مقاله پژوهشی

یک پروتکل تشخیص و احراز هویت بیمار به منظور افزایش امنیت

افسانه شرفی، سپیده آدابی، علی موقر رحیم‌آبادی و صلاح ال مجید

چکیده: امروزه فناوری اطلاعات همراه با گسترش روزافزون اینترنت اشیا، جهان فیزیکی را به تعامل بیشتر با محرک‌ها، حسگرها و دستگاه‌ها سوق داده است. نتیجه این تعامل، برقراری ارتباط "هر زمان و هر مکان" در دنیای واقعی است. خلأ تحقیقی که بتواند در کنار فراهم‌ساختن پروتکلی چندلایه و بسیار امن (پروتکلی که هم‌زمان، کار شناسایی و احراز هویت را انجام می‌دهد) و در عین حال بار محاسباتی کمی داشته باشد، احساس می‌شود. بنابراین در حوزه سلامت و درمان و به منظور پایش از راه دور بیمارانی با معلولیت جسمی و ذهنی (مانند بیماران فلج مغزی و قطع نخاع) نیاز مبرم به یک پروتکل بسیار امن وجود دارد. پروتکل پیشنهادی ما در این مطالعه یک پروتکل دولایه به نام "شناسایی- احراز هویت" می‌باشد که بر اساس EEG و اثر انگشت ساخته شده است. همچنین مرحله احراز هویت ما، الگوریتم اصلاح‌شده دیفی- هلمن است. این الگوریتم به دلیل مشکل امنیتی (وجود نفر سوم) نیاز به اصلاح دارد که روش پیشنهادی با دریافت اثر انگشت و سیگنال EEG بیمار، با دقت بسیار بالا و سرعت بالایی قادر به انجام احراز هویت بیمار است. پروتکل پیشنهادی با استفاده از داده‌های ۴۰ بیمار مبتلا به آسیب نخاعی ارزیابی شده و نتایج پیاده‌سازی، امنیت بیشتر این پروتکل را نشان می‌دهد. صحت عملکرد این پروتکل مورد بررسی قرار گرفته و زمان پردازش آن در مرحله احراز هویت نیز به ۰٫۰۲۱۵ ثانیه کاهش یافته است.

***کلیدواژه:* اینترنت اشیا، احراز هویت، امنیت، سیگنال EEG.**

۱- مقدمه

اینترنت اشیا (IoT)[1] شبکه‌ای متشکل از تمامی دستگاه‌هایی است که می‌توانند از طریق اینترنت به یکدیگر اتصال یابند. می‌توان به این دستگاه‌ها از راه دور دسترسی پیدا کرد و با استفاده از زیربنای شبکه موجود، آنها را کنترل نمود. بنابراین IoT مشارکت انسان با فناوری را کاهش می‌دهد، صحت و کارایی آن را بهبود می‌بخشد و در نتیجه منجر به سود اقتصادی می‌شود [۱]. به طور کلی، هدف اصلی IoT، ارائه یک زیرساخت شبکه با پروتکل‌های ارتباطی و نرم‌افزاری ارتباطی است که این پروتکل‌ها عبارت هستند از: پروتکل صف‌بندی پیشرفته پیام (AMQP)[2]، انتقال دورسنجی صف پیام (MQTT)[3]، خدمات کشف داده (DDS)[4]، انتقال حالت بازنمودی (REST)[5]، پروتکل مسیریابی (RPL)[6] و پروتکل انتقال ابرمتن (HTTP)[7] [۲] که اجازه اتصال و ادغام حسگرهای فیزیکی/ مجازی، رایانه‌های شخصی، دستگاه‌های هوشمند، اتومبیل‌ها و مواردی مانند یخچال، ماشین ظرف‌شویی، ماکروویو غذا و داروها را در هر زمان و در هر شبکه می‌دهد [۳].

اینترنت اشیا از اهمیت خاصی برخوردار است، زیرا اشیا وقتی بتوانند خود را به صورت دیجیتالی ارائه کنند، نهایتاً به پدیده‌ای بسیار فراتر از کلیتی که در واقعیت هستند، تبدیل خواهند شد. در چنین شرایطی ارتباط اشیا دیگر محدود به ما نیست، بلکه آنها با اشیای اطراف، داده‌های یک پایگاه داده و ... نیز در ارتباط قرار می‌گیرند [۴].

اینترنت اشیا از مجموعه‌ای از اشیای هوشمند تشکیل شده که در آن یک شیء هوشمند دارای ویژگی‌های زیر است [۵]:

۱) یک تجسم فیزیکی و مجموعه‌ای از شاخصه‌های فیزیکی (یعنی اندازه، شکل و ...) را دارا است.
۲) دارای حداقل توانایی‌های ارتباطی از قبیل توانایی دریافت پیام‌های ورودی و پاسخ‌گویی است.
۳) یک شناسه منحصر به فرد دارد.
۴) حداقل به یک نام و یک آدرس مرتبط باشد که نام، توصیف معنی‌داری از آن شیء بوده و آدرس همان رشته خوانا توسط ماشینی است که بتوان برای ارتباط با شیء از آن بهره برد.
۵) دارای برخی قابلیت‌های محاسباتی پایه‌ای (جزئی تا پیچیده) باشد.
۶) می‌تواند مجهز به وسایلی برای درک پدیده‌های فیزیکی (مثل حرارت، نور و سطح تابش الکترومغناطیسی) باشد.

به منظور برقراری امنیت در سرویس‌ها و دستگاه‌های IoT، چالش‌های امنیتی و حریم خصوصی از جمله حفاظت از داده و حریم خصوصی کاربر، احراز هویت و مدیریت هویت، مدیریت اعتماد، مجوزدهی و کنترل دسترسی، امنیت پایانه به پایانه و مقاومت در برابر حملات وجود دارد [۶].

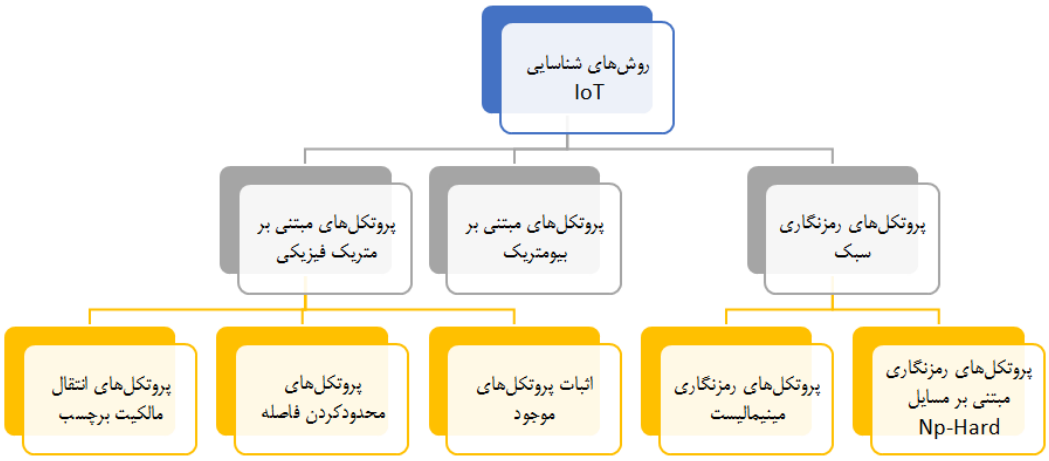
وجود اشیای هوشمند در دنیای اینترنت اشیا موجب می‌شود که ابزارهای جمع‌آوری کننده داده یا ردیابی در همه جا حاضر باشند، اما این ویژگی‌های مثال‌هایی از تهدیدات حریم خصوصی هستند که گسترش دنیای اینترنت اشیا را محدود می‌کنند [۷].

برای برقراری یک نشست امن بین دو طرف و تأیید اصالت و درستی آن نشست، در طی سال‌های گذشته پروتکل‌های احراز هویت بسیاری ارائه گردیده است. محققین مختلفی در زمینه امنیت در IoT به تحقیق

این مقاله در تاریخ ۲۱ فروردین ماه ۱۴۰۰ دریافت و در تاریخ ۳۰ مهر ماه ۱۴۰۰ بازنگری شد.

افسانه شرفی، گروه مهندسی کامپیوتر، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران، (email: a.sharafi1620@gmail.com).
سپیده آدابی، گروه مهندسی کامپیوتر، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران، (email: adabi.sepideh@gmail.com).
علی موقر رحیم‌آبادی، گروه مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران، (email: movaghar@sharif.edu).
صلاح ال مجید، دانشکده علوم کامپیوتر، دانشگاه لینکلن، انگلستان، (email: salmajeed@lincoln.ac.uk).

1. Internet of Things
2. Advanced Message Queuing Protocol
3. Message Queue Telemetry Transport
4. Data Distribution Service
5. Representational State Transfer
6. Recognition of Prior Learning
7. Hypertext Transfer Protocol



شکل ۱: پروژه‌ها و فعالیت‌های پژوهشی در شناسایی- احراز هویت [۱۸].

پرداخته‌اند. با توجه به مطالعات انجام‌شده بر روی پیشینه پژوهش، نویسندگان به این نتیجه رسیدند که عمده تحقیقات در زمینه برقراری امنیت از طریق احراز هویت صورت گرفته است. در این پروتکل‌ها برای ایجاد کلید نشست از روش رمزنگاری کلید عمومی در سطح گسترده‌ای استفاده می‌شود و در اکثر پروتکل‌های احراز هویت، طرفین یک نشست برای آن یک کلید محرمانه یا به اصطلاح کلید خصوصی ایجاد می‌کنند تا در طی پروسه جاری از آن برای رمزنگاری استفاده نمایند.

در این مقاله یک پروتکل دومرحله‌ای پیشنهاد شده که ضمن برقراری امنیت، زمان پردازش در مرحله احراز هویت را به زیر یک ثانیه کاهش می‌دهد و باعث افزایش سرعت و برقراری امنیت می‌شود. در این روش از سیگنال الکتروانسفالوگرافی مغزی بیمار و اثر انگشت بیمار استفاده گردیده است.

