به نام خدا

پژوهشکده علوم کامپیوتر

پیشنهاد همکاری به عنوان تک پروژه مقیم

عنوان پروژه:

طراحی و تحلیل امنیتی پروتکل‌های احرازهویت مبتنی بر رمزنگاری خم‌بیضوی مورد استفاده در TMIS

Design and security analysis of ECC based authentication protocols used in TMIS

مجری:

معصومه صفخانی

بهمن ماه ۱۴۰۱

عنوان طرح:

طراحی و تحلیل امنیتی پروتکل‌های احرازهویت مبتنی بر رمزنگاری خم‌بیضوی مورد استفاده در TMIS

مجری اصلی: دکتر معصومه صفخانی

آدرس محل کار: تهران، لویزان، دانشگاه تربیت دبیر شهید رجایی، دانشکده مهندسی کامپیوتر، گروه نرم افزار

چکیده: ادغام اینترنت اشیاء و پیشرفت‌های حوزه پزشکی، زمینه جدیدی به نام سامانه‌های اطلاعات پزشکی مراقبت از راه دور[1] یا همان TMIS را ایجاد نموده است. شبکه بی‌سیم بدن[2] نیز یک فناوری در جهت استفاده از سامانه‌های اطلاعات پزشکی مراقبت از راه دور و نظارت بر خصوصیات زیستی بیماران می‌باشد. توسعه شبکه بی‌سیم بدن و سامانه‌های مراقبت پزشکی پوشیدنی[3] نقش کلیدی در پایش سلامت ایفا می‌کنند. شبکه بی‌سیم بدن شبکه‌ای شامل حسگرهای پزشکی می‌باشد که این حسگرها قابلیت تعبیه بر روی بدن بیمار را دارند و علائم حیاتی و زیستی بیماران مانند فشار خون و... را اندازه‌گیری نموده، این داده‌ها را جمع‌آوری کرده و آن‌ها را به سرورهای پزشکی از طریق کانال بی‌سیم ارسال می‌کنند. بنابراین، اطلاعات حساس ارسالی بیماران که بر روی کانال ارسال شده است، می‌تواند به حملات مختلف آسیب‌پذیر باشد. در واقع پزشکی هوشمند علاوه بر مزایای چشمگیرش، مشکلات حریم خصوصی و امنیتی بسیاری را به همراه دارد. لذا حفظ حریم خصوصی افراد از حملات متنوع موجود بر روی شبکه‌های عمومی بزرگ‌ترین چالش در پیاده‌سازی این سامانه است. از این‌رو، طراحی پروتکل‌های امنیتی احرازهویت سبک‌وزن برای این سامانه‌ها با کمترین هزینه‌های محاسباتی و ارتباطی به یک چالش اصلی تبدیل شده است. از آنجایی که رمزنگاری خم‌بیضوی یک الگوریتم رمزنگاری کلیدعمومی است که نسبت به رمزنگاری مبتنی بر RSA از یک کلید با اندازه کوچک‌تر استفاده می‌کند، ما در این پیشنهاد طرح، بر تحلیل امنیتی پروتکل‌های احراز هویت مبتنی بر خم بیضوی که اخیراً ارائه‌شده و ادعای امن‌بودن را داشته‌اند، تمرکز کرده‌ایم. سپس با استفاده از ابزارهای تحلیل امنیتی موجود نسبت به بهبود امنیتی آن‌ها و ارائه طرح‌های جدید اقدام خواهیم نمود.

کلید واژه‌ها: اینترنت اشیاء، رمزنگاری خم بیضوی، مدل اوراکل تصادفی، Scyther، Proverif[4]، AVISPA

Abstract:

The integration of the Internet of Things and advances in the field of medicine has created a new field called Telecare Medical Information Systems (TMIS). The wireless body area network is also a technology for using remote care medical information systems and monitoring patients' biological characteristics. The development of wireless body area networks and wearable medical care systems plays a key role in health monitoring. The wireless body area network is a network that includes medical sensors that can be embedded on the patient's body and measure vital and biological signs of the patient, such as blood pressure. These sensors collect these data and send them to the medical servers through the wireless channel. Therefore, sensitive information sent by patients over the wireless channel can be vulnerable to various attacks. In fact, in addition to its significant benefits, smart medicine brings many privacy and security problems. Therefore, protecting people's privacy from various attacks on public networks is the biggest challenge in implementing this system. Therefore, the design of lightweight authentication security protocols for these systems with the lowest computational and communication costs has become a major challenge. Since elliptic curve cryptography is a public key encryption algorithm that uses a smaller key than RSA-based encryption, in this proposal we focus on the security analysis of authentication protocols based on elliptic curve cryptography that have recently been presented and claim to be secure. Then we will use the existing security analysis tools to improve their security and present new schemes.

Keywords: IoT, Elliptic Curve Cryptography, Random Oracle Model, Scyther, Proverif, AVISPA

[1] Telecare Medicine Information Systems (TMIS)
[2] Wireless Body Area Networks (WBAN)
[3] Wearable Health Monitoring Systems (WHMS)

۱. مقدمه:

