گزارش مقاله

SECURE BIO-RFID SYSTEM IN ORGANIZATIONS

سیستم BIO-RFID امن در سازمان ها

نام دانشجو : محمد ایمان برادر

نام استاد : دکتر سمیه جاسبی

دانشگاه آزاد اسلامی واحد علوم تحقیقات – دانشکده مکانیک و برق و کامپیوتر

رشته تحصیلی: دکتری کامپیوتر

گرایش: معماری سیستم های کامپیوتری

بهار ۱۴۰۰

۱- تعریف مساله و هدف اصلی مقاله

۱-۱ سوال اصلی مطرح شده در مقاله چیست؟

امروزه کارتهای RFID تقریباً در همه کارهای روزمره ما مورد استفاده قرار می گیرند و آنها را بدون تماس می کند. ما درهایی با کارت کنترل دسترسی و اعتبار/ بدهی داریم که از پرداخت های بدون تماس استفاده می کنند. ما تقریباً در همه سازمانها کارتهای کارمند یا دانشجو داریم که از فناوری RFID برای خدمات استفاده می کنند. در سازمان ها ، این کارت های RFID به اسناد و دارایی های خصوصی دسترسی پیدا می کنند ، که اگر این فناوری دارای جریان و مسائل امنیتی باشد ، خطر نگران کننده ای است. در صورت پرداخت بدون تماس ، شخص باید کارت را بکشد یا کارت را روی خواننده قرار دهد تا معامله کامل شود. هیچ راهی یا روشی برای احراز هویت واقعی کاربر به غیر از اطلاعات موجود در برچسب وجود ندارد. در بدترین سناریو ، اگر کارت به اشتباه وارد شده باشد ، دشمن می تواند به تمام دارایی های خصوصی و اسناد مهم شخص دسترسی پیدا کند. به همین ترتیب ، آن شخص می تواند معاملات بدون تماس و بدون هیچ گونه ردپای داده ای از خود انجام دهد. علاوه بر این ، برچسب های RFID فعلی به راحتی تکثیر می شوند ، این بدان معنی است که سرویس هایی که از RFID در یک سازمان استفاده می کنند در معرض خطر هشدار دهنده ای قرار دارند. همچنین در مواردی که اطلاعات کاربر به راحتی در معرض دید دیگران قرار می گیرد ، مسائل مربوط به حریم خصوصی ایجاد می شود. همچنین ، جیب بری دیجیتالی که با بازیابی اطلاعات از نزدیک یا از طریق خواننده انجام می شود ، یک مسئله امنیتی نگران کننده است. راه حل پیشنهادی با هدف ادغام بیومتریک و RFID با استفاده از آخرین فن آوری ها انجام می شود.

۱-۲ چه مشکلی باید برطرف شود؟

عدم وجود امنیت در فاش شدن اطلاعات هویتی کارت های RFID همیشه از جمله مشکلات تحقیقات در حوزه RFID بوده است به این معناست که اطلاعات مالک RFID از امنیت کافی برخوردار نیست همچنین با توسعه فناوری دیجیتال در سراسر جهان ، هکرهای مخرب در حال یافتن راه هایی برای نفوذ به فناوری های مورد استفاده مردم هستند. اگر ما تقریباً در همه کارهای روزمره از دسترسی به ساختمان ، پارک ماشین و خرید یک قهوه در استارباکس از RFID استفاده می کنیم ، احتمال زیادی وجود دارد که هر کسی با ابزار و سخت افزار مناسب بتواند کارت ما را تکثیر کند و از خدمات مشابه استفاده کند و مشکل دیگر این که RFID مجوز کاربر را

ارائه نمی دهد یعنی شما می توانید با در دست داشتن کارت RFID دیگری تمام حساب بانکی او را سرقت ببرید و کسی در لحظه متوجه نشود.

