی desktop و برنامه کاربردی جاواکارت ۲ را نشان می‌دهد ۴۶
- شکل ۱۸: دی‌گرام توالی که تقابل مکن برنامه کاربردی از راه دور و برنامه کاربردی جاواکارت ۲ ۴۶
- شکل ۱۹: مقایسه سخت‌افزار هدف کارت هوشمند در ویاچس متصل، نسبت به ویاچس های قبلی ۴۷
- شکل ۲۰: دی‌گرام توالی تقابل مکن برنامه‌های کاربردی desktop/mobile و برنامه کاربردی جاواکارت ۳ ۴۸
- شکل ۲۰: معماری سطح بالا تکنولوژی ویاچس متصل ۵۰
- شکل ۲۱: مدل ارتباط کلانیتی سروری در جاواکارت ۵۱
- شکل ۲۲: متد Service در جاواکارت ۵۱
- شکل ۲۳: طول عمر یک برنامه servlet ۵۲
- شکل ۲۴: معماری فناوری ویاچس متصل جاواکارت ۳ ۵۳
- شکل ۲۵: پشته TCP/IP ویاچس متصل جاواکارت ۳ ۵۳
- شکل ۲۶: مرور کلری سیستم رای‌گیری ۵۵
- شکل ۲۸: مراحل پروتکل امن رای‌گیری ۵۵
- شکل ۲۹: معماری چارچوب تصدیق ۵۶
- شکل ۳۰: بلوک دی‌گرام ساخت ماژول در JC2 1.1 ۵۷

- شکل ۳۱: دبی سطح بالا از پروتکل DAA ۵۹
- شکل ۳۲: معماری REVS با استفاده از کارت هوشمند و FINREAD TCB ۶۳
- شکل ۳۳: ۱. اتصال جاواکارت ۳ به رایانه و ارائه خدمات با واسطه یک نرم افزار به شبکه ۶۷
- شکل ۳۴: ۲. اتصال جاوا کارت ۳ به رایانه و ارتباط با شبکه با ایجاد یک پل مجازی و ارائه خدمات مستقیم در شبکه به شکل مجازی. ۶۸
- شکل ۳۵:۳. اتصال مستقیم جاواکارت ۳ به شبکه بدون رگزر به رایانه. ۶۸
- شکل ۳۶: تصویری برگه رای سه تایی ۷۲
- شکل ۳۷: روش رسیدن مخفی ۷۳
- شکل ۳۸: ساختار و معماری J-FUCI ۸۱
- شکل ۳۹: نمودار مورد کاربرد پروتکل رای گچی اینترنتی پیشنهادی J-FUCI ۸۲
- شکل ۴۰: کلاس دلیگرام پروتکل J-FUCI ۸۳
- شکل ۴۱: دلیگرام ماشینی حالت برای رای پروتکل J-FUCI ۸۳
- شکل ۴۲: دلیگرام ماشینی حالت به ازای قازهای پروتکل J-FUCI ۸۳
- شکل ۴۳: نمودار مورد کاربرد در پروتکل J-FUCI ۸۴
- شکل ۴۴: نمودار توالی پیام های مبادله شده بین واحدهای انتخابی در پروتکل J-FUCI ۸۵
- شکل ۶۰: معماری PC/SC ۱۱۰
- شکل ۶۱: معماری جدید کتابخانه کارت هوشمند مایکروسافت ۱۱۱
- شکل ۶۲: معماری منطقی 24727 ۱۱۲
- شکل ۶۴ - شمای بخش های استاندارد ISO/IEC 24727 ۱۱۳
- شکل ۶۶: مراحل توسعه اپلت جاواکارت ۱۱۴
- شکل ۶۷: مراحل گسترش و بارگذاری اپلت جاواکارت ۱۱۵
- شکل ۶۸: مدل Message-Passing بین کارت و کارت خوان ۱۱۶
- شکل ۶۹: ساختار درخواست APDU ۱۱۶
- شکل ۷۰: ساختار پاسخ APDU ۱۱۷
- شکل ۷۲: ارتباطات سرپرست جاواکارت/ترمیال ۱۱۸
- شکل ۷۳ : ساختار متد process() ۱۲۰