شبکه اینترنت اشیاء برای اتصال اشیاء به یکدیگر از طریق اینترنت در زمینه‌های مختلف مناسب است [۱][۲][۳]. این شبکه در سال‌های اخیر گسترش یافته است. یکی از این زمینه‌ها، خدمات پزشکی بر روی بستر اینترنت است که هزینه رفتن به بیمارستان را کاهش می‌دهد و زمان را ذخیره می‌کند [۶]. در واقع با پیشرفت روزافزون فناوری، پزشکان می‌توانند خدمات بهداشتی را از راه دور و در بستر اینترنت به افراد ارائه دهند. ارائه این خدمات پزشکی و بهداشتی، محدود به مکان و زمان نیست و از این‌رو بیمار می‌تواند بدون مراجعه به مراکز درمانی از این خدمات پزشکی استفاده کند [۳]. خدمات ارائه‌شده در این سامانه شامل اطلاع از وضعیت بیماران، مراقبت از افراد سالمند، دریافت اطلاعات دارویی و... است [۱]. از این‌رو، یکی از فناوری‌های اساسی در اینترنت اشیاء، سامانه‌های اطلاعات پزشکی مراقبت از راه دور است [۷]. در سامانه‌های اطلاعات پزشکی مراقبت از راه دور، حسگرها یا برچسب‌ها وضعیت بیمار و اطلاعات زیستی آن را اندازه‌گرفته و این اطلاعات را با استفاده از دستگاه‌های تلفن همراه مانند PDA، فناوری شناسایی فرکانس رادیویی[1]، شبکه‌های بی‌سیم و بستر اینترنت به سرور ارسال می‌نمایند. سرور وظیفه ذخیره‌سازی اطلاعات پزشکی محافظت‌شده بیمار را دارد. برقراری ارتباط در فناوری شناسایی فرکانس رادیویی با حضور سه مولفه صورت می‌پذیرد: برچسب فناوری شناسایی فرکانس رادیویی، سرور و برچسب‌خوان فناوری شناسایی فرکانس رادیویی. در این فناوری برچسب فناوری شناسایی فرکانس رادیویی در ابتدا به اشیا و افراد متصل می‌شود. این افراد وظیفه ارسال اطلاعات و داده‌های زیستی بدن بیمار را به سرور پایگاه داده دارند [۲]. فرایند استفاده از خدمات این سامانه وابسته به ثبت‌نام کاربر در پایگاه داده سرور است [۱۱]. پزشکان می‌توانند به این سامانه وارد شوند و سوابق پزشکی بیماران خود، تاریخچه داروهای تجویزی، نتایج و آزمایش‌ها را بررسی‌کنند و تجویزهای لازم را در خصوص بیمار موردنظر ارائه نمایند [۳]. هم‌چنین بیماران می‌توانند به سامانه وارد شوند تا سوابق پزشکی خود، نتایج آزمایش‌ها و... را مشاهده نمایند و از راه دور به خدمات بهداشتی دسترسی پیدا کنند [۱۲]. به‌طورکلی ساختار سامانه‌های اطلاعات‌پزشکی مراقبت از راه دور شامل چهار بخش اصلی: پزشک، بیمار، بستر عمومی اینترنت و پایگاه داده سرور است [۱۳]. در شکل ۱ معماری این سامانه جهت ارائه خدمات پزشکی از راه دور مبتنی بر فناوری شناسایی فرکانس رادیویی نشان داده‌شده‌است [۱۴]. همه این خدمات مستلزم وجود فراهم‌شدن بستر و پروتکلی است که کاربران موجود در این سامانه احرازهویت متقابل شوند تا خدمات ارائه‌شده مورد سوءاستفاده قرار نگیرد [۱][۴]. هم‌چنین سامانه‌های اطلاعات‌پزشکی مراقبت از راه دور بستری مناسب را جهت خدمات پزشکی مبتنی بر شبکه بی‌سیم بدن فراهم می‌کنند. معماری این شبکه مبتنی بر دو لایه است که در شکل ۱ نشان داده‌شده‌است. لایه اول آن مبتنی بر شبکه‌ای با برد کوتاه همراه با حسگرهای پزشکی مناسب بر روی بدن بیمار است [۱۰]. این حسگرها جهت جمع‌آوری اطلاعات زیستی بیمار و ارسال این اطلاعات به سرور به دستگاه‌هایی به نام PDA متصل می‌شوند. سپس در لایه دوم، این دستگاه‌ها با استفاده از بستر اینترنت اطلاعات جمع‌آوری‌شده را به پایگاه داده سرور ارسال می‌کنند [۲]. اطلاعاتی که در شبکه بی‌سیم بدن ارسال می‌شود، اطلاعات بسیار حساسی هستند و پتانسیل بالایی را جهت اعمال حمله دارند [۱۲]. پس محرمانه‌بودن و یکپارچگی این اطلاعات بسیار حائز اهمیت است [۸][۴]. در نتیجه پیشرفت‌های زیاد در زمینه‌ی خدمات پزشکی، سامانه‌های مراقبت پزشکی پوشیدنی را نیز ایجاد کرده است [۸] که تعداد زیادی حسگر[2] برای جمع‌آوری داده در زمینه‌های مختلف اینترنت اشیاء استفاده می‌شوند [۴][۵]. همان‌طورکه در شکل ۲ نشان داده شده است، یک سامانه مراقبت پزشکی پوشیدنی شامل سه شرکت‌کننده است: مدیر شبکه[3]، سرور کاربرد[4] و کاربر شبکه بی‌سیم بدن[5]. شبکه بی‌سیم بدن، نقش اصلی در صنعت

---

[1] Radio Frequency IDentification

[2] Sensors

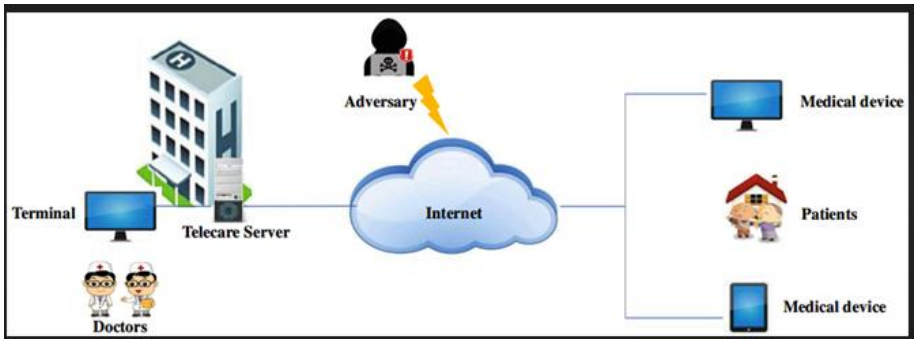
[3] Network Manager (NM)

[4] Application Server (AS)

[5] WBAN User (U)

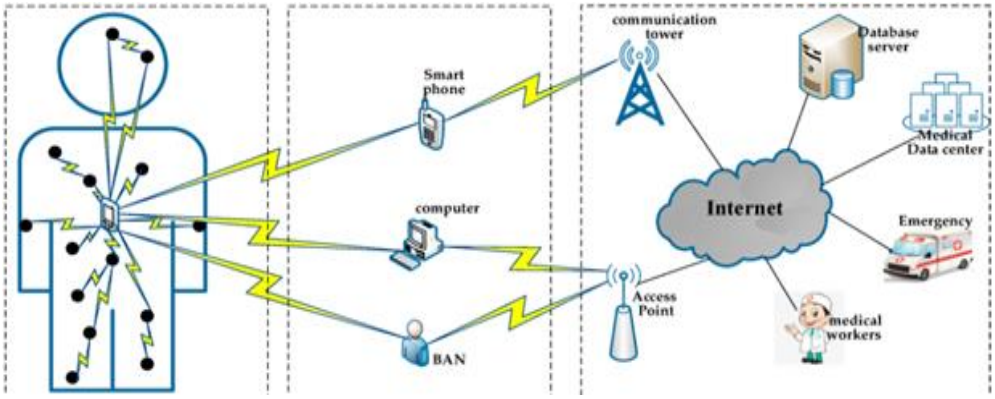
پزشکی برای اطلاع از وضعیت سلامت بیماران در سامانه‌های مراقبت پزشکی پوشیدنی بازی می‌کند [۹][۱۰]. شبکه بی‌سیم بدن شامل حسگرهای پزشکی مختلف است که بر روی بدن بیماران مجهز شده‌اند، پارامترهای علائم حیاتی بیماران از قبیل دما، فشارخون و... را اندازه‌گیری می‌کنند و داده اندازه‌گیری شده را از طریق اینترنت به عنوان یک شبکه به سرورهای پزشکی ارسال می‌نمایند [۱۱][۱۲]. از آن‌جایی‌که حسگرهای ارتباطی برای اندازه‌گیری اطلاعات حساس بیماران در کانال‌های ناامن استفاده می‌شوند، بنابراین، کل سامانه دربرابر تهدیدات آسیب‌پذیر است و در نتیجه حفظ حریم خصوصی[1] افراد، حفظ گمنامی کاربران[2] و دیگر خواص امنیتی تبدیل به یک چالش بزرگ در پیاده‌سازی یک سامانه امن مناسب شده است و بنابراین باید گمنامی و حریم خصوصی کاربران مصون از تهدیدات امنیتی باشد [۱۳][۱۴][۱۵]. همان‌طور که اطلاعات پزشکی به حملات امنیتی مختلف آسیب‌پذیر است [۱۶]، بنابراین طرح‌های مختلف جهت تضمین امنیت داده [۱۷][۱۸][۱۹] توسعه یافته‌اند. هم‌چنین سامانه‌های مراقبت پزشکی پوشیدنی شامل چندین دستگاه و حسگر پزشکی است، که با یکدیگر از طریق کانال بی‌سیم ارتباط برقرار می‌کنند. همان‌طورکه در شکل ۳ نشان داده شده است، سه شرکت‌کننده به نام‌های مدیر شبکه، سرور کاربرد و کاربر در این مدل وجود دارند. مدیر شبکه مسئول راه‌اندازی سامانه و فرایند ثبت‌نام است، که شامل متخصصین، کلینیک‌های پزشکی، بیمارستان‌ها و مراکز سلامت می‌باشد [۲۱][۲۲]. در این مدل، سرورهای پزشکی به عنوان هستارهای[3] جداگانه با کلیدهای خصوصی در نظر گرفته می‌شوند [۲۳]. هر کاربر هنگامی‌که به سامانه وصل می‌شود، باید از طریق یک کانال امن در مدیر شبکه ثبت‌نام کند. هم‌چنین، مدیر شبکه اطلاعات ضروری هر کاربر را تولید خواهد کرد و آن‌ها را از طریق یک کانال امن برمی‌گرداند [۶]. بنابراین، کاربران می‌توانند از کلید خصوصی و اطلاعات ضروری خودشان برای ورود به سرور کاربرد از راه دور استفاده کنند، تا به طور متقابل به یکدیگر احرازهویت شوند و کلید جلسه را برای ایجاد ارتباطات امن در کانال‌های عمومی و ناامن تولید نمایند. هر هستار سامانه‌های مراقبت پزشکی پوشیدنی به طور خلاصه در زیر توصیف شده است [۱۸][۲۰].

