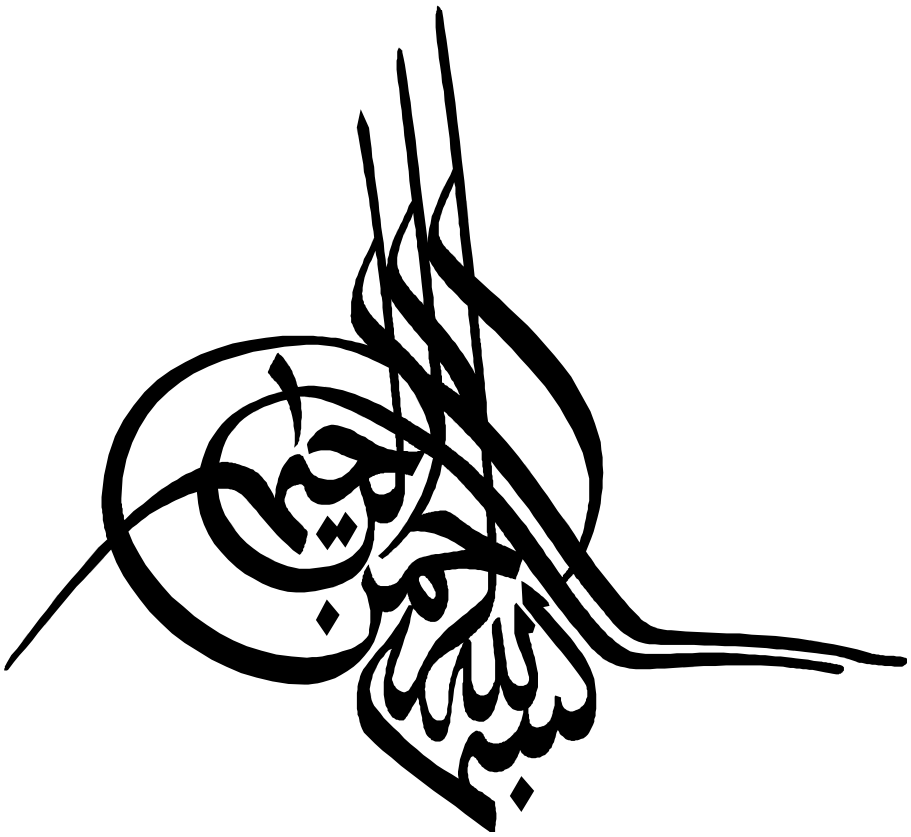

بسم الله الرحمن الرحيم

دانشگاه قم
دانشکده مهندسی کامپیوتر
پایان‌نامه دوره کارشناسی ارشد
رشته فناوری اطلاعات
گرایش تجارت الکترونیک

عنوان:

بررسی انواع معماری‌های زیرساخت کلید عمومی و ارائه یک معماری زیرساخت کلید عمومی مناسب و منطبق با زیرساخت‌های ایران

استاد راهنما :

دکتر علی اصغرعمیدیان

استاد مشاور:

دکتر حمیدرضا ربیعی

نگارنده :

امینه مقصودی خسروشاهی

پاییز 90

تقدیم به

پدر و مادر عزیزم،

که یار و یاور همیشگی من بوده‌اند و

همسرم که همیشه حمایتم کرده است.

تشکر و قدردانی

حمد و سپاس خدای را که توفیق کسب دانش و معرفت را به ما عطا فرمود. در اینجا برخود لازم می‌دانم از تمامی اساتید بزرگوار، به ویژه اساتید دوره کارشانسی ارشد که در طول سالیان گذشته مرا در تحصیل علم و معرفت و فضائل اخلاقی یاری نموده‌اند تقدیر و تشکر نمایم.

از استاد گرامی و بزرگوار جناب آقای دکتر علی‌اصغر عمیدیان که راهنمایی اینجانب را در انجام تحقیق، پژوهش و نگارش این پایان نامه تقبل نموده‌اند نهایت تشکر و سپاسگزاری را دارم.

از جناب آقای دکتر حمیدرضا ربیعی به عنوان مشاور که با راهنمایی خود مرا مورد لطف قرار داده‌اند کمال تشکر را دارم.