فهرست جداول

عنوان صفحه

.....۱۳	جدول ۱: پروتکل امضای کور
.....۳۴	جدول ۲: ویژگی‌های پیش‌بینی شده و نشده زبان جاوا
.....۸۶	جدول ۳: پروتکل امضای کور قابل لینک
.....۸۸	جدول ۴: محتوای بانک اطلاعاتی مرکزی در پالمن فاز ثبت نام
.....۸۹	جدول ۵: محتوای بانک اطلاعاتی مرکزی در پالمن فاز رای‌گهی
.....۹۰	جدول ۶: محتوای بولتن برد در فاز جمع‌آوری
.....۹۰	جدول ۷: محتوای بانک اطلاعاتی مرکزی در پالمن فاز شمارش
.....۹۱	جدول ۸: محتوای بولتن برد پس از شمارش آرا
.....۹۳	جدول ۹: متغیرهای مشمول در المان Time_variable
.....۱:۱...	جدول ۱۰: جدول مقایسه ویژگی‌های امریکی پروتکل J-FUCI با سای پروتکل‌ها

فصل ۱ مقدمه

۱-۱ پیشگفتار

رای گیری الکترونیک که به معنای اخذ رای یا شمارش آراء به صورت الکترونیکی است از دهه 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 مینی‌م بسیاری برای رای گیری 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، رای گیری الکترونیکی بصورت ایده‌آل تنها در این کشور انجام می‌شود. سیستم رای گیری الکترونیکی دارای مزایای بسیاری می‌باشد، هم‌چون: نتایج صحیح و سریع و جدول بندی^۱ شده، هزینه‌های کمتر، دسترسی راحتتر، ریسک انسانی کمتر و درجهی دقت بالاتر.

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

- رای گیری ایستگاهی: فرد رای‌دهنده برای اخذ رای باید به ایستگاه‌های رای گیری مراجعه کند و از ماشینهای رای گیری کیوسکی استفاده کند.
- رای گیری الکترونیک از راه دور^۲: این روش شامل رای از طریق تلفن همراه، تلفنهای با قابلیت سیستم تون، تلویزیونهای کابلی یا راههای دیگر میشود. رای گیری الکترونیک اینترنتی مبتنی بر وب هم می تواند در این دسته قرار بگیرد.
- رای گیری اینترنتی^۳

انتخابات الکترونیکی از نظر پیاده‌سازی در جامعه دارای چند شکل کلی است که هر کدام 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 آراء در پایگاه داده صورت گرفته و شمارش و تجمیع آراء 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

¹Tabulated

²Remote electronic voting

³i-voting

دارد، امضای دیجیتالی تولید می‌شود. بدین ترتیب 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. بدین ترتیب رایگیری به صورت کاملاً 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 رای گیری الکترونیکی پرداخته می‌شود. 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 خلاصه‌های از محتوای فصول بعد را به اختصار بیان می‌نماییم.

۱-۴ نیازمندیها و ویژگیهای سیستم‌های رای گیری الکترونیکی

- هر چند که تا بحال در حوزه رایگیری الکترونیکی تعریف^۱ 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^۲: در طی زمان رایگیری تمامی محاسبات باید در طول مدت منطقی انجام گیرد و رایدهنده مجبور نباشد که تا ایدادن سایر رایدهندگان منتظر بماند.
 ۲. عملی بودن به این مفهوم که تخصص و تجهیزات اضافی برای ایدادن موردنیاز نباشد.
 ۳. کارآمدی: محاسبات در یک زمان منطقی انجام گیرند.
 ۴. قابلیت حرکت^۳: محدودیتی روی مکان رای دادن برای رایدهندگان وجود نداشته باشد.
 ۵. پایایی^۴
 ۶. قابلیت ثبت وقایع
 ۷. در دسترس پذیری 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^۱
۱۳. غیر قابل استفاده دوباره^۲: تنها یک رای معتبر به ازای هر رای‌دهنده وجود دارد.
۱۴. گمنامی^۳:
- 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^۴ 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^۵: هر کسی باید قادر باشد اعتبار کل فرآیند رایگیری را چک کند.
 - بازرسی فردی^۶: هر رای‌دهنده اطلاعاتی داشته باشد که بتواند بررسی کند که رایش در شمارش نهایی در نظر 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 رای‌هایی 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^۷: 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 Eligibility

