

!" #%\$'

چارچوب کنترل دسترسی پایدار به شبکه محاسبه ابر

چکیده:

ارتباطات متحد امکان اشتراک بی وقفه داده ها بین ابزارهای مختلف در سکوه‌های مختلف فراهم می کنند. از دیرباز، سازمان ها از سرورهای محلی برای ذخیره داده استفاده نموده اند و کارکنان با استفاده از رایانه های رومیزی دارای خط مشی امنیتی از قبل تعریف شده به داده ها دسترسی پیدا کرده اند. در عصر ارتباطات متحد، کارکنان از مزایای ابزارهای هوشمند و فن آوری بی سیم 4 جی برای دسترسی به داده ها از هر مکان و در هر زمان استفاده می کنند. پروتکل های امنیت ز جمله کنترل دسترسی طراحی شده برای ساختار سنتی هنگام ادغام ابزارهای موبایل با شبکه داخلی سازمان کافی نیست. در این زمینه ما به بررسی ویژگی های ابزارهای هوشمند برای ارتقا امنیت راهبرد کنترل دسترسی استفاده می کنند. ویژگی های پویا در ابزارهای هوشمند از جمله خطا در قفل گشایی، کاربرد نرم افزار، محل و مجاورت ابزارها را می توان برای تعیین ریسک کاربر نهایی به کار برد. در این مقاله به طور بی وقفه ویژگی های پویا را در طرح کنترل دسترسی سنتی شامل می سازیم. شامل سازی ویژگی های پویا لایه اضافی امنیت را برای کنترل دسترسی سنتی فراهم می کند. ما نشان می دهیم که کارایی الگوریتم پیشنهادی قابل قیاس با کارایی طرح های سنتی می باشد.

1-مقدمه

امروزه سازمان نیاز به ابزارهای مختلف از جمله ابزارهای هوشمند و رومیزی، ایمیل، پیام فوری، پیام صوتی، ارائه اطلاعات و کنفرانس صوتی، تصویری و وب دارند. هنگامی که این ابزارها در سیستمی ادغام می شود که امکان اشتراک گذاری داده های بی وقفه در بین وسایل را فراهم می کند، آن شبکه ارتباطات متحد نام دارد. ابزارهای هوشمند و ادغام آنها در شبکه سنتی بهره وری در بین کارکنان و نیز آسیب پذیری های امنیتی جدید را افزایش می دهد. از دیرباز سازمان ها داده ها را در سرورهای محلی ذخیره کرده اند و کارکنان با استفاده راهبردهای

کنترل دسترسی به داده ها دسترسی دارند. به هر حال روند اخیر در محاسبه ابر، برون سپاری و ابزارهای هوشمند یا ابزارهای خود را بیاور، و پهنای باند موباید گسترده سازمان ها را مقدور ساخته است تا از هر مکان و زمان اطلاعات را به اشتراک گذارند. داده ها را می توان با استفاده از ذخیره داده های عمومی از جمله فراساختار محاسبه ابر به اشتراک گذاشت که می تواند قابلیت های محاسبه انعطاف پذیر فراهم سازد، هزینه ها کاهش دهد. به طور ویژه ابزارهای خود را بیاور، به موضوع داغی پس از نظر سنجی سیسکو 2012 تبدیل شده است که پی برده است 95٪ از کارکنان اجازه دارند از ابزارهای موبایل خود درون سازمان های خود استفاده کنند. تعداد کاربرانی که از ابزارهای شخصی خود برای کار استفاده می کنند، افزایش یافته است. این روند بر خلاف سنتی است که در آن کارکنان دسترسی به ابزارهای شرکت در قالب نرم افزارهای معین و خط مشی ها برای دستیابی به امنیت دارند. اخیرا محققان بر توسعه راهبردها تاکید داشته و سامسونگ و بلک بری از فن آوری ناکس، بس 12 به ترتیب برای اجرای خط مشیه ای امنیت شرکتی در ابزار کاربر استفاده می کنند. این روند نیاز به روش های تازه برای کنترل دسترسی داده های ذخیره شده در ابر دارد. از دیرباز فرض می کنیم که دارندگان داده ها، کاربران و سرور ذخیره در یک حیطه بوده و سرور به طور کامل مورد اعتماد است. به هر حال، در ابزار خود را بیاور، محاسبه ابر و محیط برون سپاری، محرمانه بودن داده ها تضمین نمی شود چون داده ها درون محیط شخص ثالث ذخیره می شوند. شخص ثالث می تواند به اطلاعات فردی کارکنان و منابف تجاری کاربران دسترسی داشته باشد برای غلبه بر این مشکل دسترسی به داده های محرمانه در محیط توزیع یافته از طریق راهبرد کدگذاری ویژگی محور امکان پذیر است. راهبرد کدگذاری ویژگی محور به عنوان راهبرد کدنگاری نوید بخش در نظر گرفته شده و از داده های محرمانه و کنترل دسترسی به طور همزمان پشتیبانی می کند. با راهبرد کدگذاری ویژگی دارندگان داده ها می توانند داده ها را با استفاده از خط مشی های دسترسی کدگذاری کنند. فرض کنیم کارمندی با ویژگی های و کارکرد و و یا کدگذاری را انجام می دهد: مدیر یا ریس مالی و شرکت الف. لذا کارمندی که مدیر بوده و در شرکت الف استخدام می باشد می تواند فایل را کد گشایی کند. دو نوع طرح کدگذاری بر مبنای ویژگی وجود دارد: کدگذاری بر مبنای ویژگی اقتدار مجزا و کدگذاری بر مبنای

ویژگی اقتدار چندگانه. در طرح اقتدار مجزا تنها اقتدار ویژگی مسئول نظارت بر تمامی ویژگی ها می باشد. در اقتدار چندگانه چند اقتدار ویژگی مسئول مجموعه های ویژگی ها می باشند.

در مورد ابزار خود را بیاور، کد گذاری مبنی بر ویژگی نمی تواند به طور مستقیم برای حمایت از داده ها به کار رود. محرمانه بودن داده ها در طرح های کد گذاری مبتنی بر ویژگی متکی بر ویژگی های استاتیک از قبل تعریف شده از جمله مدیر، مسئول مالی، و شرکت الف می باشد. شبکه های وای فای و مجاورت ابزارها را می توان به منظور تایید هم زمان مورد استفاده قرار داد. ویژگی های جمع آوری شده از طریق ابزارهای هوشمند را ویژگی های پویا می نامیم چون بسته به جابجایی کاربر تغییر می کنند.

در این مقاله الگوریتم جدیدی مطرح می کنیم که از سازمان ها جهت ویژگی ای پویا درون طرح کد گذاری بر مبنای ویژگی جهت کنترل دسترسی مستحکم مطرح می کنیم که تازه بودن الگوریتم به خاطر موارد زیر است. 1- الگوریتم جدید ویژگی های پویا را برای طرح کد گذاری بر مبنای ویژگی اجرا می کند. 2- الگوریتم جدید امنیت طرح کد گذاری بر مبنای ویژگی را به خطر نمی اندازد. 3- الگوریتم جدید از اقتدار تک و چندگانه پشتیبانی می کند. 4- عملکرد الگوریتم جدید قابل قیاس با طرح کد گذاری امنیتی سنتی است.

