مروری بر پزشکی قانونی ابری

هاله نجفی دیارجان[1]، رضا ابراهیمی آتانی[2]، سجاد زیبافر[1]
[1]دانش آموخته کارشناسی ارشد مهندسی فناوری اطلاعات – شبکه های کامپیوتری، پردیس دانشگاه گیلان
hallenajafy@gmail.com
[2]استادیار گروه مهندسی کامپیوتردانشکده فنی دانشگاه گیلان
rebrahimi@guilan.ac.ir, sadjadzibafar@gmail.com

چکیده

رایانش ابری الگویی کم‌هزینه با کارایی بالا، برای عرضهٔ خدمات رایانشی در پاسخ به نیازهای استفاده‌کنندگان خدمات نوین حوزهٔ فناوری اطلاعات است. مسائل امنیتی موجود در رایانش ابری دلیل عدم تمایل برخی کاربران و سازمان‌ها به استفاده از زیرساخت ابری است. باوجود اقدامات پیش‌گیرانه و واکنشی که در شبکه‌ها به‌کار گرفته می‌شوند، انجام پی‌جویی و پی‌گرد مجرمان پس از وقوع جرایم و حملات سایبری لازم و ضروری است؛ امّا معماری کنونی رایانش ابری، پاسخ‌گوی نیازهای پزشکی قانونی ابری نیست؛ بنابراین روند پژوهش‌های پزشکی قانونی در این زمینه با چالش‌های بسیاری روبه‌رو است. با توجه به مزیت‌های استفاده از رایانش ابری نمی‌توان به‌دلیل مسائل امنیتی آن را نادیده گرفت. پژوهش‌گران راه‌حل‌های مختلفی برای حل چالش‌های امنیتی رایانش ابری با در نظر گرفتن ماهیت پویای رایانش ابری و مسائل قانونی ارائه داده‌اند. در این مقاله مروری، ابتدا ضمن بررسی اهمیت گذار از خدمات سنتی به خدمات ابری، مشکلات امنیتی استفاده از این خدمات را در قالب پزشکی قانونی ابری موردمطالعه قرار می‌دهیم و چالش‌ها و موضوعات باز پژوهشی در این حوزه را طبقه‌بندی می‌کنیم.

واژگان کلیدی: پزشکی قانونی ابری، رایانش ابری، امنیت، محرمانگی، اعتماد الکترونیکی، زنجیرهٔ اعتماد، گزارش ثبت (لاگ).

۱- مقدمه

رایانش ابری[1] نقطهٔ عطفی در ایجاد تحول در زیرساخت فناوری اطلاعات سازمان‌ها به‌حساب می‌آید؛ و فرصت‌های اقتصادی و فناوری‌های امیدوارکننده‌ای را فراهم کرده است. بااین‌وجود مشتریان تمایل ندارند زیرساخت‌های تجارت فناوری اطلاعات را به‌طور کامل به این قسمت واگذار کنند [۱]. مهم‌ترین دلیل این عملکرد، مشکلات امنیتی موجود در این زمینه است. با گسترش فناوری اطلاعات و ارتباطات و استفادهٔ روزافزون از فناوری‌های آن، حملات سایبری و بدافزارها با سرعت زیادی روی شبکه‌ها در حال گسترش هستند. اقدامات متقابل بسیاری برای کنترل جرایم سایبری انجام می‌گیرد. اقداماتی از قبیل چارچوب‌های حقوقی به‌منظور کنترل معیارهای فنی و حقوقی، کنترل محتوای اینترنتی، استفاده از پراکسی‌های عمومی و خصوصی، پزشکی قانونی رایانه‌ای[2]، رمزنگاری[3]، به‌کارگیری تجهیزات امنیتی مختلف و مسائلی از این قبیل. باوجود اقدامات پیش‌گیرانه و واکنشی که در شبکه‌ها به‌کار گرفته می‌شوند، انجام پی‌جویی و پی‌گرد مجرمان پس از وقوع جرائم و حملات سایبری[4] لازم و ضروری است؛ امّا معماری کنونی رایانش ابری، پاسخ‌گوی نیازهای پزشکی قانونی[5] نیست؛ بنابراین روند پژوهش‌های پزشکی قانونی در این زمینه با چالش‌های بسیاری روبه‌روست.

از طرفی رایانش ابری برای تجارت‌هایی با مقیاس کوچک و متوسط مقرون به‌صرفه‌ترین راه معرفی‌شده است؛ لذا این روش جایگزین زیرساخت‌های مدیریتی و فیزیکی پرهزینه شده است. پژوهش‌گران در [۲] با پیشنهاد تغییر زیرساخت فناوری اطلاعات یک سازمان، از یک مرکز دادهٔ[6]

[1] Cloud Computing

[2] Computer Forensics
[3] Encryption
[4] Cyber Attacks
[5] Forensics
[6] Data Center

خارجی به محیط ابری آمازون[1] ۳۷ درصد صرفه‌جویی اقتصادی را رقم زدند. با توجه به مزیت‌های استفاده از فناوری رایانش ابری در تجارت، پیش‌بینی‌های متعددی در سال‌های اخیر در این زمینه صورت گرفته است. [۴] ادعا کرده است که در سال ۲۰۱۴ سود حاصل از رایانش ابری به ۱۴۸,۸ دلار خواهد سید. مجله گارتنر سود ناشی از رایانش ابری را در سال ۲۰۱۴ معادل ۲,۱ بیلیون دلار تخمین زده و پیش‌بینی کرده است که در سال ۲۰۱۵ سود ناشی از رایانش ابری به ۳,۱ بیلیون دلار خواهد رسید [۳]. «رسانه پژوهش بازار» پیش‌بینی کرده است که بازار رایانش ابری جهانی با رشد ۳۰ درصد در سال به ۲۷۰ بیلیون دلار در سال ۲۰۲۰ خواهد رسید [۴]. درآمد ناشی از محیط ابری در سال ۲۰۱۶ حدود ۱۰۶ بیلیون دلار پیش‌بینی‌شده است که این رقم نسبت به سال ۲۰۱۵ حدود ۲۱ درصد افزایش داشته است. طبق پژوهش‌های گلدن ساکس[2] پروژه‌هایی با زیربنای رایانش ابری با نرخ رشد ۳۰ درصد سالیانه[3] از سال ۲۰۱۳ تا ۲۰۱۸ مواجه خواهند شد؛ این در حالی است که سایر سرمایه‌گذاری‌های فناوری اطلاعات دارای رشد ۵ درصد بوده‌اند[۵]. همچنین در[۶] تحلیلی از بازدهٔ درآمدی محیط ابری و برنامه‌های کاربردی بر پایهٔ رایانش ابری بیان‌شده است که مطابق با آن رشد این مجموعه از ۱۳/۵ بیلیون دلار در سال ۲۰۱۱ به ۳۲,۸ بیلیون دلار در سال ۲۰۱۶ خواهد رسید درواقع این رقم رشد ۱۹,۵ درصد دارد که بسیار قابل‌توجه است. ۴۲ درصد از تصمیم‌گیری‌های بازار فناوری اطلاعات در سال ۲۰۱۵ در سرمایه‌گذاری‌ها براساس رایانش ابری صورت گرفته است. درواقع ۷۸,۴۳ بیلیون دلار درآمد حاصل از این سرمایه‌گذاری در سال ۲۰۱۵ بوده است و با توجه به رشد مقبولیت رایانش ابری این مقدار به ۱۳۲,۵۷ بیلیون دلار در سال ۲۰۲۰ خواهد رسید[۶]. علاوه‌بر این در برخی از پیش‌بینی‌ها به استفادهٔ بیش از این حد نیز اشاره‌شده است. رایانش ابری نه‌تنها در بخش‌های خصوصی بلکه در بخش‌های دولتی نیز رشد چشم‌گیری خواهد داشت. بنا به [۷]، دولت فدرال آمریکا مقدار هزینهٔ محیط ابری را برابر با مبلغ ۷۹۲ میلیون دلار در سال ۲۰۱۴ پیش‌بینی کرده است.