۲- کارهای گذشته

در [۸]، پروتکل احراز هویت توسعه‌پذیر (EAP)[1] و در [۹] تا [۱۱] از احراز هویت توسط مرکز توزیع کلید (KDC)[2] استفاده شده است. در این روش، هر کاربر تنها یک کلید دارد که بین او و مرکز توزیع KDC مشترک است و فرایند احراز هویت و ایجاد کلید نشست از طریق KDC انجام می‌شود. در [۱۲] و [۱۳] احراز هویت با استفاده از رمزنگاری کلید عمومی (PKI)[3] صورت گرفته است. در این روش، عملیات احراز هویت را را می‌توان با استفاده از رمزنگاری با کلید عمومی انجام داد. برای انجام چنین روشی در شبکه به یک مرکز توزیع کلید عمومی به نام PKI با ساختار سرویس‌دهنده دایرکتوری نیاز داریم که بتواند گواهی‌نامه کلید عمومی را تحویل دهد. مبادله کلید مشترک به روش دیفی- هلمن[4] نیز یکی دیگر از پروتکل‌های احراز هویت است که توسط محققین زیادی به کار گرفته شده است [۱۴] تا [۱۷]. در این روش فرض می‌شود که طرفین ارتباط قبلاً با یکدیگر ملاقات نکرده و در مورد یک کلید مشترک و سری هیچ توافقی نداشته‌اند. حال آنها باید حتی با آگاهی از وجود نفر سوم در ارتباط، باز هم کلید مشترک و سری ایجاد کنند.

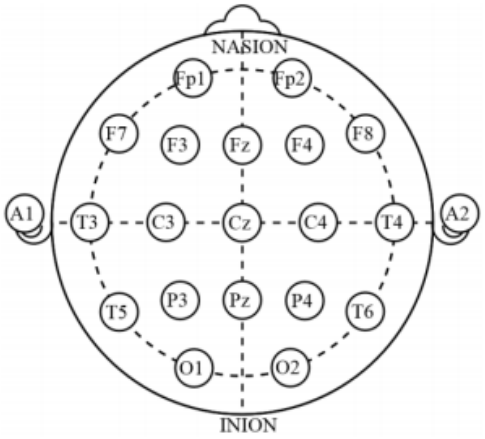
در [۱۸]، پروژه‌ها و فعالیت‌های پژوهشی در زمینه شناسایی- احراز هویت مطابق با شکل ۱ بیان شده است. مطابق با نظر چو ای و همکاران، ۳ سطح پروتکل‌های رمزنگاری سبک، پروتکل‌های مبتنی بر متریک‌های فیزیکی[5] و پروتکل‌های مبتنی بر بیومتریک، اصلی‌ترین روش‌های شناسایی و احراز هویت هستند. در سال‌های اخیر، تکنیک‌های بیومتریک (مانند اثر انگشت، شبکه عنبیه و تشخیص چهره) برای افزایش امنیت در دستگاه‌های هوشمند به جای روش‌های قدیمی (یعنی پسورد و پین‌کد) جایگزین شده است [۱۹] تا [۲۱].

در طراحی پروتکل‌های بیومتریک از پارامترهای بیومتریک مختلفی استفاده می‌گردد [۱۸]. در بین موارد گفته‌شده، الکتروانسفالوگرافی (EEG)[6] نسبت به سایر پارامترهای بیومتریک از مقبولیت بیشتری برخوردار بوده و مورد توجه محققین برای احراز هویت قرار گرفته است.

طراحی دستگاه بیومتریک نیاز به ویژگی‌های فیزیکی بیولوژیکی مانند اثر انگشت، گوش، چهره و ... دارد. مشکلات کلی این خصوصیات، فرایند کسب آسان آنها است و بنابراین تعداد حملات در این دستگاه‌ها زیاد است. برای کاهش شانس حملات در دستگاه احراز هویت تحقیقاتی جهت احراز هویت مبتنی بر امواج مغزی، EEG یک روش جایگزین است [۲۲]. این سبک احراز هویت دارای مزایای مختلفی نسبت به سایر دستگاه‌های احراز هویت است. رمز عبورها ممکن است فراموش شوند، کارت‌ها و کلیدها ممکن است گم شوند، ولی امواج مغزی همیشه حاضر هستند [۲۳]. در حقیقت می‌توان علت ارجحیت دستگاه‌های مبتنی بر EEG نسبت به دستگاه‌های بیومتریک را در امنیت بالا (نمی‌تواند تحریف شود) و بررسی این که آیا شخص زنده است یا خیر دانست [۲۴].

رابط کامپیوتر- مغز (BCI)[7] با استفاده از سیگنال‌های EEG برای احراز هویت افراد (به ویژه افراد مریض) به کار گرفته می‌شود. BCI یک ارتباط مستقیم بین کامپیوتر(ها) و مغز شخص است. دستگاهی است که کنترل دستگاه خارجی را با استفاده از سیگنال‌های اندازه‌گیری شده از مغز تسهیل می‌بخشد. BCI فعالیت‌های مغزی را اندازه‌گیری می‌کند و بنابراین سیگنال‌های مغزی مختلف به سیگنال‌های کنترلی تبدیل می‌شوند. یک EEG این امواج مغزی را با استفاده از الکترودهای غیر تهاجمی که سیگنال‌ها را ثبت می‌کنند، می‌خواند. یک الگوی منحصر به فرد را می‌توان به عنوان رمز عبور یا شناسایی بیومتریک به کار گرفت. زمانی که یک کار ذهنی را مانند تصویرسازی از یک شکل یا اجرای یک عمل انجام می‌دهیم، ذهن ما سیگنال‌های الکتریکی عصبی منحصر به

1. Extensible Authentication Protocol
2. Key Distribution Center
3. Public-Key Cryptography
4. Diffie-Hellman
5. Context-Related Physical Metrics Based Protocols
6. Electroencephalography
7. Brain-Computer Interface



شکل ۲: دستگاه ۲۰-۱۰ ثبت EEG [۳۲].

فردی تولید می‌کند. از افراد خواسته می‌شود تا کدرهایی را برای مدت زمان مشخصی انجام دهند تا سیگنال آنها کسب شود. این سیگنال‌های کسب‌شده، پیش‌پردازش گردیده و ویژگی‌های ضروری حوزه زمان و فرکانس استخراج شده و برای آموزش به دسته‌بندی‌کننده‌ها داده می‌شود. این سیگنال‌های دسته‌بندی شده برای اهداف احراز هویتی به کار گرفته می‌شوند [۲۵].

در [۲۶] بیان گردیده که استفاده از دستگاه‌های EEG در زمینه احراز هویت کاربر، دارای نقایصی همچون تجهیزات گران و ملزومات آزمایشگاهی و کاربری آن است. در این تحقیق، این دغدغه‌ها با استفاده از دستگاه EEG ارزان و به طور گسترده در دسترس به منظور بررسی قابلیت آن برای احراز هویت مورد بحث قرار گرفته‌اند. یک احراز هویت دومرحله‌ای که منجر به تقویت رمز عبور کاربر از طریق شکستن آن به بخش‌های کوچک‌تر، وابستگی به حالات ذهنی و ایجاد پد یک بار مصرف برای جلسه امن می‌شود، معرفی گردیده است. در [۲۷] یک روش دومرحله‌ای مبتنی بر EEG به منظور شناسایی شخص با دقت بالا به کار برده شده که بدین منظور از روش بردار پشتیبان SVM[1] و دسته‌بندی KNN[2] استفاده گردیده است. در این پژوهش از تعداد ۲۳ فرد مجموعاً ۹۰ سیگنال EEG اخذ شده که نتایج این پژوهش، حاکی از افزایش دقت شناسایی است. در [۲۸] یک پروتکل احراز هویت دومرحله‌ای دوطرفه با استفاده از امنیت سخت‌افزاری به نام (PUF)[3] با توجه به محدودیت‌های حافظه و انرژی دستگاه‌ها پیشنهاد شده است. همچنین از نظر زمان محاسبه و امنیت، آن را با پروتکل‌های مربوط در سناریوی اینترنت اشیای بهداشتی مقایسه کرده‌اند تا مناسب‌بودن و قدرت آن را نشان دهند. در [۲۹] یک روش شناسایی بر اساس سیگنال الکتروانسفالوگراف برای اینترنت اشیا ارائه گردیده که از دوربین استفاده شده است. این مقاله امنیت را مورد بررسی قرار داده و دقت روش شناسایی را ۹۲٪ تخمین زده است. دقت رمز عبور در این روش افزایش یافته ولی سربار زیاد در این روش باعث افزایش زمان پردازشی می‌شود.

در [۳۰] سیگنال الکتروانسفالوگرافی از ۴۶ بیمار دریافت شده و آزمایش تشخیص شناسایی بر روی آنها اعمال گردیده است. کلاس‌بندی برای سیگنال الکتروانسفالوگرافی یک‌کاناله انجام شده و دقت ۹۵/۴۸٪ را در مدت زمان ۲ ثانیه در بخش شناسایی به دست آورده است.

اکثر روش‌های ارائه‌شده یا فقط دارای مرحله شناسایی یا مرحله احراز هویت هستند و اگر هم هر دو مرحله را داشته باشند، تعداد سیگنال‌های نمونه آنها زیاد است. لذا نیاز به روشی که شناسایی و دقت بالایی داشته باشد، وجود دارد و بنابراین در این مقاله یک پروتکل مبتنی بر مرحله شناسایی و مرحله احراز هویت که فقط از یک سیگنال به عنوان نمونه استفاده می‌کند ارائه شده است.

۳- روش پیشنهادی

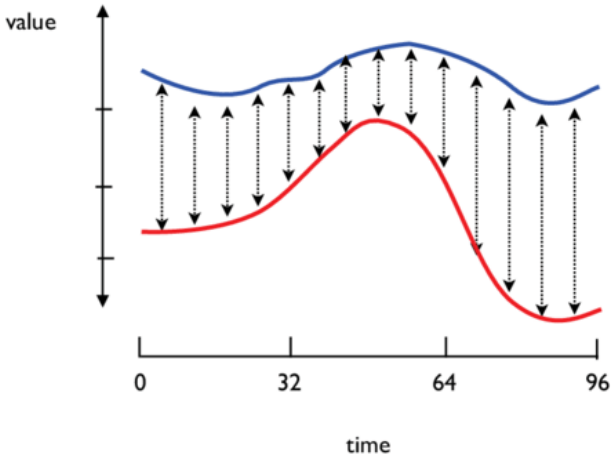
روش پیشنهادی که در این پژوهش ارائه گردیده است، یک پروتکل دولایه شناسایی- احراز هویت می‌باشد که احراز هویت در دو حالت غیر بهینه و بهینه صورت می‌گیرد و بر اساس EEG و اثر انگشت است. این پروتکل بهبودیافته دیفی- هلمن است که با ترکیب اثر انگشت و سیگنال مغزی با برقراری امنیت، زمان پردازش در مرحله احراز هویت را نیز بهبود داده است. استفاده از یک پروتکل امنیتی تک‌لایه مبتنی بر EEG می‌تواند منجر به یک دستگاه با امنیت پایین تحت معرض حملات مختلف شود. بنابراین ارائه پروتکلی که با در نظر گرفتن چالش‌های پیش روی احراز هویت مبتنی بر EEG بتواند امنیت بالایی نیز داشته باشد، امری ضروری است. در ادامه، ابتدا مختصری در مورد سیگنال EEG توضیح داده می‌شود و سپس پروتکل پیشنهادی با استفاده از سیگنال EEG و اثر انگشت تشریح می‌گردد.