2- آثار مربوطه

کنترل دسترسی مسئله امنیتی سنتی استو مدل های زیادی در ادبیات مطرح شده اند. در سال 1996 ساندو با همکاران مدل کنترل دسترسی تحقق پذیر با عنوان کنترل دسترسی نقش محور معرفی نمود که اقتدار و اجرا را راحت می نمود. مدل های کنترل دسترسی نقش محور متعددی پیشنهاد شده اند. زانگ و پاراشار مدل کنترل دسترسی نقش محور را برای پشتیبانی از اطلاعات زمینه به نام طرح کنترل دسترسی پویا آگاه از زمینه گسترش دادند (2). در (2) کاربری با اسناد دسترسی بر اساس نقش خود (یک سری ویژگی ها) و اطلاعات زمینه تعیین می شود. منابع مجموعه نقش ها را حفظ نموده و نقش بالقوه ای برای کاربر در نظر می گیرد. آثار مشابهی در مبنای شرایط زمانی با نام کنترل دسترسی نقش محور زمانی در (4) و بر اساس دامنه رویداد و شرایط محور به

عنوان کنترل دسترس نقش محور رویداد مداری در (3) مطرح می شوند. در (4،3) رویداد قابل اندازه گیری، متغیر زمینه پویا تعریف شد که می تواند بر تصمیمات دسترس علاوه بر متغییرات زمان و مکان تاثیر گذارد. در (17) ویژگی های زمانی و مکانی برای پشتیبانی از طرح کنترل دسترس بیمار محور در مراقبت بهداشتی الکترونیکی مطرح شدند. سیستم کنترل دسترسی نقش محور موبایل که خط مشی محل و مکان را اجرا می کند در (6) مطرح شد. در (6) شی مجهز به گیرنده ارتباطات نزدیک میدان بوده و کاربر دارای مجموعه ابزار پر توان ارتباطات نزدیک میدان می باشند. لذا کاربر می تواند با تبادل اسناد با استفاده از پروتکل های ارتباطات نزدیک میدان به منابع خاصی دسترسی داشته باشد.

هاسن و الشچانک مدل گسترده ای از مدل کنترل دسترسی نقش محور برای سیستم های موبایل مطرح کردند (5). آنها مدل کنترل دسترسی نقش محور را با معرفی مفهوم نقش های محیطی به منظور کنترل مجموعه دسترس با فعال سازی/غیر فعال سازی نقش های مبتنی بر اطلاعات مکانی معرفی نمودند. در اینجا اجازه به طور پویا به نقش متکی بر مکان داده می شود. در (7) مولفین مدل کنترل دسترسی محل محور پیچیده تر مطرح نمودند. نقش را می توان به کاربر در محل تعیین شده خاص و برخی نقش ها را در محل های دیگر تعیین نمود. هر دو آثار (5 و 7) از اطلاعات مکانی و زمانی در مدل کنترل دسترسی نقش محور استفاده می کنند اما ویژگی های زمینه ای مهم دیگر را در محیط موبایل امروزی در نظر نمی گیرند. هسین-چو و یان هیسانگ راهبرد کدگذاری داده ای محل محور با مکان های استاتیک مطرح نمودند (19). هر محل استاتیک حاوی مختصات از پیش تعیین شده طولی و عرضی بود. مفهوم ژئوکدگذاری یا کدگذاری بر مبنای محل در توزیعلايه دیجیتال از سوی اسکات و دنینگ معرفی شد (18). ال ابراهیم با همکاران پروتکل کدگذاری مکانی را با محدود کردن کدگذاری پیام به محل و زمان خاص مطرح کردند (20). کدگذاری این اثر شبیه (19) بود که در آن محل ها ایستا بودند. ویجیایالاکاشیمی و پالانیولو با کدگذاری منحنی هذلولی در شبکه های حس گر بی سیم تعیین محل ایمنی مطرح نمودند (21). کریمی و کلانتری (22) پروتکل کدگذاری محلی مطرح نمودند

که به گره های موبایل این امکان را می دهد با یکدیگر ارتباط برقرار کنند راهبرد مشابهدی برای ابزارهای موبایل در (23) مطرح شد. در (8) چارچوب کنترل دسترسی با استفاده از پروتکل آی.ای.ای.ای. 802.11 مطرح می شود که به موجب آن دسترس به شبکه ناحیه محلی بی سیم امکان پذیر است. هنگامی که کاربر این زمینه می تواند اسناد محرمانه را از طریق پروتکل آی.ای.ای.ای. 802.11 دریافت می کند. مولفین در (9) روشی مطرح کردند که به بررسی و تحلیل میزنا حمایت مدل کنترل دسترسی می پردازد. جدول 1 این آثار را با آثار مشتمل بر ویژگی پویا مقایسه می کند که در آن علامت تیک را به منزله پشتیبانی و ضربدر به معنای عدم پشتیبانی است. ساهای و واترز (10) کدگذاری مبتنی بر ویژگی را مطرح نمودند و در آن کدگذاری مبتنی بر هویت پیام را تحت چند ویژگی معرفی نمودند که شامل هویت فازی می باشد. دو نوع طرح کدگذاری ویژگی محور خط مشی اصلی تو سط گویال با همکاران (11) و کد گذاری مبتنی بر ویژگی خط مشی متن رمزی در (12) مطرح شد. چیس (31) سیستم کدگذاری ویژگی محور مجزا و چند منظوره را جهت نظارت بر ویژگی ها مطرح نمود. چیس و چو اثر دیگری (32) معرفی نمودند که طرح قبلی (31) را بهبود می بخشید. در (32) اقتدار مرکزی از بین برداشته شد و کلید بی نام پروتکلی را صادر نمود که به بررسی حریم کاربر می پرداخت. لکو و واترز طرح کدگذاری ویژگی محور کامل (33) معرفی کردند که نیاز به سرور مورد اعتماد نداشت. اثر (43) درباره برون سپاری پیچیدگی محاسباتی و ارتباطی کاربران با اقتدار نیمه ساختاری می باشد. طرح کدگذاری جدید برای استفاده اقتدار نیمه ساختار بدون نقض حریم مطرح شد. به هر حال ایده طرح جدید استفاده از ویژگی های ابزارهای هوشمند در اینجا مطرح می شود و نقاط ضعف و اهمیت کار جدید بررسی می شود.

	Static attributes	Dynamic attributes					Data confidentiality
		Spatial OR temporal attribute	App usage	Unlock failure	Proximity	etc	
Context aware RBAC [2]	✓	✓	x	x	x	x	x
Event driven RBAC [3]	✓	✓	x	x	x	x	x
Temporal RBAC [4]	✓	✓	x	x	x	x	x
Spatial RBAC [5]	✓	✓	x	x	x	x	x
Spatial temporal RBAC [6]	✓	✓	x	x	x	x	x
Location aware RBAC [7]	✓	✓	x	x	x	x	x
Location aware AAC [8]	✓	✓	x	x	x	x	x
Spatial-Temporal and E-health [17]	✓	✓	x	x	x	x	x
Location based encryption [18]	✓	✓	x	x	x	x	✓
Location and mobile [19]	✓	✓	x	x	x	x	✓
Geocryption [20]	✓	✓	x	x	x	x	✓
Secure localization [21]	✓	✓	x	x	x	x	✓
Location based encryption [23]	✓	✓	x	x	x	x	✓
Proposed scheme	✓	✓	✓	✓	✓	✓	✓

جدول 1

3- بیان مسئله

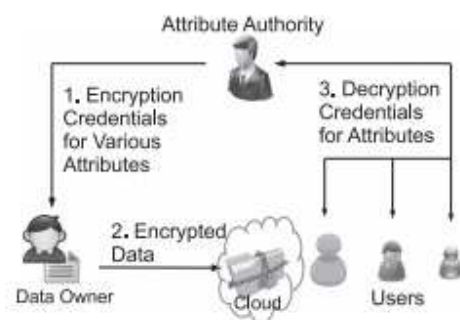
این بخش ساختار سیستم، تهدیدات حریم و امنیت مربوط به رویکرد مطرح شده و فرض های اساسی قابل اجرا در بقیه اثر را معرفی می کند.

3-1 ساختار سیستم

سیستم مطرح شده شامل چهار مولفه زیر می باشد: کاربران مجهز به یک یا چند ابزار هوشمند می باشند. ابزار هوشمند متصل به اینترنت بوده و داده های خدمات را از هر مکان و زمان را قابل دریافت می سازد. چون این روکید از رمزکنگداری منحنی هذلولی دوخطی استفاده می کند هر گونه ابزار کدگذاری آر اس ای و کد گشایی می تواند این رویکرد را اجرا کند و اندازه کلید مورد نیاز برای رمزنگاری 224 بیت است که کمتر از اندازه کلید آر اس ای 2048 است.

