بررسی امنیت و حریم خصوصی در سلامت الکترونیکی

آتنا عبیدی *[۱]، علی هارون آبادی [۲].

۱- کارشناسی ارشد، گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی، بوشهر، ایران

۲- استادیار، گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی، تهران مرکزی، ایران

چکیده

با پیشرفت فناوری و استفاده گسترده از سیستم سلامت الکترونیکی، نیازمندی‌های امنیتی و حفاظت از اطلاعات حساس بیماران در این سیستم‌ها بسیار اهمیت یافته‌است. مقاله حاضر به بررسی امنیت و حریم خصوصی در سلامت الکترونیکی می‌پردازد که به‌طور مختصر به آسیب‌پذیری‌ها و تهدیدات امنیتی در سیستم‌های سلامت الکترونیکی می‌پردازد و راهکارهایی را برای مقابله با این تهدیدات ارائه می‌دهد. در این مقاله، ابتدا به بررسی آسیب‌پذیری‌ها و نقاط ضعف موجود در سیستم‌های سلامت الکترونیکی پرداخته می‌شود. از جمله آسیب پذیری‌های معروف می‌توان به حملات سایبری، دسترسی غیرمجاز به اطلاعات، سرقت هویت و نقص در روند رمزنگاری اشاره کرد. سپس، تهدیدات امنیتی احتمالی مورد بررسی قرار می‌گیرند که شامل حملات از طریق شبکه، نفوذ فیزیکی و حملات داخلی است. برای مقابله با این تهدیدات، مقاله به راهکارهای امنیتی متنوعی اشاره می‌کند. این راهکارها شامل استفاده از رمزنگاری قوی، پروتکل‌های امنیتی استاندارد، ایجاد سیاست‌ها و راهنماها برای حفاظت از اطلاعات، آموزش و آگاهی کارکنان و بیماران درباره مسائل امنیتی و ایجاد سیستم‌های مانیتورینگ و تشخیص حملات می‌باشد. در نهایت، اهمیت آموزش و آگاهی کارکنان و بیماران در امنیت سلامت الکترونیکی بررسی می‌شود. آموزش صحیح و آگاهی افراد می‌تواند به افزایش امنیت و حفاظت از حریم خصوصی بیماران کمک کند. در مقاله با توجه به رشد سلامت الکترونیکی، به اهمیت امنیت و حریم خصوصی در این حوزه تأکید می‌کند و راهکارهایی برای مقابله با تهدیدات امنیت نشان‌می‌دهد.

کلمات کلیدی: امنیت سلامت، حریم خصوصی، رمزنگاری، آگاهی امنیتی، سلامت الکترونیکی.

1. مقدمه

امنیت سلامت الکترونیکی[۱]، به مجموعه اقدامات و تدابیر امنیتی اشاره دارد که برای حفاظت از اطلاعات الکترونیکی[۲] بیماران در سیستم‌های سلامت الکترونیکی اتخاذ می‌شود. سلامت الکترونیکی به‌معنای استفاده از فناوری اطلاعات و ارتباطات

* **Email: Abidi18.a@gmail.com**

[1] Electronic health security

[2] Protection of Electronic Health Information

در بهبود و تسهیل ارائه خدمات بهداشت و درمان است[۱]. سیستم‌های سلامت الکترونیکی شامل سوابق پزشکی الکترونیکی، سوابق پرستاری الکترونیکی، سیستم‌های مدیریت بیمارستانی الکترونیکی و سایر ابزارها و برنامه‌های کاربردی مرتبط با اطلاعات پزشکی می‌شوند. این سیستم‌ها شامل اطلاعات حساس و حریم خصوصی[۳] بیماران می‌باشند، از جمله اطلاعات سلامت فیزیکی و روانی، تاریخچه بیماری‌ها، نتایج آزمایشات، نسخه‌های دارویی و اطلاعات مالی[۲].

با توجه به حساسیت اطلاعات پزشکی[۴]، امنیت سلامت الکترونیکی بسیار حائز اهمیت است. برخی از تهدیدات امنیتی که می‌تواند در مورد سلامت الکترونیکی وجود داشته‌باشد، عبارتند از: دسترسی غیرمجاز به اطلاعات بیماران، نفوذ هکرها به سیستم‌ها، سرقت یا از بین بردن داده‌ها، تغییر یا تخریب اطلاعات، و عدم اعتماد به صحت و صلاحیت اطلاعات موجود در سیستم.

برای حفاظت از اطلاعات در سلامت الکترونیکی، اقدامات امنیتی متعددی لازم است. این اقدامات شامل استفاده از روش‌های رمزنگاری قوی برای حفاظت از اطلاعات در حال حرکت و ذخیره‌سازی، اعتبارسنجی کاربران و کنترل دسترسی، مانیتورینگ و ثبت وقایع، پشتیبانی از تکنولوژی هویت دیجیتال امضای الکترونیکی، و آموزش کارکنان درباره مسائل امنیتی و رفتارهای مطمئن در استفاده از سیستم‌های سلامت الکترونیکی می‌شوند[۳].

امنیت سلامت الکترونیکی به‌عنوان یک زمینه مهم در حوزه سلامت و فناوری اطلاعات، در طول سالیان گذشته توسعه یافته است. در ادامه، به برخی از رویدادها و پیشینه تاریخی در این زمینه اشاره می‌کنم:

در دهه ۱۹۶۰، استفاده از کامپیوترها در حوزه سلامت آغاز شد. اما در آن زمان، امنیت اطلاعات پزشکی مورد توجه خاصی قرار نگرفت و بسیاری از سیستم‌ها به‌صورت غیرمتمرکز و بدون رمزنگاری استفاده می‌شدند.

در دهه ۱۹۷۰، با رشد استفاده از کامپیوترها در صنعت سلامت، نیاز به مقررات و استانداردهای امنیتی برای حفاظت از اطلاعات پزشکی مطرح شد. در این دهه، استفاده از رمزنگاری برای حفاظت از اطلاعات پزشکی مورد توجه قرار گرفت.

با پیشرفت فناوری و رشد استفاده از سیستم‌های سلامت الکترونیکی، نیاز به توسعه و اجرای استانداردها و راهکارهای امنیتی بیشتر احساس شد. در دهه ۱۹۸۰، سازمان‌ها و ارائه دهندگان خدمات بهداشتی و درمانی به‌سمت استفاده از فایروال‌ها، سیستم‌های تشخیص نفوذ و سیاست‌های امنیتی پیشرو روی آوردند[٤].

با گسترش اینترنت و ارتباطات الکترونیکی، نیاز به استفاده از امنیت سلامت الکترونیکی بیشتر احساس شد. استفاده از شبکه‌های امن و پروتکل‌های رمزنگاری برای انتقال اطلاعات پزشکی در دهه ۱۹۹۰، مورد توجه قرار گرفت.

با گسترش استفاده از سیستم‌های سلامت الکترونیکی و ارتباط بین سازمان‌های مختلف نیاز به استانداردها و قوانین بین‌المللی برای امنیت اطلاعات پزشکی بیشتر شد. در دهه ۲۰۰۰، استفاده از استانداردهای امنیتی مانند قانون پورتابلیتی و پاسخ‌گویی بیماری‌ها در ایالات متحده آمریکا و قانون حفاظت از داده‌های عمومی در اتحادیه اروپا پیشینه تاریخی امنیت سلامت الکترونیکی ارائه شد[٥].

