پیشنهاد اجرای طرح:

تدوین شاخص های ارزیابی عملیاتی ماژول‌های رمزنگاری بر مبنای استانداردهای روز رمزنگاری

کارفرما:

مرکز توسعه تجارت الکترونیک

مجری:

سید امیر اصغری توچائی

عضو هیئت علمی دانشکدهٔ مهندسی برق و کامپیوتر

دانشگاه خوارزمی

۱. عنوان طرح: تدوین شاخص های ارزیابی عملیاتی ماژول‌های رمزنگاری بر مبنای استانداردهای روز رمزنگاری

۲. نوع طرح: کاربردی، توسعه ای

۳. خلاصه مشخصات مجری:

سید امیر اصغری توچائی

استادیار دانشکدهٔ مهندسی برق و کامپیوتر دانشگاه خوارزمی

آدرس: خیابان شهید مفتح، نرسیده به خ انقلاب اسلامی، دانشکده فنی و مهندسی، پ ۴۹ کد پستی ۱۵۷۱۹ -۱۴۹۱۱

پست الکترونیکی:asghari@khu.ac.ir

۴. مقدمه و تعریف موضوع

با توسعه روز افزون فناوری های الکترونیکی در کسب و کارها و فعالیت های اقتصادی، موضوع امنیت در این بستر از اهمیت زیادی برخوردار است. یکی از مهمترین ساز و کارهای تامین امنیت در این حوزه، زیرساخت کلید عمومی (PKI) و گواهی الکترونیکی می باشد.

ماژول های رمزنگاری نقش محوری در زیرساخت کلید عمومی ایفا می کنند. این ماژول ها دارای جنبه های سخت افزاری و نرم افزاری هستند. بنابراین اطمینان از عملکرد صحیح ماژول های رمزنگاری از جنبه سخت افزاری و نرم افزاری بسیار اهمیت دارد. بررسی و ارزیابی کارکردی و امنیتی ماژول های رمزنگاری باید مبتنی بر یک سری شاخص شفاف و قابل آزمون صورت پذیرد.

شاخص های ارزیابی ماژول های رمزنگاری بر اساس نوع داده ها، توابع عملیاتی، ساز و کارهای رمزنگاری و امنیتی فیزیکی قابل تقسیم هستند. منابع فنی و استانداردهای متنوعی به این شاخص ها پرداخته است. در هر یک از این منابع با توجه به زمینه عملیاتی ماژولها به یک جنبه از شاخص ها توجه بیشتری شده است.

بنابراین تدوین مجموعه ای یکپارچه و مبتنی بر نیازمندیهای بومی برای شاخص های ارزیابی ماژول های رمزنگاری قابل استفاده در زیرساخت کلید عمومی کشور امری ضروری می نماید.

۵. سوالات پژوهش

- مهمترین موارد استفاده از ماژول های امنیتی در زیرساخت کلید عمومی کدام است؟
- مهمترین چالش های عملیاتی و امنیتی ماژول های رمزنگاری کدام است؟
- شاخص های اصلی ماژول های رمزنگاری در منابع و استانداردهای علمی و مرجع چگونه معرفی شده است؟
- چگونه می توان مبتنی بر نیازمندی های بومی و ملاحظات فنی زیرساخت کلید عمومی مجموعه ای از شاخص های قابل آزمون برای ماژول های رمزنگاری تدوین کرد؟
- این شاخص های ارزیابی با چه روشی باید برای ماژول های رمزنگاری مورد آزمون قرار گیرند؟

۶. اهداف و خروجی های پژوهش

- تدوین سند شاخص های ارزیابی نرم افزاری ماژول های رمزنگاری
- تدوین سند ساز و کارهای رمزنگاری مورد تایید برای اهداف امنیتی در ماژول های رمزنگاری