دارندگان داده ها، داده های کد گذاری شده را به ذخیره ابر بارگذاری کرده و خط مشی های ممکن را تعریف می کنند که در نمونه ما ای تعریف بر مبنای ویژگی های استاتیک برگرفته از ای.ای. با ویژگی های پویا می باشد. ارائه دهندگان خدمات ابر ذخیره ابر و قدرت محاسباتی برای کاربران و دارندگان داده فراهم می کنند. در نمونه ما دارندگان داده ها داده های کدگذاری شده را به محل ذخیره بارگذاری می کنند در حالی که کاربر داده

های کدگذاری شده را از محل ذخیره بارگیری می کند. مقامات ویژگی دارای نقش کنترل و حفظ ویژگی های استاتیک کاربران هستند. مقامات مختلف مجموعه ویژگی های متفاوت را مدیریت می کنند کاربر باید ویژگی های خود را به مقامات ثابت کند.



شکل 1

3-2 کدگذاری ویژگی محور

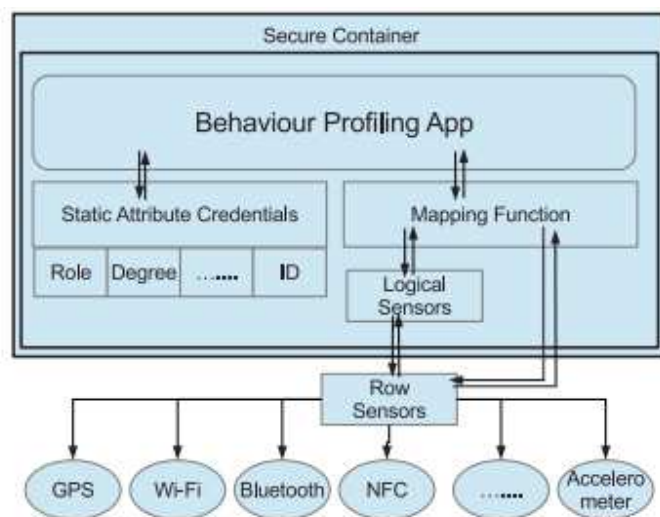
کدگذاری ویژگی محور به داده ها امکان کدگذاری می دهد به نحوی که فقط افرادی به آنها دسترسی داشته باشند که دارای اسناد برای ویژگی های ضروری هستند. در این طرح کد گذاری مقامات ویژگی های مورد اعتماد اسناد کدگذاری و کد گشایی را حفظ می کنند و ویژگی های کاربر را قبل از افشای اسناد و داده ها تایید می کنند. شکل 1 نحوه دارنده داده، ای.ای. و تعامل کاربر با یکدیگر را نشان می دهد.

3-3 تهدیدات امنیتی و حریم

چند تهدید امنیتی و حریم وجود دارد که مانعی بر سر راه طرح های کنترل دسترسی می باشند. حال لیست حمله بالقوه و ارتباط آنها با شرایط سیستم را معرفی می کنیم.

تهدیدات مربوط به هویت: تهدید اصلی به هویت عناصر پروتکل مربوط می شود و رقیب ممکن است به عنوان هویت خود را جا زده و سعی می کند هویت مشروع از خود جلوه دهد. هدف ما جلوگیری از این رقیب ها می

باشد. تهدیدات حریم: کاربر به منظور دریافت کلید کد گشایی نیاز به فراهم سازی ویژگی های خود برای مقامات می باشد. لذا نوعی از مقامات مخرب ممکن است به این ویژگی های کاربر دست یابد. هدف ما فراهم سازی تضمین حریم برای کاربران است. حملات برخورد: هر مقام ویژگی مجموعه ای ویژگی ها را در سیستم ما مدیریت می کند اما ممکن است با یکدیگر برخورد کنند تا ویژگی های کاربر را استنباط کنند. این کار باعث می شود مقامات مخرب به ویژگی ها دست یابند هدف ما محافظت در برابر حملات به برخورد در کاربر نهایی و مقامات ویژگی می باشد. فریب ویژگی پویا: ابزاری هوشمند از جمله کاربرد نرم افزار و حس گرهای محلی ویژگی پویا را به دست می آورند و لذا دارنده داده ها باید اطمینان حاصل کند که ابزار کاربر دستکاری نشده باشد. در اینجا باید یک سری فن آوری ها برای تضمین عدم تقلب در ویژگی ها در نظر داشت. فریب ردیابی: نرم افزار نصب شده درون ابزار کاربر باید داده های حس گر را جمع آوری کند تا ارزش ویژگی های پویا را تعیین کند. اگر نرم افزار مخرب باشد آنگاه شخص ثالث می تواند به داده ها دست یابد. لذا داشتن فن آوری های پشتیبان کاربران از مورد حمله واقع شدن از سوی اشخاص ثالث حائز اهمیت است.



شکل 2

4- طرح کدگذاری ویژگی محور ایستا و پویا برای اقتدار ویژگی منحصر به فرد

4-1 فرض ها و اصول طراحی

در طرح پیشنهادی فرض می کنیم که کاربران دارای نرم افزار نصب شده در ابزار هوشمند خود هستند که ویژگی های پویا را به دست می آورد تا در کنار ویژگی های ایستا متناسب با خط مشی تعریف شده از سوی دارنده داده ها باشد. ویژگی های پویا از جمله محل، زمان، دما، نویز، نور و حضور ابزارهای دیگر و تعامل بین کاربر و گوشی هوشمند یا ترکیبی از آنها در (37-40) به کار رفت تا خط مشی های دسترسی در محیط ابزار هوشمند بررسی شود. در (28) مولفین طرح دسترسی برای کنترل پویای ابزار قفل زمان و روش قفل گشایی مطرح نمودند. شکل 2 نرم افزار پروفایل رفتاری را نشان می دهد که در زمینه ایمن نصب شده و کارفرمایین استفاده کننده از سکوی نرم افزار از جمله ناکس یا بی بی اس 12 بر آن نظارت دارند.

ترکیب های دوخطی: گیریم G_1 و G_2 دو گروه رده اول q بوده و g_1, g_2 مولد G_1 و G_2 باشند. حال نقشه دو خطی را چنین فرض می کنیم $G_1 \times G_2 \rightarrow G_T$ که دارای خواص زیر است: 1- دو خطی: $\hat{e}(x^a, y^b) = \hat{e}(x, y)^{ab}$ ، وجود دارد، $a, b \in \mathbb{Z}_q, \forall x \in G_1, \forall y \in G_2$ ، تجزیه ناپذیری: به ازای $\forall x \in G_1, \forall y \in G_2, \hat{e}(x, y) \neq 1$. 3- قابلیت محاسبه: \hat{e} محاسبه موثر می باشد.

انضمام لاگرانج: سهم رمز شامیر از راهبرد انضمام لاگرانج برای دستیابی به رمز از میان رمزهای مشترک می پردازد. فرض کنید که $p(x) \in \mathbb{Z}_p[x]$ چند جمله ای $k-1$ درجه بوده و رمز برابر $s=p(0)$ است. گیریم

$S = \{x_1, x_2, \dots, x_k\}$ و ضریب لاگرانج برای x_i در S برابر باشد با

$$\Delta_{x_i, S}(x) = \prod_{x_j \in S, x_j \neq x_i} \frac{x - x_j}{x_i - x_j}$$

به ازای مقادیر متفاوت K در $p(x_1), p(x_2), \dots, p(x_k)$ چند جمله ای $p(x)$ را می توان طبق زیر نوشت

$$p(x) = \sum_{x_i \in S} p(x_i) \prod_{x_j \in S, x_j \neq x_i} \frac{x - x_j}{x_i - x_j} = \sum_{x_i \in S} p(x_i) \Delta_{x_i, S}(x),$$

لذا رمز S بر طبق زیر به دست می آید

$$s = p(0) = \sum_{x_i \in S} p(x_i) \prod_{x_j \in S, x_j \neq x_i} \frac{0 - x_j}{x_i - x_j}.$$

تطبیق دهی: تابع مقایسه خطی را به عنوان M در نظر می گیریم. این تابع دو ورودی از حس گر ابزار هوشمند و دارنده داده دارد. دارنده داده باید داده های حس گر مورد نیاز و عملیات بولین را انجام دهد. خروجی تابع بله یا خیر است.

