ارائه یک روش جدید و امن برای گوشی‌های هوشمند در ابر

جواد حمیدزاده [۱]، مهناز زارع [۲]، آرزو صبری [۳]
[۱] عضو هیئت علمی، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی سجاد، مشهد، ایران
j_hamidzadeh@sadjad.ac.ir
[۲] دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر، دانشگاه بین المللی امام رضا (ع)، مشهد، ایران
Mahnaz.zare86@gmail.com
[۳] دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر، دانشگاه بین المللی امام رضا (ع)، مشهد، ایران
Arezu.sabri92@gmail.com

چکیده

گوشی‌های هوشمند با داشتن کاربردهایی شبیه به کامپیوتر و قابلیت حمل به یکی از مهم‌ترین وسایل در زندگی مردم تبدیل شده‌اند و در کنار این استفاده گسترده، بدافزارهای آن‌ها نیز به سرعت در حال افزایش هستند. از این رو امروزه ایجاد امنیت در گوشی‌ها از اهمیت بالایی برخوردار است که متاسفانه علاوه بر واقف نبودن و عدم توجه کاربران به این امر، محدود بودن منابع گوشی (مانند قدرت پردازش) پیاده‌سازی چندین راه حل امنیتی همزمان را بر روی گوشی بسیار مشکل می‌سازد. یکی از بهترین راه‌حل‌ها استفاده از ابر و محیط شبیه‌ساز در آن است. در روش پیشنهادی تمامی اطلاعات و ورودی‌ها و خروجی‌های گوشی برای بررسی به محیط شبیه‌ساز تعبیه شده در ابر ارسال می‌شود و نتایج به گوشی اعلام می‌شود. ایجاد امنیت و محرمانگی در داده‌های ارسالی بین گوشی و ابر با استفاده از رمزنگاری و تسهیم راز علاوه بر شناسایی بهتر بدافزارها از مزایای روش پیشنهادی می‌باشد.

کلمات کلیدی

گوشی‌های هوشمند، ابر، بدافزار، امنیت، رمزنگاری، تسهیم راز، تشخیص نفوذ.

۱-مقدمه

با توجه به پیشرفت روزافزون تکنولوژی در کامپیوترها و گوشی‌های تلفن همراه، نیاز به امنیت و تسریع در انجام کارها بیشتر احساس می‌شود. در گذشته ما از تلفن همراه فقط برای برقراری تماس و یا فرستادن پیامک استفاده می‌کردیم، اما با پیشرفت‌های صورت گرفته، اکنون از تلفن‌های همراه بجز موارد ذکر شده، برای اتصال به اینترنت، خریدهای اینترنتی، دریافت فایل با استفاده از بلوتوث، مکان‌یابی و غیره استفاده می‌شود. با توجه به این نکته که گوشی‌های هوشمند از ساختار نرم افزاری شبیه به کامپیوترهای شخصی استفاده می‌کنند، آن‌ها هم مانند کامپیوتر در برابر ریسک‌های امنیتی آسیب‌پذیر هستند. از این رو پیوسته باید هوشیار و محتاط باشیم تا تلفن همراه و اطلاعات ما در برابر حملات بدافزارها و مهاجمان سایبری در امان بماند.

بدافزارهای گوشی‌ها را می‌توان به دو دسته عمده تقسیم‌بندی کرد: ۱) بدافزارهایی که متناسب با قابلیت‌های سخت‌افزاری و نرم‌افزاری گوشی‌ها طراحی می‌شوند، ۲) بدافزارهایی که بصورت عمومی و مشترک با بدافزارهای کامپیوتر هستند. نکته مهم و قابل توجه این است که این بدافزارها می‌توانند علاوه بر حمله به حریم خصوصی و امنیت گوشی‌های کاربران، حملات هماهنگ در مقیاس بزرگ بر روی زیرساخت‌های ارتباطی انجام دهند [1].

ابتدایی‌ترین و ساده‌ترین کارهای صورت گرفته جهت شناسایی و مقابله با بدافزارها، طراحی آنتی ویروس (یا در حالت کلی برنامه‌های کاربردی امنیتی) و نصب و اجرای آن‌ها بر روی گوشی‌ها است. اما همانطور که اشاره شد اجرای آنتی‌ویروس‌ها (حتی آنتی‌ویروس‌هایی که مخصوص گوشی طراحی شده‌اند) با وجود منابع محدود گوشی‌ها کارامد نیست. به عنوان مثال آنتی‌ویروس موبایل گارد[۱] که آنتی‌ویروسی برای گوشی‌های اندرویدی است برای اسکن یک پوشه ۲۰۰ مگابایتی روی یک گوشی اندروید ۱۰٪ از شارژ باتری و ۴۰ دقیقه زمان نیاز دارد [1]. در اینجا توجه به نتایج یک آزمایش که در سال ۲۰۱۲ توسط Symantec صورت گرفته نیز بسیار تامل برانگیز است. در این آزمایش برای تشخیص یک بدافزار بر روی گوشی هوشمند از ۹ آنتی‌ویروس مختلف استفاده کردند و در این میان فقط یکی از آن‌ها توانست بدافزار را تشخیص دهد [2]. حال این سوال مطرح می‌شود که آیا با ظرفیت‌های یک گوشی هوشمند در حال حاضر، داشتن هر ۹ آنتی‌ویروس بر روی آن امکان‌پذیر است؟