۷. مراحل اجرای پژوهش

- بررسی شرایط و نیازمندی های ماژول های رمزنگاری برای استفاده در زیرساخت کلید عمومی کشور
- مطالعه و بررسی اسناد و استانداردهای ملی و بین المللی مرتبط با ماژول های رمزنگاری
- استخراج و دسته بندی شاخصه های عملیاتی ماژول های رمزنگاری
- استخراج و دسته بندی ساز و کارها و الگوریتم های رمزنگاری ماژول های رمزنگاری
- تدوین سند شاخصهای ارزیابی عملیاتی ماژول های رمزنگاری
- تدوین سند ساز و کارها و الگوریتم های رمزنگاری مورد تایید برای ماژول های رمزنگاری

- تدوین سند روش آزمون شاخص های ماژول های رمزنگاری

۸. روش های مورد استفاده در اجرای پژوهش

- مطالعه تطبیقی اسناد و منابع کتابخانه ای و الکترونیکی
- استفاده از ابزارهای مدلسازی نرم افزاری

۹. هزینه اجرا

ردیف	عنوان	نفر ساعت	هزینه واحد (ریال)	هزینه کل
۱	بررسی شرایط و نیازمندی های ماژول های رمزنگاری برای استفاده در زیرساخت کلید عمومی کشور	۲۵	۵۰۰،۰۰۰	۲۵،۰۰۰،۰۰۰
۲	مطالعه و بررسی اسناد و استانداردهای ملی و بین المللی مرتبط با ماژول های رمزنگاری	۲۵	۵۰۰،۰۰۰	۲۵،۰۰۰،۰۰۰
۳	استخراج و دسته بندی شاخصه های عملیاتی ماژول های رمزنگاری	۷۵	۵۰۰،۰۰۰	۷۵،۰۰۰،۰۰۰
۴	استخراج و دسته بندی ساز و کارها و الگوریتم های رمزنگاری ماژول های رمزنگاری	۷۵	۵۰۰،۰۰۰	۷۵،۰۰۰،۰۰۰
۵	تدوین سند شاخصهای ارزیابی عملیاتی ماژول های رمزنگاری	۲۰۰	۵۰۰،۰۰۰	۱۲۵،۰۰۰،۰۰۰
۶	تدوین سند ساز و کارها و الگوریتم های رمزنگاری مورد تایید برای ماژول های رمزنگاری	۲۰۰	۵۰۰،۰۰۰	۱۲۵،۰۰۰،۰۰۰
۷	تدوین سند روش آزمون شاخص های ماژول های رمزنگاری	۶۰	۵۰۰،۰۰۰	۵۰،۰۰۰،۰۰۰
	مجموع	۶۶۰	–	۳۳۰،۰۰۰،۰۰۰

۱۰. زمان بندی اجرا

ردیف	هفته ۱	هفته ۲	هفته ۳	هفته ۴	هفته ۵
۱	❊				
۲	❊				

۳		❊			
۴		❊			
۵			❊		
۶				❊	
۷					❊

۱۱. سوابق اجرایی مجری طرح

سابقهٔ کارهای اجرایی دانشگاهی

۱. مدیر گروه پردیس بین الملل رشتهٔ مهندسی کامپیوتر دانشگاه خوارزمی
۲. مدیر گروه تحصیلات تکمیلی رشته مهندسی کامپیوتر موسسه آموزش عالی شهاب دانش قم
۳. مدیر گروه تحصیلات تکمیلی رشته مهندسی کامپیوتر دانشگاه آزاد اسلامی قم
۴. مدیر گروه تحصیلات تکمیلی رشته مهندسی کامپیوتر موسسه آموزش عالی ابرار تهران