- **کاربر:** هدف نهایی کاربر، دسترسی به خدمات پزشکی ارائه شده با سرور کاربرد است. در ابتدا، کاربر باید در مدیر شبکه ثبت‌نام شود. بعد از ثبت‌نام موفق، کاربر باید به منظور استفاده از این خدمات، با استفاده از سرور کاربرد احرازهویت گردد.
- **سرور کاربرد:** سرور کاربرد باید از طریق مدیر شبکه ثبت‌نام و احرازهویت شود، تا بتواند خدمات پزشکی را به کاربران قانونی پیشنهاد دهد. سرور کاربرد می‌تواند شامل بیمارستان‌ها، پزشکان متخصص و کلینیک‌ها باشد.
- **مدیر شبکه:** وظیفه این سرور، ثبت‌نام کاربران جهت دسترسی به خدمات پزشکی، ثبت‌نام سرورکاربرد و دادن مجوز به کاربران جهت استفاده از خدمات پزشکی ارائه شده با سرور کاربرد است.

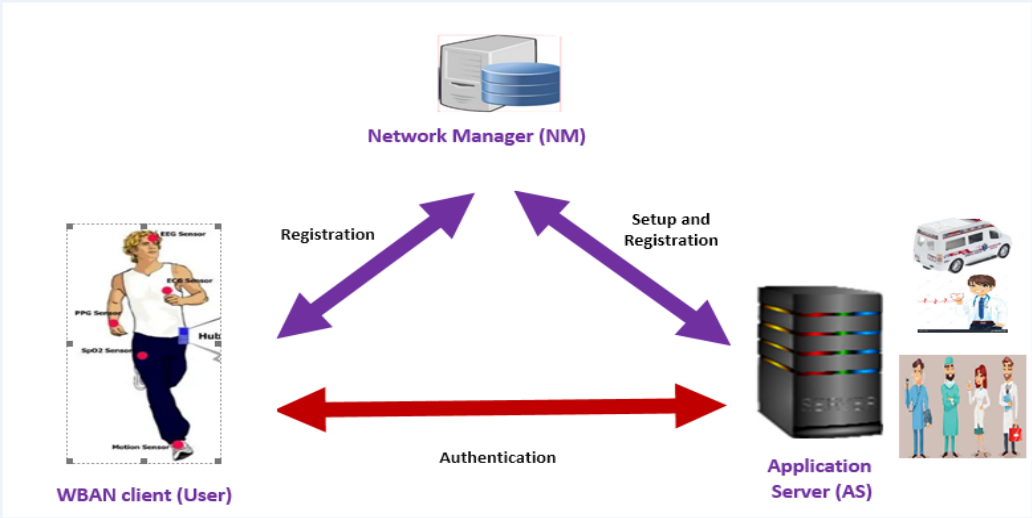


شکل ۱. معماری سامانه‌های اطلاعات‌پزشکی مراقبت از راه دور [۱۲].

[1] Privacy
[2] User Anonymity
[3] Entity

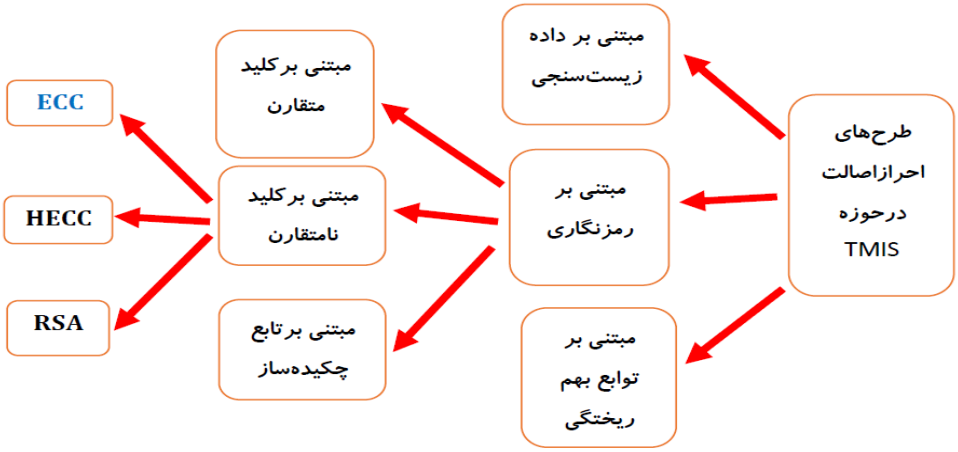


شکل ۲: معماری شبکه بی‌سیم بدن [۱۲].



شکل ۳: معماری سامانه‌های مراقبت پزشکی پوشیدنی.