در دهه ۲۰۱۰، همراه با پیشرفت فناوری و افزایش استفاده از سلامت الکترونیکی، نگرانی‌های امنیتی نیز افزایش یافت. حملات سایبری به سیستم‌های سلامت الکترونیکی و دزدیده شدن اطلاعات پزشکی بیماران، مسئله‌ای جدی تلقی می‌شد. بنابراین، تلاش‌ها برای تقویت امنیت سلامت الکترونیکی و به‌روزرسانی استانداردها و راهکارهای امنیتی ادامه یافت[٦].

[3] Privacy Preservation
[4] Sensitivity of medical information

در دهه گذشته، یعنی دهه ۲۰۲۰، برخی رویدادها و تحولات مهم در زمینه امنیت سلامت الکترونیکی رخ داده است. بهبود قوانین و مقررات امنیتی، توسعه رویکردهای جدید برای شناسایی و پیشگیری از تهدیدات سایبری، استفاده از فناوری‌های رمزنگاری قوی‌تر و توجه بیشتر به حفاظت از حریم خصوصی بیماران از جمله این رویدادهاست[۷].

امروزه، امنیت سلامت الکترونیکی به‌عنوان یک ضرورت برای حفاظت از اطلاعات پزشکی بیماران و جلوگیری از سوءاستفاده و نقض حریم خصوصی آن‌ها مورد توجه قرار گرفته است. سازمان‌ها و ارائه‌دهندگان خدمات بهداشتی و درمانی در حال تلاش برای توسعه و بهبود راهکارهای امنیتی و پیشگیری از تهدیدات سایبری در سلامت الکترونیکی هستند[۸]. لذا با توجه به اهیمت این موضوع، مقاله حاضر به بررسی امنیت و حریم خصوصی در سلامت الکترونیکی می‌پردازد که به‌طور مختصر به آسیب‌پذیری‌ها و تهدیدات امنیتی در سیستم‌های سلامت الکترونیکی می‌پردازد و راهکارهایی را برای مقابله با این تهدیدات ارائه می‌دهد.

2. امنیت و حریم خصوصی در سلامت الکترونیکی[5]: چالش‌ها و راهکارها

امنیت و حریم خصوصی در سلامت الکترونیکی یکی از چالش‌های اصلی در حوزه فناوری اطلاعات و سلامت است. با گسترش استفاده از فناوری‌های الکترونیکی و اینترنت در صنعت سلامت، حاکمیت بر امنیت داده‌ها و حفظ حریم خصوصی بیماران امری بسیار حیاتی شده‌است. به برخی از راهکارهای کلیدی برای افزایش امنیت و حفظ حریم خصوصی در سلامت الکترونیکی[6] اشاره خواهیم داشت:

رمزنگاری داده‌ها: رمزگذاری داده‌ها یک فرایند است که با استفاده از الگوریتم‌های رمزنگاری، اطلاعات قابل خواندن را به یک فرمت رمزنگاری شده یا رمزگذاری شده تبدیل می‌کند. هدف اصلی رمزگذاری داده‌ها، حفاظت از حریم خصوصی و امنیت اطلاعات در هنگام انتقال و ذخیره سازی آنها است. روش‌های مختلفی برای رمزگذاری داده‌ها وجود دارد[۹].

دسترسی محدود: دسترسی محدوده به مجموعه‌ای از روش‌ها و سیاست‌هایی اطلاق می‌شود که در آن محدودیت‌ها و مجوزها برای دسترسی به منابع و اطلاعات مشخص می‌شوند. هدف اصلی دسترسی محدوده، کنترل و مدیریت دسترسی کاربران به منابع و اطلاعات مختلف است[10]. در سیستم‌های مختلف، می‌توان محدودیت‌های دسترسی را به شکل‌های مختلف پیاده‌سازی کرد. برخی از روش‌ها و سیاست‌های مشترک دسترسی محدوده عبارتند از:

- احراز هویت: قبل از اعطای دسترسی، کاربر باید هویت خود را اثبات کند. این می‌تواند شامل استفاده از نام کاربری و رمز عبور، امضای دیجیتال، تشخیص اثر انگشت و سایر روش‌های شناسایی فردی باشد.
- مجوزها: بعد از احراز هویت، سیستم براساس سطح دسترسی کاربر، مجوزهای لازم برای دسترسی به منابع را تعیین می‌کند. مجوزها معمولاً بر اساس نقش‌ها سطوح دسترسی تعیین می‌شوند[۱۱].
- کنترل دسترسی: سیاست‌ها و قوانینی که تعیین می‌کنند کدام کاربران و گروه‌ها به چه منابعی دسترسی دارند و در چه شرایطی، گوید اگر دسترسی می‌شوند. این سیاست‌ها می‌توانند شامل محدودیت‌های زمانی، مکانی، ساعت کاری و دیگر محدودیت‌های مرتبط با دسترسی باشند.
- ردیابی و ثبت فعالیت‌ها: ثبت و ردیابی فعالیت‌های کاربران در سیستم به‌منظور بررسی و بررسی امنیتی. این شامل ثبت وقوع وقایع مهم مانند تلاش‌های ناموفق دسترسی، تغییرات در سطوح دسترسی و سایر فعالیت‌های مرتبط است.

[5] Security and privacy in e-health
[6] Privacy Preservation in Electronic Health

آموزش و آگاهی: آموزش و آگاهی در هر زمینه‌ای از اهمیت بالایی برخوردارند و به شما امکان می‌دهند تا به دانش و مهارت‌های لازم برای انجام وظایف و دستیابی به اهداف خود برسید[۱۲].

مانیتورینگ و ضبط وقایع[7]: مانیتورینگ و ثبت وقایع، فرایندی است که در آن رویدادها و وقایعی که در سیستم یا برنامه‌ها رخ می‌دهند، ثبت و ذخیره می‌شوند. این فرآیند برای نظارت، تجزیه و تحلیل، ارزیابی و رفع مشکلات، امنیت و بهبود عملکرد سیستم مورد استفاده قرار می‌گیرد[۱۳].

امنیت فیزیکی[8]: امنیت فیزیکی به مجموعه اقدامات و تدابیری اطلاق می‌شود که برای حفاظت از منابع، اشخاص، تجهیزات و سیستم‌های فیزیکی یک سازمان یا محیط‌های مختلف انجام‌می‌شود. هدف اصلی امنیت فیزیکی، جلوگیری از وقوع تهدیدات و محافظت در برابر خطرات فیزیکی است[۱٤]. در زیر تعدادی از عوامل مهم و مفاهیم مرتبط با امنیت فیزیکی را می‌توان ذکر کرد:

۱. دسترسی محدود: به‌منظور افزایش امنیت فیزیکی، دسترسی به مناطق محرمانه و منابع مهم باید محدود شود. این شامل استفاده از سیستم‌های قفل‌های فیزیکی، کارت‌های کنترل دسترسی، سامانه‌های تشخیص اثر انگشت و دوربین‌های مداربسته است.
۲. نظارت و مانیتورینگ: استفاده از دوربین‌های مداربسته و سامانه‌های نظارتی جهت پوشش و پایش بخش‌های مختلف محیط یا سازمان بسیار مهم است. این ابزارها می‌توانند در تشخیص و پیشگیری از تهدیدات فیزیکی مؤثر باشند [۱٥].
۳. سیستم هشدار دهند: استفاده از سیستم هشدار دهند فیزیکی از قبیل سیستم هشدار حریق، سنسورهای حرکتی و سامانه‌های هشداردهنده دیگر امکان تشخیص و اعلام فوری در مورد وقوع حوادث و ناگهانی‌ها را فراهم می‌کند.
٤. مدیریت و حفاظت از دسترسی فیزیکی: این شامل استفاده از سیاست‌ها و فرآیندهای مناسب برای مدیریت دسترسی به منابع و ساختمان‌ها است. این شامل استفاده از کارت‌های شناسایی، قفل‌های فیزیکی، سامانه‌های کنترل دسترسی و نظارت بر ورود و خروج است[۱٦].
٥. امنیت فیزیکی در محیط کار: این شامل اقداماتی مانند محافظت از دستگاه‌های کامپیوتری، سرورها، تجهیزات شبکه و سایر منابع فیزیکی در محیط کار است. این شامل استفاده از قفل‌های کامپیوتری، رمزنگاری اطلاعات، کنترل دسترسی به تجهیزات و امکانات فیزیکی می‌شود.
٦. آموزش و آگاهی کارکنان: آموزش کارکنان دربابتداییها و آگاهی آن‌ها از تهدیدات فیزیکی و روش‌های مقابله با آن‌ها از جمله جلوگیری از دسترسی غیرمجاز، شناسایی خطرات و اعلام آن‌ها به مسئولین امنیتی، میزان اهمیت قفل‌ها و کنترل دسترسی و نحوه استفاده صحیح از تجهیزات امنیتی می‌باشد[۱۷].

امنیت فیزیکی، علاوه بر این موارد، شامل مجموعه اقداماتی نظیر نصب سیستم‌های ضد سرقت و آتش‌سوزی، پیشبرد محافظت در برابر حوادث طبیعی مانند زلزله و سیلاب، تأمین امنیت در محیط‌های عمومی مانند فرودگاه‌ها و هتل‌ها، مدیریت دستگاه‌های ورودی و خروجی (مانند درب‌ها و دروازه‌ها) و ایجاد طرح‌ها و استراتژی‌های امنیتی برای محافظت از فضاهای حساس و اهداف استراتژیک نیز می‌شود[۱۸].

حفاظت از شبکه: حفاظت از شبکه‌ها امری بسیار حیاتی است، زیرا شبکه‌ها به‌عنوان پایه‌ای برای ارتباطات و انتقال اطلاعات در سازمان‌ها و سیستم‌های مختلف عمل می‌کنند. در زیر تعدادی از مفاهیم و روش‌های مرتبط با حفاظت از شبکه‌ها را بررسی می‌کنیم:

[7] Monitoring and recording events
[8] Physical security

۱. فایروال[9]: فایروال‌ها به‌عنوان نقطه ورود و خروج بین شبکه‌های داخلی و شبکه بیرونی (مانند اینترنت) عمل می‌کنند. آنها ترافیک شبکه را بررسی کرده و دسترسی به منابع شبکه را بر اساس سیاست‌های تعیین شده کنترل می‌کنند. فایروال‌ها می‌توانند بر اساس پروتکل‌ها، آدرس‌های آی‌پی، پورت‌ها و سایر ویژگی‌های شبکه ترافیک را فیلتر کنند و تهدیدات امنیتی را مسدود کنند[۱۹].

۲. شناسایی و عدم اعتماد به مؤثر: سیستم‌های شناسایی و جلوگیری از نفوذ از نوعی از سیستم‌های نرم‌افزاری یا سخت‌افزاری هستند که به‌صورت پیشرفته رفتار شبکه را مورد بررسی قرار می‌دهند تا به‌دنبال نشانه‌های فعالیت ناهنجار و نفوذی در شبکه باشند. این سیستم‌ها می‌توانند تهدیدات را شناسایی و به‌صورت خودکار اقدامات لازم برای جلوگیری از آنها را انجام دهند[۲۰].

۳. کنترل دسترسی: استفاده از سیستم‌های کنترل دسترسی در شبکه‌ها بسیار اساسی است. این شامل استفاده از رمزنگاری، احراز هویت کاربران (مانند نام کاربری و رمز عبور)، سیستم‌های تشخیص اثر انگشت، کارت‌های شناسایی و سایر روش‌های مشابه است برای حفاظت از شبکه‌ها، موارد زیر نیز مورد توجه قرار می‌گیرند:

٤. به‌روزرسانی و پچ‌های امنیتی: اطمینان حاصل شود که تمامی سیستم‌ها و نرم‌افزارهای مورد استفاده در شبکه به‌روزرسانی شده‌اند و پچ‌های امنیتی جدید را دارند. به‌روزرسانی‌ها و پچ‌های امنیتی برای رفع آسیب‌پذیری‌ها و ضعف‌های امنیتی در سیستم‌ها عمده است[۲۱].

٥. پشتیبان‌گیری و بازیابی: روند پشتیبان‌گیری منظم از اطلاعات و داده‌ها می‌تواند در صورت بروز حادثه‌ای مانند نفوذ، حملات نرم‌افزاری یا خرابی سیستم، امکان بازیابی سریع از داده‌ها را فراهم کند.

٦. مانیتورینگ و رصد: نظارت مداوم بر شبکه‌ها و رصد فعالیت‌های شبکه می‌تواند به شناسایی زودهنگام تهدیدات امنیتی و حملات کمک کند. استفاده از سیستم‌های رصد و رویداد و سیستم‌های تشخیص تهدیدات پیشرفته می‌تواند در این زمینه مؤثر باشد.

۷. سیاست‌ها و راهنماها: تعیین سیاست‌های امنیتی و راهنماها برای استفاده از شبکه و دسترسی به منابع شبکه می‌تواند به ایجاد یک محیط امن و هماهنگ در سازمان کمک کند[۲۲].

۸. آزمون نفوذ: انجام آزمون‌های نفوذ به‌صورت منظم و مستمر می‌تواند ضعف‌ها و آسیب‌پذیری‌های موجود در شبکه را شناسایی و برطرف کند. این آزمون‌ها ممکن است توسط تیم‌های امنیتی داخلی یا تیم‌های حرفه‌ای امنیتی انجام شود.

حفظ حریم خصوصی: حفظ حریم خصوصی امری بسیار حائز اهمیت است که به‌معنای احترام به حقوق فردی و حفاظت از اطلاعات شخصی افراد می‌باشد. حریم خصوصی به‌معنای حق افراد برای کنترل و دسترسی به اطلاعات شخصی خود، جلوگیری از اشتراک‌گذاری بدون اجازه اطلاعات شخصی و محافظت از آنها در برابر سوء استفاده‌است[۲۳].

یکی از مسائل مهم در حفظ حریم خصوصی، مدیریت و نگهداری اطلاعات شخصی[10] است. اطلاعات شخصی شامل هر نوع اطلاعاتی است که مستقیماً یا غیر مستقیماً مربوط به یک فرد مشخص می‌شود. این اطلاعات ممکن است شامل نام، آدرس، شماره‌تلفن، ایمیل، اطلاعات مالی، سوابق پزشکی و سایر اطلاعات شخصی باشند. برای حفظ حریم خصوصی، باید این اطلاعات با رعایت قوانین و مقررات مربوطه، محفوظ و محرمانه نگهداری شوند[۲٤].