۱-۳ چه ضرورتی برای مطرح شدن مسئله است؟

در این دوره مدرن که فناوری دیجیتال درگیر طوفان جهانی است ، بیومتریک نقش مهمی در امنیت پزشکی قانونی داشته است. برای شناسایی از الگوهای منحصر به فرد صفات بیولوژیکی یا فیزیکی کاربر استفاده می کند. چون تقریباً غیرممکن است که ۲ نفر یکسان باشند در ویژگی های بیومتریک ، این فناوری همچنین در چندین سازمان به عنوان یک اقدام امنیتی مانند کنترل دسترسی و شناسایی شخصی مورد استفاده قرار گرفته است. چندین بیومتریک در دنیای مدرن مانند اسکن اثر انگشت ، اسکن عنبیه و تشخیص چهره وجود دارد. این موارد به عنوان محافظتی برای داده های مهم در برابر حملات احتمالی هکرها با استفاده از روش هایی مانند brute force اجرا می شوند ، زیرا عبور از نام کاربری و رمزهای عبور آسان است.

برای دستیابی به یک دنیای دیجیتال ، این فناوری در حال حاضر در گذرنامه های الکترونیکی در سراسر جهان و برنامه های معاملاتی تلفن همراه مانند Apple Pay و Samsung Pay مورد استفاده قرار گرفته است که به نوعی شناسایی بیومتریک مانند اسکن اثر انگشت ، تشخیص چهره و اسکن عنبیه نیاز دارد. . به طور مشابه ، فناوری RFID در کارت های خودپرداز مانند Visa، Mastercard و American Express استفاده شده است. اکثر سازمان ها از جمله دانشگاه آسیا و اقیانوس آرام از فناوری RFID برای انجام کارهای مختلف از کنترل دسترسی تا پرداخت استفاده می کنند. متأسفانه ، هیچ راهی برای شخص وجود ندارد تا در واقع کارهای انجام شده از طریق کارت را تأیید کند. این بدان معنی است که هر شخصی می تواند از کارت متعلق به شخص دیگری استفاده کند.

از این رو ، تلفیق بیومتریک و RFID انقلابی در امنیت شخصی در این سازمان ها ایجاد خواهد کرد. این پروژه نه تنها به چگونگی پیاده سازی فناوری بلکه به منظور کاهش مسائل امنیتی در هر دو فناوری در پیگیری ایمن ترین سیستم Bio-RFID متمرکز است.

۱- ٤ چه روشهایی قبلا برای این کار انجام شده؟

از آنجا که از فناوری RFID و بیومتریک در سراسر جهان در چندین سازمان استفاده شده است ، محققان و کارشناسان جهانی اهمیت بالایی در ایجاد امنیت آنها قائل شده اند. چندین تحقیق و مقاله در مورد چگونگی امکان تلفیق این دو فناوری و چگونگی ایجاد انقلابی در احراز هویت منتشر شده است. به همین ترتیب ، پالایش

امنیت داده ها در داخل RFID به عنوان یک موضوع تحقیقاتی بزرگ برای بسیاری از محققان در سراسر جهان تبدیل شده است. از این رو ، چندین پیشنهاد برای دستیابی به امنیت و غیرقابل کنترل بودن این دستگاه ها وجود دارد.

- درحوزه دستگاه های RFID غیرفعال:

اکثر برچسب های RFID منفعل هستند ، به این معنی که منبع تغذیه فعال به عنوان باتری ندارند. این برچسب های RFID برای تغذیه مدارهای RFID با استفاده از ترکیب یکسوسازها و خازن ها از خواننده های برگشتی استفاده می کند. (Lowe، ۲۰۱۵) حق ثبت اختراع منتشر شده توسط آقای Lowe نشان می دهد که چگونه RFID و Biometrics می توانند ادغام شوند. لوو همچنین به چالش دیگر پیاده سازی از جمله فناوری ، پیکربندی ها و پروتکل های متعدد استفاده شده در RFID های فعلی اشاره کرد. این پروتکل های مختلف از فرکانس ها ، تعداد بیت ها و طرح های مختلف استفاده می کنند. ۲ پروتکل اصلی عبارتند از پروتکل Global Proximity که از میدان تحریک ۱۲۵ کیلوهرتز و پروتکل ISO1443 / ITEC که از میدان تحریک ۱۳,۵٦ مگاهرتز استفاده می کند. (Lowe ، ۲۰۱۵). لوو پیشنهاد کرد که نصب ماژول های مختلف در تعداد زیادی از دستگاه ها ، مسائلی را که کل فرآیند را به صرفه می کند و جلوگیری از مشکلات مربوط به استانداردها و پروتکل های مختلف صنعتی را حل می کند. علاوه بر این ، هنگام اجرای راه حل ، می توان با استفاده از بلوک های عملکردی برای پردازش RFID و بیومتریک ، مصرف برق را تا حد زیادی کاهش داد.