۳-۱ الکتروانسفالوگرافی

مغز انسان یک ارگانیسم الکتروشیمیایی است. فعالیت الکتریکی نورون‌های مغزی به سطح جمجمه می‌رسند و این فعالیت الکتریکی بسیار ضعیف و در حد میکروولت است. نوار مغزی، الکتروانسفالوگرافی یا EEG ثبت فعالیت الکتریکی مغز از طریق نصب الکترودهای سطحی بر روی سر و به صورت غیر تهاجمی است. تفکیک‌پذیری زمانی سیگنال EEG برای سیگنال‌های مغز کمتر از یک میلی‌ثانیه است که برتری این سیگنال بر سایر روش‌های ثبت سیگنال محسوب می‌شود. برای افزایش تفکیک‌پذیری مکانی نیز از تعداد الکترود بیشتری در BCIهای مدرن (۲۵۶ الکترود) استفاده می‌شود [۳۱].

امروزه محل قرارگیری الکترودها در حین ثبت همگی استاندارد شده‌اند. یکی از استانداردهای متداول، دستگاه بین‌المللی ۲۰-۱۰ است که در آن سطح مغز به پنج ناحیه پیشانی[4]، پس سر[5]، آهیانه‌ای[6]، حاشیه‌ای[7] و گیجگاهی[8] تقسیم می‌گردد و تعدادی الکترود مطابق با شکل ۲ در محل‌های معینی از این پنج ناحیه قرار داده می‌شوند که هر یک با اندیس خاصی مشخص می‌گردند. این استاندارد برای افراد مختلف و در سنین مختلف قابل استفاده است. در نام‌گذاری شماره الکترودها باید دقت کرد که اندیس‌های زوج مربوط به الکترودهای نیم‌کره راست مغز و اندیس‌های فرد مربوط به نیم‌کره چپ هستند. اندیس‌های z هم مربوط به کانال‌هایی است که دقیقاً بر روی مرز میان دو نیم‌کره مغز واقع شده‌اند. همچنین در این استاندارد دو الکترود با نام‌های $A1$ و $A2$ به عنوان مرجع سنجش سایر پتانسیل به استخوان پشت گوش‌های چپ و راست متصل می‌شوند [۳۱].

1. Support Vector Machine
2. K-Nearest Neighbors
3. Physical Unclonable Functions
4. Frontal
5. Occipital
6. Partial
7. Limbic
8. Temporal



شکل ۳: مثالی از فاصله اقلیدسی بین دو سری.

سیگنال EEG برآیند فعالیت الکتریکی هزاران نورون مغزی است که در سطوح عمقی و سطحی قرار دارند. این سیگنال در هر نقطه انعکاس الکتریکی فعالیت‌های نورون‌های مغز در آن نقطه است، اما رزولوشن فضایی آن محدود بوده و به تعداد الکترون‌ها بستگی دارد. در سیگنال‌های EEG، مؤلفه‌های با فرکانسی فوق‌العاده بالا خیلی زیاد دیده می‌شوند که از نظر کلینیکی مگر در شرایط خاصی اهمیتی ندارند. به همین دلیل در نمونه‌برداری عادی، محدوده خاصی از فرکانس‌ها در نظر گرفته می‌شود که از نظر فیزیولوژی اعصاب و روان دارای اهمیت بیشتری هستند. این محدوده بین ۱ تا ۱۰۰ هرتز و در حالت محدودتر بین ۰٫۳ تا ۷۰ هرتز است. در یک فرد بالغ نرمال بیدار، محدوده فرکانس‌های پایین (۰٫۳ تا ۷ هرتز) و فرکانس‌های بالا (بالاتر از ۳۰ هرتز) به ندرت دیده می‌شود، در حالی که فرکانس‌های متوسط بین ۸ تا ۱۴ هرتز و فرکانس‌های بالا بین ۱۴ تا ۳۰ هرتز، ریتم غالب را تشکیل می‌دهند. طبقه‌بندی معمول ریتم‌های اصلی EEG بر اساس محدوده‌های فرکانسی صورت می‌گیرد که عبارت هستند از: دلتا (δ) (۰٫۱ تا ۴ هرتز)، تتا (θ) (۴ تا ۸ هرتز)، آلفا (α) (۸ تا ۱۳ هرتز)، بتا (β) (۱۳ تا ۳۰ هرتز) و گاما (γ) (بالای ۳۰ هرتز) [۳۱].

در جدول ۱ بازه‌های فرکانسی مختلف و فعالیت‌های ذهنی انجام‌شده آنها آمده است.

۳-۲ پروتکل پیشنهادشده

در ادامه جزئیات دو مرحله پیشنهادی در پروتکل دولایه شناسایی- احراز هویت پیشنهادشده در این مقاله بحث می‌گردد.

مرحله شناسایی

در مرحله شناسایی، زمانی که وضعیت اورژانسی می‌شود و نیاز به مراقبت و درمان وجود دارد، حسگرهای متصل به بدن بیمار، سیگنال EEG را اخذ کرده و از طریق اینترنت به پایگاه داده بیمارستان منتقل می‌کند. علاوه بر این، بیمار باید انگشت خود را روبه‌روی دستگاه اثر انگشت قرار دهد تا اطلاعات اثر انگشت وی نیز به پایگاه داده بیمارستان منتقل گردد. روش شناسایی مورد استفاده در تحقیق حاضر، تطبیق الگوی مبتنی بر فاصله اقلیدسی (ED)[1] است که توسط گوی و همکاران [۳۲] معرفی شده است. فاصله اقلیدسی، روشی برای نشان‌دادن فاصله بین دو نقطه در فضای اقلیدسی است. برای دو سری زمانی، روش اقلیدسی،

جدول ۱: بازه‌های فرکانسی سیگنال EEG [۳۳].

باند	فرکانس (هرتز)	وضعیت مغز
δ	۰٫۱-۴	خواب عمیق یا بیهوشی
θ	۴-۸	خواب و رؤیادیدن
α	۸-۱۳	آرام و بدون حرکت و حالت هوشیار
β	۱۳-۳۰	آرامش همراه با تفکر
γ	۳۰-۱۰۰	فعالیت‌های حرکتی

مجموع فاصله بین دو نقطه را به عنوان میزان فاصله مطابق با (۱) به دست می‌آورد (شکل ۳ را ببینید). اگر مقدار فاصله کم باشد می‌توان نتیجه گرفت که بین دو سری، شباهت‌های زیادی وجود دارد و در غیر این صورت دو سری زمانی، متفاوت از هم تلقی می‌شوند. با این حال، ضعف روش ED این است که اگر تأخیر زمانی یا ناهماهنگی در دو سری وجود داشته باشد، روش ED مقدار شباهت ضعیفی از خود نشان داده و به سختی مشخص‌کننده شباهت بین دو سری خواهد بود

$$ED = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + ?+ (p_N - q_N)^2} \qquad (1)$$

که در آن $\{p_1, p_2, \ldots, p_N\}$ و $\{q_1, q_2, \ldots, q_N\}$ مؤلفه‌های دو سری p و q با تعداد N نمونه است.

در روش ED، مقادیر حداقل فاصله برای ارزیابی شباهت بین دو سری استفاده شده و سپس درباره پذیرش/ رد شناسایی تصمیم گرفته می‌شود. بدین منظور، نیازمند به مقایسه الگوی EEG ذخیره‌شده در پایگاه داده بیمارستان و سیگنال ارسالی از طرف بیمار هستیم. برای یک بیمار خاص، الگوهای EEG در واکنش به محرک‌های بصری مشابه در آزمایش‌های مختلف در طول زمان، مشابه هم باقی می‌مانند. اما برای افراد مختلف، الگوهای مغزی آنها حتی برای محرک‌های مشابه، متفاوت از هم می‌باشند. بنابراین پس از جمع‌آوری الگوی جدید، نیاز به تجزیه و تحلیل برای شناسایی صاحب آن است. ما ابتدا آنها را با الگوهایی که از قبل شناخته شده است (ذخیره‌شده در پایگاه داده بیمارستان)، مقایسه و فاصله بین الگوی جدید و الگوی مرجع ذخیره‌شده را محاسبه می‌کنیم. نهایتاً کمترین فاصله به عنوان ملاک تصمیم در نظر گرفته می‌شود. شکل ۴ فرایند کلی مرحله شناسایی را نشان می‌دهد.

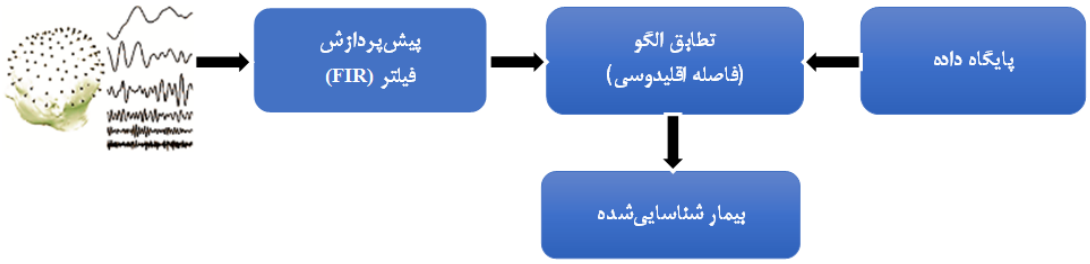
اگر الگوی EEG دریافتی با الگوی موجود متناسب نباشد، در این صورت سیگنال دریافتی به عنوان سیگنال جعلی (حمله) در نظر گرفته شده و عملیات متوقف گردیده و هشداری به بیمارستان ارسال نمی‌شود. با این حال اگر الگوی سیگنال EEG موفقیت‌آمیز به تأیید برسد، در این صورت عملیات شناسایی بیمار موفق بوده و لایه دوم پروتکل که مربوط به احراز هویت مبتنی بر روش دیفی- هلمن است، باز می‌شود.

