بررسی روش های مبتنی بر بیومتریک برای حفظ امنیت سیستم شبکه بی سیم بدن

مریم سلیمیان ، بهرنگ برکتین*
دانشکده مهندسی کامپیوتر، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

چکیده - شبکه بی‌سیم بدن (WBAN) یک تکنولوژی جدیداست که خدمات بهداشتی درمانی برای کنترل بیمار از راه دور ویا تصمیم گیری در مورد درمان وی ارائه می‌دهد . این سیستم دارای سه لایه است وبا تمام محاسنی که داردمشکلاتی از قبیل مسیریابی ، محدودیت انرژی وحفظ امنیت داده هارا نیز دارا می باشد .به دلیل آنکه WBAN با اطلاعات پزشکی حیاتی سر وکار دارد ارائه امنیت در این شبکه بسیار مهم است .بنابراین باید امنیت داده ها در زمان جمع آوری ،پردازش وانتقال آنها حفظ شود .منظور از امنیت ،حفظ محرمانگی و صحت داده ها می باشد .درراستای حل مشکل حفظ امنیت سیستم WBAN روش هائی ارائه شده است .در این مقاله روش ها ی استفاده شده براساس کلید دسته بندی وبا هم مقایسه شده اند،با توجه به مقایسه انجام شده راحت ترین و مناسب ترین ویژگی بیومتریک به عنوان کلید ، ویژگی بیومتریک اثر انگشت می باشد.

کلمات کلیدی : شبکه بی‌سیم بدن ، امنیت ، بیومتریک ، اثرانگشت

۱- مقدمه :

شبکه بی‌سیم بدن (WBAN) سیستمی است که خدمات بهداشتی درمانی را ارائه می‌دهد و امروزه برخی از مردم برای بهبود و ارتقاء سطح زندگی‌خود ازآن استفاده می‌نمایند.WBAN تکنیکی است که از آن برای رصد سلامت بیمار از راه دور و گردآوری اطلاعات مربوطه از طریق حسگرهای تعبیه‌شده استفاده می‌شود. یک WBAN شامل تعدادی حسگر کوچک، کم‌وزن و یک هماهنگ‌کننده(PDA) می‌باشد. حسگرها می‌توانند داخل بدن، روی پوست و اطراف آن قرار گیرند و اطلاعات جمع‌آوری و ارسال نمایند. سیستم WBAN پارامترهای معین بدن از قبیل ECG ، EEG ، دما ، فشار خون ، ضربان قلب ، قند خون و سایر پارامترها را محاسبه می‌کند.این سیستم اصولاً در۳ لایه طراحی می‌شود. در لایه اول داده‌ها توسط سنسورها از بدن انسان جمع‌آوری می‌شوند .در لایه دوم داده‌ها به سرور منتقل می‌شوند.در لایه سوم سرور (پزشک) با بررسی داده ها عمل موردنیاز را مشخص می‌نماید. این سیستم علاوه بر مزایایی که داردبا مشکلاتی مانند حفظ امنیت داده ها ، محدودیت انرژی و مسیریابی همراه است . از آنجایی که داده‌های موجود در این سیستم پزشکی است از اهمیت بالایی برخوردارند . بنابراین باید امنیت داده‌ها حفظ شود. امنیت بدین معنا است که داده در هنگام جمع‌آوری، انتقال، پردازش و ذخیره‌سازی در برابر دسترسی کاربران غیرمجاز به‌طور امن محافظت گردد تا محرمانگی، صحت و قابل‌اعتماد بودن داده را در برگیرد.در رابطه با عمده تهدیدهای امنیتی، باید از دو سطح گسترده از اقدامات امنیتی یعنی رمزگذاری و احراز هویت بهره برد.عدم محرمانگی موجب افشاء اطلاعات پزشکی می‌شود وبه دنبال آن مشکلاتی برای بیمار به وجود می‌آورد. برخی از این مشکلات شامل تحقیربیمار، درمان نادرست، از دست دادن شغل ، محرومیت فرد از پوشش بیمه‌ی سلامت ، شرمساری عمومی و بی‌ثباتی روحی بیمار می‌باشند. عدم صحت داده ها باعث می‌شود داده غلط به سرور برسد وبه دنبال آن موجب شود که برخی اوقات با درمان نادرست یا تجویز داروهای نامناسب زندگی بیمار به خطرافتد و حتی باعث مرگ وی شود. ساختار مقاله به شرح زیر است : بخش دو مروری بر کارهای گذشته می‌باشد . بخش سوم مقایسه مقالات بررسی شده می‌باشد.بخش چهارم به نتیجه گیری اختصاص یافته است.