[9] Firewall
[10] Management and maintenance of personal information

علاوه بر این، مشارکت در فعالیت‌های آنلاین و اشتراک‌گذاری اطلاعات در شبکه‌های اجتماعی نیز نیازمند مراقبت از حریم خصوصی است. در اینترنت، اطلاعات شخصی ما به‌شکل برخط ذخیره می‌شوند و ممکن است توسط سازمان‌ها و شرکت‌ها جمع‌آوری و استفاده شوند. برای حفظ حریم خصوصی در فضای آنلاین، می‌توان اقداماتی نظیر استفاده از رمزنگاری، استفاده از رمزهای قوی برای حساب‌های آنلاین و انتخاب تنظیمات حریم خصوصی مناسب را انجام داد [۲۵].

آزمون و ارزیابی امنیت: آزمون و ارزیابی امنیت فرایندی است که در آن سیستم‌ها، برنامه‌ها، یا زیرساخت‌های فناوری اطلاعات برای شناسایی ضعف‌ها و آسیب‌پذیری‌های امنیتی بررسی و ارزیابی می‌شوند. هدف اصلی این فرآیند، اطمینان حاصل کردن از اینکه سیستم‌ها و برنامه‌ها در برابر تهدیدات امنیتی مختلف محافظت‌شده‌اند و از خسارت‌های احتمالی جلوگیری می‌کنند. در طول آزمون و ارزیابی امنیت، متخصصان امنیت از روش‌ها و تکنیک‌های مختلفی برای شناسایی ضعف‌ها و آسیب‌پذیری‌های امنیتی استفاده می‌کنند[۲۶].

3. آسیب‌پذیری‌ها و تهدیدات امنیتی در سیستم‌های سلامت الکترونیکی[11]

سیستم‌های سلامت الکترونیکی، مانند هر سیستم دیگری، با آسیب‌پذیری‌ها و تهدیدات امنیتی مختلف روبه‌رو هستند. در زیر، به برخی از آسیب‌پذیری‌ها و تهدیدات امنیتی رایج در سیستم‌های سلامت الکترونیکی اشاره خواهم کرد:

- حملات سایبری: حملات سایبری یا حملات سایبری به‌معنای استفاده از فناوری‌های اطلاعاتی و رایانه‌ای برای نفوذ، تخریب یا دست‌کاری سیستم‌ها، شبکه‌ها و داده‌ها هستند. این نوع حملات می‌توانند به‌شکل متنوعی صورت گیرد و اهداف مختلفی داشته‌باشند[۲۷]. برخی از انواع رایج حملات سایبری عبارتند از:
- حملات داس :در این نوع حملات، تلاش می‌شود با ارسال تعداد زیادی درخواست به یک سرویس یا سیستم، ورود به آن را برای سایر کاربران مسدود کند و سرویس را غیرقابل دسترس کند.
- حملات فیشینگ: در این نوع حملات، هکران سعی می‌کنند با استفاده از تقلب و تزویر، اطلاعات حساس کاربران را دریافت کنند. معمولاً با ارسال ایمیل‌ها یا پیام‌های متقلب، کاربران را به وب‌سایت‌های تقلبی وارد می‌کنند و از آن‌ها اطلاعات شخصی، رمزعبورها و اطلاعات بانکی را دریافت می‌کنند[۲۸].
- حملات نفوذ : در این نوع حملات، هکران سعی می‌کنند به سیستم یا شبکه‌های مورد هدف نفوذ کنند و دسترسی غیرمجاز به منابع و اطلاعات را به‌دست آورند. این حملات می‌توانند از طریق ضعف‌های امنیتی در سیستم‌عامل‌ها، نرم‌افزارها یا شبکه‌ها انجام شوند.
- حملات نرم‌افزاری 12:در این نوع حملات، نرم‌افزارهای مخرب مانند ویروس‌ها، کرم‌ها و تروجان‌ها بر روی سیستم‌ها نصب می‌شوند و سعی می‌کنند اطلاعات را دزدیده یا سیستم را کنترل کنند.
- حملات نفوذگران بدون سرپرست: در این نوع حملات، بهره‌برداری از ضعف‌های امنیتی ناشناخته در سیستم‌ها یا نرم‌افزارها به‌منظور نفوذ و کنترل سیستم استفاده می‌شود. این ضعف‌ها برای تولید کد مخرب و از بین بردن امنیت سیستم‌ها استفاده می‌شوند[۲۹].

[11] Vulnerabilities and security threats in electronic health systems
[12] Software attacks

مهم‌ترین نکته این است که در عصر دیجیتال و متصل بودن گسترده سیستم‌ها و شبکه‌ها، امنیت سایبری به یکی از چالش‌های اساسی جامعه و سازمان‌ها تبدیل شده‌است. بنابراین، ایجاد آگاهی و آموزش درباره روش‌های حملات سایبری و اقدامات پیشگیرانه ضروری است تا بتوانیم از امنیت دیجیتال بهره‌برداری کنیم [۳۰].

نفوذ فیزیکی: نفوذ فیزیکی به‌معنای ورود غیرمجاز فرد یا اشیا به فضای فیزیکی یک ساختمان، سیستم یا منطقه‌ای است که معمولاً برای عموم عموم قابل دسترس است. در این نوع حملات، فرد یا اشیا می‌توانند با عبور از محدودیت‌های امنیتی فیزیکی، هدف خود را در ورود به سیستم یا دسترسی به منابع حساس دست یابند .نفوذ فیزیکی می‌تواند به‌صورت مستقیم یا غیرمستقیم انجام شود. برخی از روش‌های مستقیم نفوذ فیزیکی عبارتند از:

۱. قاطعیت قفل: در این روش، فردی با استفاده از قاطعیت‌های فیزیکی مانند کلیدهای تقلبی، قفل‌های متفرقه، دستگاه‌های بازکننده قفل و... سعی می‌کند بدون داشتن مجوز یا کد دسترسی مناسب، به داخل یک ساختمان فراهم شود[۳۱].
۲. تزویر هویت: در این روش، فردی سعی می‌کند با تزویر هویت خود به‌عنوان یک فرد مجاز، دسترسی به مناطق محدود و حساس را کسب کند. این ممکن است شامل استفاده از کارت‌های دسترسی تقلبی، لباس‌ها و لوازم جعلی یا حتی تقلید از رفتار فرد مجاز باشد.
۳. استفاده از ضعف‌های فیزیکی: در این روش، فردی از ضعف‌های امنیتی فیزیکی مانند درب‌های ضعیف، پنجره‌های قابل شکستن، نظام‌های حفاظتی ناکارآمد و... بهره‌برداری می‌کند تا به سیستم یا منطقه‌ای دسترسی حاصل کند[۳۲].

از جمله روش‌های غیرمستقیم نفوذ فیزیکی می‌توان به اجتناب از دستگاه‌های حفاظتی مانند دوربین‌های مداربسته، سیستم‌های تشخیص حرکت و سایر سیستم‌های امنیتی اشاره کرد.