با توجه به اطلاعات و داده‌های زیاد، برنامه‌های کاربردی مختلف و جدید، تحلیل و بررسی داده‌ها و همچنین محدودیت‌های پردازش، حافظه، ذخیره‌سازی و منابع باتری در گوشی‌های هوشمند که یک چالش کلیدی در اجرای راه‌حل‌های مؤثر امنیتی بر روی گوشی‌های هوشمند است؛ نیاز به محیط خارج از محدوده گوشی‌های هوشمند (محیطی مانند ابر) جهت پیاده‌سازی راه‌حل‌های امنیتی بیشتر احساس می‌شود [3].

ساختار ادامه مقاله به شرح زیر می‌باشد. در بخش ۲ پژوهش‌های مرتبط بررسی می‌گردد و در بخش ۳ روش پیشنهادی برقراری امنیت در گوشی‌های هوشمند مبتنی بر ابر شرح داده می‌شود و در ادامه در بخش ۴، ارزیابی روش پیشنهادی را خواهیم داشت. نتیجه‌گیری و کارهای آینده آخرین بخش این مقاله خواهد بود.

۲- پژوهش‌های مرتبط

در [4] یک سرویس امنیت داده ارائه نمودند که داده‌ها و مدیریت امنیتی را بدون افشا شدن اطلاعات کاربر به ابر برون سپاری می‌کند. سرویس امنیت داده ارائه شده سربار مدیریت امنیتی را از سمت کاربر سیار حذف کرده و فقط بعضی اعمال رمزنگاری قبل از بارگذاری فایل روی ابر توسط او انجام می‌شود. انجام همین اعمال رمزنگاری که شامل ارزیابی‌های جفت شدن عظیم و محاسبات نمایی می‌باشد باعث مصرف انرژی قابل توجهی در دستگاه سیار خواهد شد.

در [5] یک پروتکل سرویس امنیتی برای گوشی‌های هوشمند با استفاده از مفهوم رایانش ابری سیار ارائه نمودند. در این روش از احراز هویت استفاده شده و به وضعیت دستگاه سیار و شبکه توجه می‌شود. همچنین همواره لیست داده‌ها جهت عاری بودن از داده‌های مخرب بررسی می‌شود. روش کار به این صورت است که وضعیت گوشی هوشمند به سرور تایید کننده فرستاده می‌شود تا استفاده از سرویس‌های رایانش ابری کنترل شود، یعنی برای سرویس‌دهی به وضعیت دستگاه سیار توجه می‌شود. سرور تایید کننده نیز برحسب شرایط و سیاست‌های از پیش تعریف شده پاسخ تایید یا رد را ارسال می‌کند. به عنوان یک سناریو اگر کاربر دستگاه سیار درخواست داده داشته باشد، این درخواست به سرور تایید کننده ارسال می‌شود و در اینجا چک می‌شود که لیست داده فاقد داده‌های مخرب باشد. چک کردن لیست داده‌ها جهت عاری بودن آن‌ها از داده‌های بدخواهانه به صورت موثری در این روش انجام می‌شود که موجب تامین امنیت در سطح مناسبی می‌شود.

در [6] نیز روشی ارائه نمودند که از رمزنگاری نامتقارن برای تامین محرمانگی و جلوگیری از هک شدن داده‌ها استفاده می‌کرد. البته استفاده از رمزنگاری نامتقارن معایبی به همراه دارد که از آن جمله می‌توان به مصرف توان و پهنای باند بالا اشاره کرد. همچنین به این روش حمله جعل سرور نیز وارد می‌باشد.

در [1] برای شناسایی بدافزارهای موبایل از محیط ابر استفاده شده است، در این روش عامل سرویس‌گیرنده تمام اطلاعات ورودی و خروجی را ضبط کرده و برای ابر ارسال می‌کند. در محیط شبیه‌سازی شده در ابر این اطلاعات پردازش شده و درصورت وجود خطا یا مشکلی به عامل سرویس-گیرنده اطلاع داده می‌شود. به این دلیل که داده‌ها در محیط ابر و توسط چندین برنامه امنیتی تحلیل می‌شوند، امکان تشخیص داده‌های مخرب افزایش می‌یابد. البته در این مقاله، در مورد چگونگی نحوه ارسال داده‌ها به ابر و ارسال هشدار از ابر برای عامل سرویس گیرنده صحبتی نکرده‌است.