فرض دیفی-هلمن دو خطی تغییر یافته تصمیمی: فرض کنید چالش گر $a, b, c, z \in \mathbb{Z}_p$ به طور تصادفی انتخاب می کند. فرض دیفی-هلمن دو خطی تغییر یافته تصمیمی آن است که هیچ مخرب و رقیب زمانی چند جمله ای نمی تواند این عوامل سه گانه را تشخیص دهد. ما از این ویژگی برای اثبات از طریق نقض این مسئله استفاده می کند که الگوریتم پیشنهادی ما طرحی در برابر حملات معروف است.

2-4 طرح پیشنهادی

مغیر با طرح کدگذاری ویژگی محور سنتی توصیف شده در بخش 2-3، در این بخش نشان خواهیم داد که چگونه می توان به طور موثر ویژگی های پویا را در طرح کدگذاری ویژگی سنتی جای داد که در آن دارنده داده ها می تواند داده ها را با استفاده از اسناد مقام ویژگی و نیز ویژگی های پویا شامل ساخت. شبیه کدگذاری ویژگی محور سنتی (11)، الگوریتم مطرح شده همچنین شامل چهار الگوریتم فرعی زیر است. ساختار: الگوریتم ساختار از پارامتر امنیت λ به عنوان وردی و گروه دو خطی خروجی و مجموعه ای از پارامترها استفاده می کند. پارامترهای $q, g, G1$ پارامترهای عمومی اند و $\{T_i = g^{A_i}\}, Y = \bar{e}(g, g)^y$ کلیدهای عمومی ویژگی های حفظ شده با اقتدار و $y, t_{A,i} \in \mathbb{Z}_q$ به ازای هر ویژگی i کلیدهای خصوصی مقامات ویژگی اند.

صدور کلید: مسئول ویژگی کلید کد گشایی برای کاربر فراهم می کند که دارای یک سری ویژگی ها با تولید تصادفی چند جمله ای P_u به ازای u می باشد. به هر حال $P_u(0) = y'$ به ازای تمامی کاربران برقرار است. آنگاه مسئول ویژگی اسناد کد گشایی $D_i(u)$ برای کاربر u در اُمین ویژگی صادر می کند.

کدگذاری: الگوریتم کد گذاری یک سری ویژگی های حفظ شده با مسئول ویژگی و نیز ویژگی های پویا دارنده داده ها به عنوان داده های ورودی حفظ می کند. آنگاه متن رمز داده ها را خروجی جلوه می دهد. در این مرحله دارنده داده ها کلید خصوصی S_A و S_B و کلیدهای عمومی متناظر E_α و E_i تولید می کند.

کد گشایی: الگوریتم کد گشایی اسناد کد گشایی دریافتی از مسئول ویژگی را اتخاذ نموده و پارامترهای ویژگی را از بزار هوشمند و متن رمزی را به عنوان ورودی قبول کرده و سپس داده های اولیه را به عنوان خروجی بیرون می دهد. نرم افزار پروفیل رفتار به طور ایمن مقدار شبکه ویژگی های پویا مورد نیاز را توام با Y^{SA} به دست می آورد. رمزگشایی موفقیت آمی زاست اگر و تنها اگر

$$= h(M(a_{c,1}) || M(a_{c,2}) || \dots || M(a_{c,n})).$$

$$h(M(a'_{c,1}) || M(a'_{c,2}) || \dots || M(a'_{c,n}))$$

در حالت رمزگشایی، نرم افزار پروفایل رفتاری از قبل در دستگاه هوشمند کاربر نصب شده و محل خود را تعیین می کند. تابع تطبیق دهی m که داده های ورودی صاحب داده ها را وارد می کند و خروجی آنی آری و خیر است و اگر میزان ریسک کمتر از آستانه تعریف شده باشد آنگاه این تابع m آری است. در بخش 7 درباره امنیت پروفایل رفتاری بحث خواهیم کرد.

3-4 بازی امنیت

به منظور اجتناب از آسیب پذیری امنیت، طرح های مبتنی بر ویژگی باید در برابر مدل هویت گزینشی ایمن باشند. در مدل گزینشی هویت رقیب مخرب باید هویت های چالش امیز جهت چالش کشیدن مطرح کند. سپس

چالش گر پارامترهای ضروری را تهیه کرد و برای رقیب می فرستد. اگر رقیب نتواند پیام را کد گشایی کند، آنگاه طرح پیشنهادی در برابر مدل هویت ایمن است.

ساختار: چالش گر مرحله ساختار الگوریتم و تشکیل آن را اجرا نموده و به پارامترهای عمومی را به رقیب می گوید. جستجوی کلید رمز: رقیب اجازه دارد هر تعداد جستجوی کلید رمز انجام دهد. چالش: رقیب دو پیام m0 و m1 به چالش گر در زمینه شاهد می فرستد. حال چالش گر به طور تصادفی یکی از پیام ها را انتخاب می کند. جستجوهای کلید رمز بیشتر: رقیب اجازه دارد جستجوی کلید رمز بیشتر انجام دهد تا زمانی که می خواهد. حدس: حال رقیب حدس می زند کدام پیام از سوی چالش گر کد گذاری شده است. رقیب زمانی موفق است که پیام صحیح را با احتمال $\frac{1}{2} + \epsilon$ حدس بزند که در آن ϵ تابع غیر قابل صرف نظر می باشد.

Setup \mathcal{S}

- AA generates group bilinear parameters: $g, g, \mathbb{G}_1, \leftarrow \mathcal{S}(1^\lambda; \sigma)$, for a given security parameter λ and $\sigma \in \{0, 1\}^{poly(\lambda)}$.
- AA randomly generates secrets $y, t_{i,j} \in \mathbb{Z}_q$ for each attribute i ($1 \leq i \leq N$) where N is the total number of attributes monitored by the authority.
- AA publishes the corresponding public keys $\{T_i = g^{t_{i,j}} \mid \forall i \in \{1, \dots, N\}\}$ and $Y = \hat{e}(g, g)^y$.

Key Issuing \mathcal{KG}

- To issue decryption keys for user u , AA chooses a random polynomial p_u with degree $d - 1$ where $p_u(0) = y$. It should be noted that $p_u(0)$ for any users should be equivalent to y .
- AA generates decryption credential for i^{th} attribute for u as: $D_u(i) = g^{p_u(t_{i,j})}$ where $\forall i \in A_U$ (A_U denotes the attributes set of u).

Encryption \mathcal{E}

Data owner encrypts data m for attribute set $A_m = A_A \cup A_C$, where $A_A = \{a_{a,1}, \dots, a_{a,i}\}$ denotes the attributes maintained by AA and $A_C = \{a_{c,1}, \dots, a_{c,n}\}$ denotes the dynamic attributes defined by the data owner, as follows:

- * Data owner randomly chooses $s_A, s_B \in \mathbb{Z}_q$ and encrypts the data as $Enc_m = mY^{s_B}$.
- * Data owner computes $E_0 = h(M(a_{c,1}) || M(a_{c,2}) || \dots || M(a_{c,n}))Y^{s_A + s_B}$, $E_i = g^{t_{i,j} s_A}, \forall i \in A_A$, where $h: \{0, 1\}^* \rightarrow \mathbb{Z}_q$ is a secure hash function, M is a mapping function of dynamic attributes and $||$ denotes concatenation.
- * Now data owner uploads $CT_m = \{Enc_m, E_0, E_i, \forall i \in A_A \text{ and } A_C\}$ into the cloud.