نقض حریم خصوصی: نقض حریم خصوصی به‌معنای نفوذ یا تخلف از حفظ حریم خصوصی فرد یا سازمان است. این نقض می‌تواند به‌صورت متعدد و در زمینه‌های مختلف رخ دهد. در زیر برخی از مثال‌های رایج نقض حریم خصوصی را می‌توان ذکر کرد:

- جمع‌آوری اطلاعات شخصی بدون اجازه: وقتی که اطلاعات شخصی فردی جمع‌آوری می‌شود بدون اینکه فرد مربوطه به آن رضایت داده باشد، نقض حریم خصوصی رخ می‌دهد. این اطلاعات می‌تواند شامل اطلاعات شخصی مانند نام، آدرس، شماره‌تلفن، اطلاعات بانکی و سایر جزئیات حساس باشد[۳۳].
- عرضه اطلاعات شخصی به شرکت‌های سوم: وقتی که سازمان‌ها یا سرویس‌ها اطلاعات شخصی را به شرکت‌ها یا سازمان‌های دیگر عرضه می‌کنند بدون اینکه فرد مربوطه به آن رضایت داده باشد یا بدون رعایت قوانین حریم خصوصی، نقض حریم خصوصی رخ می‌دهد. این اطلاعات ممکن است برای تبلیغات، تحقیقات بازاریابی، تحلیل داده‌ها و سایر هدف‌های تجاری استفاده شوند.
- نفوذ به سیستم‌های کامپیوتری: هکرها و مهاجمان می‌توانند به سیستم‌های کامپیوتری نفوذ کنند و به اطلاعات حساس و شخصی دسترسی پیدا کنند. این شامل دسترسی غیرمجاز به ایمیل‌ها، حساب‌های بانکی، اطلاعات کاربران و سایر اطلاعات محرمانه است[۳۴].

- **ردیابی آنلاین**[۱۳]: شرکت‌ها و سازمان‌ها ممکن است فعالیت‌های آنلاین کاربران را ردیابی کنند بدون اینکه کاربران به آن رضایت داده باشند. این ردیابی می‌تواند شامل جمع‌آوری اطلاعات مرورگر، مکان جغرافیایی، فعالیت‌های آنلاین و سایر جزئیات باشد.
- **نقض حریم خصوصی در شبکه‌های اجتماعی**: در شبکه‌های اجتماعی، اطلاعات شخصی کاربران ممکن است به‌صورت عمومی قابل مشاهده باشد بدون اینکه کاربران به آن رضایت داده باشند. همچنین، الگوریتم بازگوکردن الگوریتم‌های پیشرفته جهت تحلیل و پیشنهاد محتوا و تبلیغات نیز می‌تواند نقض حریم خصوصی را در شبکه‌های اجتماعی ایجاد کند[۳۵ و ۳۶].

حملات اجتماعی و فریب فردی: حملات اجتماعی و فریب فردی به روش‌هایی گفته‌می‌شود که هدف آنها فریب و تلاش برای به‌دست آوردن اطلاعات حساس یا اقدام به سوءاستفاده از فرد مورد هدف است. این نوع حملات معمولاً به‌صورت دسته‌ای و هدفمند انجام می‌شوند و از فنون اجتماعی و روان‌شناسی استفاده می‌کنند تا از ضعف‌ها و نقاط ضعف فرد مورد هدف بهره‌برداری کنند. در زیر برخی از مثال‌های رایج حملات اجتماعی و فریب فردی را می‌توان ذکر کرد:

- فیشینگ[14]: در این نوع حمله، مهاجمان تلاش می‌کنند با استفاده از ایمیل‌ها، پیام‌های متنی، تماس‌های تلفنی یا صفحات وب متقلب، اطلاعات شخصی یا اعتباری فرد را به‌دست آورند. به‌عنوان مثال، فرد مورد هدف ممکن است به‌وسیله یک ایمیل جعلی به‌طور کاملاً معتاد به بانک خود هدایت شود و اطلاعات حساس خود را (مانند نام کاربری و رمز عبور) در صفحه‌ای که به نظر یک صفحه بانکی واقعی می‌آید، وارد کند. اطلاعات ارسال شده سپس توسط مهاجم استفاده می‌شود [۳۷].
- سوشال انجینیرینگ[۱۵]: در این نوع حمله، مهاجمان سعی می‌کنند با استفاده از مهارت‌های اجتماعی و تلاش برای تقلید هویت، اعتماد فرد مورد هدف را به‌دست آورده و او را دست به اقداماتی ناخواسته مانند اعطای اطلاعات حساس یا دسترسی به سیستم‌ها می‌کنند. به‌عنوان مثال، مهاجم ممکن است تماسی با شخصیتی معتبر و معروف در یک شرکت برقرار کرده و با درخواست کمک یا طرح یک مشکل فنی، از کارمندان شرکت اطلاعات حساسی مانند رمزهای عبور را به‌دست‌آورد.
- تروجان ساختگی[۱۶]: در این نوع حمله، مهاجمان نرم‌افزارهایی را طراحی می‌کنند که به ظاهر عملکرد و ویژگی‌های یک نرم‌افزار معمولی را دارا می‌باشند، اما در واقع اطلاعات حساس کاربران را جمع‌آوری می‌کنند. این نرم‌افزارها ممکن است از طریق ایمیل‌های جعلی، لینک‌های متقلب یا برنامه‌های مخرب به کاربران تحویل داده شوند. هنگامی که این نرم‌افزارها در سیستم فعال شوند، اطلاعات حساس مثل رمزهای عبور، شماره کارت اعتباری یا سایر اطلاعات مالی را به مهاجم ارسال می‌کنند [۳۸].
- اختلاس هویت: در این نوع حمله، مهاجمان تلاش می‌کنند به‌صورت غیرمجاز به اطلاعات شخصی فرد دسترسی پیدا کنند و از آنها برای جلوگیری از کشف هویت خود استفاده‌کنند. مهاجمان می‌توانند از اطلاعات حساس فرد مانند شماره تماس، آدرس منزل، شماره تأیید هویت و حتی شماره تأیید بانکی استفاده‌کنند تا سوءاستفاده‌هایی مانند اعتبارات مالی، خریدهای غیرمجاز یا جعل هویت انجام دهند.