ارائه تمامی خدمات از راه دور مستلزم احرازهویت متقابل افراد شرکت‌کننده در سامانه‌های اطلاعات پزشکی مراقبت از راه دور است. چارچوبی که به وسیله آن احرازهویت صورت می‌پذیرد پروتکل نام دارد. طبقه‌بندی طرح‌های احرازهویت در سامانه‌های اطلاعات پزشکی مراقبت از راه دور در شکل ۴ نشان داده شده است [۴]. تمامی طرح‌های احرازهویت در جهت شناسایی هویت کاربر در پایگاه داده سرور مستلزم تایید هویت کاربر و توافق کلید هستند. طبقه‌بندی تمامی طرح‌های احرازهویت ارائه شده در زیر به طور خلاصه شرح داده شده است[۳]. در جدول ۱ طبقه‌بندی طرح‌های احرازهویت ارائه شده اخیر برای سامانه‌های اطلاعات پزشکی مراقبت از راه دور، مبتنی بر سال ارائه هر طرح، طرح بهبود یافته برای آن‌ها و ویژگی‌های امنیتی نقض شده هر طرح مشخص گردیده است.



شکل ۴: طبقه‌بندی طرح‌های احرازهویت در سامانه‌های اطلاعات‌پزشکی مراقبت از راه دور [۴].

۱-۱ طرح‌های احرازهویت مبتنی بر رمزنگاری

در این نوع از طرح‌ها، تمامی پیام‌های مبادله‌شده جهت شناسایی هویت کاربر و توافق‌کلید به صورت رمزشده در کانال ارسال می‌شوند که تنها کاربر مجاز و سرور قادر به رمزگشایی این پیام‌های ارسالی با کلید توافق‌شده هستند[۴]. طرح‌های احرازهویت مبتنی بر رمزنگاری می‌توانند مبتنی بر رمزنگاری کلیدعمومی یا نامتقارن، رمزنگاری کلید متقارن و توابع چکیده‌ساز باشند[۲].

- طرح‌های احرازهویت مبتنی بر رمزنگاری کلید متقارن

رمزنگاری کلید متقارن روشی سریع و کارامد به شمار می‌آید. به دلیل این‌که در آن از یک کلید مشترک برای رمزنگاری و رمزگشایی پیام‌ها استفاده می‌شود [۴]. هم‌چنین در صورتی‌که تعداد پیام‌ها زیاد باشد این روش در پردازش بسیار مناسب است. الگوریتم‌های AES و DES نمونه‌ای از الگوریتم‌های رمزنگاری مبتنی بر کلید متقارن هستند [۲۳].

- طرح‌های احرازهویت مبتنی بر رمزنگاری کلید عمومی

در این نوع الگوریتم، از دو کلید جهت رمزنگاری و رمزگشایی پیام‌ها استفاده می‌شود، که یکی از کلیدها به عنوان کلید عمومی برای رمزنگاری پیام‌ها و کلید دیگر به عنوان کلید خصوصی برای رمزگشایی پیام‌ها استفاده می‌شود [۲۴]. این الگوریتم نسبت به الگوریتم احراز هویت مبتنی بر رمزنگاری کلید متقارن دارای امنیت بیش‌تری است، به دلیل اینکه کلید عمومی در اختیار همه قرار می‌گیرد ولی کلید خصوصی مخفی بوده و تنها در اختیار کاربر مربوطه قرار می‌گیرد. چند نمونه از الگوریتم‌های رمز کلید عمومی عبارتند از [۴][۲]:

- الگوریتم رمزنگاریRSA و الگوریتم امضای دیجیتال استاندارد DSA [۲۳]
- الگوریتم رمزنگاری خم‌بیضوی ECC [۲۵]
- الگوریتم رمزنگاریHECC [۱] [۴]

رمزنگاری خم‌بیضوی یک الگوریتم رمزنگاری کلیدعمومی است که نسبت به رمزنگاری مبتنی بر RSA از یک کلید با اندازه کوچک‌تر استفاده می‌کند. پس رمزنگاری خم بیضوی نسبت به RSA امنیت مشابهی را با اندازه کلید کوچک‌تر

[1] Hyper ECC

فراهم می‌کند. از این رو در این پیشنهاد طرح ما روی پروتکل های احراز هویت مبتنی بر رمزنگاری خم بیضوی یا همان ECC تمرکز خواهیم نمود.

۱-۲- طرح‌های احرازهویت مبتنی بر توابع چکیده‌ساز

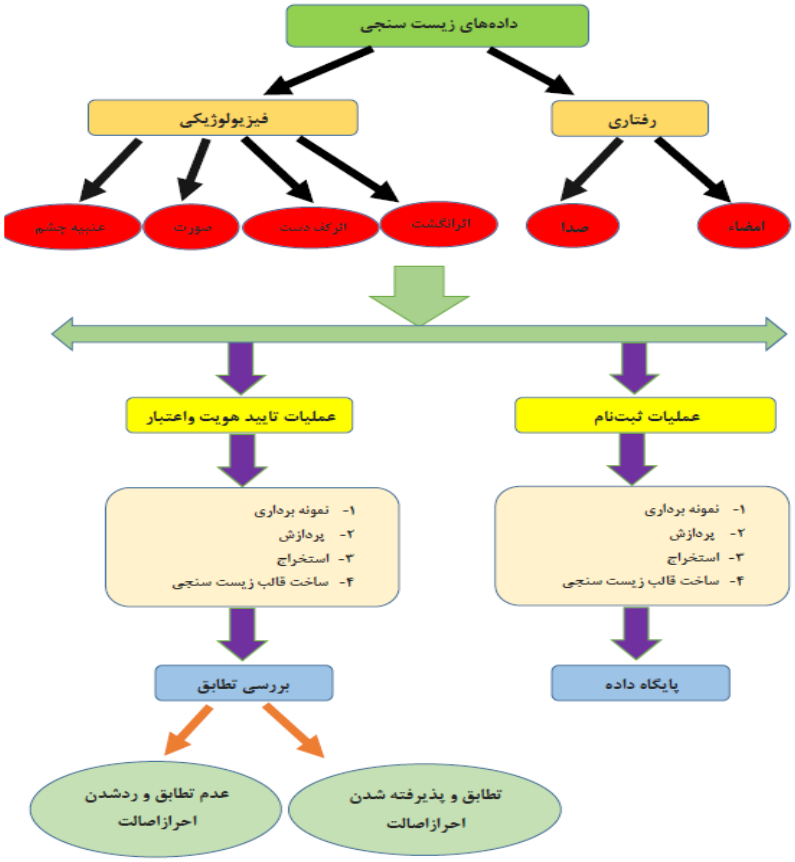
توابع چکیده‌ساز توابعی یک‌طرفه هستند که به‌منظور فشرده‌سازی و تولید چکیده‌ای منحصربه‌فرد از پیام‌ها با طول دلخواه به کار می‌روند. از نمونه توابع چکیده‌ساز می‌توان توابع SHA، HMAC و MAC را نام‌برد [۴].

۱-۳- طرح‌های احرازهویت مبتنی بر داده زیست‌سنجی

استفاده هم‌زمان از خواص زیستی کاربر مثل اثر انگشت، DNA و خواص رفتاری کاربر مثل امضا، صدا در طرح‌های احرازهویت مبتنی بر دو عامل از عوامل افزایش میزان امنیت است. ترکیب داده‌های زیست‌سنجی بیمار با سایر روش‌های احرازهویت موجب ارائه یک سامانه مبتنی بر چند عامل می‌شود. مبتنی بر این داده‌های زیست‌سنجی، کلیدهای مختلفی در رمزنگاری وجود دارد که این کلیدها به کلیدهای زیست‌سنجی معروف هستند. ویژگی منحصربه‌فرد این کلیدها به‌صورت زیر است [۴].