سابقهٔ کارها و پروژه‌های اجرایی برون دانشگاهی

۱. مشاور رئیس مرکز آمار ایران، از سال ۱۳۹۹ تا کنون
۲. مشاور رئیس پژوهشکده آمار ایران، مرکز آمار ایران، از سال ۱۳۹۹ تاکنون
۳. مشاور رییس مرکز فناوری اطلاعات و رسانه های دیجیتال، وزارت فرهنگ و ارشاد اسلامی، از سال ۱۳۹۹ تاکنون
۴. مشاور دبیر شورای اجرایی فناوری اطلاعات، وزارت ارتباطات و فناوری اطلاعات، از سال ۱۳۹۸ تا کنون
۵. مدیر پروژه اولویت دار دولت الکترونیکی استعلام اصالت مدارک آموزشی رسمی کشور در سال ۱۳۹۹
۶. مدیر پروژه استعلام اصالت مدرک تحصیلی دیپلم در دبیرخانه شورای اجرایی فناوری اطلاعات در سال ۱۳۹۹

۷. مدیر پروژه استعلام اصالت مدارک تحصیلی آموزش عالی در دبیرخانه شورای اجرایی فناوری اطلاعات در سال ۱۳۹۹
۸. مدیر پروژه ثبت نام غیرحضوری دانشجویان جدیدالورود سال ۱۳۹۹ در دبیرخانه شورای اجرایی فناوری اطلاعات
۹. سرپرست معاونت زیرساخت کلید عمومی و امنیت اطلاعات تجاری وزارت صنعت، معدن و تجارت از سال ۱۳۹۶
۱۰. مدیریت سامانهٔ تدارکات الکترونیکی دولت در وزارت صنعت، معدن و تجارت از سال ۱۳۹۵
۱۱. مشاور ریاست مرکز توسعهٔ تجارت الکترونیکی کشور از سال ۱۳۹۵
۱۲. مشاور معاونت آموزش، پژوهش و فناوری وزارت صنعت، معدن و بازرگانی در زیرساخت کلید عمومی و امنیت اطلاعات تجاری، از سال ۱۳۹۵
۱۳. مدیریت بخش تحقیق و طراحی معماری کلان ایجاد مرکز داده جهت استقرار بانکداری متمرکز در بانک تجارت در سال ۱۳۹۲
۱۴. عضویت در گروه طراحی مرکز عملیات امنیت بانک تجارت جهت استقرار بانکداری متمرکز در بانک تجارت در سال ۱۳۹۲
۱۵. نظارت و ارزیابی راهبری و پایش سامانه واکنش به رخداد و مدیریت مرکز عملیات امنیت بومی در مرکز تحقیقات و فناوری اطلاعات وزارت ارتباطات و فناوری اطلاعات
۱۶. مدیریت زیرسیستم استانداردسازی سیستم نرم‌افزاری سهباد دانشگاه صنعتی مالک اشتر و مدیریت زیرسیستم راهبری و گزارشات
۱۷. طراحی و پیاده‌سازی شبکهٔ سوئیچینگ کشوری در شرکت پردازش داده‌ها به عنوان کارشناس سخت‌افزار
۱۸. طراحی و پیاده‌سازی میکروماهواره آتست در دانشگاه امیرکبیر به عنوان کارشناس سخت‌افزار در زیرسیستم فرمان و مدیریت داده‌ها
۱۹. طراحی و پیاده‌سازی میکروماهواره ناهید در دانشگاه امیرکبیر به عنوان کارشناس سخت‌افزار در زیرسیستم فرمان و مدیریت داده‌ها
۲۰. تحلیل و طراحی مراکز دادهٔ با حجم ذخیره‌سازی بالا به عنوان کارشناس شبکه در پروژهٔ انجام سرباز نخبگی

تالیف کتاب‌ها:

۱. سیستم‌های تحمل‌پذیر اشکال، تالیف سید امیر اصغری، سپیده شریفانی، سیده لیلی میرطاهری، انتشارات آکادمیک، ۱۳۹۸
۲. اشکال‌زدایی کد نرم‌افزار، تالیف علیرضا صدیقی، سید امیر اصغری، سیده لیلی میرطاهری، انتشارات دانشگاه خوارزمی، ۱۳۹۸
۳. ۱۰۰۰ سوال در سیستم‌عامل، تالیف سید امیر اصغری، حسین پدرام، انتشارات نیاز دانش، ۱۳۹۷
۴. کامپیوتر با رویکرد کاربردی، تالیف رضا شهبازیان، سیده لیلی میرطاهری، سید امیر اصغری، انتشارات کتاب آیلار، ۱۳۹۷
۵. آزمون نرم‌افزار. تالیف سید امیر اصغری، گلنوش عبائی، ۱۳۹۶
۶. پایگاه‌های دادهٔ پیشرفته برای داده‌های عظیم. تالیف محمدرضا احمدی، داود ملکی، احسان آریانیان، سید امیر اصغری، انتشارات نیاز دانش، ۱۳۹۵.
۷. بازاریابی اینترنتی. تالیف سید امیر اصغری، انتشارات ماناکتاب، ۱۳۹۴
۸. ریزپردازنده. تالیف محمد مهدی همایون پور- سید امیر اصغری- فرزاد حصار، انتشارات شیخ بهایی اصفهان، ۱۳۹۴(مرجع انتخاب شدهٔ وزارت علوم برای درس زبان‌های اسمبلی و ریزپردازنده)
۹. شبکه‌های SAN در Data Center. تالیف سید امیراصغری، افشین سوزنی، انتشارات نیاز دانش، ۱۳۹۱
۱۰. مخابرات سیّار، افشین سوزنی، لادن اسماعیلی، سید امیر اصغری، انتشارات نیاز دانش، ۱۳۹۱
۱۱. کاربرد سیستم‌های نهفته در اندازه‌گیری و کنترل. تالیف احمد کاردان – سید امیراصغری، انتشارات کیان رایانه، ۱۳۸۷
۱۲. پورت‌های سریال. تالیف سید امیراصغری- مرتضی انصاری نیا، انتشارات نهر دانش، ۱۳۸۷
۱۳. میکروکنترلر و نمونه‌های کاربردی. تالیف سید امیر اصغری، انتشارات کیان رایانه، ۱۳۸۷

ترجمهٔ کتاب ها:

۱. مقدمه‌ای بر سیستم‌های نهفته و بی‌درنگ، ترجمهٔ سید امیر اصغری، سپیده شریفانی، انتشارات نیاز دانش، ۱۳۹۵
۲. مخابرات ماهواره‌ای، ترجمهٔ امیر مهدی‌رضایی، سید امیر اصغری، انتشارات نیاز دانش، ۱۳۹۲
۳. شبکه‌های بی‌سیم، ترجمهٔ سید امیر اصغری، احسان آریانیان، انتشارات نیاز دانش، ۱۳۹۱(مرجع انتخاب شدهٔ وزارت علوم برای درس شبکه‌های بی‌سیم)

٤. شبکه‌های ارتباطی (تالیف لئون گارسیا)، ترجمهٔ سید امیر اصغری، مصطفی غلامی، پوریا محمدی یقینی، انتشارات کتاب نیاز، چاپ اول۱۳۸۹، چاپ دوم ۱۳۹۰ (مرجع انتخاب شدهٔ وزارت علوم برای درس شبکه‌های کامپیوتری).
٥. مفاهیم سیستم عامل (تالیف سیلبرشاتز)، ترجمهٔ سید امیر اصغری، کاظم غظنفری، فرهاد محمدیان، علی ایلخانی، انتشارات کتاب نیاز، ۱۳۸۹ (مرجع انتخاب شدهٔ وزارت علوم برای درس سیستم-عامل).