استفاده از فناوری رایانش ابری افزایش انعطاف‌پذیری و کارایی را برای سازمان‌ها در برداشته است. خدمات مجازی به‌دلیل وجود سرعت در پیکربندی مجدد، انعطاف‌پذیری بیش‌تری دارند. همچنین بدون نیاز به افزودن سخت‌افزار جدید و یا وجود سخت‌افزار در حالت آماده‌به‌کار، از قابلیت مقیاس‌پذیری پشتیبانی می‌کنند. درنتیجه، از طریق حذف افزونگیِ محاسباتی و ذخیره‌سازی، استفاده از رایانش ابری می‌تواند هزینه‌های خدمات فناوری اطلاعات را کاهش دهد [۸].

باوجود همهٔ مزیت‌های ذکرشده، رایانش ابری مشکلات فراوانی را برای سازمان‌ها و مراجع مقررات‌گذار رایانش ابری به‌وجود آورده است. ساختار پیچیدهٔ رایانش ابری و فقدان استانداردهای لازم از جنبه‌های مختلف مانند تعریف، توافقات سطح خدمت[4] و امنیت داده[5] ازجمله موانعی هستند که پژوهش‌گران درزمینهٔ پزشکی قانونی رایانش ابری[6] با آن مواجه‌می‌شوند [۹]. به‌صورتی‌که پیش‌بینی‌شده است، جرایم سایبری در بریتانیا سالانه ۲۷ بیلیون یورو هزینه‌ساز خواهند بود؛ و درزمینهٔ تجارت حدود ۲۱ بیلیون یورو از طریق سرقت مالکیت علمی و جاسوسی ضرر مالی خواهند داشت. همین‌طور برای دیگر کاربران نیز این مشکلات وجود خواهد داشت؛ بنابراین حفظ محرمانگی[7] داده‌ها یکی از نگرانی‌های کاربران محیط‌های ابری است. به نقل از خدمات تحت وب آمازون، حملات بات‌نت[8] در زیرساخت آمازون اتفاق افتاده است [۱۰]. همچنین یک هکر چینی با کشف رمز رایانامه Gmail نشان داد که بستر رایانش ابری هدفی برای حملات خصمانه است.

محیط‌های ابری از مدل مرسوم چندمستأجری و مجازی‌سازی جهت تأمین کارایی بهتر از منابع استفاده می‌کنند. به‌هرحال این شاخص‌های بنیادی از محیط ابری درواقع شمشیری دو لبه است. همین ویژگی‌ها منجر به ایجاد جرایم و حملات مبتنی بر رایانش ابری می‌شوند و کاربران آن‌ها به‌سختی می‌توانند از این حملات جلوگیری نمایند. با توجه به بررسی IDCI[9]، ۷۴ درصد از فعالیت‌های فناوری اطلاعات و CIO[10]s از محیط ابری استفاده نمی‌کنند [۱۱]. مسائل امنیتی یکی از مهم‌ترین دلیل جلوگیری و بی‌میلی شرکت‌ها برای مهاجرت به دنیای محیط ابری است. برخی از حملات بر رایانش ابری نگرانی‌ها و دغدغه‌های امنیتی را بیش‌ازپیش تشدید کرده‌اند. برای مثال حمله بات‌نت با استفاده از زیرساخت محیط ابری آمازون در سال

[1] Amazon Cloud
[2] Goldman Sachs Study
[3] Compound Annual Growth Rate-CAGR

[4] Service Level Agreement
[5] Data Security
[6] Cloud Forensics
[7] Confidentiality
[8] Botnet Attack
[9] Ingersoll District Collegiate Institute
[10] Chief Information Officer

۲۰۰۹ گزارش شد. گذشته از حملات ناشی از زیرساخت محیط ابری، متجاوزان می‌توانند با استفاده از ویژگی محیط‌های ابری، حملاتی به سامانه‌های دیگر انجام دهند. برای مثال، یک مهاجم می‌تواند صدها ماشین مجازی را به‌منظور انجام حمله DDOS اجاره نماید. بعد از این‌که حمله را با موفقیت انجام داد، او می‌تواند همه مواردی را که برای ردیابی مهاجم موردنیاز است با خاموش‌کردن ماشین مجازی پاک کند. همچنین مجرم می‌تواند فایل‌های محرمانه‌اش (مانند قاچاق کودکان، مستندات تروریست‌ها) را در محیط‌های ابری نگهداری کند و می‌تواند همهٔ شواهد را از رسانهٔ محلی خود جهت پاک‌سازی آن، نابود سازد [۱].

بنابراین باوجود مزیت‌ها و نگرانی‌های مطرح‌شده، پژوهش در مورد پزشکی قانونی دیجیتالی در رایانش ابری ضروری به نظر می‌رسد. با توجه به راه‌اندازی مراکز دادهٔ استانی در چند ماه اخیر و اینترانت ملی در آیندهٔ نزدیک، استفاده از خدمات مبتنی‌بر ابر در کشور روند صعودی خواهد گرفت و موضوع «پزشکی قانونی ابری» به‌عنوان یک امتیاز برای افزایش امنیت رایانش ابری باید در فرآیند طراحی و رصد این زیرساخت جامع کشوری لحاظ شود؛ ازاین‌رو پاسخ‌گویی گردانندگان خدمات ابری کشور در مقابل جرایم، می‌تواند در افزایش استفاده از این فناوری کمک‌کننده باشد.

در این مقاله مروری ابتدا ضمن بررسی اهمیت پزشکی قانونی ابری، مشکلات امنیتی و آسیب‌های احتمالی استفاده از خدمات ابری را در قالب پزشکی قانونی ابری مورد مطالعه قرار می‌دهیم و چالش‌ها و موضوعات بازپژوهشی در این حوزه را طبقه‌بندی می‌کنیم.

در ادامه ساختار کلی مقاله بدین‌شرح زیر ارائه می‌شود: در بخش دوم مفهوم پزشکی قانونی ابری بیان می‌شود. بخش سوم شامل مدل‌های فرآیند پزشکی قانونی دیجیتالی و تشریح مراحل ارائه‌شده است. در بخش چهارم ابزارهای رایج پزشکی قانونی در محیط ابری ارزیابی شده است. بخش پنجم شامل چالش‌های موجود در پزشکی قانونی ابری در هر مرحله از فرآیند پژوهش است. بخش ششم راه‌حل‌های ارائه‌شده را جهت حل چالش‌های معرفی‌شده، معرفی می‌کند. در بخش هفتم زمینه‌های کاری آینده و مشکلات بازپژوهشی در این زمینه معرفی‌شده‌اند و در انتهای مقاله جمع‌بندی می‌شود.

۲- پزشکی قانونی ابری

برای ردیابی هر جرم مربوط به محیط‌های ابری، پژوهش‌گران پزشکی قانونی باید پژوهش‌های پزشکی قانونی دیجیتالی را در محیط‌های ابری انجام دهند، به این شاخهٔ خاص از پزشکی قانونی، پزشکی قانونی ابری گفته می‌شود. پزشکی قانونی ابری را به‌عنوان اصول و جریان برنامه‌های کاربردی پزشکی قانونی رایانه‌ای در محیط‌های رایانش ابری تعریف می‌کنیم. ازآنجاکه رایانش ابری براساس دسترسی شبکه‌های پهناور است و همچنین پزشکی قانونی شبکه[1]، پژوهش‌های پزشکی قانونی را در شبکه‌های خصوصی و همگانی اجرا می‌کند، پژوهش‌گران در [۱۲] پزشکی قانونی ابری را به‌عنوان زیرمجموعه‌ای از پزشکی قانونی شبکه معرفی می‌کنند. دشواری تعریف پزشکی قانونی ابری ازاین‌جهت است که هیچ تعریف دقیق و جامعی از رایانش ابری یا پزشکی قانونی دیجیتالی که مورد پذیرش عموم باشد، وجود ندارد. یکی از فراگیرترین تعاریف از پزشکی قانونی دیجیتالی تعریفی است که نخستین‌بار توسط نخستین همایش پژوهش‌هایی پزشکی قانونی DFRWS[2] در سال ۲۰۰۱ آمده است:

«استفاده روش‌های اثبات‌شدهٔ علمی جهت حفاظت، جمع‌آوری، اعتبار سنجی، شناسایی، تحلیل، تفسیر، مستندسازی و ارائه شواهد دیجیتالی که از منابع دیجیتالی به وجود آمده‌اند، باهدف سهولت در بازسازی صحنه جرم، یا کمک به‌پیش بینی فعالیت‌های مخرب جهت جلوگیری از عملیات طرح‌ریزی‌شده قبلی است».