- درحوزه تلفیق بایومتریک و RFID برای احراز هویت:

(Srivastava، K. Awasthi and Mithal، ۲۰۱۸) پیشنهاد کردند که با استفاده از ژنراتور PRNG و یک تابع هش بیومتریک برای احراز هویت متقابل برچسب و حامل آن می تواند امنیت برچسب RFID را افزایش دهد و از دسترسی غیر مجاز جلوگیری کند . این راه حل دارای دو مرحله است. مرحله ثبت نام و مرحله احراز هویت متقابل. در مرحله ثبت نام ، کاربر الگوی بیومتریک خود را در برچسب RFID و رمزگذاری شده آن با استفاده از یک عملکرد هش قوی ثبت می کند. در مرحله دوم ، داده ها با استفاده از یک سرور مقایسه و احراز هویت می شوند. تجزیه و تحلیل امنیتی در آنجا نشان داد که راه حل پیشنهادی سرکشی عظیمی در برابر حملات متداول مانند جعل و حملات Man-in-the-middle دارد. (Bian و همکاران ، ۲۰۲۰) همچنین یک راه حل مشابه ارائه داده است که در آن آنها از PUF عملکرد غیرقابل جسمی غیرفعال کننده ، استخراج کننده فازی و بیومتریک برای طراحی یک پیشنهاد احراز هویت به نام Bio-AKA استفاده می کنند که به عنوان احراز هویت دو عاملی عمل می کند. استفاده از استخراج کننده فازی و PUF در محلول پیشنهادی نفوذ در امنیت را تقریباً غیرممکن می کند.

(Dargan & Kumar، ۲۰۲۰) اظهار داشتند که سیستم های بیومتریک با موفقیت نیازهای دنیای مدرن دیجیتال را جلب می کنند. سیستم های بیومتریک در مقایسه با تدابیر امنیتی قدیمی مانند رمز عبور و کد PIN از امنیت و اطمینان بیشتری برخوردار هستند زیرا به راحتی از یک پایگاه داده هک می شوند. علاوه بر این ، شناسایی مکرر کاربر با اقدامات خودکار داخلی ، باعث افزایش امنیت سیستم می شود و روند احراز هویت را سریعتر و ایمن تر می کند. علاوه بر این ، (Nappi، Ricciardi and Tistarelli، ۲۰۱۸) اشاره کردند که به دلیل عدم سازش بالاتر سیستم بیومتریک در برابر تهدیدها و حملات ، نیاز به تغییر اینترنت از چیزهای بیومتریک است.

- درحوزه امنیت داده های ذخیره شده در RFID با استفاده از رمزگذاری و پروتکل ها:

(یونگ ، یونگ و یون ، ۲۰۱۷). راه حلی برای تأیید اعتبار و جلوگیری از قرار گرفتن اطلاعات در مورد کاربر برچسب RFID با هکرها با استفاده از PUF پیشنهاد کرد. این کار با ایجاد مقدار پاسخ به مقدار چالش در طی فرآیند انجام می شود. واحد دریافت کننده شامل شناسه خواننده است در حالی که واحد ذخیره سازی شامل شناسه برچسب RFID و اولین مقدار چالش است. احراز هویت با انتقال چندین کد احراز هویت بین خواننده و RFID در پاسخ به مقادیر مختلف چالش انجام می شود.