به منظور ارزیابی روش فاصله اقلیدسی به عنوان یک نوآوری و بهبود این روش با پوشش ضعف آن که در (۲) نمایش داده شده است، از حاصل تقسیم اندازه تفاضل مجموع دامنه‌های دو سیگنال مرجع و سیگنال ارسالی بیمار بر ماکسیمم مقدار دامنه سیگنال مرجع استفاده می‌کنیم

$$y = \frac{\left|\sum_i Ar_i - \sum_i A1_i\right|}{\max Ar} \quad , \; 1 \le i \le 10 \qquad (2)$$

که Ar دامنه سیگنال مرجع و $A1$ دامنه سیگنال بیمار است. چنانچه مقدار y کمتر از ۱۰ باشد، شناسایی با موفقیت مورد پذیرش قرار می‌گیرد و در غیر این صورت رد می‌شود. بنابراین کاملاً واضح است که شرط

1. Euclidean Distance



شکل ۴: فرایند کلی مرحله شناسایی.

ذکرشده می‌تواند به عنوان یک فیلتر اولیه بسیار خوب برای شناسایی سیگنال‌های جعلی به کار گرفته شود.

مرحله احراز هویت

در این مرحله اطلاعات سیگنال EEG و اثر انگشت بیمار (بیمار باید انگشت خود را بر روی دستگاه اثر انگشت بگذارد تا اطلاعات آن به پایگاه داده بیمارستان ارسال شود) به اعداد طبیعی تبدیل می‌شوند. تبدیل سیگنال EEG به اعداد طبیعی به این صورت است که فرایند قدر مطلق اندازه دامنه‌های سیگنال کنار هم قرار می‌گیرد تا یک عدد تک‌رقمی حاصل شود. به عنوان مثال، فرض کنیم سیگنال EEG دارای ۵ نمونه با دامنه‌های [۴٫۸، ۱٫۶-، ۵٫۲، ۳٫۷، ۱۲٫۳] باشد. فرایند این اعداد برابر است با [۵، ۲-، ۵، ۴، ۱۲] و بنابراین عدد حاصل از سیگنال EEG به صورت (۳) خواهد بود

$$EEGNumber = '۱۲۴۵۲۵' \quad (۳)$$

استخراج اعداد اثر انگشت نیز از طریق استخراج مینوشیای اثر انگشت حاصل می‌شود. هر دو عدد حاصل از EEG و اثر انگشت اعداد منحصر به فرد هستند اما تعداد این ارقام زیاد (شاید بیش از ۵۰۰ رقم) است و بار محاسباتی الگوریتم دیفی- هلمن با این تعداد ارقام بسیار زیاد می‌شود. بنابراین به عنوان یک ایده جدید و امن، کامپیوتر پایگاه داده عدد تصادفی $n<۱۰۰۰$ را انتخاب می‌کند و سپس از ارقام $n+۱۱$ تا $n+۱۵$ اثر انگشت را انتخاب می‌نماید. اگر عدد به دست آمده مشابه به عدد ذخیره‌شده در پایگاه داده بیمارستان باشد، پروتکل ادامه می‌یابد و در غیر این صورت، عملیات متوقف خواهد شد. پس از آن کامپیوتر یک عدد تصادفی $k<l$ تولید می‌کند. سپس مجموع دامنه سیگنال ارسالی از طرف بیمار $(e۲)$ و سیگنال ذخیره‌شده در پایگاه داده بیمارستان $(e۱)$ بین k و ۱ را محاسبه می‌کند (نتیجه آن یک عدد m رقمی است) و آنها را با هم مقایسه می‌نماید. اگر اختلاف بین دو عدد کمتر از ۲۵٪ باشد (۲۵٪ ضریب دقت می‌باشد که به طور فرضی انتخاب شده است)، پروتکل ادامه می‌یابد و در غیر این صورت متوقف می‌شود. اگر این مرحله با موفقیت همراه باشد، اعداد حاصل از اثر انگشت و سیگنال EEG با هم ترکیب شده و یک عدد $m+۵$ رقمی تشکیل می‌دهند که آن را به عنوان پارامتر p در نظر می‌گیریم (شکل ۵). همچنین $p۱$ اثر انگشت ارسالی بیمار و $p۲$ اثر انگشت ذخیره‌شده در پایگاه داده بیمارستان می‌باشد. رویکرد مشابهی برای تولید عدد q اتخاذ می‌شود، با این تفاوت که اعداد بین $n+۵۱$ و $n+۵۳$ از اثر انگشت انتخاب می‌شوند که نتیجه آن یک عدد سه‌رقمی است. فرایند کلی مرحله احراز هویت در شکل ۵ نشان داده شده است.

در مرحله بعدی، الگوریتم دیفی- هلمن، عملیات تولید کلید مشترک را انجام داده و اگر این کلید یکسان باشد، هشدار به بیمارستان ارسال گردیده و آمبولانس به محل سکونت بیمار ارسال می‌شود.

پروتکل دیفی- هلمن دارای ۴ مرحله است:

۱) الگوریتم تولید پارامترهای دامنه

پارامترهای (p,q,g) را پارامترهای دامنه می‌نامیم.

ورودی: طول بیت مورد نیاز برای پیمانه p و مقسوم‌علیه اول q

خروجی: پارامترهای (g)

۱) تولید عدد اول تصادفی q با طول بیت مورد نیاز

۲) انتخاب عدد زوج تصادفی j با طول بیت $\text{bitlen}(p)-\text{bitlen}(q)$؛ (bitlen: طول بیت)

۳) محاسبه $p=jq+۱$. اگر p عدد اول نباشد، برو به مرحله ۲.

۴) انتخاب عدد تصادفی h در بازه $۱<h<p-۱$

۵) محاسبه $g=h^j$ به پیمانه p. اگر $g=۱$ برو به مرحله ۴.

۶) به دست آوردن (p,q,g)

۲) الگوریتم تصدیق پارامترهای دامنه

ورودی: پارامترهای (p,q,g)

خروجی: «تصدیق پارامترها» یا «عدم پذیرش پارامترها»

۱) بررسی این که آیا $۱<g<p-۱$ است. اگرنه، اعلام «عدم پذیرش پارامترها» و توقف.

۲) بررسی این که آیا q اول است. اگرنه، اعلام «عدم پذیرش پارامترها» و توقف.

۳) بررسی این که آیا p اول است. اگرنه، اعلام «عدم پذیرش پارامترها» و توقف.

۴) محاسبه $p-۱$ به پیمانه q. اگر این مقدار برابر صفر نباشد، اعلام «عدم پذیرش پارامترها» و توقف.

۵) محاسبه g^q به پیمانه p. اگر این مقدار برابر ۱ نباشد، اعلام «عدم پذیرش پارامترها» و توقف.

۶) اعلام «تصدیق پارامترها»

۳) الگوریتم تولید جفت کلید

ورودی: پارامترهای (p,q,g)

خروجی: جفت کلید خصوصی/عمومی سمت A، (a,A) و سمت B، (b,B)

سمت A:

۱) سمت A عدد a را در بازه $[۲,q-۲]$ انتخاب می‌کند.

۲) محاسبه $A=g^a$ به پیمانه p

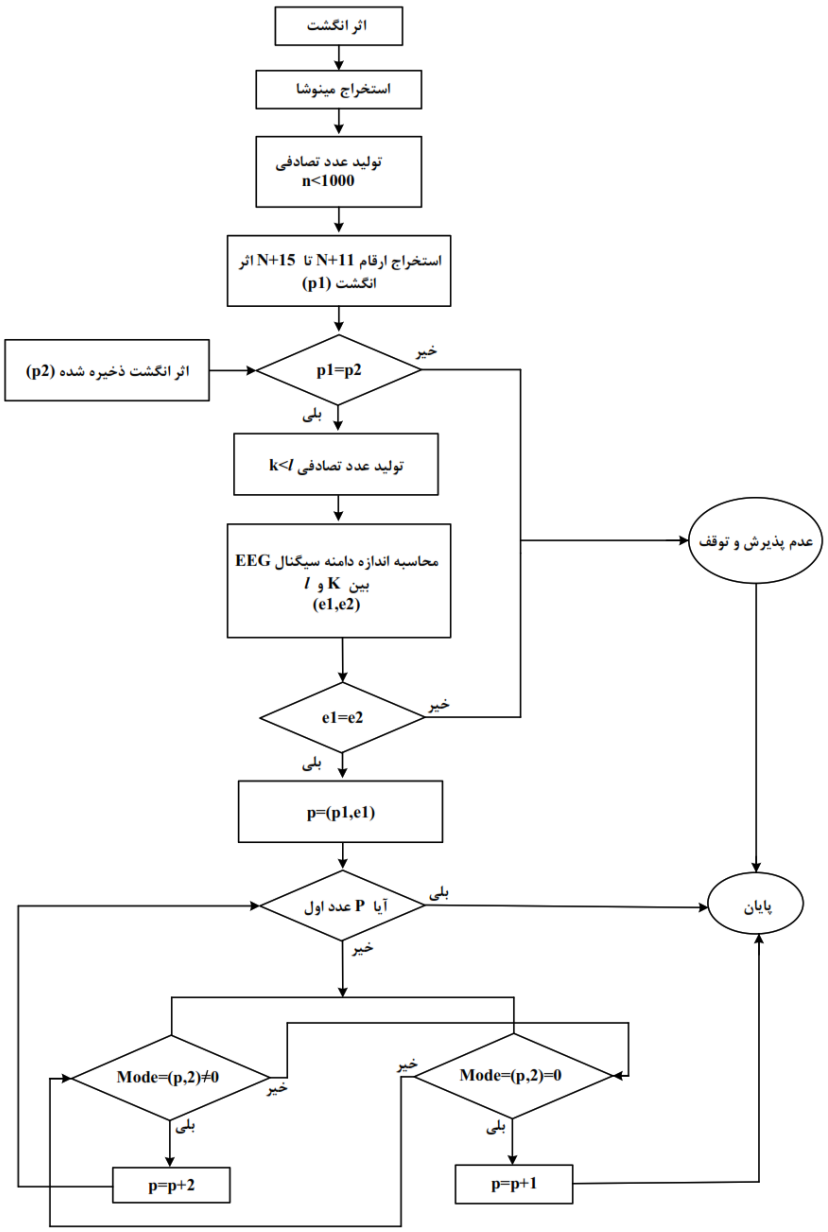
۳) به دست آوردن (a,A). نگهداری a به عنوان رمز. ارسال A به سمت B.

سمت B:

۱) سمت B عدد b را در بازه $[۲,q-۲]$ انتخاب می‌کند.

۲) محاسبه $B=g^b$ به پیمانه p

۳) به دست آوردن (b,B). نگهداری b به عنوان رمز. ارسال B به سمت A.



شکل ۵: نحوه تولید پارامتر p از اثر انگشت و سیگنال EEG.