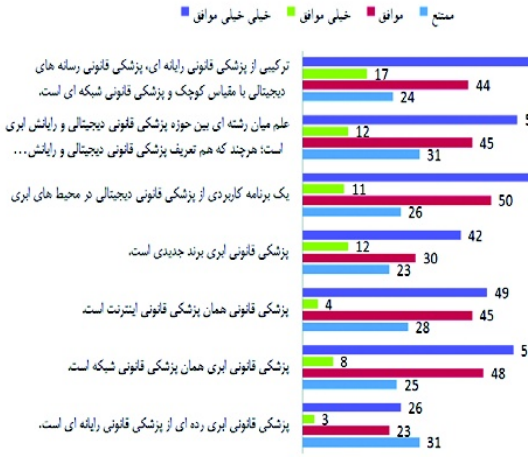
در پاسخ به تعریف پزشکی قانونی ابری در[۱۵] از ۱۲۳ شرکت‌کننده که از متخصصان درزمینهٔ فناوری اطلاعات هستند، نظرسنجی به عمل آمد که نتیجهٔ نظرسنجی در (شکل ۱) قابل‌مشاهده است.

نتایج نشان می‌دهد که اکثریت کارشناسان در مورد تعریف ذیر توافق دارند:

«پزشکی قانونی ابری ترکیبی از پزشکی قانونی رایانه‌ای سنتی، پزشکی قانونی تجهیزات دیجیتالی در مقیاس‌کوچک و پزشکی قانونی شبکه است»، مطابق با شکل، ۶۱ درصد با این نوع تعریف موافق بوده‌اند و ۱۷ درصد به‌طورکامل با این تعریف موافق بوده‌اند. با توجه به این نظرسنجی، کارشناسان معتقدند که پزشکی قانونی ابری، نه طبقه‌ای از پزشکی قانونی رایانه‌ای است و نه به‌طور کامل به‌عنوان حوزه‌ای جدید مطرح‌شده است؛ درواقع می‌توان گفت که ترکیبی از فن‌های پزشکی قانونی سنتی در محیط‌های رایانش ابری است.

[1] Network Forensics
[2] Digital Forensics Research Conference

(جدول ۱) تفاوت بین پزشکی قانونی سنتی و ابری را با توجه به معیارهای اساسی نشان می‌دهد.



شکل ۱: ارزیابی کمی میزان مقبولیت پزشکی قانونی ابری در بین کارشناسان حوزه امنیت در سال ۲۰۱۳ [۱۳]

مدل‌های فرآیند پزشکی قانونی دیجیتالی

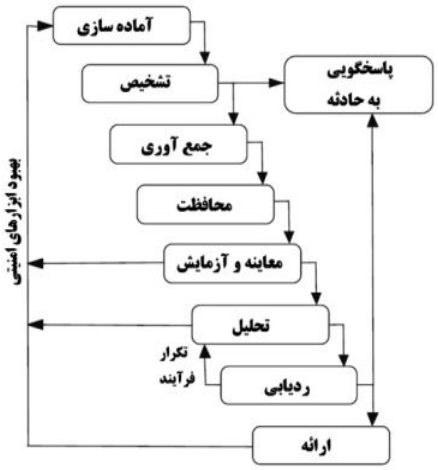
در همایش DFRWS برای نخستین‌بار مدل فرآیندی برای پزشکی قانونی دیجیتال در محیط‌های شبکه‌ای ارائه شد [۴۱]. مدل‌های زیادی با مراحل مختلف پیشنهاد شده است. در سال ۱۹۸۴، پولیت در[۱۵] و در سال ۲۰۰۷ در [۶۱] روشی برای برخورد با پژوهش‌های دیجیتالی ارائه داد. به‌طوری‌که نتایج از نظر علمی قابل اعتماد و از نظر قانونی قابل‌قبول برای دادگاه باشد. این چارچوب از چهار مرحلهٔ اکتساب، شناسایی، ارزیابی و پذیرش تشکیل شده است. از سال ۲۰۰۱، چارچوب‌های کاری و مدل‌های فرآیندی متنوعی برای اجرای پژوهش‌های پزشکی قانونی دیجیتالی پیشنهاد شده است. در سال ۲۰۰۲ در [۷۱] فرآیند پژوهش‌های پزشکی قانونی دیجیتال با هدف استفاده عمومی ارائه شد. این فرآیند از شش مرحلهٔ شناسایی، حفظ و نگهداری، جمع‌آوری، بررسی، تجزیه‌وتحلیل، ارائه و نتیجه‌گیری تشکیل‌شده است. پژوهش‌گران در [۱۸،۱۹،۲۰،۲۱،۲۲] مدل‌های مختلفی را پیشنهاد داده‌اند. تمام مدل‌های ذکرشده برای پژوهش‌گران دیجیتالی قابل اجرا هستند. در سال ۲۰۱۰ پژوهش‌گران در [۳۲] مدلی برای تجزیه تحلیل پزشکی قانونی شبکه براساس مدل‌های موجود ارائه داده‌اند. (شکل ۲) مراحل مختلف این مدل را نشان می‌دهد. این مدل در بین مدل‌های ارائه‌شده در سال‌های اخیر مورد توجه خاصی قرارگرفته است و به‌عنوان اساس کار بسیاری از پژوهش‌ها مورداستفاده قرار می‌گیرد. در ادامه مراحل مختلف این مدل را توضیح خواهیم داد.

۲-۱- آماده‌سازی

در این گام زمینه‌سازی‌های لازم برای مجموعه‌ای از وظایف انجام می‌شود. این مرحله تضمین می‌کند که پژوهش‌گر پزشکی قانونی به‌درستی آموزش‌دیده و زیرساخت برای کنترل پژوهش‌ها مناسب است.

جدول ۱: مقایسه پزشکی قانونی سنتی و ابری [۹]

فاز	فرآیندها	پزشکی قانونی رایانه‌ای	پزشکی قانونی ابری
رایانه	رمزنگاری و ارزیابی صحنه	بلی	خیر
	مستندسازی صحنه	بلی	خیر
	جمع‌آوری مدارک، منبع مدرک	سخت‌افزار فیزیکی	تصویر مجازی
	محل جمع‌آوری مدارک	صحنه جرم	مرکز داده CSP
	انتقال بسته	فیزیکی	به‌طور الکترونیکی با اینترنت
	ذخیره‌سازی مدارک دیجیتالی	اتاق بایگانی مدارک	مرکز داده CSP
جمع‌آوری	زمان جمع‌آوری	سریع	آهسته
	جمع‌آوری اطلاعات RAM	بلی	به‌سختی
	درهم سازی MD5	آهسته	ارائه‌شده
	بازیابی داده‌های پاک‌شده	ممکن	به‌سختی
	جمع‌آوری آبرداده	شدنی	امکان از دست دادن آبرداده
	مُهر زمانی	دقیق	سخت به دلیل مشکلات همزمانی
بررسی	جمع‌آوری مدارک	سخت‌افزار- خدمت دهنده شبکه	CSP
	رمزنگاری	آهسته	سریع



شکل ۲: مدل فرآیند عمومی برای پزشکی قانونی شبکه [۲۳]

۲-۲- تشخیص

درصورت بروز هرگونه پدیدهٔ غیرمتعارف، ابزارها، به‌کاررفته‌شده و هشدارهایی تولید می‌شود. این ابزارها ممکن است یک حفرهٔ امنیتی یا نقض سیاستی خاص را تشخیص دهند. با تجزیه‌وتحلیل پارامترهای مختلف وقوع حمله تشخیص داده می‌شود و جریان فرآیند به گام بعدی تغییر موضوع می‌دهد. این احتمال نیز وجود دارد که با بررسی پارامترها خطا در ارسال هشدار تشخیص داده شود.