Decryption \mathcal{D}

- * User downloads CT_m from the cloud and checks the required attributes to decrypt m .
- * User computes $\hat{e}(E_i, D_u(i)) = \hat{e}(g, g)^{p_u(t_{i,j}) s_A}$ where $i \in A_A \cap A_U$.
- * Using interpolation technique, u can compute $Y^{s_A} = \hat{e}(g, g)^{p_u(0) s_A} = \hat{e}(g, g)^{y s_A}$.
- * Now corporate app installed in users mobile device computes the hash value of dynamic attributes such as current location, risk-level associated with current location and risk-level associated with user behavior and outputs $h(M(a'_{c,1}) || M(a'_{c,2}) || \dots || M(a'_{c,n}))$.
- * User can decrypt the data as follows (only if $h(M(a'_{c,1}) || M(a'_{c,2}) || \dots || M(a'_{c,n})) = h(M(a_{c,1}) || M(a_{c,2}) || \dots || M(a_{c,n}))$)

$$Enc_m \cdot \frac{h(M(a'_{c,1}) || M(a'_{c,2}) || \dots || M(a'_{c,n}))Y^{s_A}}{E_0} = mY^{s_B} \cdot \frac{h(M(a'_{c,1}) || M(a'_{c,2}) || \dots || M(a'_{c,n}))Y^{s_A}}{h(M(a_{c,1}) || M(a_{c,2}) || \dots || M(a_{c,n}))Y^{s_A + s_B}} = m.$$

شکل 3

5- طرح کد گذاری ویژگی محور پویا و ایستا برای مسئول ویژگی های چندگانه

در طرح ها و سناریو تک مسئول، فقط مسئول ویژگی بر تمامی ویژگی ها نظارت کرده و اسناد کد گذاری و کد گشایی فراهم می کند. در این حالت مسئول ویژگی قدرت زیدی داشته و می تواند تمامی داده ها را کد گشایی کرده و از ویژگی های کاربران مطلع است. اما وقتی فایل دستکاری شود نمی توان حریم کاربر را بازیابی کرد که یکی از نقص های طرح تک مسئول کد گذاری ویژگی محور می باشد.

لذا گزینه ایمن تر و راحت تر برای نظارت بر مجموعه ویژگی ها آن است که از سوی مسئول های متفاوت صورت بگیرد. حال به طور خلاصه به شرح الگوریتم های فرعی می پردازیم:

تشکیل و ساختار: الگوریتم تشکیل پارامتر امنیت λ را به عنوان ورودی اتخاذ کرده و خروجی آن گروه دو خطی و یک سری پارامتر است. پارامترهای $q, g_1, g_2, G_1, G_2, G_T$ عمومی اند. پارامترهای v_k و x_k کلیدهای خصوصی شناخته شده برای مسئول ویژگی و کلیدهای عمومی $y_k = g_1^{x_k}$ و $Y_k = \hat{e}(g_1, g_2)^{v_k}$ شناخته شده برای همه اند. پارامتر $\hat{T}_{k,i}$ نشان دهنده امنیت ویژگی حفظ شده با امنیت مسئول ویژگی بوده و کلید عمومی متناظر برابر $T_{k,i} = g_2^{\hat{T}_{k,i}}$ می باشد.

صدور کلید: کاربر و مسئول ویژگی پروتکل صدور کلید بی نام پیشنهادی در (32) را اجرا می کنند. کاربر اسناد کد گشایی D_{kj} را برای امنیت ویژگی با همکاری با امنیت مسئول ویژگی محاسبه می کند. هنگامی که کاربر به تمامی D_{kj} دست یافت، D_u را پس از $S_{k,i}$ محاسبه می کند.

کد گذاری: الگوریتم کد گذاری مجموعه ای از ویژگی های حفظ شده با مسئولین ویژگی و نیز مجموعه ای از ویژگی ها تعریف شده با دارنده داده ها به عنوان ورودی حفظ می کند. آنگاه متن رمز داده ها را خروجی بیرون می دهد. این مرحله همانند نمونه مسول تک ویژگی می باشد.

کد گشایی: الگوریتم کد گشایی اسناد کد گشایی دریافتی از مسئولین ویژگی ها و پرامترهای پویا به دست آمده از ابزار ههوشمند و متن رمز به عنوان ورودی را دریافت کرده و داده های اولیه را به عنوان خروجی بیرون می دهد.

نرم افزار پروفایل رفتار به طور ایمن مقدار شبکه را ویژگی های مورد نیاز پویا و Y^{SA} محاسبه می کند. کدگشایی

$$h(M(a_{c,1})||M(a_{c,2})|| \dots ||M(a_{c,n})).$$

زمانی موفق است که اگر و تنها اگر

$$h(M(a'_{c,1})||M(a'_{c,2})|| \dots ||M(a'_{c,n})) =$$

باشد.

Setup S: For a given security parameters λ and $\sigma \in \{0, 1\}^{poly(\lambda)}$, group bilinear parameters are generated by the attribute authorities as follows: $q, g_1, g_2, G_1, G_2, G_T \leftarrow S(1^\lambda; \sigma)$. Now, attribute authorities interact with each other and execute the following:

- k^{th} AA randomly chooses $v_k \in_R \mathbb{Z}_q$ and computes $Y_k = \hat{e}(g_1, g_2)^{v_k}$, and sends Y_k to the other attribute authorities, where each AA computes $Y = \prod Y_k = \hat{e}(g_1, g_2)^{\sum v_k}$.
- Each pair of attribute authorities shares a secret, k^{th} authority and j^{th} authority randomly choose $s_{kj} \in \mathbb{Z}_q$ such that $s_{kj} = s_{jk}$.
- k^{th} authority randomly chooses $x_k \in \mathbb{Z}_q$ and computes $y_k = g_1^{x_k}$. Using the shared secret $s_{k,j}$ and u , attribute authorities k and j computes $y_k^{x_j/(s_{kj}+u)}$ and $y_j^{x_k/(s_{kj}+u)}$, respectively.
- k^{th} AA randomly chooses a secret $t_{k,i} \in \mathbb{Z}_q$ for i^{th} attribute, and computes the corresponding public key as $T_{k,i} = g_2^{t_{k,i}}$ ($\forall i \in \{1, \dots, N_k\}$ and $k \in \{1, \dots, K\}$), where N_k is the number of attributes monitored by authority k .

Key Issuing KG: User u executes the following steps with each authority k :

- For $j \in \{1, \dots, K\} / \{k\}$, user gets the $D_{kj} = g_1^{R_{kj}} y_k^{x_j/(s_{kj}+u)}$ for $k > j$ or $D_{kj} = g_1^{R_{kj}} y_k^{(s_{kj}+u)/x_j}$ if $k < j$, where $R_{k,j} \in \mathbb{Z}_q$ is a random value.
- After obtained all D_{kj} , user computes $D_u = \prod_{(k,j) \in \{1, \dots, N\} \times \{1, \dots, N\} / \{k\}} D_{kj} = g_1^{R_u}$, where $R_u = \sum_{(k,j) \in \{1, \dots, N\} \times \{1, \dots, N\} / \{k\}} R_{k,j}$.
- If user u satisfies d_k number of attributes, then k^{th} AA randomly picks a d_k -degree polynomial $p_{k,u}$ with $p_{k,u}(0) = v_k - \sum_{j \in \{1, \dots, K\} / \{k\}} R_{k,j}$.
- Authority k computes $S_{k,i} = g_1^{p_{k,u}(t_{k,i})}$, $i \in [1, \dots, N_k]$, $\forall k$.

Encryption E: Data owner encrypts data m for attribute set $A_m = A_A^1 \cup A_A^2 \cup \dots \cup A_A^K \cup A_C$ as follows (i.e. A_A^k , $\forall k$ denotes the attribute set maintained by k th AA):

- Data owner randomly picks $s_A, s_B \in_R \mathbb{Z}_q$ and encrypts the data as follows: $Enc_m = mY^{s_A}$.
- Data owner computes $E_0 = h(M(a_{c,1})||M(a_{c,2})|| \dots ||M(a_{c,n}))Y^{s_A+s_B}$, $E_1 = g_2^{s_A}$, $\{C_{k,i} = T_{k,i}^{s_A}, i \in A_A^k, \forall k \in [1, \dots, N]\}$.
- Now Data owner uploads $CT_m = \{Enc_m, E_0, E_1, C_{k,i} \forall i \in A_A \text{ and } A_C\}$ into the cloud.