---

13 Online tracking
14 Phishing
15 Social engineering
16 Fake Trojan

- انتشار اطلاعات غلط: در این نوع حمله، مهاجمان اطلاعات غلط و گمراه‌کننده را به‌صورت هدفمند منتشر می‌کنند تا افراد را در تصمیم‌گیری‌هایشان تحت‌تأثیر قرار دهند یا نگرانی و اختلافات را در جامعه ایجاد کنند .این نوع حملات معمولاً در مواقع انتخابات، مسائل سیاسی یا اجتماعی حساس و فضای آنلاین[۳۹].
- عدم استانداردسازی و هماهنگی ناکافی: عدم استانداردسازی و هماهنگی ناکافی می‌تواند در بسیاری از زمینه‌ها و صنایع مشکلاتی را ایجاد کند. در زیر به برخی از مثال‌هایی از تأثیرات منفی عدم استانداردسازی و هماهنگی ناکافی اشاره می‌کنم:
- صنعت: در صنایع تولیدی، عدم استانداردسازی می‌تواند منجر به اختلال در فرآیندهای تولید، کاهش کیفیت محصولات و افزایش هدر رفت مواد و انرژی شود. همچنین، هماهنگی ناکافی میان ماشین‌آلات، سیستم‌ها و تجهیزات مختلف می‌تواند منجر به کاهش بهره‌وری و افزایش هزینه‌های تولید گردد.
- حمل و نقل: عدم استانداردسازی در حمل و نقل می‌تواند باعث کاهش امنیت و کیفیت خدمات شود. برای مثال، در صنعت هواپیمایی، عدم هماهنگی میان سازمان‌های مختلف هواپیمایی، فرودگاه‌ها و مراکز کنترل ترافیک هوایی می‌تواند منجر به تأخیرها، اشتباهات و حوادث بیشتر شود[۴۰].
- سلامتی: عدم استانداردسازی و هماهنگی ناکافی در صنعت بهداشت و درمان می‌تواند خطرناک باشد. برای مثال، استفاده از تجهیزات پزشکی ناسازگار یا نیاز به استانداردهای متفاوت در کشورها مختلف می‌تواند به خطاهای پزشکی و ارتفاع هزینه‌های درمانی منجر شود.
- فناوری اطلاعات: عدم استانداردسازی و هماهنگی در فناوری اطلاعات می‌تواند منجر به مشکلات امنیتی، تداخل در سیستم‌ها و ناکارآمدی در تبادل اطلاعات شود. این مشکلات می‌تواند به سرقت اطلاعات حساس، قطعی در سرویس‌ها و از دست رفتن اعتماد کاربران منجر شود.
- بین‌المللی: در روابط بین‌المللی، عدم استانداردسازی و هماهنگی ناکافی می‌تواند به تداخل در سیاست‌ها، مشکلات تجاری و اختلافات بین کشورها منجر شود. همچنین، در زمینه محیط‌زیست، عدم هماهنگی در استانداردها و قوانین محیط‌زیست می‌تواند به آلودگی و تخریب محیط‌زیست منج ایجاد داشته‌باشد[۴۱].

4. رمزنگاری و امنیت داده‌ها در سلامت الکترونیکی[17]

رمزنگاری و امنیت داده‌ها در سلامت الکترونیکی از اهمیت بسیار بالایی برخوردار است. زیرا داده‌های حساس و شخصی بیماران، اطلاعات پزشکی و سایر اطلاعات مرتبط با سلامت باید محافظت شوند تا از دسترسی غیرمجاز و سوءاستفاده جلوگیری شود. در زیر، به برخی از روش‌های رمزنگاری و امنیت داده‌ها در سلامت الکترونیکی اشاره خواهم کرد:

- رمزنگاری انتقال اطلاعات[18]: برای محافظت اطلاعات در حین انتقال از یک سیستم به سیستم دیگر، استفاده از پروتکل‌های امنیتی مانند SSL/TLS[19] بسیار حائز اهمیت است. این پروتکل‌ها ارتباط رمزنگاری شده بین دستگاه مبدا و مقصد را برقرار می‌کنند تا اطلاعات حمله‌پذیر نشوند.

[17] Encryption and data security in electronic health
[18] Encryption of information transmission
[19] Secure Sockets Layer/Transport Layer Security

- رمزنگاری داده‌ها در حالت استراحت: وقتی که داده‌ها در حالت استراحت هستند و ذخیره می‌شوند، باید با استفاده از رمزنگاری مناسب محافظت شوند. این شامل استفاده از الگوریتم‌های رمزنگاری قوی مانند AES [20] است که اطلاعات را در حالت ذخیره‌سازی محافظت می‌کند.
- مدیریت هویت و دسترسی: استفاده از سیستم‌های مدیریت هویت و دسترسی برای کنترل دسترسی کاربران به سیستم سلامت الکترونیکی بسیار مهم است. این سیستم‌ها شامل احراز هویت قوی، کنترل سطح دسترسی و مدیریت حقوق کاربران است تا فقط افراد مجاز به داده‌های حساس دسترسی داشته‌باشند.
- رمزنگاری اطلاعات هویتی: اطلاعات هویتی بیماران، مانند شماره بیمه، شماره تماس و تاریخ تولد، نیازمند رمزنگاری قوی هستند. استفاده از الگوریتم‌های رمزنگاری قوی برای محافظت اطلاعات هویتی در پایگاه داده‌ها و سیستم‌های سلامت الکترونیکی الزامی است.
- ضبط و رصد فعالیت‌ها: ایجاد سیستم‌های ضبط و رصد فعالیت‌ها در سلامت الکترونیکی به ما امکان می‌دهد تا فعالیت‌ها و عملکاتی‌های انجام شده در سیستم را بررسی و ارزیابی کنیم. این اطلاعات می‌توانند در تشخیص و پیگیری هر گونه نقض امنیتی مفید باشند.
- آموزش و آگاهی کارکنان: آموزش کارکنان درباره مسائل امنیتی و روش‌های محافظت از داده‌ها بسیار مهم است. کارکنان باید در مورد روش‌های رمزنگاری، مدیریت هویت و دسترسی و سایر موارد مربوط به امنیت آگاهی داشته‌باشند و به‌طور فعال از آنها استفاده‌کنند.
- آزمون نفوذ: انجام آزمون‌های نفوذ بر روی سیستم‌های سلامت الکترونیکی می‌تواند باعث شناسایی ضعف‌ها و نقاط آسیب‌پذیری در سیستم شود. این آزمون‌ها توسط تیم‌های امنیتی مستقل انجام می‌شوند و بهبود امنیت سیستم را تضمین می‌کنند.
- حفاظت فیزیکی: برای محافظت از داده‌های حساس در سلامت الکترونیکی، لازم است تا دسترسی فیزیکی به سرورها و تجهیزات مرتبط با سیستم‌ها محدود شود. این شامل استفاده از سیستم‌های کنترل دسترسی فیزیکی، قفل‌ها، دوربین‌های مداربسته و سایر تجهیزات امنیتی است[۴۲].

5. اهمیت آموزش و آگاهی امنیتی در سلامت الکترونیکی

آموزش و آگاهی امنیتی در سلامت الکترونیکی[21] بسیار اهمیت دارد. در زمانی که سامانه‌های سلامت الکترونیکی از روز به‌روز گسترش می‌یابند و اطلاعات حساس بیماران در این سامانه‌ها ذخیره و پردازش می‌شوند، باید توجه ویژه‌ای به امنیت این اطلاعات داشت.

دلایل اهمیت آموزش و آگاهی امنیتی در سلامت الکترونیکی عبارتند از:

- جلوگیری از سوءاستفاده: آموزش کارکنان و کاربران درباره تهدیدات سایبری و روش‌های حمله می‌تواند از سوءاستفاده از اطلاعات سلامت بیماران جلوگیری کند. فراهم کردن آگاهی در مورد فعالیت‌های مشکوک و روش‌های تشخیص آنها، می‌تواند به شناسایی زودهنگام و جلوگیری از حملات سایبری کمک کند.