۲-۳- پاسخ به حادثه

پاسخ ارائه‌شده در این مرحلهٔ وابسته به نوع حملهٔ تشخیص‌داده‌شده و سیاست‌های سازمانی و قانونیِ موجود است. با توجه به شرایط، تصمیم مناسبی جهت ادامهٔ بررسی و دست‌یابی به مدارک گرفته می‌شود.

۲-۴- جمع‌آوری

این مرحله مهم‌ترین مرحل در روند پژوهش‌های پزشکی قانونی به‌حساب می‌آید؛ بنابراین باید با استفاده از ابزارهای نرم‌افزاری و سخت‌افزاری امن به جمع‌آوری مدارک قابل‌قبول پرداخته شود.

۲-۵- محافظت

در این مرحله یک رونوشت از داده‌های مورد بررسی برای پاسخ‌گویی به مسائل قانونی، نگهداری و محافظت می‌شود؛ علاوه‌بر این‌یک درهم‌سازی از داده‌ها نیز تهیه می‌شود. در روند پژوهش‌ها از داده‌های رونوشت استفاده می‌کنند.

۲-۶- بررسی

داده‌های به‌دست‌آمده از مرحلهٔ قبلی، ممکن است دارای افزونگی و یا تناقض باشد؛ ازاین‌رو مرحلهٔ بررسی این اطمینان را می‌دهد که نیاز به جستجوی قاعده‌مند است تا هیچ‌کدام از اطلاعات حیاتی از دست نرود. همچنین یک مجموعه‌داده‌ای که شامل اطلاعات کم ولی دارای مدارک با احتمال بالاست، تشخیص داده می‌شود.

۲-۷- تجزیه‌وتحلیل

در این گام، روش‌های داده‌کاوی[1] و محاسباتی برای جستجوی داده‌ها و تطابق الگوهای حمله استفاده می‌شود. الگوهای حمله در کنار هم قرار داده شده و برای درک هدف و متدولوژی مهاجم، تجزیه تحلیل می‌شود.

[1] Data Mining

۲-۸- آزمایش

مرحلهٔ آزمایش، داده‌هایی را برای پاسخ و تعقیب قانونی مهاجم فراهم می‌سازد. این مرحله، به‌وسیلهٔ دستگاه‌های میانی و مسیرهای ارتباطی، از نتایج مرحله قبلی برای به دست‌آوردن مسیری از قربانی به نقطه شروع حمله استفاده می‌کند. ممکن است نیاز به یک سری ویژگی‌های بیش‌تری از مرحله تحلیل باشد و ازاین‌رو، این دو مرحله به‌صورت نسبی برای رسیدن به نتیجه‌گیری ایفا خواهند شد.

۲-۹- ارائه

ارائه، مرحلهٔ نهایی مدل فرآیند بوده که در آن موارد زیر تحقق می‌یابد:

- آماده‌سازی مستندات سامانه برای برآورده‌سازی نیازمندی‌های قانونی صورت می‌گیرد.
- برای درک آسان‌تر، از مجازی‌سازی برای ارائه نتایج استفاده می‌شود.
- کل مستندات برای ارجاعات آینده نگهداری می‌شود.

همهٔ این دستورالعمل‌ها قبل از ظهور فناوری رایانش ابری مطرح‌شده و اغلب فرض بر این بوده است که پژوهش‌گر دسترسی فیزیکی و کنترل کاملی روی سیستم و وسایل هدف به‌ویژه به رسانه‌های ذخیره‌سازی دارد. این فرضیات برای پژوهش‌ها در محیط‌های ابری شدنی نیست. پزشکی قانونی دیجیتالی سنتی شامل تصرف تجهیزات و وسایل کاربران مشکوک است که به پژوهش‌گران اجازهٔ نگهداری، کسب، تحلیل و ارائهٔ شواهد در حالت قانونی را می‌دهد. ناهمگنی در محیط ابری و افزایش چشم‌گیر مقدار ذخیره‌سازی رایانش ابری، بدان معناست که این مراحل در مورد مشتری، شبکه و ارائه‌دهندهٔ خدمات ابری در زمینهٔ فن‌ها و ابزارهای متعارف، چالش‌های قابل‌توجهی را به‌وجود می‌آورد. (جدول ۲) مکان‌های احتمالی وجود مدارک را نشان می‌دهد که پژوهش‌گر پزشکی قانونی لزوماً به‌تمامی آن‌ها دسترسی ندارد.

۳- ارزیابی ابزارهای پزشکی قانونی موجود در محیط ابری

پژوهش‌گران در [۴] با استفاده از ابر عمومی EC2 از بستر تحت وب آمازون، در بستر آزمایشی زنده آمارهای موجود را بررسی کرده‌اند. (جدول ۳) نتایج سه آزمایش جمع‌آوری مدارک پزشکی قانونی ابری با استفاده از ابزارهایِ رایج موجود است؛ و زمان بازیابی داده و اعتماد موردنیاز در

سیستم‌عامل مهمان، هایپرویزور، سیستم‌عامل میزبان، سخت‌افزار میزبان، شبکه و مؤلفه‌های خدمات تحت وب آمازون را نشان می‌دهد.

جدول ۲: مکان‌های احتمالی وجود مدارک در رایانش ابری [۹]

مکان‌های احتمالی مدارک	مؤلفه‌های ابری
سیستم تشخیص نفوذ میزبان محتوای وب‌سایت و سیستم مرورگر فایجریان‌ها و سیستم دسترسی سیستم چت کردن ذخیره‌گاه برنامه	مشتری
سیستم دسترسی سیستم تبادل محتوی بسته محتوی سرآمد	شبکه
سیستم فایجریان‌ها سیستم دسترسی مدیر داده‌های IDS و NetFlow ذخیره‌سازی داده (در مورد مشتری‌های IaaS)	ارائه‌دهنده خدمات ابری

نصب EnCase و FTK در آزمایشِ یک، موفقیت‌آمیز بود؛ با این کار توانایی جمع‌آوری صفحهٔ سخت و تصویر حافظهٔ راه دور به‌وجود آمد. تحلیل این تصاویر با ابزارهای EnCase و FTK، خط زمانی فعالیت‌ها را که شامل نصب Apache و ایجاد و حذف صفحه وب بوده آشکار کرد. تحلیل به‌دست‌آمده شامل مواردی که باعث ایجاد تردید در صحت داده‌ها شود، نبوده است. سرعت جمع‌آوری فرآیند موردنظر به دانش پژوهش‌گران در مورد چگونگی به‌کارگیری عامل راه دور و پهنای باند شبکه جهت انتقال داده‌ها بستگی دارد. جهت انتقال ۳۰GB تصویر صفحه و ۲ GB تصویر حافظه به‌طورتقریبی دوازده ساعت برای هرکدام از ابزارهای EnCase و FTK زمان لازم بوده است.

آزمایش دوم با موفقیت انجام شد و نتیجهٔ کار، تصویر کامل از درایو و خط زمانی صحیح بوده است. درون‌نگری ماشین مجازی[1] ابزار قدرتمندی در پزشکی قانونی است و اجازه پژوهش زنده از میزبان، بدون‌آشکارشدن وجود پژهش‌گر را فراهم می‌کند.؛ البته درون‌نگری، ویژگی خاصی است که باید در محیط ابری توسط ارائه‌کنندهٔ خدمات، پیاده‌سازی شود. با این آزمایش از طریق تأیید اعتبار، صحت تصویر به دست آمد. ازآنجایی‌که پژوهش‌گران به صفحهٔ فیزیکی دسترسی داشته‌اند، توانستند با مقایسهٔ مقدار درهم‌ساز ابری با تصویر EnCase صفحهٔ اصلی، به‌درستی آن پی ببرند.