در[7] نیز روشی ارائه کردند که از Secret Sharing برای امنیت داده‌ها استفاده می‌کند، به این صورت که داده‌ها بجای اینکه بر روی فقط یک ابر ذخیره ذخیره شوند، به n قسمت تقسیم شده و بر روی چندین ابر مختلف قرار می‌گیرند، با این‌کار حتی اگر متخاصم بتواند به یک ابر دسترسی داشته باشد، نمی‌تواند به داده ما دست یابد. البته با توجه به این نکته که نیاز به چندین ابر مختلف داریم، هزینه کاربر افزایش می‌یابد.

در [8] نیز یک طرح احراز هویت مبتنی بر رمز عبور ارائه شده که به صورت مناسبی از ویژگی سیستم رمزنگاری منحنی بیضوی استفاده کرده است. طرح فوق علاوه بر تامین امنیت دارای سربار پردازشی و ارتباطی بسیار پایینی نیز می‌باشد که باعث شده این طرح برای دستگاه‌های سیار سودمند باشد.

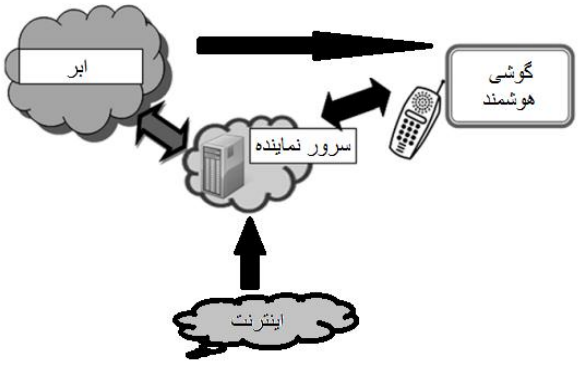
در روش پیشنهادی ما، محرمانگی و صحت داده‌ها مورد توجه قرار می‌گیرد. در این روش از رمزنگاری، توابع درهم‌ساز و فشرده‌سازی استفاده می‌شود که باعث برقراری امنیت بین گوشی و ابر می‌شود. همچنین باتوجه به ذخیره‌سازی و شناسایی بدافزارها بر روی ابر، مشکل حافظه کم و قدرت پردازش محدود گوشی‌های هوشمند نیز حل می‌شود. که در بخش‌های آتی بطور مفصل در مورد روش صحبت خواهد شد.

۳- روش پیشنهادی

در ابتدا معماری سطح بالایی از روش برقراری امنیت در گوشی‌های هوشمند در ابر را بصورت اجمالی معرفی کرده و سپس به بررسی روش پیشنهادی می‌پردازیم.

گوشی هوشمندی که یک نرم افزار به نام عامل سرویس گیرنده[۲] بر روی آن نصب و در حال اجراست، یک سرور نماینده[۳] و یک شبیه‌ساز در محیط ابر مولفه‌های اصلی در این روش هستند [1]، شکل شماره (۱). نخستین بار که گوشی در ابر ثبت نام می‌شود، نرم افزار عامل سرویس گیرنده بر روی گوشی نصب می‌شود. عامل همه اطلاعات مورد نیاز ماکت دستگاه ثبت نام شده در محیط شبیه‌سازی شده، ورودی‌های کاربر و سنسورها از رابط‌های دستگاه را ضبط و ثبت می‌کند [1] که برای کاهش مصرف پهنای باند، بهتر است عامل کلاینت فقط ورودی‌های دستگاه را ضبط کند و آن‌ها را برای شبیه ساز ارسال کند.

در آن سوی ارتباط، یک شبیه‌ساز در محیط ابر قرار دارد که یک ماکت شبیه‌سازی شده از هر دستگاه ثبت نام شده را اجرا می‌کند. این کپی شبیه‌سازی شده (ماکت) دقیقا شامل سیستم فایل‌ها و سیستم عامل مربوط به گوشی هوشمند اصلی است. ماکت بطور مداوم و همزمان خودش را از طریق دریافت ورودی‌های کاربر توسط عامل سرویس گیرنده متناظر با گوشی اصلی، همگام نگه می‌دارد [1].



شکل (۱): چارچوب کلی روش امنیتی مبتنی بر ابر

البته مهم‌ترین کاری که در شبیه‌ساز اتفاق می‌افتد، اجرای موازی راه‌حل‌های امنیتی مختلف مانند آنتی‌ویروس‌ها و تشخیص‌دهنده‌های نفوذ برای محافظت از گوشی هوشمند در برابر تهدیدات امنیتی است درحالی‌که به علت محدود بودن منابع گوشی، نمی‌توان از راه حل‌های امنیتی یا آنتی‌ویروس‌های مختلف بر روی گوشی استفاده کنیم. شبیه‌ساز هنگام شناسایی ویروس یا عوامل مخرب یک هشدار به عامل سرویس گیرنده مربوطه جهت اجرای اقدامات مورد نیاز می‌فرستد.