چکیده

با رشد فناوری اطلاعات و ارتباطات و پیچیده‌تر شدن زندگی بشر، برای پاسخ به این پیچیدگی، دولت‌ها ناگز به ایجاد دولت الکترونیک می‌باشند. در حال حاضر کشور ما نیز نیازمند ورود به عرصه دولت الکترونیک است، برای ورود کشور به این عرصه صدور گواهینامه‌های الکترونیکی برای کاربران دولت الکترونیک امری ضروری است. از این رو برای صدور گواهینامه‌های الکترونیکی در کشور اقدام به ایجاد مراکزی موسوم به مراجع صدور گواهینامه الکترونیکی شده است. به دلیل وجود ارتباطات مختلف مابین عناصر دولت الکترونیک جهت حفظ یکپارچگی و سهولت در این ارتباطات، ایجاد و افزایش چنین مراکزی باید به صورت یکپارچه و تحت یک مدیریت مرکزی و سیاست‌های یکسان انجام شود. برای این امر نیازمند وجود یک معماری مناسب (مدل اعتماد) برای زیرساخت کلید عمومی کشور هستیم. در این پروژه سعی شده است با غلبه بر چالش‌های موجود در این مسأله و ارزیابی مدل‌های اعتماد مختلف بر اساس پارامترهای مهم ارزیابی، یک مدل اعتماد تکاملی برای زیرساخت کلید عمومی کشور ارئه گردد. مدل ارائه شده منطبق بر زیرساخت‌های قانونی و فنی موجود در کشور بوده و ضعف‌های معماری موجود را پوشش می‌دهد. از سوی دیگر با توجه به اینکه با گذر زمان و افزایش کاربردهای فناوری اطلاعات و ارتباطات در کشور نیازمندی‌های جدیدی ایجاد خواهد شد، مدل ارائه شده به جهت حالت تکاملی خود امکان گسترش بهینه زیرساخت کلید عمومی در کشور را فراهم می‌کند. حالت تکاملی مدل باعث سهولت در گسترش کاربردهای زیرساخت کلید عمومی و افزایش زیرساخت‌های کلید عمومی جدید در کشور خواهد شد.

کلمات کلیدی: زیرساخت کلید عمومی، گواهینامه الکترونیکی ، معماری (مدل اعتماد)، مرکز صدور گواهی‌نامه الکترونیکی

فـهـرست مـطـالـب

فـهـرست شـکـل‌هـا

فـهـرست جـدول هـا

فصل اول

مفاهیم اولیه

1- مقدمه

رویکرد خاصی مانند تامین امنیت اطلاعات دیجیتالی، یکی از موانع و چالش‌های اصلی در به کارگیری فناوری اطلاعات در سطوح مختلف مصرف‌کنندگان به شمار می‌رود.

دولت الکترونیکی روشی برای فراهم‌کردن دسترسی آسان شهروندان به اطلاعات و خدمات دولت و همچنین برای انجام کسب‌وکار داخلی دولت از طریق اینترنت است. مشکلی که روند پیشرفت سرمایه‌گذاری دولت‌ها در این حوزه را مختل می‌کند، طراحی باز[1] اینترنت است که باعث سهولت در استراق سمع، رهگیری، نظارت و جعل ارتباطات بر روی اینترنت است. این موارد دلیل بی‌میلی شهروندان و دولت‌ها در استفاده از اینترنت برای داده‌های حساس مالی و قانونی است.

مسائلی که کاربران اینترنت با آن روبرو هستند به دو دستهٔ محرمانگی[2] و احراز هویت[3] تقسیم می‌شوند. رمزنگاری[4]، امضای دیجیتال[5] و گواهی دیجیتال[6] مکانیزم‌های مختلف پوشش دهندهٔ سرویس‌های محرمانگی اطلاعات، احراز هویت، جامعیت داده[7] و انکارناپذیری[8] هستند.

رمزنگاری روشی امن برای حفاظت داده‌های دیجیتال در محیط‌های ناامن از دسترسی‌های غیرمجاز می‌باشد. ولی این روش‌ها هیچ اقدامی در راستای اعتبارسنجی محتوای متن و حفاظت از اطلاعات در مقابل تغییر و دستکاری آنها انجام نمی‌دهند.