Decryption D

- User downloads CT_m from the cloud and checks the required attributes to decrypt m .
- For each authority k :
 - Using $S_{k,i}$ and the corresponding $C_{k,i}$, user computes $\hat{e}(S_{k,i}, C_{k,i}) = \hat{e}(g_1, g_2)^{s_A p_{k,u}(t_{k,i})}$.
 - User interpolates all $\hat{e}(g_1, g_2)^{s_A p_{k,u}(t_{k,i})}$ and gets $P_{k,u} = \hat{e}(g_1, g_2)^{s_A p_{k,u}(0)} = \hat{e}(g_1, g_2)^{s_A (v_k - \sum_{j \in A_A^k} R_{k,j})}$.
- User multiplies all $P_{k,u}$'s together and gets $Q = \hat{e}(g_1, g_2)^{s_A \sum_{k \in A_A} v_k - s_A R_u} = \frac{Y^{s_A}}{\hat{e}(g_1^{v_k}, g_2^{s_A})}$.
- Now corporate app installed in users' mobile device computes $h(M(a'_{c,1})||M(a'_{c,2})|| \dots ||M(a'_{c,n}))$.
- User can decrypt the data as follows (only if $h(M(a'_{c,1})||M(a'_{c,2})|| \dots ||M(a'_{c,n})) = h(M(a_{c,1})||M(a_{c,2})|| \dots ||M(a_{c,n}))$)

$$Enc_m \cdot \frac{h(M(a'_{c,1})||M(a'_{c,2})|| \dots ||M(a'_{c,n}))Q_0(D_u, E_1)}{E_0} = mY^{s_B} \cdot \frac{h(M(a'_{c,1})||M(a'_{c,2})|| \dots ||M(a'_{c,n}))Y^{s_A}}{h(M(a_{c,1})||M(a_{c,2})|| \dots ||M(a_{c,n}))Y^{s_A+s_B}} = m.$$

شکل 4

6- تحلیل عملکرد

در این بخش، هزینه محاسباتی و ارتباطاتی مربوط به الگوریتم های مسئول منحصر به فرد و چندگانه مطرح شده در این مقاله را تحلیل می کنیم. طوری که در بخش آثار مربوطه گفته شد، آثار مربوط به الگوریتم های پیشنهادی طرح های کدگذاری مبتنی بر ویژگی سنتی اند. لذا کارایی الگوریتم های پیشنهادی با مقایسه آنها در ازای این طرح های سنتی نشان داده می شود.

6-1 پیچیدگی محاسباتی

حال طرح تک مسئول کدگذاری مبتنی بر ویژگی را پس از طرح کدگذاری مبتنی بر ویژگی چند گانه در نظر می گیریم. در طرح تک مسئول کاربر در طی مرحله کدگشایی وارد محاسبه شده و دارنده داده وارد مرحله کدگذاری می شود. می توانیم هزینه های محاسباتی مراحل تشکیل و صدور کلید را نادیده بگیریم چون آنها را می توان در طی زمان بیکاری انجام داد. چون هزینه محاسباتی تابع شبکه ناچیز است زمان محاسباتی را C_p , C_m , C_{ex} در نظر می گیریم. حال فرض می کنیم تعداد ویژگی های کدگذاری n بوده و تعداد کل ویژگی های پویا مورد استفاده دارنده داده ها d باشد که جدول 3 مقدار زمان کل مورد نیاز را نشان داده است. شکل 5 پیچیدگی محاسباتی طرح کدگذاری ویژگی محور را در برابر طرح پیشنهادی نشان می دهد. شکل 6 به مقایسه طرح پیشنهادی و طرح سنتی می پردازد که از لحاظ پیچیدگی زمانی تعداد مختلف مسائل ویژگی می باشد. یکی از نقائص طرح های کدگذاری ویژگی محور آن است که پیچیدگی به طور خطی به ازای تعداد ویژگی های استاتیک افزایش می یابد.

	Testbed 1 (ms)	Testbed 2 (ms)
C_p	14.6	491.2
C_{ex}	2.8	34.1
C_m	1.8	20

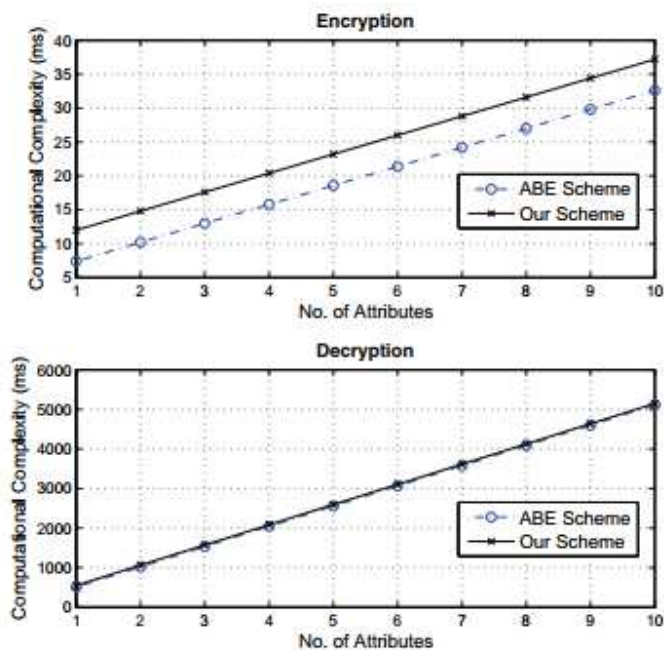
جدول 2

6-2 پیچیدگی ارتباطی

حال به بحث هزینه های ارتباطی طرح های پیشنهادی و طرح های سنتی کدگذاری ویژگی محور می پردازیم. در هر دو طرح هزینه های ارتباطی متکی بر مرحله صدور کلید و بارگذاری و بارگیری داده ها می باشد. چون مرحله صدور کلید به طور خالص متکی بر ارتباط بین مسئول ویژگی و دارنده داده ها است، هزینه ارتباط برای مدل ما و طرح های سنتی برابر است. در طی بارگیری و بارگذاری داده ها، مولفه های افزوده شده به طرح های پیشنهادی E_0 و $A_{C..}$ اند. باید خاطر نشان نمود که اندازه E_0 160 بیت بوده و $A_{C..}$ نشان دهنده ویژگی های پویا به کار رفته در طی کدگذاری است یعنی 2^d تعداد بیت مورد نیاز برای نشان دادن ویژگی های پویا منظور می شود. در کل افزایش در هزینه ارتباطات در الگوریتم پیشنهادی قابل صرف نظر است.

	ABE scheme	Proposed scheme
Enc.	$(n+1)C_{ex} + C_m$	$(n+2)C_{ex} + 2C_m$
Dec.	$nC_p + nC_m$	$nC_p + (n+2)C_m$

جدول 3



شکل 5

7- تحلیل حریم و امنیت

در بخش 3-3 تهدیدات امنیتی و حریم الگوریتم های پیشنهادی را دسته بندی کردیم. در این بخش به بررسی هر مسئله پرداخته و الگوریتم خود و میزان استحکام آن در برابر تهدیدات امنیتی و حریم تایید می کنیم.

7-1 کاهش تهدید هویت

رقیب می تواند به عنوان کاربر یا مسئول ویژگی خود را جا بزند. حال به بحث این موارد می پردازیم. طبق شکل 3 و 4 کلیدهای عمومی مربوط به مسئول های ویژگی به طور آنلاین منتشر شده و کلیدهای متناظر خصوصی برای مقامات شناخته شده است. در عین حال، محاسبه کلیدهای خصوصی از عمومی امکان پذیر نیست. در طی کد گذاری و کد گشایی دارندگان داده ها و کاربران از مسئولین ویژگی استفاده می کنند. دارنده داده و کاربر می تواند از مسئول ویژگی بهره ببرد. ابزار کاربر می تواند در دسترس حمله کننده قرار بگیرد جایی که اسناد ویژگی

استاتیک کاربر در ابزار ذخیره می شود. رفتار مخرب ممکن است شبیه رفتار کاربر مجاز نباشد لذا نرم افزار پروفایل رفتار در حل اجرا در ابزار کاربر شبکه را هوشیار می سازد که درخواست خدمات را رد کند.