در این ساختار، سرور نماینده ترافیک‌های ورودی یک دستگاه را برای ماکت شبیه‌سازی شده مربوط به خودش در داخل ابر تکرار می‌کند. همچنین ترافیک خروجی ماکت را برای اجتناب از تکرار درخواست بلاک می‌کند (مثلا برای جلوگیری از خرید مجدد یک آیتم از یک وب سایت فروشگاه آنلاین).

پس از آشنایی با مولفه‌های معماری روش پیشنهادی، اکنون به بررسی مکانیزم شناسایی بدافزارها در گوشی‌های هوشمند در محیط ابر می‌پردازیم. می‌توان اطلاعات ورودی و خروجی گوشی‌ها را به دو دسته کلی تقسیم‌بندی کرد: ۱) اطلاعات انتقالی از طریق اینترنت، ۲) اطلاعات انتقالی از طریق بلوتوث، usb و غیره.

برای حالت اول، که اطلاعات و بدافزارهایی از طریق اینترنت می‌توانند وارد گوشی شوند؛ بین شبکه اینترنت، ابر و گوشی، یک سرور نماینده قرار دارد. یعنی وقتی کاربر گوشی بر روی یک لینک و یا صفحه اینترنتی کلیک کند، سرور یک نمونه برای گوشی و یک نمونه از آن را برای ابر می‌فرستد. همزمان هم گوشی و هم ابر اطلاعات را دارند، یعنی سرور یک نسخه از پاسخ‌های برگشتی را علاوه بر گوشی به ابر نیز ارسال می‌کند تا فعالیت‌های معمول اینترنتی کاربر مختل نشود. در اینجا برای حفظ محرمانگی و صحت اطلاعات جهت جلوگیری از جعل و دستکاری، از یک پروتکل ارتباطی امن، بین ابر و ماکت دستگاه در شبیه ساز استفاده می‌شود. حال ابر اطلاعات دریافتی را اسکن می‌کند و اگر ویروس و یا مورد مشکوکی را تشخیص داد، به گوشی اطلاع می‌دهد. در اکثر مواقع شبیه ساز اقدامات لازم (مانند حذف فایل آلوده و غیره) را نیز برای گوشی، ارسال می‌کند.

برای حالت دوم که در مورد اطلاعاتی است که از طریق بلوتوث، usb و غیره وارد گوشی هوشمند می‌شوند، عامل سرویس گیرنده که بر روی گوشی نصب می‌شود تمام ورودی‌ها را ثبت کرده و به شبیه ساز در ابر جهت تجزیه و تحلیل ارسال می‌کند. برای جلوگیری از جعل و حمله فرد میانی داده‌ها را باید قبل از ارسال رمز کنیم تا کسی در بین راه نتواند به آن دسترسی داشته باشد و محرمانگی و صحت آن به خطر بیفتد. از سوی دیگر جهت احراز هویت و اطمینان از ابر، کلید رمزنگاری را با استفاده از روش تسهیم راز حد آستانه‌ای [9] بین ماکت دستگاه در ابر و فراهم کنندگان ابر تقسیم کرده و در زمان رمزگشایی با گردآوری آن‌ها توسط ماکت به کلید می‌توان دست یافت.

در اینجا، برای رمزگشایی داده نیاز به حضور گروهی از افراد مجاز (t) (که زیر مجموعه مجاز نیز نامیده می‌شوند) از مجموعه کل افراد مرتبط با موضوع (n) است؛ که سهم راز (همان کلید رمزگشایی) را که در ابتدا بین آنان تقسیم شده است را ارائه دهند. روش پیشنهادی در این حالت از سه مرحله تعیین پارامترهای اولیه، ارسال اطلاعات به محیط شبیه‌ساز و تحلیل اطلاعات ارسالی تشکیل شده است. همچنین می‌توان مرحله مستندسازی و بایگانی اطلاعات اسکن شده بر روی محیط شبیه‌ساز را نیز در نظر گرفت که این مرحله جهت استناد در آینده می‌تواند کاربرد داشته باشد. در ادامه به شرح کامل‌تر مراحل می‌پردازیم.

۱) تعیین پارامترهای اولیه

پس از ثبت نام و ایجاد ماکت دستگاه گوشی در ابر و نصب نرم افزار عامل سرویس گیرنده بر روی گوشی هوشمند، ابتدا عامل سرویس گیرنده و ماکت دستگاه یک کلید خصوصی برای خود انتخاب کرده و پس از محاسبه کلید عمومی، آن را ثبت می‌کنند. حال با استفاده از روش توافق کلید دیفی هیلمن [10]، یک کلید مشترک اصلی بین عامل سرویس گیرنده و ماکت توافق می‌شود.