- دشوار بودن جعل این کلیدها
- دشوار بودن حدس این کلیدها
- عدم نیاز به حفظ کردن آن‌ها

فرایند طرح‌های احرازهویت مبتنی بر داده‌های زیست‌سنجی در شکل ۵ نشان‌داده‌شده‌است.



شکل ۵: فرایند طرح‌های احرازهویت مبتنی بر داده‌های زیست سنجی [۴].

۲. پیشینه تحقیق:

در سال‌های اخیر پروتکل‌های احرازهویت و توافق‌کلید بسیاری ارائه شده است. بیش‌تر پروتکل‌های احرازهویت ارائه‌شده اخیر مبتنی بر خم بیضوی هستند. به‌دلیل‌اینکه سطح امنیت مشابهی را در مقایسه با الگوریتم رمزنگاری RSA با اندازه کلید کوچک‌تر فراهم می‌کنند. به‌طوری که خم بیضوی امنیت را با کلید ۱۶۰ بیتی فراهم می‌کند، درحالی‌که همین میزان سطح امنیت در RSA با کلید ۴۰۹۶ بیتی فراهم می‌شود. پس استنتاج می‌شود که میزان پیچیدگی محاسباتی کاهش می‌یابد [۲]. در جدول ۱ طبقه‌بندی طرح‌های احرازهویت مبتنی بر خم بیضوی ارائه شده اخیر، پروتکل بهبودیافته آن‌ها و ویژگی‌های امنیتی نقض شده هر طرح مشخص گردیده است[۲۶].

جدول ۱: پروتکل‌های ارائه‌شده اخیر برای سامانه‌هایTMIS

ردیف	نام طرح	سال ارائه	ویژگی طرح	نوع حمله	روش احرازهویت	طرح بهبودیافته
۱	لمپورت و همکارانش[۱] [۲۴]	۱۹۸۱	طرح احراز هویت در کانال ارتباطی ناامن برای شبکه بی‌سیم بدن	حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۲	عظیم و همکارانش[۲] [۲۵]	۲۰۰۵	طرح توافق کلید برای شبکه محلی[۳] بی‌سیم	حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۳	وتو و همکارانش[۴] [۲۶]	۲۰۰۶	طرح پایش سلامت برای شبکه بی‌سیم بدن	حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۴	ویل و همکارانش[۵] [۲۷]	۲۰۰۷	پروتکل امنیتی در شبکه‌های حسگر بی‌سیم بدن[۶]	حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۵	پرنیل و همکارانش[۷] [۲۸]	۲۰۰۸	طرح ارائه شده برای شبکه‌های بی‌سیم	حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۶	لی و همکارانش[۸] [۲۹]	۲۰۱۰	طرح امنیتی برای شبکه اطلاعات پزشکی مراقبت از راه دور	حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۷	یو و همکارانش[۹] [۳۰]	۲۰۱۰	طرح ارائه شده در خصوص شیوه افزایش امنیت در شبکه‌های بی‌سیم بدن	حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۸	مانا و همکارانش[۱۰] [۳۱]	۲۰۱۱	طرح ارائه شده برای شبکه بی‌سیم بدن	حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۹	یه و همکارانش[۱۱] [۳۲]	۲۰۱۳	پروتکل مبتنی بر عملیات نمایی پیمانه‌ای برای سامانه‌های پایش سلامت بی‌سیم	حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۱۰	ژائو و همکارانش[۱۲] [۳۳]	۲۰۱۴	پروتکل موثر برای شبکه‌های بی‌سیم بدن	حمله تکرار	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۱۱	طرح لو و همکارانش[۱۳] [۲۷]	۲۰۱۵	پروتکل موثر برای شبکه‌های بی‌سیم بدن	حمله گمنامی، حمله ردیابی، حمله افشای هویت و حدس‌زدن گذرواژه برون‌خط	مبتنی بر رمزنگاری خم بیضوی	طرح جیانگ و همکارانش۱۴ [۲۸]
۱۲	هی و ضدلی[۱۵] [۳۴]	۲۰۱۵		حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.

[1] Lamport et al.
[2] Azim et al.
[3] LAN
[4] Otto et al.
[5] Boyle et al.
[6] WSN
[7] Preneel et al.
[8] Li et al.
[9] Liu et al.
[10] Mana et al.
[11] Yeh et al.
[12] Zhao et al.
[13] Lu et al
[14] Jiang et al
[15] He and Zeadly

ردیف	نام طرح	سال ارائه	ویژگی طرح	نوع حمله	روش احرازهویت	طرح بهبودیافته
۱۳	طرح آرشاد و رسول‌زادگان[1] [۲۹]	۲۰۱۶		حمله جعل هویت کلید توافق‌شده	مبتنی بر رمزنگاری خم بیضوی	طرح استاد شریف و همکارانش۲ [۳۰]
۱۴	لیو و همکارانش۳ [۳۵]	۲۰۱۶	طرح یک دوری برای شبکه‌های بی‌سیم بدن	حمله جعل کلید، حمله حدس کلید جلسه	مبتنی بر رمزنگاری خم بیضوی	لی و همکارانش۴ [۳۷]
۱۵	طرح چیو و همکارانش[5] [۳۱]	۲۰۱۶		عدم وجود گمنامی و محرمانگی پیشرو، حمله جعل	مبتنی بر رمزنگاری خم بیضوی	طرح دیباک و همکارانش[6] [۳۲]
۱۶	طرح چاندراکار و همکارانش۷ [۳۳]	۲۰۱۷		حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۱۷	طرح لی و همکارانش[8] [۳۴]	۲۰۱۷	ارزیابی امنیتی طرح لیو و همکارانش و ارائه یک طرح ارزیابی یک دوری برای شبکه‌های بی‌سیم بدن	نقض محرمانگی پیشرو، حمله فرد در میانه، عدم وجود احرازهویت متقابل،	مبتنی بر رمزنگاری خم بیضوی	طرح سوجانیا و همکارانش[9] [۳۵]
۱۸	یساد و همکارانش۱۰ [۹]	۲۰۱۷	ارائه یک طرح برای شبکه‌های پزشکی بی‌سیم بدن	حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۱۹	وو و همکارانش۱۱ [۳۶]	۲۰۱۷	طرح احرازهویت سبک‌وزن برای دستگاه‌های مرتبط با سرور ابری	حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۲۰	طرح لی و همکارا ن[12] [۳۶]	۲۰۱۸		حمله جعل، پیوندناپذیری و عدم‌برخورداری از ویژگی ناشناس بودن	مبتنی بر رمزنگاری خم بیضوی	طرح مهیت و همکاران۱۳ [۳۷]
۲۱	طرح کی و همکارا ن[14] [۳۸]	۲۰۱۸		حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است
۲۲	امین و همکارانش۱۵ [۷]	۲۰۱۸	ارائه یک شبکه پزشکی بزرگ	حمله جعل و حمله تکرار	مبتنی بر رمزنگاری خم بیضوی	طرح جیانگ و همکارانش۱۶
۲۳	طرح استاد شریف و همکاران۱۷ [۳۹]	۲۰۱۹		حمله حدس و جعل گذرواژه، حمله جعل کلید، حمله داخلی، حمله تکرار	مبتنی بر رمزنگاری خم بیضوی	طرح نیکوقدم و همکاران۱۸ [۴۰]
۲۴	طرح کارثیگیونی و همکاران۱۹ [۴۱]	۲۰۱۹		حمله تکرار، حمله منع سرویس، عدم وجود احرازهویت متقابل بین سرور و کاربر	مبتنی بر رمزنگاری خم بیضوی	طرح الزهرانی و همکاران۲۰ [۴۲]
۲۵	طرح ساهو وهمکارا ن[21] [۴۳]	۲۰۱۹		حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۲۶	طرح کومار و همکاران[22] [۴۴]	۲۰۱۹		حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است
۲۷	سوجانیا و همکارا ش[23] [۲۰]	۲۰۱۹	ارزیابی امنیتی طرح لی و همکارانش و ارائه یک پروتکل احرازهویت گمنام برای سامانه‌های مراقبت پزشکی پوشیدنی	حمله افشای مقادیر مخفی توسط مهاجم داخلی غیرفعال، حمله جعل، حمله تکرار و حمله ناهمزمان‌سازی	مبتنی بر رمزنگاری خم بیضوی	(ECCPWS)