یک شکل خاص از رمزنگاری که به عنوان رمزنگاری کلید عمومی[9] شناخته شده است، نیازمندی‌های اینترنت را تکمیل می‌کندامضای دیجیتال روش دیگری است که از رمزنگاری بهره می‌گیرد. در مکانیزم امضای دیجیتال مبتنی بر کلید عمومی افراد از طریق کلید عمومی خود شناسایی می‌شوند. در نتیجه باید ارتباط قابل اطمینانی بین صاحب کلید و کلید وجود

---

[1] Open Design
[2] Privacy/Confidentiality
[3] Authentication
[4] Cryptography
[5] Digital Signature
[6] Digital Certificate
[7] Data Integrity
[8] Non-Repudiation
[9] Public Key Cryptography

داشته باشد. برای این منظور از گواهی الکترونیکی استفاده می‌شود که می‌تواند هویت یک شخص

را به کلید عمومی آن مرتبط سازد. این کار زیر نظر مرکز صدور گواهی دیجیتال[1] (CA) انجام خواهد شد. در حقیقت، گواهی دیجیتال یک بستهٔ اطلاعاتی به فرمت مشخص(که حاوی اطلاعاتی شامل مشخصات صاحب گواهی، تاریخ صدور، تاریخ اعتبار، مشخصات صادر کننده گواهی، کلید عمومی، کاربرد گواهی و...) است که توسط یک مرکز و یا به عبارتی به وسیلهٔ یک کلید خصوصی امضا شده‌است.

هر مرکز صدور گواهی دیجیتال، دارای یک کلید عمومی[2] و یک کلید خصوصی[3] است که توسط کلید خصوصی گواهی کاربران را امضا و آن‌ها را منتشر می‌نماید. اعتبار این مراکز به صورت مستقیم یا غیر مستقیم، سلسله مراتبی یا درهم از طرف دولت‌ها تامین می‌شود. این مراکز می‌توانند به صورت متمرکز یا توزیع شده باشند. بدلیل گستردگی روزافزون تعاملات دیجیتالی و تامین امنیت آنها، نیاز به مراکز مختلف صدور گواهی دیجیتال شدیداً احساس می شود. گسترش این مراکز باید به صورتی باشد که هم اعتبار آنها کاهش پیدا نکرده و زیر سوال نرود و هم یکپارچگی آنها حفظ شود.

بهترین رویکرد برای صدور گواهینامه‌های دیجیتالی روشی است که به زیرساخت کلید عمومی[4] (PKI) شهرت یافته است و همچنین موضوع اصلی این پایان‌نامه می‌باشد. زیرساخت زیرساخت کلید عمومی یک سیستم کاربردی و قابل اعتماد برای انتشار کلیدهای عمومی ارائه می‌کند و همچنین اتصال مابین یک کلید عمومی منتشر شده و هویت نگهدارندهٔ کلید را تضمین میکند. در این روش اتصال مابین یک کلید عمومی و نگهدارندهٔ آن با امضای دیجیتالی یک موجودیت ثالث قابل اعتماد[5] تضمین می‌شود. یک موجودیت ثالث قابل اعتماد در یک زیرساخت کلید عمومی شبیه به دفاتر اسناد رسمی در جهان واقعی است. از این رو همهٔ

[1] Certificate Authority (CA)
[2] Public Key
[3] Private Key
[4] Public Key Infrastructure (PKI)
[5] Trusted third party (TTP)

زیرساخت اصلی سیستم‌های کلید عمومی وابسته به یک یا چند نقطهٔ اعتماد[1] است، طراحی و چیدمان این نقاط اعتماد واقعاً یک چالش بوده و موضوع اصلی بحث ماست.

طراحی و آرایش یک زیرساخت کلید عمومی زمانی که یک زیرساخت برای استفادهٔ دولت مدل سازی می‌شود، بسیار مشکل است. ارتباطات مابین دولت در مقایسه با یک سازمان تجاری بسیار پیچیده است. هر سازمان دولتی باید برای انجام وظایفش با شهروندان، سازمانهای کسب‌و کار عمرانی و سازمان‌های دولتی در ارتباط باشد. زمانی که این ارتباطات در محیط الکترونیکی محقق می‌شود دولت باید بنا به طبیعت حساس وظایف خود، بسیار محتاط باشد.