همچنین عامل سرویس گیرنده یک چند جمله‌ای تصادفی، $f(x)$، حداکثر از درجه t را انتخاب می‌کند و بر اساس آن سهم افراد را محاسبه و پس از رمزکردن با کلید عمومی افراد، بصورت محرمانه برای آنان ارسال می‌کند. سپس یک میدان گالوا $GF(p)$، که p عدد تصادفی اول بزرگی است، را انتخاب کرده و سپس پارامتر عمومی $g \in GF(p)$ را انتخاب کرده و بصورت عمومی اعلام می‌کند. حال کلید رمزنگاری k برابر است با $g^{f(0)}$ که عامل سرویس گیرنده از آن برای رمز کردن اطلاعات ارسالی به ابر استفاده می‌کند و برای تولید کلید هر بار کافیست فقط یک g جدید انتخاب و اعلام شود. شرح کامل مراحل به همراه فرمول‌های آن در شکل (۲) آمده است.

۲) ارسال داده به ابر

پس از جمع‌آوری داده‌های ورودی و خروجی گوشی، عامل سرویس گیرنده جهت حصول اطمینان از صحت آن‌ها در حین ارسال، ابتدا با استفاده از توابع درهم‌ساز یکطرفه چکیده گرفته و سپس فایل‌ها را برای کمتر شدن حجم آن‌ها فشرده می‌کند. حال مقدار چکیده را به اطلاعات فشرده شده الحاق کرده و سپس با کلید k رمز و ارسال می‌کند. در اینجا بهترین الگوریتم درهم‌ساز SHA-512، بهترین روش رمزنگاری متقارن AES [6]، بهترین روش رمزنگاری نامتقارن مبتنی بر ECC [11] و بهترین روش فشرده سازی [1] Run-Length Encoding (RLE) که یک الگوریتم فشرده سازی بدون اتلاف داده است استفاده می‌شود. مراحل در شکل (۱) نشان داده شده است.

۳) تحلیل اطلاعات

پس از دریافت بسته ارسالی، در اولین گام برای رمزگشایی هر سه نفر از مجموعه افراد مجاز بصورت جداگانه سهم خود را محاسبه و به ماکت دستگاه گوشی در ابر ارسال می‌کنند. همانطور که اشاره شد یکی از اعضای این مجموعه حتما ماکت گوشی می‌باشد.

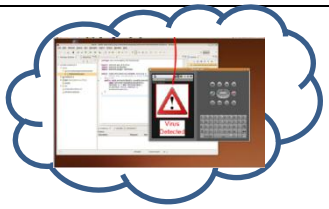
$$C_i = g^{s_i} \qquad (۱)$$

C_i: سهم ارسالی افراد.

s_i: سهم افراد.

حال با استفاده از فرمول زیر کلید k را محاسبه می‌کند:

$$k = g^{f(0)} = \prod_{j=1}^{t} \left(c_{i,j}\right)^{b_j} \qquad (۲)$$



تعیین پارامترهای اولیه

انتخاب کلید خصوصی (k_s) و سپس کلید عمومی (k_{pub}).

توافق کلید مشترک اصلی (k_{Master})، با روش توافق کلید دیفی هیلمن.

K_{Master}

انتخاب n نقطه مختلف از میدان گالوا GF(p) که بصورت عمومی اعلام می‌شود.

$x_i \in GF(p)$, $i=1,2,\ldots,n$

انتخاب t ضریب تصادفی از میدان گالوا GF(p) که محرمانه هستند.

$a_0, a_1, \ldots a_{t-1}$

و انتخاب a_0 بعنوان کلید یا همان راز.

تشکیل چند جمله‌ای:

$f(x)=a_0+a_1x+a_2x^2+\ldots+a_{t-1}x^{t-1}$

محاسبه سهم افراد:

$S_i=f(x_i)$, $i=1,2,..,n$

$E_{pubi}(S_i), x_i$

دریافت پارامترها و ذخیره‌سازی.

انتخاب کلید خصوصی (k_s) و سپس کلید عمومی (k_{pub})

توافق کلید مشترک اصلی (k_{master})، با روش توافق کلید دیفی هیلدمن.

ارسال داده به ابر

انتخاب پارامتر مولد میدان، g.

در نتیجه k یا همان کلید نشست برابرست با:

$k=g^{f(0)}$

g

دریافت پارامتر عمومی.

جمع‌آوری اطلاعات و داده‌های ورودی و خروجی گوشی، m.

محاسبه چکیده با استفاده از توابع درهم‌ساز:

h(m)

فشرده کردن داده‌ها با الگوریتم RLE:

z(m)

الحاق داده‌های فشرده شده با چکیده: $M=z(m)||h(m)$

$E_k(M)$

تحلیل اطلاعات

دریافت سهم شرکا علاوه بر محاسبه سهم خود:

$C_i = g^{s_i}$, $i=1,2,\ldots,t$

محاسبه کلید رمزگشایی k:

$$k = g^{f(0)} = \prod_{j=1}^{t} \left(c_{i,j}\right)^{b_j}$$

بطوریکه:

$$b_j = \prod_{\substack{1 \le l \le t \\ l \ne j}} \frac{x_{i,l}}{x_{i,l} - x_{i,j}} \pmod p$$

رمزگشایی داده‌های دریافتی:

$M' = D_k(M)$, $M' = z(m')||h(m)$

خارج کردن داده ها از فشردگی.