² Unreusability

³ Anonymity

⁴ Verifiability

⁵ Public verifiability

⁶ Individual verifiability

⁷ Vote and go

نرم افزار 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 کارت خوان باید توسط خود افراد خریداری شود. بنابراین در اینجا پیچیدگی فرآیند نصب نرم افزار، نبود. دانش تحویل امضای دیجیتال از جمله موانع استفاده همه گیر از این سیستم می باشد.

- پسورد یکبار مصرف.

- اطلاعات بیومتریک (سیستم رایگیری الکترونیکی باید دارای یک حافظه بسیار امن برای نگهداری تمپلتهای بیومتریک باشد).

یک سیستم رایگیری اینترنتی علاوه بر موارد 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

مجموعه‌های از واحدهای انتخاباتی نباید بتوانند برای آرا توطئه بریزند و جلوی رای دادن رای دهندگان را بگیرند. این ویژگی را باید با اندازه گیری تعداد واحدهای متحد برای دخالت در انتخابات تعیین نمود.

۲۴. در دسترس پذیری: 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. امن سازی رایانه سمت رای دهنده برای اطمینان از معتمد بود بستر رای دهنده.

۱-۴ مشکلات امنیتی (چالش ها) سیستم های رایگیری الکترونیکی و اینترنتی

در این قسمت، مشکلات سیستم های رای گیری الکترونیکی و اینترنتی بیان می شود:

الف: رای گیری الکترونیکی

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

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

ب: رای گیری اینترنتی

پروتکل های ارائه شده برای کاربردهای رایگیری اینترنتی علاوه بر اینکه باید نیارمندیها 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 زیر اشاره نمود:
- حملات عدم سرویس‌دهی^۱: 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 توزیع شده^۲ به سرورهای حاوی تمپلیت های بایومتریک پیش از رایگیری و در حین آن بسیار خطرناک است.
 - 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^۳، در سیستم‌های رایگیری الکترونیکی قابل جبران نیست. اگر سیستم بایومتریک بعنوان متدی برای کنترل دسترسی استفاده شود، در صورت عدم کارکرد درست می‌توان با روش‌های سنتی آن را دور زد^۴ اما این کار در رایگیری الکترونیکی امکانپذیر نمی‌باشد در اینصورت حملاتی هم‌چون DDOS می‌تواند اثرات بسیار مخربی را بر جای بگذراند.
 - چگونگی تصدیق هویت امن رایدهندگان بطوریکه امنیت مورد انتظار را ارائه و سربار هزینه‌های 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 رای که در سیستم ثبت می‌شود، همانیست که او انتخاب کرده است. برای این مسئله دو راهحل ارائه می‌شود:
 - o راه حل ۱: تولید رسید برای هر رایدهنده. در فصل‌های 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 Services(DOS)

² DDOS

³ Fail safe

⁴ Bypass

میان باید به رایدهنده تحویل داده شود، باید به اندازه‌های 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^۱ که تمامی آرای ذخیره شده در سرروهای شمارنده^۲ در این برد نشان داده می‌شود.
 - در پروتکل‌های رایگیری اینترنتی و الکترونیکی معمولاً از هر دو 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 اکثراً هم از ویندوز استفاده می‌کنند که اگر آخرین بروزرسانی‌های امنیتی را انجام نداده باشد، در صورت اتصال به اینترنت در مقابل ویروسها و کرمها بسیار آسیبپذیر است. این ویروسها و کرمها می‌توانند کاری کنند که رایها خراب و یا گم شوند و در صورتیکه ثبت کاغذی وجود نداشته باشد، ایجاد دوباره این آرا غیر ممکن می‌شود.
- راه حل: مهاجرت به یک سیستمعامل باز
 - آسیب‌پذیری‌های زیرساخت اینترنت
 - سادگی خرید و فروش رای: بر طبق [۴] خرید و فروش رای^۳ 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 آلوده‌های^۴ 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