1–1 مفاهیم اولیه زیر ساخت کلید عمومی

هدف از این فصل معرفی مفاهیم اولیه این پروژه است به نحوی که درک بیان مسئله آسان شود. این فصل به دو بخش تقسیم می‌شود. بخش اول با مروری کلی بر رمزنگاری و انواع آن، امضای دیج÷یتال و توابع درهم‌ساز[2] آغاز می‌شود، سپس مفاهیم کلی و جزئیات فنی زیرساخت کلید عمومی اعم از اجزا و عملکردهای اصلی زیرساخت کلید عمومی، گواهی دیجیتال، خط-مشی‌ها و سیاست‌های گواهی‌نامه[3] و توزیع و انتشار اخبار و اطاعیه‌های ابطال گواهی‌نامه ارائه شده و در بخش دوم مفهوم اعتماد[4] برای زیرساخت کلید عمومی معرفی می‌شود و انواع مدل-های اعتماد[5] زیرساخت کلید عمومی برای معماری‌های مختلف زیرساخت کلید عمومی تعریف می‌شود. ارائه این مطالب به جهت ایجاد آشنایی با عملکردها و مدل‌های زیرساخت کلید عمومی و پایه‌ای برای ارائهٔ مدل زیرساخت کلید عمومی دولتی است

1–1–1امضای دیجیتال

مفهوم امضا در محیط‌های دیجیتالی با مفهوم امضا در محیط‌های سنتی تفاوت اصولی دارد و امضا در محیط های دیجیتالی باید بسته به محتوای دادهٔ مورد امضا برای هر نامه متفاوت

[1] Trust Anchor
[2] Hash Functions
[3] Certification Policy
[4] Trust
[5] Trust Models

باشد.روش‌های تولید و اعتبارسنجی امضاهای دیجیتال از طریق علم رمزنگاری امکان‌پذیر است. برای این منظور، از الگوریتم‌های نامتقارن و همچنین توابع درهم‌ساز استفاده می شود.

در دنیای مجازی امروز هر مکانیزمی که بتواند سه نیاز زیر را در خصوص اسناد و مدارک دیجیتالی برآورده کند، «امضای دیجیتالی» نامیده می‌شود:

أ. دریافت‌کنندهٔ سند یا پیام الکترونیکی بتواند هویت صاحب سند را به درستی تشخیص دهد و از جعلی نبودن آن اطمینان حاصل کند.

ب. صاحب و امضاکنندهٔ سند بعداً نتواند محتوای سند یا پیام ارسالی خود را به هیچ طریقی انکار کند.

ج. یک متقلب شخص ثالث نتواند پیام‌ها یا اسناد جعلی تولید و آن‌ها را به دیگران منتصب کند.

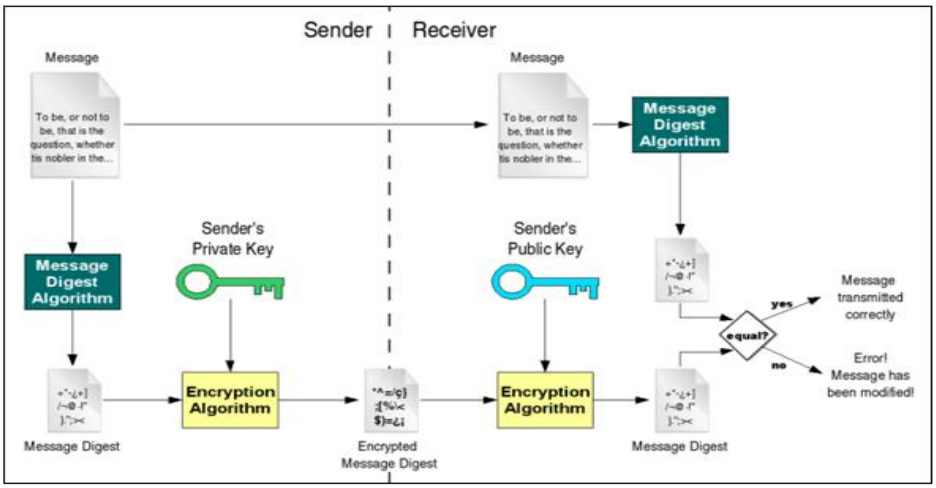
نیازهای فوق در سیستم‌های اقتصادی و مرتبط با گردش پول و اعتبار حیاتی است و برای جلوگیری از هرگونه جعل و کلاه‌برداری و حفظ منافع طرفین یک پیش‌نیاز به شمار می‌آید.