[1] Arshad and Rasoolzadegan
[2] Ostad Sharif et al
[3] Liu et al.
[4] Li et al.
[5] Chiou et al
[6] Deebak et al
[7] Chandrakar et al
[8] Li et al
[9] Sowjanya et al
[10] Yessad et al.
[11] Wu et al.
[12] Li et al.
[13] Mohit et al.
[14] Qi et al.
[15] Amin et al.
[16] Jiang et al.
[17] Ostad Sharif et al.
[18] Nikooghadam et al.
[19] Karthigaiveni et al.
[20] Alzahrani et al.
[21] Sahoo et al.
[22] Kumar et al.
[23] Sowjanya et al.

ردیف	نام طرح	سال ارائه	ویژگی طرح	نوع حمله	روش احرازهویت	طرح بهبودیافته
۲۸	طرح گارج و همکارا ن[1] [۴۵]	۲۰۲۰		حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۲۹	طرح شرالی و همکارا ن[2] [۴۶]	۲۰۲۰		حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۳۰	طرح روی و همکارا ن[3] [۴۷]	۲۰۲۰		حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.
۳۱	طرح ساهو و همکارا ن[4] [۴۸]	۲۰۲۰		حمله‌ای برای آن گزارش نشده است.	مبتنی بر رمزنگاری خم بیضوی	بهبودی برای آن ارائه نشده است.

۳. دلایل انجام طرح:

برقراری ارتباط در سامانه‌های اطلاعات‌پزشکی مراقبت از راه دور، منوط به احرازهویت متقابل کاربران به وسیله سرورهای پزشکی است. در راستای تحقق این هدف، طراحان پروتکل‌های احرازهویت و توافق‌کلید بسیاری را پیشنهاد داده‌اند. کارایی این طرح‌ها مستلزم وجود خصوصیاتی از قبیل: پیوندناپذیری، ناشناس‌بودن، حفظ حریم‌خصوصی و... است. تمامی این ویژگی‌های امنیتی جهت ارائه یک سازوکار برای مبادله کلید مخفی بین سرور و کاربر است تا به واسطه این ویژگی‌ها، امنیت در برابر حملات موجود از قبیل: جعل‌هویت، انکارسرویس و... فراهم‌شود. همان طور که گفته شد از آن جایی که رمزنگاری خم بیضوی امنیت یکسانی با دیگر اولیه‌های رمزنگاری اما با طول کلید کم‌تر فراهم می کند، خیلی از محققان به ارائه پروتکل های احراز هویت با استفاده از آن پرداخته‌اند ولی امنیت آنها توسط محققان مستقل بررسی نشده تا به امنیت آنها اطمینان حاصل شود. از این رو می‌توان ضرورت انجام این تحقیق را به موارد زیر خلاصه نمود.

- لزوم تحلیل امنیت پروتکل‌های احرازهویت مبتنی بر رمزنگاری خم بیضوی ECC موجود جهت اطمینان از امنیت آن‌ها و استفاده بدون نگرانی از آن‌ها در کاربردهای مختلف
- آزمودن امنیت الگوریتم‌های احرازهویت مبتنی بر رمزنگاری خم بیضوی ECC موجود با استفاده از انواع روش‌های صوری و غیر صوری و انواع ابزارهای تحلیل امنیتی
- بهبود امنیت پروتکل‌های امنیتی مبتنی بر رمزنگاری خم بیضوی ECC موجود برای رفع خطاها و ایرادات امنیتی آن‌ها
- طراحی پروتکل‌های امنیتی مبتنی بر رمزنگاری خم بیضوی ECC جدید مقاوم در برابر انواع حملات فعال و غیر فعال

و در نهایت تمام این اهداف منجر به پیاده‌سازی یک درگاه احراز هویت امن مبتنی بر رمزنگاری خم بیضوی ECC در کاربردهای سلامت الکترونیک خواهد شد.

۴. اهداف و محصولات طرح:

[1] Garg et al.
[2] Sherali et al.
[3] Roy et al.
[4] Sahoo et al.

هدف اصلی از این طرح تکمیل دستاوردهای طرح زیر است که در سال ۱۴۰۱ توسط مجری انجام شده است:
"بهبود امنیت خصوصی در سامانه‌های مراقبت پزشکی از راه دور "
در کنار این هدف اصلی، اهداف دیگری که به‌دست خواهند آمد به شرح زیر است:

۱. تحلیل و در نهایت افزایش امنیت طرح‌های احراز هویت موجود مبتنی بر رمزنگاری خم بیضوی
۲. ارائه پروتکل‌های احراز هویت امن جدید مبتنی بر رمزنگاری خم بیضوی

۳. برنامه و نحوهٔ اجرای طرح:

در راستای همین اهداف، اقدامات زیر در جهت تحلیل امنیتی طرح‌های احراز هویت موجود مبتنی بر رمزنگاری خم بیضوی و بهبود امنیت آنها انجام‌خواهدشد.