در آزمایش سوم از طریق بستر تحت وب آمازون تصویر صفحه با موفقیت و امنیت به دست آمد. همچنین توانایی بارگیری اطلاعات درایو درون EnCase و FTK به‌آسانی و با تأیید محتوا و ارائه گزارش با محتوای مناسب جهت هر فایل وجود داشت.

این گزارش شامل موارد زیر برای هر فایل بوده است.

- تاریخ انتقال
- زمان انتقال
- مکان ذخیره‌سازی
- جمع تطبیقی MD5
- تعداد بایت‌ها

در این مورد دستیابی به داده، حدود پنج روز طول کشید و هزینه‌ای حدود ۱۲۵ دلار صرف شد. استفاده از EnCase و FTK آسان‌تر است. با وجود زمان موردنیاز جهت تنظیم و آموزش استفاده از توانایی‌های راه دور این ویژگی بسیار مناسب است. زمان دوازده‌ساعتی مورد نیاز جهت بازیابی تصویر صفحه به‌صورت قابل توجهی کوتاه‌تر از زمان ۱۲۰ساعتهٔ مورد نیاز در بستر تحت وب آمازون برای یک مقدار داده است.

۴- پزشک قانونی دیجیتالی در محیط‌های ابری

در این بخش چالش‌های پزشکی قانونی ابری را بررسی می‌کنیم. این چالش‌ها با توجه به مدل فرآیند پزشکی قانونی دیجیتالی مطرح‌شده‌اند. در هر مرحله از روند پژوهش‌ها پزشکی قانونی ابری، پژوهش‌گر با مسائلی در زمینه‌های شناسایی و جمع‌آوری، ثبت وقایع، حفظ زنجیره اعتماد، نگهداری داده‌های مورد اعتماد و ارائه به مرجع قانونی مواجه خواهد شد.

۴-۱- جمع‌آوری داده‌های پزشکی قانونی

جمع‌آوری مدارک دیجیتالی[2] سخت‌ترین گام در جریان پژوهش‌های پزشکی قانونی است. هر اشتباهی که در مرحلهٔ جمع‌آوری اتفاق بیفتد تا مرحلهٔ بررسی، گزارش و ارائه منتشر خواهد شد و در تمام مسیر فرآیند پژوهش تأثیر خواهد داشت.

[1] Virtual machine introspection

[2] Digital Evidence

آزمایش	ابزار	وضعیت جمع‌آوری مدارک	زمان موردنیاز (ساعت)	اعتماد موردنیاز
۱	EnCase	موفقیت‌آمیز	۱۲	سیستم‌عامل مهمان /هایپرویزور/سیستم‌عامل میزبان/سخت‌افزار میزبان/شبکه
۱	FTK	موفقیت‌آمیز	۱۲	سیستم‌عامل مهمان/هایپرویزور/سیستم‌عامل میزبان/سخت‌افزار میزبان/شبکه
۱	FTK Imager(disk)	موفقیت‌آمیز	۱۲	سیستم‌عامل مهمان/هایپرویزور/سیستم‌عامل میزبان/سخت‌افزار میزبان/شبکه
۱	Fast dump	موفقیت‌آمیز	۲	سیستم‌عامل مهمان/هایپرویزور/سیستم‌عامل میزبان/سخت‌افزار میزبان/شبکه
۱	Memoryze	موفقیت‌آمیز	۲	سیستم‌عامل مهمان/هایپرویزور/سیستم‌عامل میزبان/سخت‌افزار میزبان/شبکه
۱	FTK Imager (memory)	موفقیت‌آمیز	۲	سیستم‌عامل مهمان/هایپرویزور/سیستم‌عامل میزبان/سخت‌افزار میزبان/شبکه
۱	Volume Block Copy	موفقیت‌آمیز	۱۴	سیستم‌عامل مهمان/هایپرویزور/سیستم‌عامل میزبان/سخت‌افزار میزبان/شبکه
۲	Agent Injection	موفقیت‌آمیز	۱	هایپرویزور/سیستم‌عامل میزبان/سخت‌افزار میزبان/شبکه
۳	AWS Export	موفقیت‌آمیز	۱۲۰	متخصصین خدمات تحت وب /سیستم‌عامل میزبان متخصصین/سخت‌افزار و نرم‌افزار/سخت‌افزار خدمات تحت وب/نرم‌افزار خدمات تحت وب

جدول ۳: نتایج سه آزمایش جمع‌آوری مدارک پزشکی قانونی ابری با استفاده از ابزارهای رایج [۲۴]

براساس [۲۵] مدارک، در سه حالت مختلفِ استراحت، جنبش و در حال اجرا، در محیط ابری می‌توانند در دسترس باشند؛ در داده‌هایی که فضای صفحه را اشغال کرده است، به‌عنوان داده‌های در استراحت جمع‌آوری می‌شوند. داده‌هایی که می‌تواند از یک حالت به حالت دیگر منتقل شود، به‌عنوان داده‌های در جنبش نامیده می‌شوند. گاهی داده‌ها را به‌صورت «قابل اجرا» داریم. برای مثال تصویر لحظه‌ای یک حالت از سیستم؛ در این صورت می‌توانیم دادهٔ «قابل اجرا» را بارگذاری و اجرا کنیم و به داده‌های در استراحت یا جنبش دسترسی پیدا کنیم.

در پزشکی قانونی ابری جریان جمع‌آوری داده‌ها براساس مدل خدمت و توسعهٔ محیط ابری تغییر می‌کند .در ادامه به بررسی برخی از ویژگی‌هایی که باعث تشدید مشکلات در مرحله جمع‌آوری داده در پزشک قانونی ابری نسبت به پزشک قانونی رایانه‌ای می‌شود، می‌پردازیم.

۴-۱-۱- عدم دسترسی فیزیکی

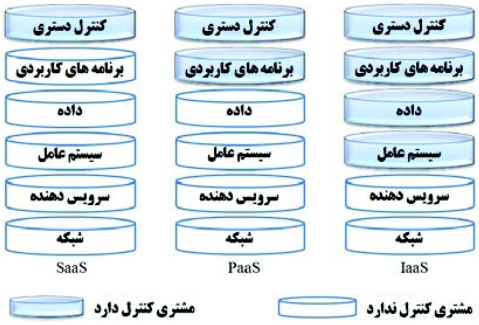
عدم دسترسی فیزیکی مدارک دیجیتالی باعث مشکل‌ترشدن جریان جمع‌آوری مدارک در پزشکی قانونی ابری می‌شود. جریان‌های ثابت پزشکی قانونی دیجیتالی و ابزارهای موجود، فرض را بر آن گذاشته‌اند که به رایانه‌ها دسترسی فیزیکی داریم. درحالی‌که در پزشکی قانونی ابری موقعیت‌ها متفاوت هستند. گاهی حتی نمی‌دانیم داده در کدام مکان قرارگرفته است؛ همچنین داده می‌تواند در بین تعداد زیادی میزبان در چندین مرکز داده توزیع شده باشد [**Error! Reference source not found.**]. (شکل ۳ و ۴) تفاوت جمع‌آوری اطلاعات در محیط ابری نسبت به پزشکی قانونی سنتی را نشان می‌دهد.

شکل۳: روال جمع آوری داده در پزشکی قانونی سنتی

شکل ۳: جمع آوری داده در پزشکی قانونی ابری [۸]

۴-۱-۲- کنترل کمتر در محیط‌های ابری و وابستگی به فراهم‌کننده خدمات ابری

در پزشکی قانونی رایانه‌ای سنتی، پژوهش‌گران کنترل کاملی بر مدارک دارند. برای مثال صفحه سخت توسط پلیس ضبط می‌شود؛ امّا در محیط ابری کنترل روی‌داده‌ها براساس مدل خدمت و توسعه مشخص می‌شود. (شکل ۵) میزان محدودیت کنترل مشتریان در لایه‌های مختلف برای سه مدل خدمت، «نرم‌افزار به‌عنوان خدمت[1]»، «زیرساخت به‌عنوان خدمت[2]» و «بستر به‌عنوان خدمت[3]» را نشان می‌دهد. به همین دلیل در اکثر مواقع برای جمع‌آوری مدارک دیجیتالی از محیط‌های رایانش ابری به فراهم‌کنندهٔ خدمات ابری[4] وابسته خواهیم بود، این مسألهٔ تبدیل به گلوگاهی جدّی در مرحله جمع‌آوری‌شده است.