(Srivastava، K. Awasthi and Mithal، ۲۰۱۸) پروتکلی را ارائه داد که در آن از PRNGمولد تعداد شبه تصادفی و از تابع هش قوی استفاده می شود. آنها از مکانیزم شناسایی استاتیک استفاده می کنند که در آن برچسب شناسه به جای تغییر شکل در مکانیزم شناسایی دینامیک ، در طول فرآیند احراز هویت به طور مداوم ثابت باقی می ماند. با این حال ، هر دو این مکانیزم ها به دلیل استفاده از PRNG در برابر حملات آسیب پذیر نیستند. هدف از این روش افزایش کارایی و کاهش هزینه استقرار به دلیل بسته های توابع هش مورد استفاده در این فناوری است.

(Bian و همکاران ، ۲۰۲۰) طرح احراز هویت دو عاملی را با استفاده از PUF، Fuzzy Extractors و biometrics پیشنهاد کردند. استخراج کننده های فازی در طول ثبت نام و ورود به سیستم یک الگوی بیومتریک را جمع آوری و بازیابی می کنند. طرح پیشنهادی هیچ داده بیومتریک را در ذخیره سازی دستگاه ذخیره نمی کند تا خطر نشت را به حداقل برساند. (Kardaş و همکاران ، ۲۰۱۲) پروتکل مشابهی را پیشنهاد می کنند که از PUF برای جلوگیری از حملات کانال جانبی برچسب RFID استفاده می کند که در آن اطلاعات حساس RFID به دلیل مجوزهای حساب و مناطق حافظه محافظت شده در معرض آن قرار دارد. این کار با استفاده از PUF و سایر رمزنگاری های قوی در برچسب و رمزنگاری کلید عمومی در خواننده انجام می شود.

- درحوزه استگانوگرافی در RFID برای جلوگیری از شبیه سازی:

تحقیق در مورد چگونگی اجرای استگانوگرافی برای جلوگیری از جعل موضوع بسیار جالبی بوده است. استگانوگرافی ، هنر پنهان کردن داده ها در داخل داده ها و رمزنگاری ، دوعالی برای جلوگیری از شبیه سازی است. (Al Hamami & Alhafez، ۲۰۱٦) راه حلی را پیشنهاد داده است که از استگانوگرافی برای ذخیره یک مقدار محاسبه شده مخفی در تصویر استفاده می کند. در طی فرایند تبادل کلید Diffie-Hellman ، خواننده مقداری را از طریق شبکه رمزگذاری شده ایمن ضبط می کند. این مقدار با مقداری که توسط خواننده در عکس ذخیره شده مقایسه می شود. اگر هر دو مقدار مشابه باشند ، اسناد کلون یا جعل نشده اند. برعکس ، خواننده به سیستم در مورد جعل هشدار می دهد که مکانیزمی ایمن برای شناسایی شبیه سازی ایجاد می کند. به همین ترتیب ، (Wimalasiri & Jeyamohan، ۲۰۱۸) یک راه حل مشابه پیشنهاد داده است که در آن یک علامت علامت دیجیتال با استفاده از یک کلید صحیح ٤ رقمی تصادفی در تصویر ذخیره می شود. این راه حل پیشنهاد استفاده از رمزگذاری AES (Advanced Encryption Standard) برای ذخیره داده های مربوطه در پایگاه داده هنگام ثبت نام به همراه داده های علامت چاپ و کلید رمزگذاری است. در طول تأیید ، داده های بازیابی شده و داده های ذخیره شده در پایگاه داده برای بررسی اعتبار و قانونی بودن سند مقایسه می شود.

۱- ۵ روش پیشنهادی ارائه شده چیست؟

سیستم RFID بیومتریک از یک حسگر اثر انگشت و یک تراشه RFID تشکیل شده است.کاربر می تواند اثر انگشت خود را در کارت RFID ثبت کند. هنگام تکمیل معامله یا فرآیند با استفاده از کارت ، کاربر انگشت خود را برای احراز هویت روی حسگر قرار می دهد. معامله یا فرآیند فقط درصورتی انجام می شود که اثر انگشت با کاربر مجاز مطابقت داشته باشد و احراز هویت دو عاملی را امکان پذیر می کند. اعتقاد بر این است که این فناوری به راحتی در سازمانها اجرا می شود زیرا خوانندگان RFID موجود نیازی به جایگزینی با خوانندگان جدید ندارند ، و این باعث می شود کل فرآیند مقرون به صرفه باشد.