۲- مروری بر کارهای گذشته:

در روش های ارائه شده برای حفظ امنیت از ویژگی بیومتریک به عنوان کلید رمزنگاری استفاده شده است .این روش ها به پنج دسته تقسیم شده اند که به صورت زیر می باشند :

۲-۱-ایجاد امنیت درسیستم با استفاده از ویژگی های بیومتریک چهره وعنبیه :

در طرحی یک تکنیک مبتنی برویژگی های بیومتریک چهره وعنبیه که شامل سه مرحله می باشد ارائه شده است. در این تکنیک ابتدا ویژگی های چهره وعنبیه استخراج شده با هم ترکیب شده اند وکلید رمز نگاری ایمن ۲۵۶ بیتی از قالب بیومتریک چند بعدی تولید میشود.

محاسنی بدین شرح برای آن مطرح شده است:

بیومتریک نقش مهمی در سیستم حفاظت دارد، شناخت عمده و حفاظت از امنیت فقط به سیستم بیومتریک بستگی دارد و بطور کلی کلید بیومتریک یک کلید امن می‌باشد، منحصر به فرد است و همیشه همراه و در دسترس کاربر است و نیازی به حفظ کردن آن نیست [1].

اما علیرغم وجود امتیازات و محاسن مطرح شده این روش معایبی نیز دارد که عبارت‌اند از:

هزینه استخراج ویژگی بیومتریک عنبیه در هنگام ثبت در پایگاه داده اولیه بالا می‌باشد. در زمان تأیید اعتبار برای استفاده از ویژگی عنبیه تجهیزات ویژه‌ای نیاز می‌باشد که نمی‌تواند اغلب اوقات در دسترس باشد.

۲-۲- استفاده از ویژگی‌های بیومتریک عنبیه و اثرانگشت

یک طرح رمزنگاری تصویر جدید با استفاده از کلید بیومتریک چند متغیره غیرقابل‌برگشت می‌باشد بدین‌صورت که نقاط ویژگی اثرانگشت و عنبیه با استفاده از الگوریتم استخراج ویژگی SLGS استخراج می‌شوند و به دنبال آن مکانیسم هرج‌ومرج برای تغییر دادن ویژگی‌های بردارها استفاده می‌شود و درنهایت آن‌ها را برای تولید یک کلید بیومتریک ترکیب می‌کند. انسان‌ها به‌سختی می‌توانند کلید رمزنگاری طولانی را به یاد بیاورند در این طرح از ویژگی‌های بیومتریک انسان که در طبیعت منحصر به فرد است و مهاجم به‌سختی می‌تواند آن را حدس بزند استفاده شده است [2]. با وجود محاسن ذکر شده برای استفاده از ویژگی بیومتریک عنبیه در WBAN تجهیزات ویژه‌ای نیاز است که دارای هزینه بسیار بالایی می‌باشد.

در طرحی دیگر پیاده‌سازی عملی با استفاده از اثر انگشت و عنبیه به عنوان بیومتریک و استخراج فازی برای استخراج کلید بیومتریک پیشنهاد می‌شود. این طرح یک سناریوی بیومتریک PKI و یک تحلیل عمیق امنیتی برای آن را تعریف می‌کند. این تحقیق سیستم Bio PKI را پیشنهاد می‌کند که در آن کلید خصوصی هرگز ذخیره نمی‌شود و از بیومتریک کاربر استفاده می‌شود. دستگاه مورد استفاده برای ضبط اطلاعات بیومتریک گوشی هوشمند است.

محاسنی که این طرح دارد بدین شرح است: بیومتریک‌های چندبعدی امنیت بیشتری را ارائه می‌دهند زیرا به دست آوردن دو یا چند بیومتریک بطور همزمان مشکل تر است.دلایل استفاده از سیستم‌های چند منظوره محدودیت حد بالا و امنیت می‌باشد. محدودیت بالا حداکثر تعداد الگوهای قابل‌تشخیص است. استفاده از بیومتریک‌های چندبعدی ممکن است ضروری باشد، زیرا ممکن است امنیت بیشتری و آنتروپی کلیدی ارائه شود.هنگامی‌که سیستم بیومتریک چندمنظوره استفاده می‌شود، عملکرد به‌طور قابل‌توجهی نسبت به همتای تک بیومتریک افزایش می‌یابد.