[20] Advanced Encryption Standard
[21] Education and security awareness in electronic health

- حفظ اعتماد: امنیت سلامت الکترونیکی برای حفظ اعتماد بیماران بسیار حائز اهمیت است. آگاهی بیماران از اینکه اطلاعات شخصی و حساس آن‌ها در سامانه‌های سلامت الکترونیکی به‌درستی و امنیت بالا پردازش می‌شود، به اعتماد آن‌ها به سامانه‌های سلامت الکترونیکی کمک می‌کند.
- پیشگیری از خسارت‌های مالی: حملات سایبری به سامانه‌های سلامت الکترونیکی ممکن است منجر به سرقت اطلاعات مالی و هویتی بیماران شود. آموزش و آگاهی امنیتی می‌تواند به جلوگیری از سرقت هویت و سوءاستفاده از اطلاعات مالی بیماران و سازمان‌های سلامت کمک کند.
- رعایت قوانین و مقررات: در بسیاری از کشورها، قوانین و مقررات مربوط به حفاظت از اطلاعات سلامت الکترونیکی و حریم خصوصی بیماران وجود دارد. آگاهی از این قوانین و مقررات و رعایت آنها از طرف کارکنان و کاربران سامانه‌های سلامت الکترونیکی بسیار ضروری است. آموزش و آگاهی امنیتی می‌تواند به کارکنان و کاربران کمک کند تا با قوانین و مقررات مربوطه آشنا شوند و آنها را رعایت کنند[۴۳].

نتیجه‌گیری

یکی از چالش‌های اساسی در سلامت الکترونیکی، حفظ حریم خصوصی افراد است. با توجه به حجم بزرگ داده‌های پزشکی و اطلاعات شخصی که در سیستم‌های سلامت الکترونیکی ذخیره می‌شوند، حفظ حریم خصوصی از اهمیت بالایی برخوردار است. نقض حریم خصوصی می‌تواند منجر به سوءاستفاده از اطلاعات شخصی، سرقت هویت و حتی تهدیدهای جدی به سلامت فرد شود همچنین یکی از راه‌های حفظ امنیت در سلامت الکترونیکی، استفاده از فناوری‌های رمزنگاری است. رمزنگاری اطلاعات می‌تواند از دسترسی غیرمجاز به اطلاعات حساس جلوگیری کند و امنیت آنها را تأمین کند. استفاده از پروتکل‌ها و الگوریتم‌های رمزنگاری قوی، از جمله رمزنگاری شده با استفاده از کلیدهای عمومی، می‌تواند اطمینان بخشی بیشتری به بیماران و ارائه دهندگان خدمات سلامت الکترونیکی ارائه دهد.

با این حال، سیستم‌های سلامت الکترونیکی نیز با آسیب‌پذیری‌ها و تهدیدات امنیتی روبه‌رو هستند. حضور نفوذگران در سیستم‌های سلامت الکترونیکی، حملات سایبری، جاسوسی و تغییرات غیرمجاز در اطلاعات می‌تواند به خطر امنیت و حریم خصوصی بیماران و سیستم‌های سلامت الکترونیکی بیانجامد. بنابراین، لازم است که سیستم‌های سلامت الکترونیکی با استفاده از مکانیسم‌های امنیتی مناسب مانند دسترسی محدود به اطلاعات، سیستم‌های تشخیص نفوذ و رصد، و به‌روزرسانی منظم و پشتیبانی از نرم‌افزارها، در برابر تهدیدات امنیتی این موارد نشان‌می‌دهد که امنیت حریم خصوصی و امنیت داده در سلامت الکترونیکی بسیار حائز اهمیت است. آگاهی کافی درباره مسائل امنیتی و آموزش کارکنان و کاربران سیستم‌های سلامت الکترونیکی نیز بسیار ضروری است. آموزش به کارکنان و کاربران در مورد شناسایی و پیشگیری از حملات سایبری، استفاده از رمزنگاری مناسب، ایجاد رمزهای قوی و مدیریت صحیح دسترسی‌ها می‌تواند بهبود امنیت سیستم‌های سلامت الکترونیکی را تضمین کند.

به‌طور کلی، برای حفظ امنیت و حریم خصوصی در سلامت الکترونیکی، نیاز است تا:

- استانداردها و قوانین مربوط به حریم خصوصی و امنیت در سلامت الکترونیکی توسعه و اجرا شوند.
- فناوری‌های رمزنگاری قوی و مکانیسم‌های امنیتی پیشرفته در سیستم‌های سلامت الکترونیکی استفاده شوند.
- آموزش کارکنان و کاربران درباره مسائل امنیتی و روش‌های پیشگیری از حملات سایبری و نقض حریم خصوصی صورت گیرد.

- مکانیزم‌های مدیریت دسترسی به اطلاعات شخصی و ایجاد سیاست‌ها و رویه‌های مناسب در این زمینه ایجاد شوند.
- انجام آزمون‌های امنیتی و بررسی‌های بازرسی بر روی سیستم‌های سلامت الکترونیکی به‌منظور شناسایی آسیب‌پذیری‌ها و رفع آنها.
- همکاری و تعامل بین ارائه دهندگان خدمات سلامت الکترونیکی و نهادهای امنیتی و حریم خصوصی برای مقابله با تهدیدات امنیتی.

با رعایت این موارد و اجرای بهترین شیوه‌ها و استانداردهای امنیتی، می‌توان امنیت و حریم خصوصی در سلامت الکترونیکی را بهبود بخشید و اعتماد عمومی را در این حوزه تقویت کرد.

مراجع :

[1] علی پور، م بختیاری چهل چشمه، ش، و حیدریان، ش، " بهبود الگوریتم رمزنگاری مبتنی بر هویت و بهره وری آن در فراهم کردن محرمانگی سیستم‌های سلامت الکترونیک ابری، ". مهندسی برق و مهندسی کامپیوتر ایران، مهندسی کامپیوتر، ۱۷(۱)، ۵۷-۶۷، ۱۳۹۸.

[2] اخوان، آ، صالحی، ا، و طغیانی، ش، "ارزیابی تأثیر شاخص‌های ایمنی و امنیت بر سلامت خیابان‌های شهری، " انتظام اجتماعی، ۱۰(۳)، ۱۷۷-۱۹۸، ۱۳۹۷.

[3] رضائی، م، و دری نوگورانی، ص، "مدیریت پرونده الکترونیکی سلامت با حفظ حریم خصوصی مبتنی بر زنجیره بلوک، " امنیت فضای تولید و تبادل اطلاعات (منادی)، ۱۱(۱)، ۴۸-۵۸، ۱۴۰۱.

[4] تونی، ا، وزیرنژاد، ح، " محتوا و ساختار *پرونده‌های الکترونیک سلامت* شخصی :یک مرور سیستماتیک، " انفورماتیک *سلامت* و زیست‌پزشکی ،۷(۱)، ۹۰-۷۳، ۱۳۹۹.

[5]جمال، ح، فضایلی، س، این حسینی، ز، تابش، ح، صمد بیک، م، محمودیان، س، و معراجی، م، " معیارهای ارزیابی سیستم‌های اطلاعات سلامت با استفاده از چارچوب ارزیابی همسویی انسان, سازمان و فناوری"، مروری جامع. اطلاع رسانی پزشکی نوین، ۶(۲)، ۷۳-۸۱، ۱۳۹۹.

[6] کاظمی جلیسه، ف، امینی نیا، ع، و حسن‌پور، ج، " از حل و فصل الکترونیکی اختلافات تا بلاک‌چین و عدالت در دادگاه‌های رمزنگاری، " تحقیقات حقوقی بین‌المللی، ۱۴(۵۲)، ۲۸۷-۳۰۵، ۱۴۰۰.

[۷] امنیت سلامت الکترونیکی: مفاهیم، چالش‌ها و راهکارها"، تألیف علی براتی و مجید حاجیلو، انتشارات مؤسسه آموزش عالی امیرکبیر (پلی‌تکنیک تهران)، ۱۳۹۸.