	MA-ABE scheme	Proposed scheme
Enc.	$(nk + 2)C_{ex} + C_m$	$(nk + 3)C_{ex} + 2C_m$
Dec.	$(nk + 1)C_p + (nk + 1)C_m$	$(nk + 1)C_p + (nk + 3)C_m$

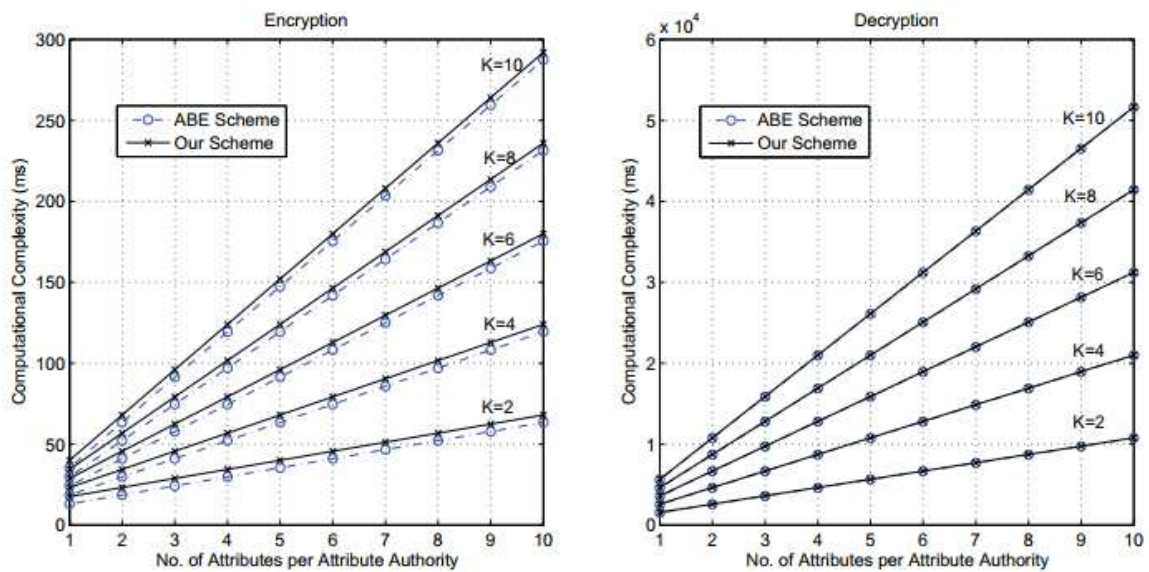
جدول 4

7-2 کاهش تهدیدات حریم

حریم کاربر زمانی آسیب پذیر است که کاربر با مسئولین ویژگی به منظور دستیابی به کلیدهای کد گشایی از جمله صدور کلید در الگوریتم فرعی تعامل برقرار می سازد. طرح های پیشنهادی در بالای ساختار کدگذاری ویژگی محور ایجاد شدند (32). در (32) کاربران و مسئولین ویژگی پروتکل صادر کننده کلید بی نام را اجرا نمودند. در شکل 4 الگوریتم فرعی صادر کننده کلید رمزگشایی کلید برای کاربر u به دست آمده از مسئول برابر می باشد. این D_{kj} با اجرای پروتکل صدور کلید بی نام به دست آمد که در آن هویت کاربر u درون کلید رمزگشایی شامل گردید.

7-3 کاهش حملات برخورد

دو نوع متفاوت حملات برخورد وجود دارد: 1- مسئولین ویژگی می توانند با یکدیگر برخورد کنند و ویژگی های کاربر را دچار اغراق سازند 2- کاربران می توانند کلیدهای رمزگشایی خود را برای دسترسی به داده هایی جمع آوری کنند که کاربران فردی به آن دسترسی ندارد. چون طرح های ما در بالای طرح کدگذاری مبتنی بر ویژگی ساخته شد طرح های پیشنهادی همچنی در برابر برخورد تا $N-2$ ویژگی مقاوم اند. لذا به بحث برخورد کاربر می پردازیم.



شکل 6

در طی صدور کلید الگوریتم فرعی به خاطر پروتکل صدور کلید بی نام ذاتی، کاربر u فقط

را به دست می آورد که در آن هویت کاربر u شامل شده درون کلید رمزگشایی معلوم $D_{kj} = g_1^{R_{kj}} y_k^{x_j/(s_{kj}+u)}$

است. استنباط $x_j/(s_{kj}+u)$ طبق حساب ارشمیدسی از $y_k^{x_j/(s_{kj}+u)}$ امکان پذیر نیست. علاوه بر این، هویت

کاربر بر حسب s_{kj} تصادفی می شود که دستکاری لبا هویت کاربر دیگر غیر ممکن است.

4-7 کاهش فریب ویژگی پویا

نرم افزار پروفایب نصب شده در گوشی کاربر را می توان برای تایید این مطلب به کار برد که آیا کاربر فعلی کاربر

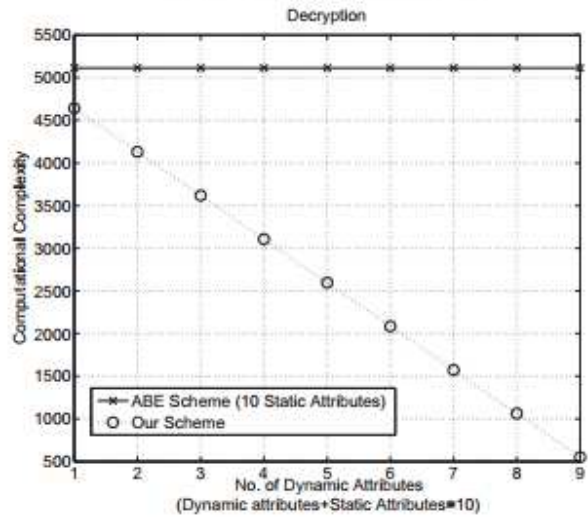
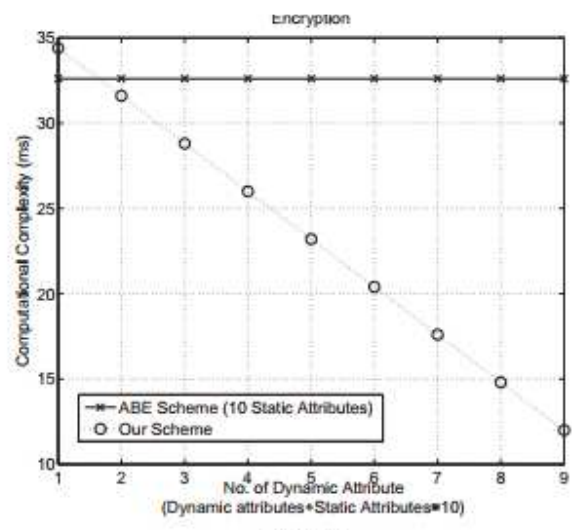
مجاز ابزار است. به هر حال چون نرم افزار پوفایل رفتار درون ابزار کاربر نصب می شود، کاربران مخرب ممکن

است در نرم افزار دستکاری کنند تا اطلاعات نادرست برای ویژگی های پویا در اختیار نهند. از جمله نرم

افزارهای ناکس سامسونگ و بی ای اس بلک بری می توانند به طور ایمن صحت و تمامیت داده ها را شناسایی

کنند بدون آنکه در کارکرد کریر اختلال ایجاد کنند. این سکوهای نرم افزاری می توانند به طور ایمن در نرم

افزارهای شرکتی نصب شوند.



شکل 7

5-7 کاهش حمله ردیابی

در بخش قبل کاربر رقیب را بررسی کردیم. به هر حال کارفرما یا دارنده داده ها می توانند رقیب باشند چون نرم افزار پروفایل رفتاری آنها داده های حس گر را از ابزار کاربر جمع آوری می کند. اگر نرم افزار مخرب باشد، آنگاه معلوم است که داده های حس گر را به کارفرمایا یا شخص ثالث می فرستد که می تواند بر داده ها نظارت داشته باشد. به هر حال بر طبق الگوریتم پیشنهادی، ضرورتی ندارد داده های حس گر را خارج از ابزار موبایل ارسال کرد.

7-6 تحلیل امنیت

قضیه 1. طرح پیشنهادی به طور معنایی در برابر حمله ساده متنی در مدل هویت انتخاب ایمنی است اگر تابع قابل صرف نظر ϵ وجود داشته باشد به طوری که در بازی امنیتی شرح داده شده در قبل هر گونه رقیب با احتمال $\frac{1}{2} + \epsilon$ موفق گردد.