معایب مطرح شده در طرح به شرح زیر است: یک فرد ممکن است یک حادثه داشته باشد که منجر به از دست دادن یک مشخصه بیومتریک گردد و ممکن است مانع از ثبت نام در سیستم بیومتریک شود، یک مشخصه بیومتریک را نمی‌توان جایگزین یا تجدید کرد، پس اگر این ویژگی‌ها در معرض خطر بیفتند، می‌توان برای همیشه از دست رفته در نظر گرفته شوند. ضعیف‌ترین پیوند PKI کلید خصوصی است. برخی مطالعات نشان داد داده‌های بیومتریک را می‌توان از یک قالب ذخیره شده بازسازی کرد و یک شکست احتمالی پایگاه داده می‌تواند ویژگی‌های بیومتریک را برای بسیاری از کاربران به خطر بیندازد [3].

۲-۳- استفاده از ویژگی بیومتریک اثرانگشت:

در این دسته۳طرح ارائه شده است که در زیر توضیح داده می‌شوند.

در طرح اول پیشنهاد شده است تا کلید تقریبی ۱۲۸ بیتی از الگوی بازدارنده اثرانگشت هر دو طرف ارتباط تولید شود. در این طرح کلید رمزنگاری متقارن با استفاده از الگوی اثر انگشت قابل لغو فرستنده و گیرنده در سایت‌های خودشان تولید می‌شود.

محاسنی که این طرح دارد به این شرح است: رویکرد فعلی حفظ حریم خصوصی اثر انگشت را با تغییر یک قالب از قالب اصلی به یک قالب قابل لغو تأیید می‌کند. مشکل ذخیره‌سازی کلید و توزیع کلید را حل می‌کند. به عنوان کلید به گیرنده ارسال نمی‌شود و همچنین در هر کجا ذخیره نمی‌شود. لازم نیست این کلید رمزنگاری، توسط کاربر به خاطر آورده شود و همچنین لازم نیست ذخیره شود. حریم خصوصی هویت اثر

انگشت نیز با استفاده از مفهوم الگوی اثر انگشت لغو حفظ می‌شود [۴] .

معایب طرح به شرح زیر است: اگر حمله کننده با مهندسی معکوس روش تولید کلید را بدست آورد می تواند داده های ارسالی را بدست آورد.

درطرح دوم مرورکلی بر استراتژی‌های تصدیق علامت‌های منحصربه‌فرد انجام می‌شود. علاوه بر این متدولوژی‌های فوق‌العاده‌ایی نیز به دقت اجرا و مورد بررسی قرار می‌گیرد. از آنجایی که اثر انگشت منحصربه‌فرد نیز ممکن است حاوی نویز باشد، بنابراین سیستم‌های تشخیص تصویر علاوه بر متمرکز شدن، بررسی متقابل لبه‌های اثر انگشت را انجام می‌دهند. محاسنی که این طرح دارد بدین شرح است : به علت استفاده از ویژگی بیومتریک ،منحصر به فرد است. به خاطر سپردن کلید توسط کاربر نیاز نمی باشد. این روش مشکل نویز اثر انگشت را برطرف نموده است [۵] .

از معایب این روش می‌توان به مشکل تعویض ناپذیر بودن کلید که در ذات ویژگی‌های بیومتریک است اشاره نمود.

در طرح سوم ، یک تکنیک برای تولید ماتریس کلیدی با استخراج نقاط مینیاتوری از ماتریس ترکیبی اثر انگشت فرستنده و گیرنده پیشنهاد شده است. این سیستم شامل چهار مرحله ثبت نام ، احراز هویت، تولید کلید و رمزنگاری می‌باشد. در مرحله ثبت نام، اثر انگشت هر دو فرستنده و گیرنده به دست می آید، همراه باکلیدشناسایی تولید شده از نقاط مینیاتوری آنها در سرور ذخیره می شود. در مرحله تأیید، اثر انگشت داده شده توسط فرستنده و اثر انگشت ذخیره شده بر روی سرور مقایسه می شود. اگرامتیاز تطابق در مقدار آستانه باشد، احراز هویت موفق است. اگر احراز هویت با موفقیت انجام شود، فرستنده تصویر مخلوط را از اثر انگشت خود و اثر انگشت گیرنده از سرور ایجاد می کند. سپس درمرحله تولید کلید، ماتریس کلید رمز نگاری از قالب های ترکیبی مینیاتوری تصویر اثر انگشت فرستنده و گیرنده تولید می شود. در اینجا ماتریس کلیدی خود معکوس 8x8تولید خواهد شد. در نهایت در مرحله رمزنگاری، تصویر اصلی به شکل ماتریس ۲۵۶ x ۲۵۶ تبدیل می شود و به زیرماتریس 8x8 تقسیم می‌گردد. هر زیر ماتریس با استفاده از هیل رمز با ماتریس کلیدی که قبلا ساخته شده است رمزگذاری می شود. تصویر رمزگذاری شده با ترکیب هر یک از زیر ماتریس رمزگذاری شده به همان ترتیب ایجاد می شود.