روش‌های متعددی برای پیاده‌سازی امضای دیجیتالی معرفی شده است که عبارتند از :

- امضاهای دیجیتالی مبتنی بر چکیده پیام؛ در این نوع مکانیزم بدون آن‌که محتوای سند رمزنگاری شود یا محرمانه ماندن آن مد نظر باشد یک امضای کوچک چند بایتی برای آن تولید می‌گردد.
- امضاهای دیجیتالی کلید متقارن مبتنی بر یک مرکز مورد اعتماد برای گواهی امضاء.
- امضاهای مبتنی بر روش‌های رمزنگاری کلید عمومی.
- امضاهای مبتنی بر تبدیل‌های مستقل از سیستم‌های رمزنگاری.

امروزه در بسیاری از کشورها قوانین قضایی مستحکمی در ایجاد در ایجاد پشتوانهٔ حقوقی برای امضاهای دیجیتالی وضع شده‌اند و دادگاه‌ها قادرند مناقشات حقوقی در این زمینه را بر اساس قوانین موجود حل و فصل کنند.

برای ایجاد امضای دیجیتال به ازای هر سند پس از مشخص کردن قالب استاندارد و دقیق برای اسناد، چکیدهٔ درهم‌فشرده شدهٔ آن را استخراج و پس از رمزنگاری با کلید خصوصی صاحب سند، به انتهای آن ضمیمه و ارسال شود. در این روش هیچ اخلال‌گری قادر نیست در میانهٔ راه در محتوای سند تغییری ایجاد کند .چرا که با تغییر در هر نقطه از پیام یا افزایش یا کاهش طول آن، چکیدهٔ آن تغییر خواهد کرد و گیرنده پس از محاسبهٔ چکیده پیام و مقایسهٔ آن با حاصل رمزگشایی شدهٔ امضاء، براحتی هرگونه هرگونه تغییرات احتمالی در پیام را تشخیص خواهد داد. شکل 1-1 نشان دهندهٔ الگوی مفهومی امضای دیجیتالی است.



شکل 1-1 الگوی مفهومی امضای دیجیتالی مبتنی بر چکیده پیام

در امضای دیجیتالی مبتنی بر چکیده پیام برای رمزنگاری کلید عمومی از الگوریتم RSA استفاده می‌شود و برای تولید چکیدهٔ پیام الگوریتمSHA-1 بکار برده می‌شود. اگرچه این الگو برای امضای دیجیتال بسیار رایج است ولی روش‌های پیچیده‌تری هم در این زمینه وجود دارد.

«استاندارد امضای دیجیتالی(DSS)[1]» یکی از این روش‌هاست که توسط ادارهٔ استاندارد دولت فدرال آمریکا به ثبت رسیده است[2]. در این روش نیز از تابع درهم سازی SHA-1 برای محاسبهٔ چکیده پیام استفاده شده ولی به جای رمزنگاری چکیده به روش RSA، از روش پیچیده‌تر «طاهرالجمال» استفاده شده است.

همانطور که میدانید، در یک سیستم رمزنگاری کلید عمومی کلیدهای خصوصی توسط صاحبان آن‌ها محرمانه نگه داشته می‌شوند، در حالی که کلیدهای عمومی متناظر با آن‌ها در یک انبارهٔ عمومی به نام صاحبانشان ذخیره می‌شوند. برای یک چنین سیستمی سؤالات احتمالی که باید پاسخ داده شود عبارتند از:

- چه کسی جفت کلید عمومی و خصوصی را تولید خواهد کرد؟
- قالب دادهٔ (کلید عمومی، هویت صاحب کلید عمومی و دیگر اطلاعات مربوطه) ذخیره شده در انباره (مخزن داده) چیست؟
- آیا مکانیزمی برای نگه داشتن این اطلاعات بدون تغییر در انباره وجود دارد؟
- چگونه می‌توان اتصال مابین کلید عمومی و هویت مدعی داشتن کلید عمومی را تضمین کرد؟
- چگونه کاربران به این انباره‌ها دسترسی خواهند داشت؟
- چگونه کاربر از هر تغییر مخرب در داده‌های ذخیره شده در مخزن آگاه خواهند شد؟
- چه اتفاقی برای کلید عمومی که کلید خصوصی مرتبط با آن به خطر افتاده است (کشف رمز شده است) می‌افتد؟
- آیا سیاست‌هایی برای تمام مسائل فوق وجود خواهد داشت؟

[1] Digital Signature Standard

[2] در سند FIPS-180 و US Patent 5231668 در ژولای 1991