شکل ۵: میزان محدودیت کنترل مشتریان در لایه‌های مختلف [۳۱]

همان‌طور که در شکل دیده می‌شود، کاربران در مدل «زیرساخت به‌عنوان خدمت» نسبت به دو مدل دیگر دارای کنترل بیشتری هستند. پایین‌بودن سطح کنترل در دو مدل «نرم‌افزار به‌عنوان خدمت» و «بستر به‌عنوان خدمت» باعث به‌وجودآمدن چالش‌های بیش‌تر برای این دو مدل در مرحلهٔ جمع‌آوری شده است؛ حتی گاهی کار جمع‌آوری غیرممکن خواهد بود؛ امّا اگر پژوهش‌گر پزشکی قانونی ابری به نحوی تصویر نمونهٔ «زیرساخت به‌عنوان خدمت» را به دست بیاورد کار بررسی و پژوهش سیستم به‌آسانی انجام خواهد شد.

در مدل‌های «نرم‌افزار به‌عنوان خدمت» و «بستر به‌عنوان خدمت» به فراهم‌کنندهٔ خدمات ابری وابسته‌ایم و تنها به سطح بالایی از اطلاعات لاگ‌ها(گزارش‌های ثبت‌شده) دسترسی داریم. مشتریان در مدل «بستر به‌عنوان خدمت» روی تمام برنامه‌های کاربردی توسعه‌یافته کنترل دارند. آن‌ها می‌توانند لاگ فعالیت‌های مختلف را جهت تسهیل در جریان پژوهش‌ها نگهداری کنند. در مقابل در مدل «نرم‌افزار به‌عنوان خدمت» مشتریان هیچ کنترلی روی لاگ فعالیت ندارند.

پژوهش‌گران در [۲۶] دشواری جمع‌آوری داده را با استفاده از یک موردکاوی فرضی در قاچاق کودکان، ارائه داده‌اند. برای پژوهش در این مورد، پژوهش‌گر پزشکی قانونی از بیت‌به‌بیت داده رونوشت می‌گیرد تا عکس و فیلم‌های مربوط به قاچاق را اثبات کند؛ امّا در محیط ابری، پژوهش‌گر خود قادر به جمع‌آوری داده‌ها نخواهد بود. ابتدا او نیاز به حکم بازرسی برای فراهم‌کنندهٔ خدمات ابری دارد. چند مشکل در رابطه با حکم بازرسی در محیط ابری وجود دارد. برای مثال حکم باید مکان مورد پژوهش را مشخص کند، امّا در محیط ابری داده‌ها ممکن است به‌طوردقیق در یک مکان و یا یک خدمت‌دهنده ذخیره‌سازی خاص نباشند. به‌علاوه داده‌ها در محیط ابری نمی‌توانند به‌وسیلهٔ خدمت‌دهندهٔ ذخیره‌سازی توقیف شوند. همچنین صفحه‌های یکسان می‌توانند شامل داده‌هایی از چند کاربر نامرتبط باشند. برای شناسایی جرایم، باید بدانیم که ماشین‌های مجازی دارای آی‌پی ایستا هستند یا نه؟ به‌طورتقریبی در همهٔ شرایط این مسألهٔ به میزان شفافیت و همکاری فراهم‌کننده خدمات ابری وابسته است [۱۲].

۴-۱-۳- داده‌های فرّار

داده‌های فرّار با خاموش‌شدن سیستم از بین خواهند رفت. زمانی که ماشین مجازی خاموش شود، اگر از نمونه ماشین مجازی تصویری نداشته باشیم، همهٔ داده‌ها از بین می‌روند. اگرچه مدل «زیرساخت به‌عنوان خدمت» دارای مزیت‌هایی نسبت به دو مدل دیگر است؛ امّا حافظهٔ فرّار درصورتی‌که داده‌ها به‌صورت همگام‌شده، به حافظهٔ پایدار منتقل نشوند،

[1] Software as a Service
[2] Infrastructure as a Service
[3] Plarform as a Service
[4] Cloud Service Provider

مشکل مهمی در مدل «زیرساخت به‌عنوان خدمت» خواهد بود؛ مانند Amazon s3 و EBC. با روشن‌شدن دوبارهٔ ماشین مجازی در «زیرساخت به‌عنوان خدمت» تمامی داده‌ها از بین خواهند رفت؛ ورودی‌های ثبت‌شده یا فایل‌های موقتی اینترنت که در محیط‌های مجازی مستقرشده و یا ذخیره‌شده‌اند، زمانی که کاربر از سیستم خارج می‌شود از بین می‌روند [۲۷]. بااین‌حال مشتریان می‌توانند با پرداخت هزینهٔ بیش‌تر به حافظهٔ پایدار دست یابند؛ البته این روی‌کرد برای تجارت‌های کوچک و یا حتی متوسط رایج و مقرون‌به‌صرفه نیست. علاوبر این‌یک کاربر بداندیش می‌تواند از این آسیب‌پذیری سوء استفاده کند. [۲۵] مشکلی جدی را با توجه به ماهیت فرّاربودن مدارک در محیط ابری معرفی می‌کند: مشکل به این صورت است که یک مالک نمونهٔ ابر می‌تواند متقلبانه ادعا کند که نمونه‌اش توسط اشخاص دیگر یا فعالیت‌های خصمانه به خطر افتاده است .اثبات نادرست‌بودن این ادعا برای پژوهش‌گران پزشکی قانونی دشوار خواهد بود.

۴-۲- موضوع اعتماد

وابستگی به شخص سوم مشکل اعتماد را در جریان پژوهش‌های پزشکی قانونی مطرح می‌کند. در موردکاوی قاچاق کودکان توسط [۶] موضوع اعتماد در جمع‌آوری مدارک برجسته شده است. بعد از صدور حکم بازرسی، پژوهش‌گر نیاز به متخصص فنی فراهم‌کننده خدمات محیط ابری، برای جمع‌آوری داده دارد. کارمند محیط ابری مجاز به انجام پژوهش‌ها پزشکی قانونی نبوده و نمی‌توان صحت اعتماد به او را در دادگاه اثبات کرد. همچنین تاریخ و مُهر زمانی داده اگر از چند سیستم فرستاده شده باشد، قابل اعتماد نخواهد بود [۲۸].

پژوهش‌گران در [۲۶] جمع‌آوری مدارک از محیط‌های ابری را بررسی کرده‌اند. یکی از نقاط ضعفی که در این پژوهش مشخص شد عدم امکان بررسی صحت تصویر صفحهٔ پزشکی قانونی در Amazon EC2 است؛ زیرا Amazon EC2 الگوریتم جمع تطبیقی مقادیر موجود در EC2 را ارائه نمی‌دهد.

۴-۳- پهنای باند وسیع

همان‌طور که در آمارها نشان داده‌شده است، مقدار مدارک دیجیتالی به‌سرعت در حال افزایش است. پژوهش‌گران در [۲۷] موضوع نیازمندی به پهنای باند بالا را، در پژوهش‌های حساس به زمان مطرح کرده‌اند. مشخصه تقاضاهای رایانش ابری نقش مهمی را در افزایش مدارک دیجیتالی در آیندهٔ نزدیک ایفا می‌کند. در پژوهش‌های پزشکی قانونی سنتی مدارک را از صفحهٔ سخت رایانهٔ مظنون جمع‌آوری می‌کنیم؛ امّا در محیط ابری این کار به‌دلیل عدم دسترسی فیزیکی به داده‌ها ممکن نیست. یکی از راه‌های دسترسی به اطلاعات ماشین مجازی، بارگیری تصویر نمونهٔ ماشین مجازی است. به‌طورطبیعی حجم بارگیری با افزایش داده‌های موجود در ماشین مجازی، افزایش می‌یابد؛ بنابراین به پهنای باند وسیع و صرف هزینهٔ بالا جهت بارگیری تصویر نیاز داریم.