سابقهٔ تدریس:

مقطع دکتری

دانشگاه آزاد اسلامی، واحد علوم و تحقیقات قم

- مباحث ویژه در شبکه‌های کامپیوتری پیشرفته
- مباحث ویژه در معماری کامپیوتر پیشرفته
- طراحی نرم‌افزارهای اتکاپذیر
- شبکه‌های میان ارتباطی
- مدیریت شبکه و امنیت فضای تبادل داده

دانشگاه آزاد اسلامی، واحد بروجرد

- طراحی سیستم‌های نهفته و بی‌درنگ
- طراحی سیستم‌های نرم‌افزاری اتکاپذیر

مقطع کارشناسی ارشد

دانشگاه خوارزمی

- طراحی سیستم‌های مطمئن از سال ۹۳
- سیستم‌عامل پیشرفته از سال ۹۴

دانشگاه غیرانتفاعی شهاب دانش قم

- طراحی نرم‌افزارهای مطمئن از سال ۹۲ تاکنون
- معماری کامپیوتر پیشرفته از سال ۹۲ تاکنون
- سیستم‌عامل پیشرفته از سال ۹۲

دانشگاه صنعتی امیرکبیر

- سیستم‌عامل پیشرفته در ترم اول سال تحصیلی ۹۱-۹۰
- مدارهای آزمون‌پذیر در ترم دوم سال تحصیلی ۸۸-۸۷

دانشگاه آزاد- تهران شمال

- مدیریت شبکه‌های مخابراتی از سال ۹۴
- سیستم‌عامل پیشرفته از سال ۹۴

مقطع کارشناسی

دانشگاه خوارزمی

- مهندسی نرم‌افزار ۱ از سال ۹۳
- مهندسی نرم‌افزار ۲ از سال ۹۳
- اصول طراحی نرم‌افزار از سال ۹۳
- سیستم‌عامل از سال ۹۳

دانشگاه صنعتی امیرکبیر

- مدارهای واسط از سال ۸۶ تا ۹۲
- مدارهای الکتریکی در ترم اول سال تحصیلی ۸۷-۸۶
- سیستم‌عامل به عنوان استاد تدریس‌یار در از سال ۸۷ تا ۹۱
- کنترل نهفته به عنوان استاد تدریس یار از سال ۸۶ تا ۹۱

دانشگاه غیرانتفاعی شهاب دانش قم

- شبکه‌های کامپیوتری ۱ از سال ۸۶ تاکنون

- شبکه‌های کامپیوتری ۲ از سال ۸۶ تاکنون
- مهندسی اینترنت از سال ۸۶ تاکنون
- تجهیزات انتقال داده از سال ۸۶ تا ۹۲
- ساختمان داده از سال ۸۶ تا ۹۲
- سیستم‌عامل از سال ۸۶ تا ۹۲
- مدیریت سیستم‌های اطلاعاتی از سال ۸۶ تا ۹۳
- شیوهٔ ارائه از سال ۸۶ تا ۹۳
- ساختمان داده از سال ۸۶ تا ۹۳
- نرم‌افزار عملی ترم اول سال تحصیلی ۸۸-۸۷
- مهندسی نرم‌افزار۱ از سال ۸۶ تاکنون

دانشگاه غیرانتفاعی ابرار تهران

- شبکه‌های کامپیوتری ۱ از سال ۹۰ تاکنون
- شبکه‌های کامپیوتری ۲ از سال ۹۰ تاکنون
- مهندسی اینترنت از سال ۹۰ تاکنون
- تجهیزات انتقال داده از سال ۹۰ تا ۹۲
- ساختمان داده از سال ۹۰ تا ۹۲
- سیستم‌عامل از سال ۹۰ تاکنون

دانشگاه غیرانتفاعی فناوران تهران

- شبکه‌های کامپیوتری ۱ از سال ۸۶ تا ۸۹
- مهندسی نرم‌افزار از سال ۸۶ تا ۸۹

دانشگاه آزاد اسلامی واحد پرند

- مبانی کامپیوتر در ترم اول سال تحصیلی ۸۷-۸۶

دانشگاه جامع علمی-کاربردی

- ارتباط و انتقال داده در ترم اول سال تحصیلی ۹۰-۹۲
- مهندسی نرم‌افزار در ترم اول سال تحصیلی ۹۰-۹۲

مخابرات تهران

- مودم‌های ارتباطی در سال ۱۳۸۸