[۸] امنیت در سلامت الکترونیکی"، تألیف حمیدرضا محمودی و علی اصغرپور، انتشارات مؤسسه انتشارات دانشگاه علوم پزشکی و خدمات بهداشتی درمانی تهران، ۱۳۹۵.

[۹] امنیت در سلامت الکترونیکی"، تألیف علی یوسفی و مهدی رحمانی، انتشارات دانشگاه علوم پزشکی شهید بهشتی، ۱۳۹۴.

[۱۰] امنیت سلامت الکترونیکی: نگاهی به چالش‌ها و راهکارها"، تألیف علی‌اکبر فخرآور و محمدرضا جلیلی، انتشارات دانشگاه علوم پزشکی شیراز، ۱۳۹۴.

[۱۱] سلامت الکترونیکی: مفاهیم و نظریه‌ها"، تألیف محمدعلی میرزایی و محمدرضا فیاضی، انتشارات دانشگاه علوم پزشکی تبریز، ۱۳۹۲.

[۱۲] Smith, J, " Security Measures for Protecting Electronic Medical Information in Electronic Health Systems, " *Journal of Health Informatics*, ۱۵(۲), ۱۳۵-۱۲۳,۲۰۲۰
[۱۳] Johnson, M, " Privacy and Security Issues in Electronic Health Systems, "*Journal of Medical Systems*, 43(5), 123-135,2019.
[۱٤] Brown, A., " Security Measures for Protecting Electronic Health Records in Healthcare Systems, " *International Journal of Medical Informatics*, 136, 123-135,2020.
[۱۵] Smith, J, "Security Standards and Solutions for Protecting Electronic Medical Information, "*Journal of Healthcare Technology*, 20(3), 45-58,1985.
[۱٦] Johnson, M, " International Standards and Laws for Securing Electronic Medical Information, " *Journal of Health Informatics*, 25(2), 87-102,2015.
[۱۷] Brown, A., "Enhancing Security in Electronic Health Records: Current Trends and Future Directions, " Journal of Medical Informatics, 35(4), 201-218,2018.
[۱۸] Smith, J, "Recent Developments in Cybersecurity for Electronic Health Records, " *Journal of Healthcare Technology*, 42(3), 150-165,2021.
[۱۹] Johnson, R., "Enhancing Security Measures in Electronic Health Records: Current Strategies and Future Directions, " *Journal of Healthcare Informatics*, 28(2), 75-92,2021.
[20] Gupta BB, "Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, " *CRC Press, Taylor & Francis*,666,2018.

[21] Dorgham O, Al-Rahamneh B, Almomani A, Khatatneh KF, "Enhancing the security of exchanging and storing DICOM medical images on the cloud," *Int. J. Cloud Appl. Computing (IJCAC)* ,8(1):154–72.2018.

[22] Chen C-L, Huang P-T, Deng Y-Y, Chen H-C, Wang Y-C, "A secure electronic medical record authorization system for smart device application in cloud computing environments," *Human-Centric Computing Information Sci*,10:1–31,2020.

[23] Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A , " Security and privacy in electronic health records: A systematic literature review," *Journal of biomedical informatics*, 46(3), 541-562.2013.

[24] Semantha, F.H.; Azam, S.; Yeo, K.C.; Shanmugam, B, "A systematic literature review on privacy by design in the healthcare sector," *Electronics* , 9, 452.2020.

[25] Nagasubramanian, G.; Sakthivel, R.K.; Patan, R.; Gandomi, A.H.; Sankayya, M.; Balusamy, B. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud," *Neural Comput.* Appl,32, 639–647,2020.
[26] Semantha, F.H.; Azam, S.; Shanmugam, B.; Yeo, K.C.; Beeravolu, A.R, "A Conceptual Framework to Ensure Privacy in Patient Record Management System," *IEEE Access*, 9, 165667–165689,2021.
[27] Moncrieff, S.; Venkatesh, S.; West, G, "A framework for the design of privacy preserving pervasive healthcare," I*n Proceedings of the 2009 IEEE International Conference on Multimedia and Expo*, New York, NY, USA,1696–1699.2009.
[28] Shrestha, N.; Alsadoon, A.; Prasad, P.; Hourany, L.; Elchouemi, A, "Enhanced e-health framework for security and privacy in healthcare system," *In Proceedings of the 2016 6th International Conference on Digital Information Processing and Communications* (ICDIPC), Beirut, Lebanon, 75–79.2016.

[29] Bhattacharya, P.; Tanwar, S.; Bodke, U.; Tyagi, S.; Kumar, N, "BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications," *IEEE Trans*. Netw. Sci. Eng, 8, 1242–1255.2019.
[30] Carey DJ, Fetterolf SN, Davis FD, Faucett WA, Kirchner HL, Mirshahi U, et al, "The Geisinger MyCode community health initiative: an electronic health record–linked biobank for precision medicine research," *Genet Med*, 18(9):906,2016.
[31] Perera, C.; McCormick, C.; Bandara, A.K.; Price, B.A.; Nuseibeh, B, "Privacy-by-design framework for assessing internet of things applications and platforms," *In Proceedings of the 6th International Conference on the Internet of Things*, Stuttgart, Germany,83–92,2016.
[32] Abdul-Ghani, H.A.; Konstantas, D, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective," *J. Sens*, 8, 22,2019.
[33]Hussien, H.M.; Yasin, S.M.; Udzir, N.I.; Ninggal, M.I.H, "Blockchain-based access control scheme for secure shared personal health records over decentralised storage," 21, 2462,2021.
[34] Demir, O.; Kocak, B, "A Decentralized File Sharing Framework for Sensitive Data," *In Proceedings of the International Conference on Big Data Innovations and Applications, Istanbul*," Turkey,142–149,2019.
[35] Fatokun, T.; Nag, A.; Sharma, S, "Towards a Blockchain Assisted Patient Owned System for Electronic Health Records," 10, 580,2021.
[36] Dehling T, Sunyaev A, "Secure provision of patient-centered health information technology services in public networks—leveraging security and privacy features provided by the German nationwide health information technology infrastructure," 24(2):89–99,2014.

[37] Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," *In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal*, 8(13), 1–5,2017.

[38] Cooper T, Fuchs K, "Technology risk assessment in healthcare facilities," *Biomed Instrum Technol*,47(3):202–7,2013.

[39] Keshta, I.; Odeh, A, "Security and privacy of electronic health records: Concerns and challenges," Egypt. *Inform*, 22, 177–183.2020.

[40] Suzuki MY, Ohnuki Y, Takeshita K.Asian Bioeth Rev, "Genetic Data Governance in Japanese Hospitals," 15(4),1-19,2023.

[41] OVIC, "Privacy by Design: Effective Privacy Management in the Victorian Public Sector; Office of the Victorian Information Commissioner: Melbourne," *Australia*,1–8,2019.

[42] Huang, J.; Qi, Y.W.; Asghar, M.R.; Meads, A.; Tu, Y, "MedBloc: A Blockchain-Based Secure EHR System for Sharing and Accessing Medical Data," In Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), *Rotorua*, 5(8),594–601,2019.

[43]Cifuentes M, Davis M, Fernald D, Gunn R, Dickinson P, Cohen DJ, "Electronic health record challenges, workarounds, and solutions observed in practices integrating behavioral health and primary care," *J Am Board Fam Med*, 28,63–72,2015.