۴-۴- چندمستأجری

در رایانش ابری، چند ماشین مجازی می‌توانند به‌صورت هم‌زمان در بستر فیزیکی یکسان به اشتراک گذاشته شوند. برای مثال داده‌های چندمشتری می‌تواند در یک مکان ذخیره‌شده باشد. این ماهیت محیط‌های ابری با تک‌مالکیتی دستگاه‌های رایانه‌ای سنتی متفاوت است. در هر مورد خصمانه، زمانی که مدارک جمع‌آوری می‌شوند، باید دو موضوع را مورد بررسی قرار دهیم: ابتدا باید اثبات کنیم که داده‌های جمع‌آوری‌شده با دیگر داده‌ها مخلوط نشده‌اند [۲۷]؛ سپس باید از حریم شخصی دیگر مستأجران در حین اجرای پژوهش‌های پزشکی قانونی حفاظت کنیم [۲۸]. این دو مورد خود باعث به‌وجودآمدن چالش‌های بیش‌تری در این زمینه شده است. ویژگی چندمستأجری[1] باعث اجرای حملهٔ هم‌کانالی[2] می‌شود که کار پژوهش و پی‌گیری آن بسیار سخت است [۲۹].

۴-۵- پزشکی قانونی زنده[3]

تعدد نقاط پایانی، به‌ویژه نقاط پایانی سیار، بازیابی داده‌ها و جمع‌آوری مدارک را با مشکل روبه‌رو کرده است. به‌دلیل تعداد زیاد منابع متصل‌شده به محیط‌های ابری، جرایم و بارکاری پژوهش‌های وابسته به این محیط زیاد است. ایجاد خط زمانی[4] یک رویداد نیازمند ایجاد هم‌زمانی است. همگام‌کردن زمان، کاری پیچیده است؛ زیرا داده‌ها در ماشین‌های فیزیکی مختلف یا مناطق جغرافیای مختلف

[1] Multi Tenancy
[2] Side-Channel Attack
[3] Live Forensics
[4] TimeLine

هستند و یا ممکن است در جریان بین زیرساخت محیط ابری و مشتریان نقاط پایانی دوردست باشد [۱۲].

۴-۶- ثبت وقایع

تحلیل لاگ پردازش‌های مختلف نقش مهمی در پژوهش‌های پزشکی قانونی ایفا می‌کند. اگرچه جمع‌آوری اطلاعات بحرانی در محیط‌های ابری به‌سادگی دستگاه‌های رایانه‌ای نیست و حتی در بعضی مواقع ناممکن خواهد بود، بااین‌حال لاگ پردازش‌ها، لاگ شبکه و لاگ برنامه‌های کاربردی در شناسایی کاربر بداندیش بسیار مهم و مفید هستند [۳۰]. پژوهش‌گران پزشکی قانونی ابری تعدادی از چالش‌های محیط ابری را براساس تحلیل و پزشکی قانونی لاگ‌ها شناسایی کرده‌اند. در ادامه این چالش‌ها را به‌طور خلاصه بیان می‌کنیم:

۴-۶-۱- عدم تمرکز لاگ‌ها

در زیرساخت محیط ابری، اطلاعات موجود در لاگ‌ها در یک مکان خاص و در خدمت‌دهندهٔ لاگ متمرکز نیستند. بیش‌تر لاگ‌ها در چند خدمت‌دهندهٔ مختلف پخش‌شده‌اند. اطلاعات لاگ چند کاربر ممکن است در یک مکان و یا در چند خدمت‌دهنده موجود باشد [۲۷].

۴-۶-۲- لاگ‌های فرّار

بعضی از لاگ ها در محیط‌های ابری فرّار هستند؛ به‌ویژه در مورد ماشین‌های مجازی این خاصیت برقرار است. اگر کاربر، ماشین مجازی خود را خاموش کند، همهٔ داده‌ها غیرقابل‌دسترس خواهند بود [۳۰].

۴-۶-۳- چندطبقه و چندلایه‌بودن

چندین لایه و طبقه در معماری محیط‌های ابری وجود دارد. لاگ‌ها در هر طبقه تولید می‌شوند. برای مثال همهٔ این لایه‌ها لاگ‌های باارزشی برای پژوهش‌های برنامه‌های کاربردی، شبکه، سیستم‌عامل و پایگاه داده پزشکی قانونی تولید می‌کنند. جمع‌آوری لاگ‌ها از چندلایه مختلف چالشی برای پژوهش‌گران پزشکی قانونی محسوب می‌شود [۳۰].

۴-۶-۴- دسترس‌پذیری لاگ‌ها

لاگ‌های تولیدشده در لایه‌های مختلف باید در دسترس ذی‌نفعان مختلف سیستم مانند مدیر سیستم، پژوهش‌گر پزشکی قانونی و توسعه‌دهنده باشد. مدیر سیستم باید لاگ‌های مربوط به رفع مشکل سیستم را در اختیار داشته باشد. توسعه‌دهنده به لاگ‌ها برای تعمیر ایرادهای برنامه‌های کاربردی نیاز دارد. پژوهش‌گر پزشکی قانونی به لاگ‌هایی که در پیش‌برد پژوهش‌ها کمک می‌کنند، نیاز دارد [۲۸]؛ ازاین‌رو، باید سازوکارهایی جهت کنترل دسترسی، متناسب با نیاز واقعی افراد در یک روش امن و آشکارا در نظر گرفته شود، به‌طوری‌که هر یک از افراد با حدومرز مشخصی اجازهٔ دسترسی به قسمت‌های مختلف سیستم را داشته باشند.

۴-۶-۵- وابستگی به فراهم‌کنندهٔ خدمات ابری

در حال حاضر برای به‌دست‌آوردن لاگ‌ها در همهٔ شرایط به فراهم‌کنندگان خدمات ابری وابسته‌ایم. دسترسی به لاگ‌ها متناسب با مدل خدمت ارائه‌شده متغیر خواهد بود. در مدل «نرافزار به‌عنوان خدمت» مشتری هیچ لاگی را از سیستم به دست نمی‌آورد؛ مگر اینکه فراهم‌کنندهٔ خدمات ابری، اطلاعات لاگ را تأمین کند. در مدل «بستر به‌عنوان خدمت» فقط امکان به‌دست‌آوردن لاگ برنامهٔ کاربردی از سمت مشتری وجود دارد. برای به‌دست‌آوردن لاگ‌های شبکه، پایگاه داده و یا سیستم‌عامل به فراهم‌کنندهٔ خدمات ابری وابسته‌ایم [۱]. برای مثال Amazon لاگ مربوط به توازن بار را برای مشتری فراهم نمی‌کند [۱۰]. در پژوهش‌های اخیر [۳۰] بیان کرد که قادر به کسب داده‌های لاگ MySql از Amazon's Relational Database Service نبوده است. در مدل «زیرساخت به‌عنوان خدمت» مشتریان به لاگ شبکه و پردازش دسترسی ندارند؛ امّا در قسمت‌های دیگر قادر به ذخیرهٔ اطلاعات لاگ هستند.

۴-۶-۶- فقدان اطلاعات بحرانی در لاگ ها

قالب استانداری برای لاگ‌ها وجود ندارد. لاگ‌های در دسترس، ازآنجاکه از لایه‌های متفاوت و ارائه‌دهندگان متفاوت به دست می‌آیند، دارای قالب‌های ناهمگون هستند. علاوه‌بر این موضوع، تمامی اطلاعات بحرانی مورد نیاز پژوهش‌های پزشکی قانونی در لاگ‌ها ثبت نمی‌شود. چه کسی؟ چه زمانی؟ کجا؟ و چرا [۳۰].