محاسنی که این طرح دارد بدین شرح است : از روشی جدید برای ارائه امنیت دو سطح با استفاده از تصاویر منتقل شده بیومتریک اثر انگشت در شبکه جهانی وب استفاده می‌شود. سیستم پیشنهادی، توانایی رمزگذاری را با استفاده از میانگین متحرک تغییر شدت (UACI) و همچنین افزایش سرعت فرایند رمزگذاری با استفاده از ماتریس کلیدی خود معکوس **8x8**را تضمین می کند [6] .

معایب طرح به شرح زیر است: این طرح به علت عملیات پیچیده رمزنگاری به زمان زیادی برای رمزنگاری داده نیاز دارد . بنابراین برای سیستم WBAN مناسب نمی‌باشد.

۲-۴- استفاده‌ازویژگی‌بیومتریک غیر استاتیک (پویا) :

در این طرح الگوریتم رمزنگاری کارآمد مبتنی بر روش تولید کلید، کلید بیومتریک پیشنهاد شده است. ویژگی بیومتریک غیر استاتیک (یعنی پویا) مانند الکتروکاردیوگرام (ECG) برای تولید کلید استفاده می شود.

محاسنی که این طرح دارد بدین شرح است: الگوریتم رمزنگاری پیشنهاد شده از لحاظ زمان و استفاده از حافظه محاسبه شده است و نتایج نشان می دهد که الگوریتم پیشنهادی از الگوریتم های کل متداول برتر است [7] .

معایب طرح به شرح زیر است: با توجه به اینکه ویژگی بیومتریک ارائه شده از روی پوست گرفته می شود ، ممکن است به علت متفاوت بودن دو قسمت پوست که از آنها گرفته می شود که بر اثر خراش یا کبودی یا حادثه ای متفاوت شده باشند، داده ها تغییر کنند و باعث شوند رمز حاصله متفاوت باشد .

۲-۵- استفاده از ویژگی بیومتریک شبکیه:

این طرح از بیومتریک شبکیه برای تولید کلید استفاده می کند، کلید به طور مستقیم از اطلاعات بیومتریک شبکیه انسان تولید می شود بطوریکه رگ های خونی شبکیه در پایگاه داده ذخیره نمی شود. این مقاله سه ویژگی بیومتریک شبکیه ای مانند تعداد نقاط انتهایی، نقاط غیر حساس و جزایر را ارائه می دهد. این کار تاکید بر وحدت این سه ویژگی است که باعث می شود یک کلید رمزنگاری امن ایجاد شود. این کار یک الگوریتم جدید را به نام الگوریتم متحد سازی EBI معرفی می کند که هدف آن یکتا سازی (یونیک) از سه ویژگی به منظور ایجاد کلید رمزنگاری امن تر است. این تحقیق بر افزایش اثربخشی تولید کلید از طریق شناسایی شبکیه تمرکز دارد. هدف از این طرح، ارائه راه امن برای تولید کلید با استفاده از ویژگی های بیومتریک شبکیه منحصر به فرد است و احتمال تکراری را کاهش می دهد.

محاسنی که این طرح دارد بدین شرح است: این حالت عملیات در امنیت شبکه باعث پیچیدگی بیشتری برای هکرها می شود. به خوبی ثابت شده است که ساختار شبکیه پایدار و

دائمی است که برای فرد به فرد منحصر به فرد است. این به این دلیل است که شبکه عروق خونی در شبکیه پیچیده است که دوقلوهای یکسان نیز الگوی مشابهی ندارند. روش شناسایی شبکیه، دارای ویژگی های دقیق تر و قابل اطمینان بیومتریک است [8].

معایب طرح به شرح زیر است: برای اسکن شبکیه تجهیزات پزشکی لازم است. این روش به علت نیاز به تجهیزات خاص و وجود بیماری‌هایی مانند گلوکوم در WBAN قابل‌استفاده نمی‌باشد.

۳- مقایسه مقالات بررسی شده :

در جدول ۱ به کمک پارامتر های بیان شده مقالات بررسی شده در بخش قبلی با یکدیگر مقایسه شده اند.