هدف این مقاله ایمن سازی فناوری کنونی RFID برای کاهش خطرات مرتبط با استفاده از RFID در سازمان ها است. سیستم Bio-RFID به اعتبار قانونی حامل کارت کمک می کند تا کارت را قابل اعتمادتر و محافظت کند. علاوه بر این ، این سیستم با سیستم RFID فعلی بر مشکلات امنیتی غلبه خواهد کرد.

اهداف سیستم عبارتند از:

- از شبیه سازی و تکثیر داده ها در RFID جلوگیری کنید: این سیستم جدید با استفاده از پروتکل های PUF و رمزگذاری قوی همراه با استگانوگرافی برای کاهش هرگونه تهدید به دستکاری و تکثیر داده ها در داخل تراشه RFID ، بازیابی اطلاعات درون RFID را برای هر هکر تقریباً غیرممکن می کند.

- از داده های داخل RFID محافظت کنید: با استفاده از فناوری PUF، RFID با استفاده از چندین انتقال کد تأیید اعتبار بین برچسب RFID و گیرنده ، از نظر فیزیکی غیرقابل حذف است.
- مجوز ایمن را در RFID ارائه دهید: با تلفیق بیومتریک اثر انگشت و RFID ، این سیستم انقلابی در صنعت RFID ایجاد خواهد کرد. با استفاده از آخرین فن آوری اسکن اثر انگشت ، احراز هویت متقابل بایومتریک و RFID ، احراز هویت دو عاملی در RFID قرار می گیرد.

۲- توضیح راه حل پیشنهادی مقاله برای حل مسئله

۲-۱ روش پیاده سازی شده برای حل مسئله مقاله به چه صورت است؟ (بصورت گام به گام توضیح داده شود)

سیستم پیشنهادی از کارتهای RFID بیومتریک با رمزگذاری داخلی مانند PUF عملکرد غیرقابل حذف فیزیکی و AES سیستم رمزگذاری پیشرفته استفاده خواهد کرد. علاوه بر این ، یک علامت دیجیتال دیجیتالی در پایگاه داده کاشته می شود تا از کلون شدن کارت جلوگیری کند. سیستم پیشنهادی ما در کارتهای RFID بیومتریک و کارتهای RFID معمولی استفاده خواهد شد. موارد عادی و بدون سنسور بیومتریک به برنامه تلفن همراه در دستگاه همراه با نوعی بیومتریک به عنوان احراز هویت احتیاج دارند.

پس از دریافت کارت ، کاربر با استفاده از سنسور داخلی یا دستگاه تلفن همراه بایومتریک خود را ثبت می کند. الگوی بیومتریک توسط استخراج کننده فازی بازیابی می شود و سپس با مقدار هش در سرور همراه با داده های دیگر رمزگذاری می شود. در هنگام تأیید ، کارت داده ها و هش های موجود در سرور را با داده های بازیابی شده از سنسور مقایسه می کند. اگر اعتبار و داده مطابقت داشته باشد ، روند ادامه می یابد. برای هر کار یا فرآیند انجام شده از طریق کارت ، یک فرآیند احراز هویت متقابل انجام می شود تا حامل کارت مالک تأیید شده باشد. این سیستم از PRNG ، یک عملکرد هش قوی و پروتکل PUF برای تولید یک عدد تصادفی برای برقراری ارتباط با خواننده با استفاده از مقادیر مختلف چالش و پاسخ جلوگیری می کند تا از حملات احتمالی مانند جیب بری دیجیتال ، اسکیمینگ و غیره جلوگیری کند. از این رو ، این پروتکل موج رادیویی ایمنی ایجاد می کند اتصال بین دو دستگاه تمام کارهایی که از طریق کارت RFID با استفاده از برنامه تلفن همراه انجام می شود ، به کاربر اطلاع می یابد. به همین ترتیب ، سیستم از استگنوگرافی پیشرفته در جایی استفاده می کند که در آن مقدار علامت چاپی با استفاده از PRNG ایجاد می شود و هنگام ثبت نام در یک تصویر تعبیه شده است. این مقدار رمزگذاری