٤) الگوریتم محاسبه رمز مشترک

سمت A:

ورودی: پارامترهای (p,q,g)، B و a

خروجی: رمز مشترک Z

۱) بررسی این که آیا $1 < B < p$ و B^q به پیمانه p برابر ۱ است. اگرنه، اعلام «شکست» و توقف.

۲) محاسبه $Z = B^a$ به پیمانه p

۳) به دست آوردن Z

سمت B:

ورودی: پارامترهای (p,q,g)، A و b

خروجی: رمز مشترک Z

۱) بررسی این که آیا $1 < A < p$ و A^q به پیمانه p برابر ۱ است. اگرنه، اعلام «شکست» و توقف.

۲) محاسبه $Z = A^b$ به پیمانه p

۳) به دست آوردن Z

تفاوتی که الگوریتم پیشنهادی با پروتکل دیفی- هلمن دارد، مرحله اول است که مربوط به تولید پارامترهای دامنه می‌باشد. هر دو پارامتر q و g از اطلاعات مربوط به سیگنال EEG و مینوشیای اثر انگشت به دست خواهند آمد و البته این اعداد باید اعداد اول باشند. به جای تولید تصادفی این اعداد از ترکیب سیگنال EEG و اثر انگشت، جهت افزایش امنیت از یک عدد منحصر به فرد حاصل از ترکیب سیگنال EEG و اثر انگشت استفاده خواهد شد. بنابراین مرحله اول پروتکل دیفی- هلمن به صورت زیر اصلاح می‌شود:

الگوریتم اصلاح‌شده پیشنهادی تولید پارامترهای دامنه

ورودی: پارامترهای p، q و طول بیت مورد نیاز برای p

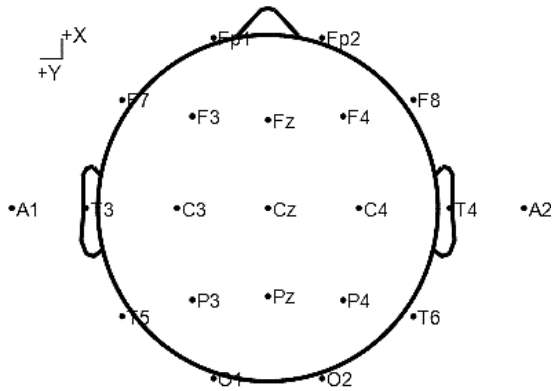
خروجی: پارامتر (g)

۱) استخراج عدد اول q و g با طول بیت مورد نیاز از ترکیب سیگنال EEG و اثر انگشت

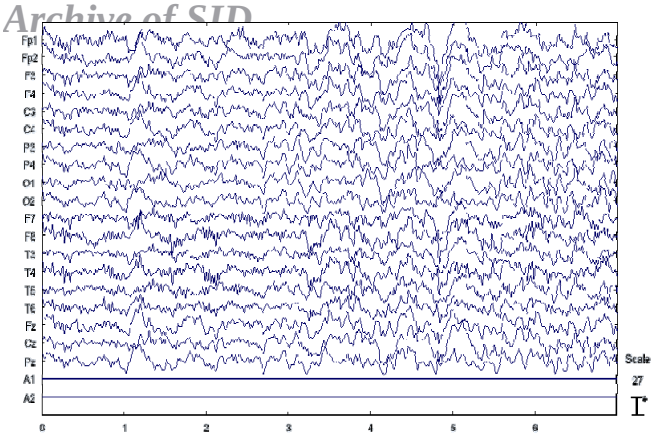
۲) انتخاب عدد زوج تصادفی j با طول بیت $\text{bitlen}(p) - \text{bitlen}(q)$؛ (bitlen: طول بیت)

۳) محاسبه $p = jq + 1$. اگر p عدد اول نباشد، برو به مرحله ۲.

۴) محاسبه g به پیمانه p. اگر $g = 1$ است، برو به مرحله ۴.



شکل ۶: موقعیت الکترودها بر روی سر.



شکل ۷: سیگنال‌های هر ۲۱ کانال برای بیمار شماره ۱.

جدول ۲: مشخصات بیماران.

چپ یا راست‌دست	سن	جنسیت	شماره بیمار	چپ یا راست‌دست	سن	جنسیت	شماره بیمار
راست‌دست	۴۷	زن	۲۱	راست‌دست	۷۶	مرد	۱
راست‌دست	۴۴	زن	۲۲	راست‌دست	۷۱	مرد	۲
راست‌دست	۴۳	زن	۲۳	راست‌دست	۶۹	مرد	۳
راست‌دست	۴۳	زن	۲۴	راست‌دست	۶۳	مرد	۴
راست‌دست	۴۳	زن	۲۵	چپ‌دست	۶۲	مرد	۵
راست‌دست	۴۰	زن	۲۶	راست‌دست	۵۸	مرد	۶
راست‌دست	۳۶	زن	۲۷	راست‌دست	۵۸	مرد	۷
راست‌دست	۳۳	زن	۲۸	راست‌دست	۵۲	مرد	۸
راست‌دست	۳۰	زن	۲۹	راست‌دست	۴۷	مرد	۹
راست‌دست	۲۳	زن	۳۰	چپ‌دست	۳۴	مرد	۱۰
راست‌دست	۳۱	زن	۳۱	راست‌دست	۲۸	مرد	۱۱
راست‌دست	۶۰	زن	۳۲	راست‌دست	۶۶	زن	۱۲
راست‌دست	۴۶	زن	۳۳	راست‌دست	۶۱	زن	۱۳
راست‌دست	۴۱	زن	۳۴	راست‌دست	۵۷	زن	۱۴
چپ‌دست	۴۹	زن	۳۵	راست‌دست	۵۴	زن	۱۵
راست‌دست	۵۲	زن	۳۶	راست‌دست	۵۳	زن	۱۶
راست‌دست	۴۸	زن	۳۷	راست‌دست	۵۱	زن	۱۷
چپ‌دست	۳۹	زن	۳۸	راست‌دست	۵۱	زن	۱۸
راست‌دست	۴۵	زن	۳۹	راست‌دست	۵۱	زن	۱۹
راست‌دست	۴۷	زن	۴۰	چپ‌دست	۴۸	زن	۲۰

۵) به دست آوردن (p)

البته با توجه به زیادبودن بار محاسباتی الگوریتم دیفی- هلمن به خاطر محاسبات زیاد هم‌نهشتی‌های اعداد اول، از روش توان‌رسانی سریع برای محاسبات هم‌نهشتی‌ها استفاده خواهد شد. در این حالت ضرب پیمانه‌ای از $n-1$ به تعداد $[\log n]$ کاهش پیدا می‌کند.

فرایند استخراج مینوشیای اثر انگشت از ۳ مرحله تشکیل شده است:

۱) گرفتن تصویر باینری

۲) نازک‌سازی تصویر باینری و تبدیل به تصویر اسکلتی[1]

۳) استخراج مینوشیا

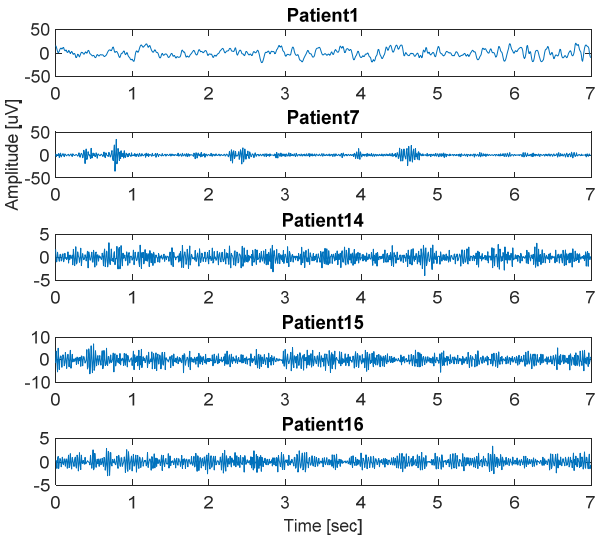
٤- ارزیابی پروتکل پیشنهادی

به منظور ارزیابی پروتکل پیشنهادی سیگنال‌های EEG، ۴۰ بیمار ضایعه نخاعی مشتمل بر ۱۱ مرد و ۲۹ زن با میانگین ۴۸/۷۵ سال از بیمارستان کسرای تهران جمع‌آوری گردیده و مشخصات این بیماران در جدول ۲ آمده است. برای اخذ سیگنال EEG بیماران، از ۲۱ الکترود مطابق با شکل ۶ استفاده شده و نمونه‌برداری در فرکانس ۱۲۵ Hz در مدت زمان ۷ ثانیه بوده که در مجموع برای هر کانال تعداد ۸۷۵ نمونه اخذ گردیده و شبیه‌سازی پروتکل پیشنهادی نیز با استفاده از نرم‌افزار Matlab انجام شده است.

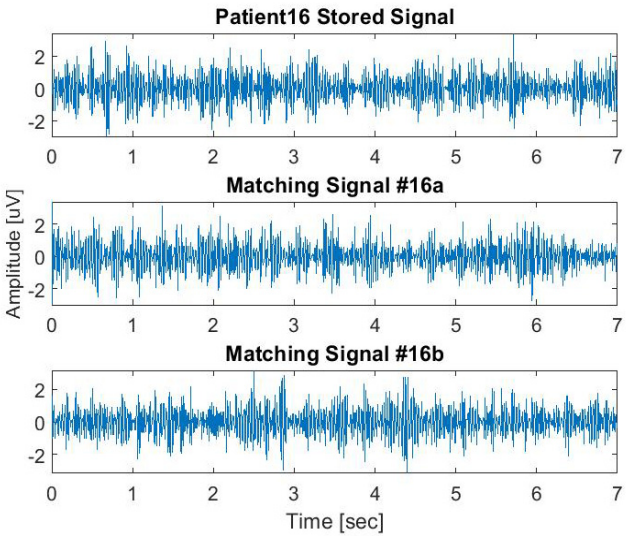
برای رفع نویزها از یک فیلتر FIR با فرکانس ۳۰ تا ۶۰ هرتز (باند گاما) به عنوان مرحله پیش‌پردازش سیگنال‌ها استفاده شده است. به عنوان نمونه، شکل ۷ سیگنال EEG بیمار ۱ را در هر ۲۱ کانال نمایش می‌دهد. پس از رفع نویزها، از داده‌های مربوط به کانال $O2$ برای انجام عملیات شناسایی و احراز هویت استفاده خواهد شد.