محاسبه مجدد چکیده از داده به دست آمده: $h(m')$

مقایسه چکیده‌های $h(m')$ و $h(m)$:

- اعلام هشدار و خطا به عامل سرویس گیرنده در صورت عدم تساوی.
- در غیر اینصورت، فایل‌ها را اسکن کرده؛ نتیجه و هشدارهای لازم را به عامل و یا کاربر گوشی اعلام می‌کند.

$E_{k_{master}}(alarm)$

اعمال دستورات ارسالی.

شکل (۲): شمای کلی طرح پیشنهادی

$c_{i,j}$: سهم نفر j ام از مجموعه افراد مجازی که سهم خود را ارسال کرده‌اند.

بطوریکه:

$$b_j = \prod_{\substack{1 \le l \le t \\ l \ne j}} \frac{x_{i,l}}{x_{i,l} - x_{i,j}} \pmod p \qquad (۳)$$

سپس داده‌ها را با کلید نشست به دست آمده رمزگشایی و اطلاعات را از حالت فشرده خارج می‌کند. اولین کاری که در شبیه‌ساز صورت می‌گیرد بررسی صحت اطلاعات دریافتی است. بدین گونه که از اطلاعات دریافتی که رمزگشایی و از حالت فشرده خارج کرده با استفاده از همان تابع درهم‌سازی که عامل سرویس گیرنده استفاده کرده (روش توافقی هنگام ثبت نام در ابر)، از اطلاعات چکیده می‌گیرد. حال چکیده‌ای را که خود به دست آورده با چکیده دریافتی مقایسه می‌کند و در صورت مشاهده هر گونه تناقضی به عامل سرویس گیرنده هشدار می‌دهد. در غیر این صورت اطلاعات را معتبر در نظر گرفته و شروع به اسکن کردن آن‌ها (با استفاده از چندین راه حل امنیتی همزمان) می‌کند و اگر درون آن‌ها بدافزاری و یا مورد مشکوکی را تشخیص داد به کاربر و یا عامل سرویس گیرنده اطلاع می‌دهد. در قسمت‌های بعدی به راه‌های هشدار پیشنهادی خواهیم پرداخت.

پس از بررسی و آنالیز، ماکت گوشی در ابر می‌تواند اطلاعات را با کلید عمومی گوشی هوشمند رمز کرده و در پایگاه داده خود ذخیره‌کند تا هر زمان که نیاز بود بتوان از آن‌ها استفاده و یا به آن‌ها استناد کرد. حال گوشی هر کدام از اطلاعاتی را که بر روی ابر فرستاده، می‌تواند از حافظه خود پاک کند.

۳-۱- راه حل‌های امنیتی در شبیه‌ساز

برای دستیابی به بالاترین حفاظت، می‌توان چندین راه حل امنیتی مختلف مبتنی بر میزبان و مبتنی بر شبکه را در محیط ابر بر روی گوشی هوشمند شبیه‌سازی کرد.

۱) اسکن کردن ویروس

شبیه‌ساز از آنتی‌ویروس‌های مختلف برای مانیتور کردن تمامی فایل‌های بر روی دستگاه به منظور پیدا کردن بدافزارهای شناخته شده استفاده می‌کند. متاسفانه آنتی‌ویروس‌های مخصوص گوشی‌های هوشمند به دلیل محدودیت‌های گوشی به خوبی عمل نکرده، در حالی‌که در شبیه‌ساز می‌توان آنتی‌ویروس‌های قدرتمند با فرکانس بالا را اجرا کرد.

۲) بررسی صحت فایل‌ها

هنگامی‌که یک سیستم به مخاطره می‌افتد، ممکن است حمله‌کننده قسمت‌های حساس سیستم فایل آن را برای دسترسی‌های آینده خود و یا فرار از شناسایی، تغییر بدهد. از این رو یک چک کننده صحت فایل می‌تواند تغییرات فایل‌های مهم را با تولید یک چکیده از آن فایل‌ها، به عنوان مثال با توابع درهم‌ساز، و مقایسه دوره‌ای آن‌ها بررسی کند.

۳) تشخیص نفوذ مبتنی بر شبکه

شبیه‌سازی مبتنی بر ابر بررسی عمقی بسته‌های ترافیک ورودی و خروجی شبکه را نیز میسر می‌کند و به نظارت بر دستگاه برای محتواهای ناقص و رفتارهای ناهنجار کمک می‌کند. مثلا می‌توان از Snort که یک روش تشخیص نفوذ مبتنی بر شبکه است استفاده کرد. همچنین می‌توان از روش‌های ترکیبی تشخیص نفوذ (ترکیب روش‌های تشخیص نقوذ مبتنی بر امضا و مبتنی بر ناهنجاری) برای شناسایی حمله‌های شناخته شده و ناشناخته استفاده کرد. یکی از بهترین روش‌های ترکیبی، ترکیب درخت تصمیم با ماشین بردار پشتیبان (SVM) است که در تشخیص حملات ناشناخته و شناخته شده بسیار خوب عمل می‌کند.