شده و در پایگاه داده سرور بارگذاری می شود. برای تعیین اصالت کارت ، مقدار در هنگام تأیید بررسی و مقایسه می شود.

۲- ۲ روش ارائه شده به چه صورت پیاده سازی شده؟(نرم افزاری یا بصورت اثبات ریاضی دقیقا توضیح داده شود)

مقاله به صورت مطالعاتی و مروری است و فاقد پیاده سازی است.

۲-۳ نحوه مقایسه ایده مطرح شده با دیگر ایدههای مطرح شده در مقاله

در این مقاله مقایسه ایده پیشنهادی با گذشته از نظر امنیت و چگونگی کاهش کلاهبرداری و سواستفاده از کارت های RFID مطرح گردید.

۳- نقاط قوت و ضعف مقاله

نقاط قوت : علیرغم چالشها و محدودیتهای متعددی که مانع استقرار سیستم در سازمانها می شود ، سیستم قطعاً از چندین جنبه امنیتی جواب می دهد و به سود سازمان است. زیرساخت های امنیتی سازمان با احراز هویت کارمندان و سهامداران پیشرفت می کند. خطر دسترسی غیر مجاز با استفاده از احراز هویت بیومتریک کاهش خطر نقض سیستم کاهش می یابد. اطلاعات حساس همچنین با استفاده از رمزگذاری قوی ایمن خواهد بود. از آنجا که بسیاری از سازمانها در حال توسعه اکوسیستم هستند که از طریق کارت داده شده توسط سازمانها امکان معاملات را فراهم می کند ، این سیستم به ایمن و مطمئن بودن فرآیند پرداخت برای کاربر کمک می کند.

نقاط ضعف : کارتهای بیومتریک هنوز در دست ساخت هستند که استفاده از کارتهای RFID بیومتریک را در سیستم محدود می کند.

٤- جمع بندی و پیشنهادات برای کارهای آتی

به عنوان یکی از اهداف اصلی سیستم ارائه تأیید هویت مطمئن از کاربر ، سیستم قطعاً تعداد کلاهبرداری ها و سواستفاده ها را کاهش می دهد. به همین ترتیب ، سیستم از نشت اطلاعات حساس که باعث حفظ یکپارچگی در یک سازمان می شود جلوگیری می کند. علاوه بر این ، وظایف روزمره ای که به نظر ما مسلم است ، باعث می شود ما از تهدیدهای دیجیتالی مختلف جلوگیری کنیم. همچنین شبیه سازی و سواستفاده از کارت ها به دلیل ادغام رمزنگاری و استگانوگرافی به شدت کاهش می یابد.

بنابراین ، این سیستم احراز هویت ایمن وظایف روزمره را که کاربر با استفاده از بیومتریک ، رمزنگاری ، استگانوگرافی و کارتهای RFID انجام می دهد و بدون هیچ زحمتی فرآیند احراز هویت را انجام می دهد. بعلاوه ، این سیستم به عنوان یک دیوار آتش در سازمانی عمل خواهد کرد که تقریباً از همه تهدیدهای خارجی جلوگیری می کند. این سیستم باعث ایجاد آگاهی در جامعه مدرن در مورد حملات دیجیتالی و اهمیت امنیت شخصی و حریم خصوصی می شود.

در پیشنهادات کار های آینده می توان به استفاده از BIO-RFID پیشنهادی در ابعاد میکرو در بدن انسان نام برد.

۵- شبیه سازی

مقاله به صورت مطالعاتی و مروری است و فاقد شبیه سازی است.