در شکل ۸ سیگنال EEG مربوط به ۵ بیمار مختلف به عنوان نمونه نشان داده شده و سیگنال‌های ۲۵ بیمار دیگر نیز به همین صورت می‌باشد. در اینجا، سیگنال مربوط به بیمار ۱۶ را به عنوان سیگنال مرجع که در پایگاه داده بیمارستان ذخیره شده است، در نظر گرفته و تمامی

1. Thinning Process



شکل ۸: سیگنال EEG ۵ بیمار مختلف در کانال O2.



شکل ۹: سیگنال‌های EEG بیمار ۱۶.

جدول ۳: نتایج مرحله شناسایی ۳۰ بیمار اول.

رد/ پذیرش	Y	ED	شماره بیمار	رد/ پذیرش	Y	ED	شماره بیمار
پذیرش	۶٫۲۵	۴٫۰۲۳	۱۶a	رد	۸۸٫۳۳	۵۰٫۳۵	۱
پذیرش	۵٫۳۵	۴۰٫۱۸	۱۶b				
رد	۲۶۵٫۱۰	۱۴۲٫۱۴	۱۷	رد	۱۰۵٫۴۲	۷۱٫۰۶	۲
رد	۹۱٫۰۶	۶۰٫۹۴	۱۸	رد	۱۱۶٫۳۹	۸۸٫۵۹	۳
رد	۱۰۹٫۶۲	۹۴٫۶۱	۱۹	رد	۷۹٫۳۳	۶۳٫۵۸	۴
رد	۷۰٫۶۱	۵۳٫۴۹	۲۰	رد	۲۲۰٫۱۴	۱۶۴٫۰۸	۵
رد	۹۴٫۷۲	۷۴٫۱۸	۲۱	رد	۱۰۵٫۴۱	۹۰٫۵۷	۶
رد	۵۶٫۷۹	۴۹٫۶۴	۲۲	رد	۴۶۶٫۷۶	۵۸٫۱۲۳	۷
رد	۱۰۶٫۷۲	۹۰٫۰۶	۲۳	رد	۹۸٫۴۲	۶۷٫۱۹	۸
رد	۹۱٫۰۶	۷۶٫۴۷	۲۴	رد	۸۰٫۹۵	۵۶٫۸۰	۹
رد	۶۲٫۰۱	۵۵٫۴۷	۲۵	رد	۱۰۱٫۷۹	۷۹٫۰۵	۱۰
رد	۱۸۷٫۴۶	۱۱۹٫۵۳	۲۶	رد	۲۴۹٫۰۱	۱۳۸٫۲۱	۱۱
رد	۱۶۴٫۲۴	۱۰۵٫۷۲	۲۷	رد	۸۶٫۳۵	۷۳٫۱۱	۱۲
رد	۸۰٫۳۱	۶۶٫۹۸	۲۸	رد	۱۳۰٫۶۰	۱۰۰٫۵۱	۱۳
رد	۶۸٫۴۱	۵۳٫۷۱	۲۹	رد	۱۹۹٫۳۸	۶۷٫۲۲	۱۴
رد	۱۰۱٫۴۷	۷۸٫۳۱	۳۰	رد	۸۶٫۹۲	۱۲۵٫۷۳	۱۵

سیگنال‌های بیماران دیگر را به عنوان سیگنال جعلی در نظر می‌گیریم که الگوریتم پیشنهادی باید به خوبی قادر به پذیرش سیگنال‌های ارسالی از طرف بیمار ۱۶ بوده و سیگنال‌های سایر بیماران را رد کرده و عملیات شناسایی و احراز هویت را متوقف سازد.

همان طور که ذکر شد، هدف ما بررسی کارایی الگوریتم پیشنهادی با توجه به سیگنال مرجع مربوط به بیمار ۱۶ است.

شکل ۹ سیگنال EEG ذخیره‌شده در پایگاه داده بیمارستان را برای بیمار ۱۶ و دو سیگنال دیگر این بیمار نشان می‌دهد. هدف این است که این دو سیگنال به همراه ۲۹ سیگنال مربوط به بیماران دیگر را ارزیابی کرده و نتیجه شکست یا موفقیت مربوط به عملیات شناسایی را بسنجیم و در ادامه، نتایج مرحله شناسایی و احراز هویت نشان داده می‌شود.

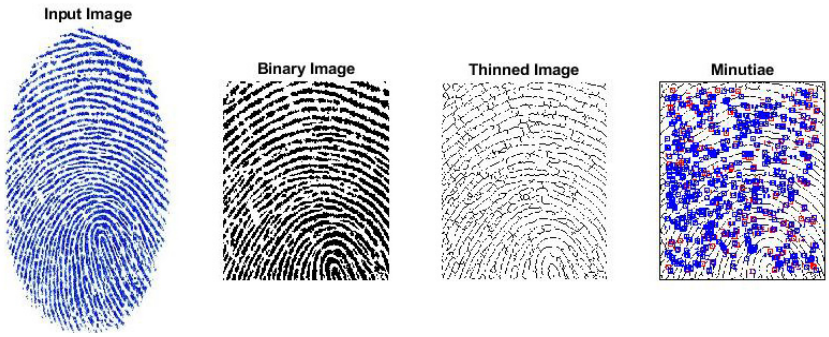
٤-١ نتایج مرحله شناسایی

نتایج حاصل از پیاده‌سازی الگوریتم پیشنهادی برای مرحله شناسایی که به طور کامل تشریح شد، در جدول ۳ آمده است. همان طور که مشخص است با در نظر گرفتن معیار پیشنهادی در این پژوهش (رابطه (۲))، تمامی سیگنال‌های مربوط به بیماران دیگر رد شده و تنها دو سیگنال مربوط به بیمار ۱۶ از مرحله شناسایی موفق عمل کرده‌اند که نشان از کارایی بالای روش پیشنهادی دارد. علاوه بر این، با توجه به نتایج نشان داده شده در این جدول، مشخص است که چنانچه صرفاً معیار فاصله اقلیدسی ED را برای مقایسه در نظر می‌گرفتیم، به خوبی قادر به رد یا پذیرش سیگنال‌ها نبودیم و با در نظر گرفتن معیار y، مرز بین رد یا پذیرش کاملاً از هم جدا شده است.

٤-٢ نتایج مرحله احراز هویت

در این بخش، سیگنال EEG ۱۶b را به عنوان سیگنالی که از مرحله شناسایی مورد پذیرش قرار گرفته است به همراه با اثر انگشت بیمار در اختیار داریم. شکل ۱۰ فرایند استخراج مینوشیا از اثر انگشت بیمار ۱۶ را نشان می‌دهد. پس از استخراج مینوشیا، عدد طبیعی حاصل از اثر انگشت از کنار هم قرار گرفتن bifurcationx و bifurcationy بر اساس (۴) به دست می‌آید

$$S = [bifurcation_x, bifurcation_y]_{1\times j} \qquad (۴)$$



شکل ۱۰: فرایند استخراج مینوشیا از اثر انگشت بیمار ۱۶.

جدول ۴: استخراج پارامترهای p و q از اثر انگشت و سیگنال EEG.

اعداد اول	p و q	تفاوت بین دو سیگنال (٪)	عدد الکتروانسفالوگرافی	عدد ذخیره‌شده الکتروانسفالوگرافی	k	عدد FP	n
۱۲۳۴۴۶۲۱	p : ۱۲۳۴۴۶۱۰	۲۰٫۵۵	۶۱۰	۵۱۳	۵۴۳	۱۲۳۴۴	۱۲۵
۸۱۴۶۰۱	q : ۸۱۴۵۸۰	۲۱٫۰۲	۵۸۰	۴۷۹	۵۱۰	۸۱۴	۵۵۱

جدول ۵: مشخصات دستگاه.

پردازنده	Intel(R) Core™ i۵
حافظه RAM	۶ GB
نوع سیستم عامل	سیستم عامل ۶۴بیتی
نسخه Matlab	R۲۰۱۷B

جدول ۶: کلید مشترک حاصل از الگوریتم دیفی- هلمن بهبودیافته و زمان پردازش مرحله احراز هویت.

زمان اجرا (ثانیه)	کلید اشتراکی	اعداد اول	
۰٫۰۲۱۵	۳۴۹۷۷۳۹	۱۲۳۴۴۶۲۱	p
		۸۱۴۶۰۱	q

که حاصل آن یک عدد j رقمی است که برای بیمار ۱۶، حاصل یک عدد ۶۱۹۲ رقمی می‌باشد. در این مرحله، پایگاه داده بیمارستان، یک عدد تصادفی $n<۱۰۰۰$ را تولید می‌کند که در اینجا برابر ۱۲۵ است. مطابق با روندنمای شکل ۵، ارقام ۱۳۶ تا ۱۴۰ از S استخراج می‌شود که برابر با ۱۲۳۴۴ است. این فرایند برای اثر انگشت ذخیره‌شده در پایگاه داده $(p_۲)$ و اثر انگشت ارسالی بیمار $(p_۱)$ انجام می‌شود. در این مرحله، یک مرحله امنیتی باز شده و این دو مقدار را با هم مقایسه می‌کند. چنانچه $p_۱=p_۲$ باشد، در این صورت مرحله بعدی شروع شده و یک عدد طبیعی دیگر از سیگنال EEG تولید می‌شود و در غیر این صورت (یعنی $p_۱\neq p_۲$) فرایند احراز هویت متوقف گردیده و سیگنال دریافتی به عنوان یک سیگنال جعلی شناخته می‌شود. در اینجا شرط $p_۱=p_۲=۱۲۳۴$ برقرار است و لذا وارد مرحله بعدی می‌شویم.