۳-۲- راه‌های هشدار

پس از شناسایی یک تهدید با استفاده از راه‌حل‌های امنیتی شبیه‌ساز، که در بالا اشاره شد، دستگاه مربوطه باید متوجه و عکس العمل مناسبی را انجام دهد. مکانیزم‌های متفاوتی می‌تواند به کار گرفته شود، از جمله:

✓ مطلع کردن عامل کلاینت

سریع‌ترین راه، ارسال یک پیغام به عامل کلاینت در حال اجرا بر روی دستگاه گوشی هوشمند است. در این حالت، علاوه بر هشدار و آگاه ساختن، شبیه‌ساز می‌تواند دستوراتی را نیز برای مقابله با تهدید کشف شده ارسال کند [1].

✓ ایمیل هشدار

برای پشتیبانی از مکانیزم‌های قبلی، در مواردی که عامل کلاینت از کار افتاده، می‌توان از ارسال ایمیل جهت آگاهی بخشیدن به کاربر از تهدید کشف‌شده استفاده کرد.

هنگامی‌که عامل کلاینت ازخطر شناخته شده مطلع شد، برای بازگشت به حالت امن خود باید یک سری واکنش های مناسب انجام دهد. حذف فایل، خاتمه دادن فرایند، پشتیبان گیری دوره‌ای، فیلترکردن شبکه، از جمله عکس-العمل‌هایی است که می‌تواند انجام شود.

۴- ارزیابی

در مقاله‌های پیشین، از ابر برای تشخیص بدافزارها استفاده شده‌است، اما به اهمیت حفظ محرمانگی داده‌ها توجهی نشده‌است. ما در روش پیشنهادی به این جنبه نیز پرداخته و برای حفظ محرمانگی از رمزنگاری استفاده کرده‌ایم. در ادامه به مقایسه و ارزیابی روش پیشنهادی خود با سایر روش‌ها می‌پردازیم.

۱) مزیت این روش نسبت به روش‌هایی که به دنبال راه‌حل‌های امنیتی درون گوشی هستند باتوجه به محدودیت منابع و ظرفیت ذخیره سازی گوشی هوشمند این است که مستقل از منابع گوشی بوده و بررسی را در محیط خارج از گوشی انجام می‌دهد.

۲) با توجه به اینکه ابر یک محیط عمومی است، پس برای حفاظت داده‌ها از رمزنگاری استفاده می‌کنیم، که حتی اگر کسی وارد حریم خصوصی ما بر روی ابر شد، نتواند به اطلاعاتمان دسترسی داشته باشد.

۳) کلید نشست بصورت کاملا تصادفی انتخاب شده و در هر ارسال پیام تغییر می‌کند. همچنین کلیدهای نشست چون کاملا از هم مستقل هستند، حتی متخاصم با بدست آوردن کلید نشست فعلی، نمی‌تواند به کلیدهای نشست قبلی یا بعدی دست یابد. همچنین نمی‌تواند به کلید اصلی که از طریق روش دیفی هیلمن توافق شده، دسترسی یابد.

۴) با توجه به این نکته که داده‌ها بصورت آشکار ارسال نمی‌شوند و از رمزنگاری برای ارسال آن‌ها استفاده می‌کنیم، پس امکان اتفاق افتادن

حملات شنود، فردمیانی و غیره، وجود ندارد.

۵) از آنجایی که اطلاعات ابتدا فشرده می‌شوند و سپس با کلید نشست که بصورت کاملا تصادفی انتخاب می‌شود، رمز می‌شوند، حمله تحلیل ترافیک بسیار سخت و یا حتی می‌توان گفت غیر ممکن می‌شود. هدف از فشرده کردن داده‌ها، بهم ریختن الگو آن‌ها می‌باشد، تا با بدست آوردن آن‌ها کسی نتواند به اصل داده‌ها دست یابد.

۶) با توجه به محدودیت حافظه و قدرت کم پردازشی گوشی هوشمند، در این روش برای رمزنگاری داده‌ها از روش متقارن استفاده می‌شود که سرعت آن نسبت به روش‌های نامتقارن بیشتر است و هزینه محاسباتی و زمان انجام آن کمتر می‌باشد .

۷) باتوجه به اینکه ابر یک محیط عمومی است و جهت جلوگیری از جعل ابر و شنود کلید نشست توسط متخاصم، از روش تسهیم راز استفاده کرده‌ایم و همچنین سهم افراد را نیز با کلید عمومی آن‌ها رمز کرده و ارسال می‌کنیم.