جدول۱- نتیجه مقایسه مقالات بررسی شده با یکدیگر

پارامتر / مقاله	پیچیدگی روش رمزنگاری	دقت روش رمزنگاری در ایجاد امنیت	آسانی تولید کلید	هزینه	انرژی مصرفی	امنیت کلید تولید شده
[۱]	کم	متوسط	کم	زیاد	متوسط	زیاد
[۲]	کم	متوسط	کم	متوسط	کم	زیاد
[۳]	کم	زیاد	متوسط	زیاد	متوسط	زیاد
[۴]	متوسط	متوسط	متوسط	کم	متوسط	زیاد
[۵]	کم	متوسط	متوسط	کم	کم	متوسط
[۶]	متوسط	زیاد	متوسط	کم	کم	متوسط
[۷]	کم	متوسط	متوسط	متوسط	کم	متوسط
[۸]	کم	زیاد	متوسط	زیاد	متوسط	زیاد

۴- **نتیجه گیری** :

در این مقاله روش های استفاده شده براساس کلید دسته بندی شده اند. روش یک ویژگی بیومتریک چهره وعنبیه ،روش دو ویژگی عنبیه واثر انگشت ، روش سه ویژگی بیومتریک اثر انگشت ، روش چهار ویژگی بیومتریک غیر استاتیک ، روش پنج ویژگی بیومتریک شبکیه می‌باشد .بامقایسه این روش ها به این نتیجه رسیدیم که برخی از آن ها پیچیدگی بیشتری دارند وحفظ امنیت داده وکلید در آن ها نیز بیشتر است .لیکن انرژیِ مصرفی در سیستم نیز بالا می باشد .در نتیجه این روش ها در سیستم ها یی که با مشکل محدودیت انرژی مواجه هستند قابل استفاده نمی باشند برخی دیگر از روش ها پیچیدگی کمتری دارند و به واسطه نوع بیومتریک استفاده شده در آن هاامنیت کلید ودقت آن هازیاد می باشد ولیکن هزینه تجهیزات استفاده شده نیز بالا است.بنابراین روش هایی که برای ایجاد کلید با استفاده ازویژگی بیومتریک مانند اثر انگشت نیازی به تجهیزات ویژه ای ندارند ،وهمچنین روش رمزنگاری نیز پیچیدگی زیادی ندارد که مصرف انرژی آن بالا باشد مناسب هستند.همچنین اگر به کمک برخی از الگوریتم ها ، مانند الگوریتم کد گذاری امنیت کلید حفظ شود ،امنیت روش نیز تامین می‌شود.

مراجع :

[1] Balamurugan, G., Dr. K.B. Jayarraman, Arulalan, V., Lokesh, V. “Multimodal Biometric Key Generation for Cryptographic Security using Face and Iris” Advances in Natural and Applied Sciences, 9(6) Special 2015, Pages: 525-530

[۲] M. SuchithraEmail author O. K. Sikha” A Novel Image Encryption Scheme Using an Irrevocable Multimodal Biometric Key” International Symposium on Security in Computing and Communication SSCC 2015: Security in Computing and ommunications pp 256-264

[۳] Lavinia Mihaela Dinca * and Gerhard Hancke “User-Centric Key Entropy: Study of Biometric Key Derivation Subject to Spoofing Attacks” *Entropy* 2017, *19*(2), 70; doi:10.3390/e19020070

[۴] Arpita Sarkar, Binod Kr Singh “Cancelable Biometric Based Key Generation for Symmetric Cryptography” International Conference on Inventive Communication and Computational Technologies (ICICCT 2017)

[۵] Lovelesh Khard, Uday Chourasia. Raju Baraskar, “Detection of PARD Attack using Key based Biometric Authentication System and Fingerprint Impression” International Journal of Computer Applications (0975 – 8887) Volume 159 – No 7, February 2017

[۶] Megha D. Randeri, Dr. Sheshang D. Degadwala, Mrs. Arpana ahajan“Image ncryption Using Key Matrix Generation from Biometric Mixed Fingerprint Image for Two Level Security” I nternational Journal of S c ientific Resear c h in Science, Engineering and Technology (ijsrset.com) , 10 – April – 2018

[۷] Mohana, Jaishankar; Bai, Vijayan Thulasi “Implementation of Efficient Cryptographic Algorithm Based on Dynamic Biometric Key Generation Technique” American Scientific Publishers Volume 14, Number 10, October 2016, pp. 1044-1048(5)

[۸] Mohammed Tajuddin , C.Nandini“More Secured Cryptographic Key Generation through Retinal Biometric using EBI Algorithm” International Journal of Engineering Innovation & Research Volume 3, Issue5, ISSN: 2277–5668 ,2014