در این مرحله، فرایند قدر مطلق دامنه‌های سیگنال EEG را محاسبه می‌کنیم و با کنار هم قرار دادن آنها، یک عدد تک‌رقمی به دست می‌آوریم که در اینجا $l=۸۱۷$ است. در این مرحله، پایگاه داده مجدد یک عدد تصادفی $k<l$ تولید می‌کند که در اینجا $k=۵۴۳$ است. حال به محاسبه مجموع ارقام بین ۵۴۳ تا ۸۱۷ دو سیگنال EEG ذخیره‌شده در پایگاه داده $(e_۲)$ و ارسالی از طرف بیمار $(e_۱)$ می‌پردازیم. در اینجا $e_۱=۶۱۰$ و $e_۲=۵۱۳$ است. حال یک مرحله امنیتی جدید باز شده و اختلاف بین این دو عدد را محاسبه می‌کند، چنانچه این اختلاف کمتر از مقدار آستانه از پیش تعیین شده ۲۵٪ (از میانگین کل اعداد محاسبه می‌شود) باشد، عملیات ادامه خواهد یافت و در غیر این صورت عملیات متوقف گردیده و سیگنال ارسالی توسط بیمار به عنوان سیگنال جعلی تلقی می‌شود. در اینجا اختلاف بین این عدد برابر ۲۰٫۵۵٪ است که کمتر از مقدار آستانه ۲۵٪ تعیین شده است. حال با قراردادن دو عدد $p_۱$ و $e_۱$ در کنار هم، عدد دامنه p برای الگوریتم دیفی- هلمن بهبودیافته مطابق (۵) به دست می‌آید

$$p=[p_۱,e_۱]=۱۲۳۴۶۱۰ \quad (۵)$$

چون عدد دامنه الگوریتم دیفی- هلمن باید اول باشد، می‌بایست عدد به دست آمده طی عملیاتی به عدد اول تبدیل شود که فرایند این کار در روندنمای شکل ۵ نشان داده شده است. در حقیقت چنانچه عدد p یک عدد زوج باشد، آن را با ۱ جمع می‌کنیم و چنانچه p یک عدد فرد باشد، آن را با ۲ جمع می‌کنیم و این کار تا مادامی ادامه می‌یابد که به عدد اول برسیم. در اینجا عدد اول حاصل‌شده برابر $p=۱۲۳۴۴۶۲۱$ است. فرایند مشابهی برای عدد q نیز اتخاذ می‌شود. نتایج حاصل از استخراج اعداد دامنه الگوریتم دیفی- هلمن در جدول ۴ نشان داده شده است.

حال اعداد به دست آمده را به الگوریتم دیفی- هلمن بهبودیافته می‌دهیم و برای احراز هویت باید به کلید مشترک دست یابیم. در اینجا به کلید مشترک ۳۴۹۷۷۳۹ می‌رسیم که نشان از موفقیت مرحله احراز هویت است. از آنجایی که باید زمان پردازش الگوریتم در دستگاه مشخص باشد، پیکربندی محیط انتخابی برای آزمون در جدول ۵ آمده است. از ترکیب سیگنال EEG و اثر انگشت برای تولید پارامترهای دامنه استفاده می‌شود. در واقع برای افزایش امنیت از یک عدد منحصر به فرد که حاصل ترکیب این دومی باشد استفاده گردیده که در نتیجه با دقت و سرعت بالایی قادر به انجام احراز هویت بیمار می‌باشد. همچنین زمان اجرای کل مرحله احراز هویت در حد چند صدم است که نشان از سرعت بسیار بالای پروتکل پیشنهادی می‌باشد و زمان اجرای الگوریتم پیشنهادی در جدول ۶ گزارش شده است. برای ارزیابی عملکرد مرحله احراز هویت، برنامه نوشته‌شده برای این مرحله چندین بار اجرا گردید و نتایج مطابق با جدول ۷ به دست آمد که نشان از عملکرد صحیح الگوریتم دارد.

۴-۳ بررسی حمله مرد میانی در پروتکل پیشنهادشده

حمله مرد میانی زمانی رخ می‌دهد که مهاجم در شبکه خود را میان دو گره قرار می‌دهد و اطلاعات را در میان این دو گره به سرقت می‌برد. روش دیفی- هلمن در برابر حمله مرد میانی امن است، اما استفاده از سیگنال الکتروانسفالوگرافی می‌تواند برای امنیت این روش مشکل ایجاد

جدول ۷: نتایج حاصل از سه اجرای مختلف مرحله الگوریتم دیفی- هلمن بهبودیافته.

کلید اشتراکی	اعداد اول	p و q	تفاوت بین دو سیگنال (٪)	عدد الکتروانسفالوگرافی	عدد ذخیره‌شده الکتروانسفالوگرافی	عدد FP	شماره اجرا
۳۴۵۲۳۳۹۲	۹۷۰۱۲۶۰۷	۹۷۰۱۲۶۰۱	۱۹٫۴۸	۶۰۱	۴۷۰	۹۷۰۱۲	#۱
	۱۵۱۵۶۱	۱۵۱۵۶۰	۱۱٫۳۳	۵۶۰	۵۰۳	۱۵۱	
۱۳۲۳۹۷۴۴	۲۶۰۳۷۴۸۱	۲۶۰۳۷۴۵۳	۱٫۵۲	۴۵۳	۴۶۰	۲۶۰۳۷	#۲
	۱۹۴۵۶۹	۱۹۴۵۵۲	۱۹٫۲۲	۵۵۲	۴۶۳	۱۹۴	
۶۲۴۷۳۶۵۸	۷۱۹۴۲۵۹۳	۷۱۹۴۲۵۸۵	۲۱٫۸۷	۵۸۵	۴۸۰	۷۱۹۴۲	#۳
	۲۱۶۳۷۹	۲۱۶۳۷۷	۲۵	۳۷۷	۲۵۷	۲۱۶	

جدول ۸: مقایسه پروتکل پیشنهادشده در مقاله با روش‌های دیگر.

پروتکل	زمان پردازش	روش شناسایی/احراز هویت
مرجع [۲۵]	۸ >	---/استخراج ویژگی مبتنی بر EEG و دسته‌بندی
مرجع [۲۹]	۲	استخراج ویژگی/استخراج ویژگی و دسته‌بندی
مرجع [۳۴]	۲ >	---/استخراج ویژگی مبتنی بر EEG و دسته‌بندی
مرجع [۳۵]	۲ >	---/استخراج ویژگی مبتنی بر EEG و دسته‌بندی بر اساس منطق فازی
پروتکل پیشنهادی	۰٫۰۲۱۵	پروتکل دولایه با احراز هویت بهبودیافته/ کلید مشترک مبتنی بر EEG و اثر انگشت

کند که در پروتکل پیشنهادشده در این مقاله، امنیت این روش برقرار گردیده است. در روش ذکرشده، به علت این که سیگنال‌های مغزی هر بار با دفعه قبلی تفاوت‌هایی دارند و دقیقاً یکسان نیستند (طبق بخش ۳) و ماهیت پویا دارند و به علاوه از اثر انگشت استفاده شده که منحصر به فرد است (طبق بخش ۴)، در نتیجه نهایی یک عدد تصادفی تولید می‌شود (طبق بخش ۴-۲) که این عدد هر بار با دفعه قبلی متفاوت خواهد بود. بنابراین امکان حمله از طرف شخص حمله‌کننده در حمله مرد میانی امکان‌پذیر نیست.

۵- نتیجه‌گیری

در این مقاله یک پروتکل دولایه شناسایی- احراز هویت بیمار مبتنی بر EEG و اثر انگشت پیشنهاد شده است. در مرحله شناسایی، در شرایط اضطراری و نیاز به مراقبت و درمان، حسگر متصل به بیمار، سیگنال EEG را دریافت و آن را از طریق اینترنت به پایگاه داده بیمارستان منتقل می‌کند. ایده اولیه پیشنهادی، یک روش بهبودیافته فاصله اقلیدسی است چرا که مشکل روش اقلیدسی این است که اگر تأخیر زمانی یا ناهماهنگی در دو سری وجود داشته باشد، روش اقلیدسی به سختی شباهت بین دو سری را نمایش می‌دهد. حال آن که در روش اقلیدسی بهبودیافته، مجموع دامنه‌های دو سیگنال مرجع که در پایگاه داده بیمارستان است و سیگنال ارسالی بیمار از یکدیگر کم گردیده و حاصل این تفاضل بر ماکسیمم مقدار دامنه سیگنال مرجع تقسیم می‌شود. فاصله بین الگوی جدید سیگنال EEG و الگوی ذخیره‌شده در پایگاه داده بیمارستان با یکدیگر مقایسه شده و کمترین فاصله به عنوان ملاک تصمیم‌گیری انتخاب می‌گردد و بیشترین شباهت را نشان می‌دهد. نهایتاً با استفاده از سیگنال EEG، بیمار قادر به شناسایی دقیق وی بوده و سیگنال‌های جعلی (حمله) را رد کرده و مورد پذیرش قرار نمی‌دهد و به این ترتیب باعث افزایش امنیت می‌شود. مرحله احراز هویت مبتنی بر الگوریتم دیفی- هلمن بهبود یافته و تفاوتی که با پروتکل دیفی- هلمن دارد، در تولید پارامترهای دامنه است. در الگوریتم دیفی- هلمن از گروه هم‌نهشتی اعداد صحیح با پیمانه p و عملگر ضرب اعداد صحیح استفاده شده است، حال آن که در روش بهبودیافته از ترکیب سیگنال EEG و اثر انگشت برای تولید پارامترهای دامنه استفاده می‌شود. در واقع برای افزایش امنیت از یک عدد منحصر به فرد که حاصل ترکیب این دومی باشد استفاده شده که در نتیجه با دقت بسیار بالا و سرعت بالایی قادر به انجام احراز هویت بیمار می‌باشد.

پروتکل پیشنهادی با استفاده از داده‌های ۴۰ بیمار مبتلا به آسیب نخاعی ارزیابی شد. نتایج ارزیابی در جداول ۶ و ۷ و نتایج مقایسه در جدول ۸ نشان می‌دهند که پروتکل پیشنهادی از منظر معیارهای دقت و سرعت پردازش و مقاومت در برابر حملات، عملکرد بهتری دارد و زمان پردازش در احراز هویت را در مقایسه با روش‌های دیگر به کمتر از ۱ ثانیه یعنی ۰٫۰۲۱۵ ثانیه رسانده است. در کارهای آتی به منظور افزایش دقت و سرعت احراز هویت، استفاده از الگوریتم فراابتکاری ژنتیک (GA)[1] جهت انتخاب تطبیق بهینه سیگنال EEG پیشنهاد می‌شود. در واقع الگوریتم‌های ژنتیک از اصول انتخاب طبیعی داروین برای یافتن فرمول بهینه جهت پیش‌بینی یا تطبیق الگو استفاده می‌کنند. الگوریتم‌های ژنتیک اغلب گزینه خوبی برای تکنیک‌های پیش‌بینی بر مبنای رگرسیون هستند. این الگوریتم‌ها با تولید نسل آغاز می‌شوند که وظیفه ایجاد مجموعه نقاط جستجوی اولیه به نام «جمعیت اولیه» را بر عهده دارند و به طور انتخابی یا تصادفی تعیین می‌شوند. از آنجایی که الگوریتم‌های ژنتیک برای هدایت عملیات جستجو به طرف نقطه بهینه از روش‌های آماری استفاده می‌کنند، در فرایندی که به انتخاب طبیعی وابسته است، جمعیت موجود به تناسب برازندگی افراد آن برای نسل بعد انتخاب می‌شود. این تصمیم به آن دلیل است که الگوریتم‌های فراابتکاری، یکی از انواع الگوریتم‌های بهینه‌سازی تقریبی هستند که قابلیت کاربرد در طیف گسترده‌ای از مسایل را دارند.