- بررسی پیشینه تحقیق
- تحلیل امنیتی پروتکل‌های احراز هویت مبتنی بر رمزنگاری خم بیضوی موجود با استفاده از نرم‌افزارهای تحلیل امنیتی خودکار مانند AVISPA، Scyther، Proverif و TAMARIN
- تحلیل امنیتی پروتکل‌های احرازهویت مبتنی بر رمزنگاری خم بیضوی موجود با استفاده از روش‌های غیرصوری و منطق‌های ریاضی مانندBAN و GNY
- مقاوم‌نمودن پروتکل‌های احرازهویت مبتنی بر رمزنگاری خم بیضوی آسیب‌پذیر در برابر حملات و بررسی امنیت نسخه‌های بهبود یافته با استفاده از انواع روش‌های صوری، غیرصوری و انواع نرم‌افزارهای تحلیل امنیتی
- طراحی پروتکل‌های احراز هویت جدید سبک وزن ایمن مبتنی بر ECC با کاربرد در سامانه‌های TMIS
- مستند سازی نتایج بدست آمده و انتشار مقاله

۴. برنامهٔ زمانی:

شماره مرحله / فعالیت	نام مرحله / فعالیت	مرحله / فعالیت پیش‌نیاز	درصد وزنی به کل پروژه	مدت زمان اجرا (ماه)	نمودار زمان‌بندی (ماه)											
					۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
۱	بررسی پیشینه تحقیق		٪۵	۱												
۲	تحلیل امنیتی پروتکل‌های احراز هویت مبتنی بر رمزنگاری خم بیضوی موجود با استفاده از نرم افزارهای تحلیل امنیتی خودکار مانند Avispa، Scyther، Proverif و TAMARIN	۱	٪۱۵	۲												

۳	تحلیل امنیتی پروتکل‌های احراز هویت مبتنی بر رمزنگاری خم بیضوی موجود با استفاده از روش‌های غیرصوری و منطق‌های ریاضی مانندBAN و GNY	۱و۲	٪۱۰	۲																			
۴	مقاوم‌نمودن پروتکل‌های آسیب‌پذیر در برابر حملات و اثبات امنیت آنها با انواع روش‌های صوری و غیرصوری و استفاده از انواع نرم‌افزارهای تحلیل امنیتی	۲-۳	٪۲۰	۲																			
۵	طراحی پروتکل‌های احراز هویت جدید سبک وزن ایمن مبتنی بر ECC با کاربرد در سامانه‌های TMIS	۲-۴	٪۲۰	۲																			
۶	مستند سازی و انتشار مقاله	۱-۶	٪۳۰	۳																			

۱. همکاران طرح:

- **دکتر معصومه صفخانی**: دکتری مهندسی الکترونیک- رمزنگاری، دانشیار گروه مهندسی نرم‌افزار دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی (https://scholar.google.com/citations?hl=en&user=C0CuSccAAAAJ&view_op=list_works&sortby=pubdate)
- دانشجویان تحت راهنمایی و تیم محققان همکار

۲. ابزار مورد نیاز:

- کامپیوتر پرسرعت برای مدلسازی و پیاده‌سازی و تحلیل امنیتی پروتکل‌های مختلف احراز هویت مبتنی بر رمزنگاری خم بیضوی ECC

۳. بودجه بندی:

ردیف	شرح هزینه	مبلغ ماهیانه (ریال)	تعداد ماه	جمع (میلیون ریال)
۱	دستمزد	۲۰۰۰۰۰۰۰	۱۲	۲۴۰
جمع کل (دویست و چهل میلیون ریال)				۲۴۰

۴. مراجع:

[1] Min Chen, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao, and Victor C.M.Leung. Body area networks: A survey. *Mobile Networks and Applications*., 16:171-193, 2011.

[2] Masoumeh Safkhani, Carmen Camara, Pedro Peris-Lopez, and Nasour Bagheri. RSEAP2: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing. *Vehicular Communications*, 28, 2021.

[3] Ankar Gupta, Meenakshi Tripathi, and Aakar Sharma. A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable device in WBAN. *Computer Communications*, 160:311-325,2020.

[4] Hamed Arshad, Vahid Teymoori, Morteza Nikooghadam, and Hassan Abbassi. On the security of a two-factor authentication and key agreement scheme for telecare medicine information systems. *Journal of Medical Systems*, 39(76), 2015.

[5] Jiaqing Mo, Wei Shen, and Weisheng Pan. An improved anonymous authentication protocol for wearable health monitoring systems. *Wireless Communications and Mobile Computing*, 2020.

[6] Xiong Li, Jieyao Peng, Mohammad S. Obaidat, Fan Wu, Muhammad Khurram Khan, and Chaoyang Chen. A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. *IEEE Systems Journal*, 14(19428538):39-50 .2019.

[7] Ruhul Amin, SK Hafizul Islam, G.P. Biswas, Muhammad Khurram Khan, and Neeraj Kumar. A robust and anonymous patient monitoring systme using wireless medical sensor networks. *Future Generation Computer System*s, 80: 483-495, 2018.

[8] Shehzad Ashraf Chaudhry, Muhammad Tawab Khan, Muhammad Khurram Khan, and Taeshik Shon. A multiserver biometric authentication scheme for TMIS using elliptic cuve cryptography. *Journal of Medical Systems*, 40(230), 2016.

[9] Nawel Yessad, Siham Bouchelaghem, Farah-Sarah Ouada, and Mawloud Omar. Secure and reliable patient body motion based authentication approach for medical body area networks. *Passive and Mobile Computing*, 42: 351-370, 2017.

[10] Mostafa Yavari, Masoumeh Safkhani, Saru Kumari, and Chien- Ming Chen. An improved blochchain- based authentication protocol for iot network management. *Security and Communication Networks*, 2020(8836214), 2020.

[11] Debiao He, Sherali Zeadally, Neeraj Kumar, and Hyouk Lee. Anonymous authentication for wireless body area networks with provable security. *IEE Systems Journal*,11(17390228): 2590-2601. 2016.

[12] He Debiao, Chen Jianhua. and Zhang Rui. A more secure authentication scheme for telecare medicine information systems. *Journal of Medical Systems*, 36:1989-1995, 2012.

[13] Xiaopeng Yan, Weiheng Li, Ping Li, Jiantao Wang, and Peng Gong. A secure biometrics-based authentication scheme for telecare medicine systems. *Journal of medical systems*,37(9972), 2013

[14] Zhu Zhian. An efficient authentication scheme for telecare medicine information systmes. *Journal of Medical Systems*, 36:3833-3838, 2012.

[15] Shehzad Ashraf Chaudhry, Husnain Naqvi, Khalid Mahmood, Hafiz Farooq Ahmad, and Muhammad Khurram Khan. An improved remote user authentication scheme using elliptic curve cryptography. *Wireless Personal Communication*, 96:5355-5373, 2017.

[16] Chun-Ta Li, Dong-Her Shih, and Chun-Cheng Wang. Cloud assisted mutual authentication and

privacy preservation protocol for telecare medical information systems. *Computers Methods and Programs in Biomedicine*. 157:191-203, 2018.

[17] Zuowen Tan. A user anonymity preserving three-factor authentication scheme for telecare medicine information systmes. *Journal of Medical Systems*, 38(16), 2014.

[18] Masoumeh Safkhani. Samad Rostampour, Ygal Bendavid. and Nasour Bagheri. IoT in medical pharmaceutical: Designing lightweight RFID security protocols for ensuring supply chain integrity. *Computer Networks*, 2020.