۸) دارا بودن چندین روش تحلیل امنیتی از دیگر مزایای این روش است. همچنین همانگونه که اشاره شد استفاده از روش تشخیص نفوذ ترکیبی به جای تشخیص نفوذ معمولی کارایی بسیار بالاتری در شناسایی حملات و بدافزارها دارد.

۹) همچنین چون logهای ارسالی (شامل Alarm ها و دستورات) که از سمت ابر به گوشی ارسال می‌شود، رمز می‌شوند؛ پس شخص متخاصم در بین راه نمی‌تواند در آن‌ها تغییری ایجاد کند.

جدول (۱): ارزیابی روش‌ها

ویژگی‌های امنیتی	Saman et al.	Heloise et al.	Hafizful et al.	Park et al	Proposed scheme
حمله حدس رمز عبور	بله	خیر	خیر	خیر	خیر
حمله تغییر	خیر	خیر	بله	خیر	خیر
حمله تکرار	خیر	خیر	خیر	خیر	خیر
حمله ورود تعداد زیادی کاربر	بله	بله	خیر	بله	خیر
حمله داخلی	بله	بله	خیر	بله	خیر
حمله ممانعت از خدمات	خیر	خیر	بله	خیر	خیر
حمله کلید شناخته شده	بله	بله	بله	خیر	خیر
حمله جعل سرور	خیر	خیر	خیر	خیر	خیر

۵- نتیجه‌گیری و کارهای آینده

در این مقاله برای رفع محدودیت‌های گوشی جهت برقراری امنیت از محیط ابر استفاده شده که علاوه بر بررسی روش‌ها و گام‌های آن، روش بهبود یافته و امن‌تری از سایر روش‌های بررسی تهدیدات در محیط‌های خارج از گوشی ارائه شده، بیان شد. ما توانستیم علاوه بر ایجاد امنیت در گوشی‌ها با اجرای چندین راه‌حل امنیتی قدرتمند، با بکارگیری رمزنگاری و تسهیم راز و کدهای تشخیص خطا، محرمانگی و صحت اطلاعات را نیز حفظ کنیم و آن را در مقابل حملات فرد میانی، شنود، جعل و غیره مصون نگه داریم. ما امیدواریم بتوانیم یک روش جایگزین امنی برای امنیت اطلاعات ارسالی بین سرور نماینده و شبیه‌ساز و همچنین برنامه‌های امنیتی کارا در ابر ارائه دهیم.

مراجع:

[1] Saman Zonouz, Amir Houmansadr, Robin Berthier, Nikita Borisov, William Sanders., "*Secloud: A cloud-based comprehensive and lightweight security solution for smartphones"*, Computers & Security, Vol. 37, pp. 215-227, 2013.

[2] Symantec. (2012) Android.jifake. [Online]. Available: http://www.symantec.com/securityresponse/writeup.jsp?docid=2012-073021-4247-99.

[3] Niroshinie Fernando, Seng W. Loke, Wenny Rahayu., "*Mobile cloud computing: A survey"*, ELSEVIER, Future Generation Computer Systems Vol. 29, pp. 84–106, 2013.

[4] Jia, Weiwei, et al. "*SDSM: a secure data service mechanism in mobile cloud computing*." Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on. IEEE, 2011.

[5] Park, Ji Soo, Ki Jung Yi, and Jong Hyuk Park. "*SSP-MCloud: A Study on Security Service Protocol for Smartphone Centric Mobile Cloud Computing*." *IT Convergence and Services*. Springer Netherlands, 2011. 165-172.

[6] Al-Hasan, Md, Kaushik Deb, and Mohammad Obaidur Rahman. "User-authentication approach for data security between smartphone and cloud ."*Strategic Technology (IFOST), 2013 8th International Forum on*. Vol. 2. IEEE, 2013.

[7] Wang, Honggang, et al. "Security protection between users and the mobile media cloud." *Communications Magazine, IEEE* 52.3 (2014).

[8] SK Hafizul Islam, G.P. Biswas, "Design of improved password authentication and update scheme based on elliptic curve cryptography", *Mathematical and Computer Modelling 57* (2013) 2703–2717.

[9] Adi Shamir., *"How to share a secret",* Communications of the ACM, Vol.22, pp.612-613, 1979.

[10] Emmanuel Bresson1, Olivier Chevassut2,3, and David Pointcheval1., *"Provably authenticated group Diffie-Hellman key exchange",* CCS '01 Proceedings of the 8th ACM conference on Computer and Communications Security, pp. 255-264, 2001.

[11] Rounak Sinha,et all., *" Performance Based Comparison Study of RSA and Elliptic Curve Cryptography*", International Journal of Scientific & Engineering Research, Vol 4, Issue 5, May-2013.

زیرنویس

[1] Smobile goaurd
[2] Client agent
[3] Proxy server