مراجع

[1] I. A. Shah, F. A. Malik, and S. A. Ahmad, "Enhancing security in IoT based home automation using Reed Solomon codes," in *Proc. IEEE Int. Conf. on Wireless Communications, Signal Processing and Networking*, pp. 1639-1642, Chennai, India, 23-25 Mar. 2016.

[2] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of Things J.*, vol. 4, no. 5, pp. 1250-1258, Oct. 2017.

[3] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: a survey," *J. of Network and Computer Applications*, vol. 88, pp. 10-28, Jun. 2017.

1. Genetic Algorithm

[4] K. Ashton, "Internet of Things," *RFID J.*, vol. 22, no. 7, pp. 97-114, Jun. 2009.

[5] D. Miorandi, S. Sicari, F. de Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," *Ad hoc Networks*, vol. 10, no. 7, pp. 1497-1516, Sept. 2012.

[6] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728-2742, Dec. 2014.

[7] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: current status and open issues," in *Proc. Int. Conf. on Privacy and Security in Mobile Systems*, 8 pp., Aalborg, Denmark, 8 pp., 11-14 May 2014.

[8] R. Dantu, G. Clothier, and A. Atri, "EAP methods for wireless networks," *Computer Standards & Interfaces*, vol. 29, no. 3, pp. 289-301, Mar. 2007.

[9] S. T. F. Al-Janabi and M. A. S. Rasheed, "Public-key cryptography enabled kerberos authentication," *Developments in E-Systems Engineering*, pp. 209-214, Dubai, United Arab Emirates, 6-8 Dec. 2011.

[10] J. Liu, Y. Xiao, and C. P. Chen, "Authentication and access control in the Internet of Things," in *Proc. IEEE 32nd Int. Conf. on, Distributed Computing Systems Workshops,* pp. 588-592, Macau, China, 18-21 Jun. 2012.

[11] M. P. Pawlowski, A. J. Jara, and M. J. Ogorzalek, "Compact extensible authentication protocol for the Internet of Things: enabling scalable and efficient security commissioning," *Mobile Information Systems*, vol. vol. 2015, pp. 1-11, Nov. 2015.

[12] I. Karabey and G. Akman, "A cryptographic approach for secure client-server chat application using public key infrastructure (PKI)," in *Proc. IEEE 11th Int. Conf. on Internet Technology and Secured Trans.,* pp. 442-446, Barcelona, Spain, 5-7 Dec. 2016.

[13] E. Cho, M. Park, and T. Kwon, "TwinPeaks: a new approach for certificateless public key distribution," in *Proc. IEEE Conf. on Communications and Network Security,* pp. 10-18, Philadelphia, PA, USA, 17-19 Oct. 2016.

[14] W. B. Hsieh and J. S. Leu, "Anonymous authentication protocol based on elliptic curve Diffie-Hellman for wireless access networks," *Wireless Communications and Mobile Computing*, vol. 14, no. 10, pp. 995-1006, Jul. 2014.

[15] N. Tirthani and R. Ganesan, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography," *IACR Cryptology ePrint Archive*, 2014, 49, 2014.

[16] P. Joshi, M. Verma, and P. R. Verma, "Secure authentication approach using diffie-hellman key exchange algorithm for WSN," in *Proc. IEEE Int. Conf. o, Control, Instrumentation, Communication and Computational Technologies,* pp. 527-532, Kumaracoil, India, 18-19 Dec. 2015.

[17] S. Kumar and R. K. Singh, "Secure authentication approach using Diffie-Hellman key exchange algorithm for WSN," *International J. of Communication Networks and Distributed Systems*, vol. 17, no. 2, pp. 189-201, Sept. 2016.

[18] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118-137, Apr. 2018.

[19] R. Vijaysanthi, N. Radha, M. J. Shree, and V. Sindhujaa, "Fingerprint authentication using Raspberry Pi based on IoT," in *Proc. IEEE Int. Conf. on Algorithms, Methodology, Models and Applications in Emerging Technologies,* 3 pp., Chennai, India, 16-18 Feb. 2017.

[20] P. Hu, H. Ning, T. Qiu, Y. Xu, X. Luo, and A. K. Sangaiah, "A unified face identification and resolution scheme using cloud computing in Internet of Things," *Future Generation Computer Systems*, vol. 81, pp. 582-592, Apr. 2018.

[21] Y. Lu, S. Wu, Z. Fang, N. Xiong, S. Yoon, and D. S. Park, "Exploring finger vein based personal authentication for secure IoT," *Future Generation Computer Systems*, vol. 77, pp. 149-160, Dec. 2017.

[22] P. Kumari and A. Vaish, "Brainwave based authentication system: research issues and challenges," *International J. of Computer Engineering and Applications*, vol. 4, no. 1, pp. 89-108. Feb. 2014.

[23] Y. S. Soni, S. B. Somani, and V. V. Shete, "Biometric user authentication using brain waves," in *Proc. IEEE Int. Conf. on Inventive Computation Technologies,* vol. 2, 6 pp., Coimbatore, India, 26-27 Aug. 2016.

[24] S. Marcel and J. D. R. Millan, "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 743-752, Feb. 2007.

[25] E. G. M. Kanaga, R. M. Kumaran, M. Hema, R. G. Manohari, and T. A. Thomas, "An experimental investigation on classifiers for Brain Computer Interface (BCI) based authentication," in *Proc. IEEE Int. Conf. on*, *Trends in Electronics and Informatics,* 6 pp., Tirunelveli, India, 11-12 May 2017.

[26] I. Švogor and T. Kišasondi, "Two factor authentication using EEG augmented passwords," in *Proc. IEEE of the ITI 34th Int. Conf. on Information Technology Interfaces,* pp. 373-378, Cavtat, Croatia, 25-28 Jun. 2012.

[27] C. Y. Cheng, *EEG-Based Person Identification System and Its Longitudinal Adaptation*, Master in Computer Science, National Chiao Tung University, Hsinchu, Taiwan, 2013.

[28] T. Alladi and V. Chamola, and Naren, "HARCI: a two-way authentication protocol for three entity healthcare IoT networks networks," *IEEE J. on Selected Areas in Communications*, vol. 39, no. 2, pp. 361-369, Feb. 2020.

[29] A. R. Elshenaway and S. K. Guirguis, "Adaptive thresholds of EEG brain signals for IoT devices authentication," *IEEE Access*, vol. 9, pp. 100294-100307, Jun. 2021.

[30] R. Zhang, B. Yan, L. Tong, J. Shu, X. Song, and Y. Zeng, "Identity authentication using portable electroencephalography signals in resting states," *IEEE Access*, vol. 7, pp. 160671-160682, 2019.

[31] A. Vallabhaneni, T. Wang, and B. He, "Brain-computer interface," *Neural Engineering,* pp. 85-121, Boston, MA: Springer, 2005.

[32] H. H. Jasper, "The ten-twenty electrode system of the International Federation," *Electroencephalogr. Clin. Neurophysiol.*, vol. 10, pp. 370-375, 1958.

[33] P. Kumari and A. Vaish, "Information-theoretic measures on intrinsic mode function for the individual identification using EEG sensors," *IEEE Sensors J.*, vol. 15, no. 9, pp. 4950-4960, Sept. 2015.

[34] Q. Gui, Z. Jin, M. V. R. Blondet, S. Laszlo, and W. Xu, "Towards EEG biometrics: pattern matching approaches for user identification," in *Proc. IEEE Int. Conf. on,,Identity, Security and Behavior Analysis,* 6 pp., Hong Kong, China, 23-25 Mar. 2015.

[35] W. Kong, L. Wang, S. Xu, F. Babiloni, and H. Chen, "EEG fingerprints: phase synchronization of EEG signals as biomarker for subject identification," *IEEE Access*, vol. 7, pp. 121165-121173, 2019.

افسانه شرفی در تحصیل خود مقطع کارشناسی را در رشته مهندسی کامپیوتر در دانشگاه آزاد واحد اراک در سال ۱۳۹۵ و در مقطع کارشناسی ارشد در رشته مهندسی کامپیوتر گرایش معماری کامپیوتر در سال ۱۳۹۰ و مقطع دکتری را در رشته مهندسی کامپیوتر گرایش معماری کامپیوتر در سال ۱۴۰۰ به پایان رسانده است. او هم‌اکنون مدیر فناوری اطلاعات و مدیرگروه کامپیوتر در دانشگاه انفورماتیک ایران است. زمینه‌های تحقیقاتی و علایق ایشان اینترنت اشیا، شبکه، پردازش سیگنال‌های مغزی و امنیت در شبکه است.

سپیده آدابی تحصیلات خود را در مقاطع کارشناسی، کارشناسی ارشد و دکترای مهندسی کامپیوتر به ترتیب در سال‌های ۱۳۸۴، ۱۳۸۶ و ۱۳۹۱ در دانشگاه آزاد اسلامی به پایان رسانده است و هم‌اکنون استادیار گروه مهندسی کامپیوتر دانشکده برق و کامپیوتر دانشگاه آزاد اسلامی واحد تهران شمال می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: شبکه‌های کامپیوتری، اینترنت اشیا، محاسبات مه، محاسبات ابر و اقتصاد ابر و مه.

علی موقر رحیم‌آبادی هم‌اکنون استاد دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف است و از بهمن ماه سال ۱۳۷۲ با این دانشگاه مشغول همکاری بوده است. نامبرده در سال ۱۳۵۶ مدرک کارشناسی را در مهندسی برق از دانشکده فنی دانشگاه تهران و در سالهای ۱۳۵۸ و ۱۳۶۴ مدارک کارشناسی ارشد و دکتری را در مهندسی کامپیوتر، اطلاعات و کنترل از دانشگاه میشیگان در آن آربور اخذ نمود. زمینه‌های پژوهشی مورد علاقه ایشان عبارتند از: مدلسازی کارایی/اتکاپذیری و درستی‌یابی شبکه‌های بی سیم، سیستم‌های توزیع شده بی‌درنگ و سیستم‌های سایبری فیزیکی.

صلاح المجید هم‌اکنون استاد و هیأت علمی دانشگاه لینکلن انگلستان است. ایشان کارشناسی ارشد خود در دانشگاه وست مینیستر در علوم کامپیوتر در سال ۱۳۸۶ و دکتری خود را در سال ۱۳۹۰در دانشگاه اسکس انگلستان به پایان رسانده است. زمینه‌های علاقه‌مندی ایشان طراحی آی-سی، سیستم‌های ارتباطی، برنامه‌نویسی، پایگاه داده، هوش مصنوعی، پردازش سیگنال‌های دیجیتال و مدارات دیجیتالی است.