اثبات. فرض کنید که رقیب زمان چند جمله ای احتمالی وجود دارد که میتواند الگوریتم ما را شکسته و چالش گری باشد که بتواند فرض ام بی دی اچ تصمیمی را با بهره گیری نقض کند. فرض می کنیم چالش گری $[g_1^a, g_1^b, g_1^c, Z]$ را در اختیار داشته و اگر پالش گری بخواهد فرض م بی دی اچ را نقض کند آنها باید $Z = e(g, g)^{\frac{ab}{c}}$ یا حداقل احتمال $\frac{1}{2} + \epsilon$ را تعیین کند.

فرض می کنیم رقیبی وجود دارد که می تواند الگوریتم پیشنهادی را بشکند. نشان می دهیم چالش گری می تواند از این رقیب برای نقض فرض ام بی دی اچ استفاده کند لذا وی باید $[g_1^a, g_1^b, g_1^c, Z]$ را درون الگوریتم پیشنهادی شامل سازد. فرض می کنیم رقیب کلید خصوصی γ را درخواست می کند. ابتدا تعریف می کنیم که $\Gamma = |\Gamma \cap \alpha|$, Γ' می تواند مجموعه ای باشد که داشته باشیم $\Gamma \subseteq \Gamma' \subseteq \gamma$, $|\Gamma| = d - 1$ و $S = \Gamma' \cup \{0\}$. حال کلیدهای $D_u(i)$ برای $i \in \Gamma'$ طبق زیر تعریف می کنیم اگر $i \in \Gamma$ آنگاه $D_u(i) = g^{s_i}$ که در آن $s_i \in \mathbb{Z}_p^*$. ما چند جمله ای $q(x)$ با درجه $d-1$ را انتخاب کردیم به طوری که اگر $i \notin \Gamma'$ آنگاه:

$$D_u(i) = \left(\prod_{j \in \Gamma} c^{\frac{\beta_j \Delta_j S(j)}{w_i}} \right) \left(\prod_{j \in \Gamma' - \Gamma} g^{\frac{\lambda_j \Delta_j S(j)}{w_i}} \right) \left(Y^{\frac{\Delta_0 S(0)}{w_i}} \right).$$

طبق این چند جمله ای چالش گری می تواند $D_u(i) = g^{\frac{q(i)}{t_i}}$ را به ازای $i \notin \Gamma'$ حل کند. حال رقیب دو پیام m_1 و m_2 را به چالش گری می فرستد. شبیه سز کد گذاری m_u را برمی گرداند. متن رمز $CT_m = \{E_0 = h(M(a_{c,1}) || \dots || M(a_{c,n}))\}_{m_u, Z, E_i = B_{i \in \alpha}^{P_i}}$. خروجی می باشد. اگر $v = 0$ آنگاه

$Z = e(g, g)^{\frac{ab}{c}}$. اگر فرض کنیم $s_A + s_B = \frac{b}{c}$ ، آنگاه داریم

$$E_i = \frac{B^{\beta_i}}{r^{s_B}} = g^{b\beta_i - s_B} = g^{\frac{b}{c}c\beta_i - cs_B} = (T_i)^{s_A} \quad \text{و} \quad E_0 = h(M(a_{c,1}) || M(a_{c,1}) || \dots || M(a_{c,n})) m_v \bar{Y}^{s_A + s_B}$$

لذا متن رمز کدگذاری تعیین شده تصادفی پیام m_v تحت کلید عمومی آلفا می باشد. اگر $v = 1$ ، آنگاه

$Z = g^z$ سپس داریم $E_0 = h(M(a_{c,1}) || M(a_{c,1}) || \dots || M(a_{c,n})) m_v e(g, g)^z$. چون تصادفی است آنگاه

E_0 عنصر تصادفی بوده و رقیب پیامی را مشاهده می کند که حاوی اطلاعات m_v نمی باشد. در اینجا تاکید

داریم که CT_m کد گذاری معتبر پیام m_v است اگر $Z = e(g, g)^{\frac{ab}{c}}$. لذا رقیب باید این مزیت ϵ را داشته

باشد. لذا اگر رقیب درست حدس بزند، آنگاه چالش گر حدس می زند که $Z = e(g, g)^{\frac{ab}{c}}$ و اگر رقیب خطا کند

آنگاه چالش گر حدس می زند که $Z \neq e(g, g)^{\frac{ab}{c}}$. لذا چالش گر مزیت $\frac{\epsilon}{2}$ در تمایز $Z = e(g, g)^{\frac{ab}{c}}$ دارد.

از این رو، رقیبی که طرح ما را با مزیت ϵ می شکند این مفهوم را می رساند که الگوریتم نقض فرض ام بی دی

اچ یا مزیت غیر قابل صرف نظر $\frac{\epsilon}{2}$ می باشد. می توانیم به این نتیجه برسیم که طرح پیشنهادی هویت انتخابی

ایمن است.

به طور مشابه این اثبات را می توان در سیستم چند مسئولیتی بسط داد. طبق (32) می توانیم مسئولیت را به

دو گروه صادقانه و غیر صادقانه تقسیم کنیم. نخست بابد پارامترهایی تشکیل دهیم تا بتوانیم مسئولین خود را به

عنان متناظر با بخش ماحاسبه ناپذیر کلیدا صلی تطبیق دهیم. آنگاه م سؤال ویژگی k^* به طور تصادفی از بین

پارامترها بر اساس این مقدار محاسبه ناپذیر انتخاب می شود. اگر معلوم شود که این مقام صادقانه که از آن

رقیب ویژگی های ناکافی برای کاربر u درخواست دارد می توانیم راهبرد بالا را مجدد استفاده کنیم (32).

8- نتایج، محدودیت ها، آثار آتی

در این مقاله، راهبرد کنترل دسترسی مستحکم را مطرح نمودیم که شامل ویژگی های ایجاد شده با ابزارهای

هوشمند جهت ایمنی بخشی به دسترسی سنتی چارچوب کنترل می باشد. در طرح های پیشنهادی صاحب داده

ها ویژگی های پویا ابزاره و شمند را با ویژگی های ایستا اقب تعیین شده در هم می آمیزد. این رویکرد لایه اضافی امنیت را به بالای چارچوب کنترل دسترسی اضافه می کند. نشان دادیم که کارایی های طرح های پیشنهادی قابل قیاس با طرح های سنتیاند و امنیت و انعطاف پذیری بهتری برای شبکه محاسبه موبایل فراهم می سازند.

8-1 محدودیت و کارهای آتی

جمع آوری و پردازش داده های حس گر برای تعیین مقادیر ویژگی های پویا، زمان و پیچیدگی ارتباطات را افزایش می دهد. در حال حاضر فرض می شود این کار به طور آف لاین و به موازات دانلود داده های کدگذاری شده از ابر انجام می شود. ارزیابی این امر برای ابزارهای هو شمند متفاوت در محیط های گوناگون امری بالقوه است. محدودیت دیگر دقت تعداد الگوریتم های موجود برای تعیین رفتار کاربر می باشد. گسترش بالقوه می تواند توسعه نرم افزاری باشد که داده ها را از سنسورهای هو شمند جمع آوری می کند. توسعه الگوریتم تازه با استفاده از راهبردهای یادگیری ماشینی جهت دسته بندی کاربرها بر اساس رفتار را می توان برای پروفایل کاربر به کار برد. در ادبیات چندین نوع کی پی- کد گذاری مبتنی بر ویژگی وجود دارد که با مدل امنیت یا بهبود پیچیدگی راهبرد کدگذاری سریع و برون سپاری محاسبات جفتی با ابر امنیت را ارتقا می دهند یعنی افزودن ویژگی در بالای این طرح ها پیچیدگی و نیز امنیت را افزایش می دهد.



این مقاله، از سری مقالات ترجمه شده رایگان سایت ترجمه فا میباشد که با فرمت PDF در اختیار شما عزیزان قرار گرفته است. در صورت تمایل میتوانید با کلیک بر روی دکمه های زیر از سایر مقالات نیز استفاده نمایید:

لیست مقالات ترجمه شده ✓

لیست مقالات ترجمه شده رایگان ✓

لیست جدیدترین مقالات انگلیسی ISI ✓

سایت ترجمه فا ؛ مرجع جدیدترین مقالات ترجمه شده از نشریات معتبر خارجی