[19] Hamed Arshad and Morteza Nikooghadam. Three-factor anonymous authentication and key agreement scheme for telecare medicine information. *Journal of Medical Systmes*, 38 (136), 2014.

[20] K Sowjanya, Mou Dasgupta, and Sangram Ray. An elliptic curve cryptoghraphy based enhanced anonymous authentication protocol for wearable health monitoring systems. *International Journal of Information Security*, 19:129-146, 2020.

[21] Jiang Qi, Ma Jianfeng, Yang Chao, Ma Xindi, Shen Jian, and Shehzad Ashraf Chaudhry. Efficient end-to-end authentication protocol for wearable health monitoring systmes. *Computers and Electrical Engineering*, 63:182-195. 2017.

[22] Jianghong Wei, Xuexian Hu, and Wenfen Liu. An improved authentication scheme for telecare medicine information systmes. *Journal of Medical Systems*, 36:3597-3604, 2012.

[23] Ashok Kumar Das, Sherali Zeadally, and Mohammad Wazid. Lightweight authentication protocols for wearable devices. *Computers and Electrical Engineering*: 63:196-208, 2017.

[24] Leslie Lamport. Password authentication with insecure communication. *Communication of the ACM*, 24(11): 770-772, 1981.

[25] Mohammad Abdol Azim and Abbas Jamalipour. An efficient elliptic curve cryptography based authenticated key agreement protocol for wireless LAN securiy. HPSR. *2005 Workshop on Performance Switchingand Routing*, 2005.

[26] Chris Otto, Aleksandar Milenkovic, Corey Sanders, and Emil Jovanov. System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia*, 1(4): 307-326.2006.

[27] David Boyle, T Newe. A survey of authentication mechanism: Authentication for ad-hoc wireless sensor network. *IEEE Sensors Applications Symposium*, 2007.

[28] Ir.Bart Preneel and Dave Singelee. *Study and Design of a Security Architecture for Wireless Personal Area Networks*. Citeceer, 2008.

[29] Xuan Hung Le, Murad Khalid, and Ravi Sankar. An efficient mutual authentication and access scheme for wireless sensor networks in healthcare. *Journal of Networks*, 6(3),2011.

[30] Jingwei Liu and Kyung Sup Kwak. Hybrid security mechanisms for wireless body area networks. *2010 Second Internationl Conference on Ubiquitous and Fiuture Networks (ICUFN)*, 71(11475046), 2010.

[31] Mohammed Mana, Mohammed Feham, and Boucif Amar Bensaber. Trust key management scheme for wireless body area networks. *International Journal of Network Security*, 12(2):75–83, 2011.

[32] Chang-Kuo Yeh, Hung-Ming Chen, and Jung-Wen Lo. An authentication protocol for ubiquitous health monitoring systems. *Journal of Medical and Biological Engineering*:415–419, 2013.

[33] Zhenguo Zhao, An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. *Journal of Medical systems*, 38(13), 2014.

[34] Debiao He and Sherali Zeadally. Authentication protocol for an ambient assisted living system. *IEEE Communications Magazine*. 53(14863802):71-77, 2015.

[35] Jingwei Liu, Lihuan Zhang, and Rong Sun. 1- RAAP: an efficient 1-round anonymous authentication protocol for wireless body area networks. *wireless communications*,16(5),2016.

[36] Fan Wu, Xiong Li, Saru Kumari, Marimuthu Karuppiah, and Jian Shen. A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server. *Computer and Electrical Engineering*, 63(14863802):168–181, 2017.

[37] Xiong Li, Jieyao Peng, Saru Kumari, Fan Wu, Marimuthu Karuppiah and Kim-Kwang Raymond Choo. An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. *Computers and Electrical Engineering*, 61:238–249, 2017.

[38] S.K.Hafizul Islam, Ruhul Amin, G.P Biswas, Mohammad Sabzinejad Farash, Xiong Li, and Saru Kumari. An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments. *Journal of King Saud University-Computer and Information Science*, 29(3):311-324,2017.

[39] Masoumeh Safkhani, Nasour Bagheri, Saru Kumari, Hamidreza Tavakoli, Sachin Kumar, and Jiahui Chen. RESEAP: an ecc-based authentication and key agreement scheme for iot applications. *IEEE Access*, 8(20140216):200851–200862, 2020

[40] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. *An Introduction to Mathematical Cryptography*. Springer, 2008.

[41] Adesh Kumari, Srinivas Jangirala, M. Yahya Abbasi, Vinod kumar, and Mansaf Alam. ESEAP: ECC based secure and efficient mutual authentication protocol using smart card. *Journal of Information Security and Applications*, 51(102443), 2020.

[42] Ashok Kumar Das, Mohammad Wazid, Animi Reddy Yannam, Joel J.P.C Rodrigues, and Youngho Park. Provably secure ECCbased device access control and key agreement protocol for iot environment. *IEEE Access*, 7(18648442):55382–55397, 2019.

[43] Ashok Kumar Das, Mohammad Wazid, Neeraj Kumar, Athanasios V Vasilakos, and Joel J.P.C Rodrigues. Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet ot things deployment. *IEEE Internet of Things Journal*,5(6):4900-4913, 2018.

[44] Masoumeh Safkhani andNasour Bagheri. Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things. *The Journal of Supercomputing*, 73:3579–3585, 2017.

[45] Masoumeh Safkhani and Mahyar Shariat. Implementation of secret disclosure attack against two iot lightweight authentication protocols. *The Journal of Supercomputing*,74:6220–6235, 2018.

[46] Danny Dolev and Andrew C.Yao. On the security of public key protocols. *IEEE Transactions on Information Theory, 29:198–208, 1983.*

[47] M Burrows, M Abadi and Roger Michael Needham. A logic of authentication. *Proceedings Mathematical Physical and Engineering Sciences*, 426:233-271, 1989.

[48] Li Gong, Roger Needham, and Raphael Yahalom. Reasoning about belief in cryptographic protocols. *IEEE Symposium on Security and Privacy*, 234–248, 1990

[49] Laura Takkinen. Analysing security protocols with AVISPA. *TKK T-110.7290 Research Seminar on Network Security*, 12(1), 2006.

[50] Cas J.F Cremers. The Scyther Tool: *Verification, Falsification, and Analysis of Security Protocols*. Springer, 2008.

[51] Ralf Kusters and Tomasz Truderung. Using proverif to analyze protocols with diffie-hellman exponentiation. *2009 22nd IEEE Computer Security Foundations Symposium*,2009.

[52] Bhawna Narwal and Amar Kumar Mohapatra, A survey on security and authentication in wireless body area networks, *Journal of Systems Architecture, ELSEVIER*, 113, 2020.

[53] Ajay Kumar, Kumar Abhishek, Xuan Liu, and Anandakumar Holdorai. An efficient privacy-preserving ID centric authentication in iot based cloud servers for sustainable smart cities. *Wireless Personal Communications*, 117:3229–3253, 2021.

[54] Samad Rostampour, Masoumeh Safkhani, Ygal Bendavid, and Nasour Bagheri. Eccbap: A secure ecc-based authentication privacy-preserving protocol for iot edge devices. *Pervasive and Mobile Computing*, 67(101194), 2020.