۴-۶-۷- زنجیره اعتماد

قابل تصدیق بودن تمامی فعالیت‌ها از نقطه مبدأ و شروع جمع‌آوری اطلاعات پزشکی قانونی تا نقطهٔ اتمام یعنی ارائه به یک مرجع قانونی، زنجیرهٔ اعتماد[1] نامیده می‌شود [۱]. این مسأله یکی از موضوع‌های اساسی در پژوهش‌های پزشکی قانونی متداول به‌حساب می‌آید. طبق زنجیرهٔ اعتماد، پژوهش‌گر باید چگونگی جمع‌آوری، تحلیل و حفاظت از مدارک را به‌گونه‌ای صریح و قابل‌قبول برای دادگاه شرح دهد. در جریان پزشکی قانونی سنتی، زنجیرهٔ اعتماد با

[1] Chain Custody

کنترل فیزیکی مدارکی چون رایانه و صفحه سخت آغاز می‌شود، اگرچه که این گام در پزشکی قانونی ابری غیرممکن است. در محیط ابری، پژوهش‌گر می‌تواند اطلاعات در دسترس را از هر ایستگاه کاری متصل به اینترنت به دست آورد. با توجه به قانون چندقلمروای، جریان‌ها و روی‌کردهای اختصاصی محیط ابری، حفاظت از زنجیرهٔ اعتماد به‌عنوان یک چالش مطرح می‌شود [۸].

پژوهش‌گران در [۲۶] مورد کاوی فرضی، وب‌سایت مبتنی بر محیط ابری را در نظر گرفته‌اند که در معرض خطر قرارگرفته است. آن‌ها به افرادی که ممکن است به مدارک دسترسی داشته باشند، اشاره می‌کنند و با توجه به این موضوع که ما برای جمع‌آوری مدارک به آن افراد وابسته‌ایم، زنجیرهٔ اعتماد در تمام مسیر پژوهش مشکوک خواهد بود. براساس نظر [۲۵] زنجیرهٔ اعتماد در پزشکی قانونی ابری با توجه به عدم اعتماد به هایپرویزور، به‌عنوان یک چالش مطرح می‌شود.

۴-۷- محدودیت ابزارهای کنونی

با توجه به ویژگی‌های توزیع‌شده و الاستیک‌بودن رایانش ابری، ابزارهای کنونی پزشک قانونی نمی‌توانند چالش‌های موجود در محیط ابری را برطرف کنند. برخی از پژوهش‌گران در نتایج پژوهش‌های خود محدودیت این ابزارها را خاطرنشان کرده‌اند [۳۱]. ابزارها و جریان‌های موجود برای محیط‌های مجازی به‌ویژه در سطح هایپرویزور، هنوز نیاز به توسعه دارند. در [۸] اشاره شده است که برای جمع‌آوری داده توسط مشتری و ارائه‌دهندهٔ خدمات ابری به ابزارهای خبرهٔ هوشمند پزشکی قانونی نیاز داریم.

۴-۸- بازسازی صحنهٔ جرم

در جریان پژوهش‌ها، گاهی پژوهش‌گر باید صحنهٔ جرم را بازسازی کند. این کار به پژوهش‌گران کمک می‌کند تا از چگونگی انجام حمله باخبر شوند؛ اگرچه در محیط‌های ابری، این مسأله مشکل‌ساز خواهد بود. بدین‌صورت که اگر مهاجم بعد از انجام فعالیت مخرب خود نمونه ماشین مجازی خود را خاموش کند، بازسازی صحنهٔ جرم برای پژوهش‌گران غیرممکن خواهد بود [۳۲].

۴-۹- عبور از مرز قانون

چندقلمروای و عبور از چارچوب قانون، چالش‌های پزشکی قانونی ابری را تشدید کرده‌اند. مراکز دادهٔ ارائه‌دهندگان خدمات ابری در سرتاسر جهان توزیع‌شده‌اند. قانون حفاظت از حریم شخصی یا قانون اشتراک اطلاعات در تمام نقاط دنیا به‌طور یکسان اجرا نمی‌شود و حتی گاهی در یک کشور نیز حالت‌های متفاوتی دارد؛ دستورالعمل‌های مربوط به قابل‌قبول‌بودن مدارک و یا دستورالعمل‌های حفاظت از زنجیرهٔ اعتماد می‌تواند در مناطق مختلف، متفاوت باشد. این مسأله زمانی اتفاق می‌افتد که مهاجم به خدمات محیط ابری یک قلمرو دسترسی دارد. با درنظرگرفتن داده‌ها او به داده‌های مقیم در قلمروهای متفاوت دسترسی دارد. تفاوت قوانین در این دو مکان می‌تواند در سرتاسر جریان پژوهش تأثیر داشته باشد. علاوه‌بر این برای موارد چندمستأجری، باید از حریم شخصی مستأجران هنگام جمع‌آوری مدارک از منابع به اشتراک گذاشته‌شده حفاظت شود؛ بنابراین باید این مسأله را در نظر بگیریم که حریم شخصی و حق امتیاز در کشورها و ایالت‌های مختلف، متفاوت است [۱۲].

۴-۱۰- ارائه

ارائه، گام نهایی پژوهش‌های پزشکی قانونی دیجیتالی است. بدین نحو که پژوهش‌گر یافته‌های خود را جمع‌آوری کرده و به دادگاه به‌عنوان مدرک ارائه می‌دهد. چالش‌هایی در این مرحله از پژوهش وجود دارد. اثبات مدارک موجود برای هیئت داوری در دادگاه در پزشکی قانونی دیجیتالی در مقایسه با ساختار پیچیده رایانش ابری تاحدودی ساده است.

اعضای هیئت‌منصفه به‌احتمال دارای دانش‌پایه‌ای در مورد رایانه‌های شخصی یا حداکثر در مورد ذخیره‌سازی محلی محرمانه هستند؛ امّا تکنسین‌های مراکز دادهٔ محیط ابری، هزار ماشین محلی را اجرا می‌کنند و هم‌زمان هزار کاربر به آن‌ها دسترسی دارند؛ فهم این مطالب برای اعضای هیئت‌منصفه مشکل خواهد بود [۳۲].

۴-۱۱- نگهداری داده‌های مورد اعتماد

سازمان‌های تجاری و پزشکی بزرگ به‌دلیل برخی از مسائل نمی‌توانند از محیط ابری استفاده کنند. نگهداری داده‌های قابل اعتماد یکی از مسائل ضروری است که فرآیند پزشکی قانونی دیجیتالی را پیچیده کرده است. پژوهش‌گران در [۳۳] مسألهٔ حفاظت از دادهٔ قابل اعتماد را این‌گونه توضیح داده‌اند: «دورهٔ نگهداری دادهٔ مورد اعتماد باید حفاظتی درازمدت را فراهم و هرگونه دخل و تصرف‌های سازمانی را ثبت کند تا از پاک‌شدن و اصلاح‌های ناخواسته در طی دوره نگهداری اجتناب شود؛ به‌علاوه باید از ایجاد دوبارهٔ موارد

پاک‌شده جلوگیری کند.» باوجوداین‌که هنوز مشکلاتی حل‌نشده در زمینهٔ اطمینان از امن‌ماندن داده‌ها در سطح ذخیره‌سازی وجود دارد، استفاده از رایانش ابری چالش‌های دیگری را به این مشکلات اضافه می‌کند [۳۵]. به برخی از موضوعات درخصوص حفاظت و تخریب موارد ضبط‌شده در رایانش ابری اشاره‌کرده‌اند.

برای مثال باید به این سؤال پاسخ مناسبی داده شود که چه کسی سیاست‌های حفاظت را در محیط ابری اجرا کند؟ استثناها چگونه بررسی می‌شوند؟ چگونه ارائه‌دهندگان خدمات ابری، این اطمینان را به کاربران می‌دهند که داده‌ها را بعد از حذف نگهداری نمی‌کنند؟ قانون‌های مختلفی در کشورهای مختلف وجود دارد که حفاظت از داده‌های قابل اعتماد را اجرا می‌کنند. فقط در امریکا حدود ده‌هزار قانون در سطح ایالت‌ها وجود دارد که سازمان‌ها را مجبور به نگهداری امن، از اسناد می‌کند [۳۵]. (جدول ۴) چالش‌های موجود در پزشکی قانونی ابری را با توجه به سه مدل خدمت نشان می‌دهد.

۵- راه‌حل‌های موجود

اگرچه چالش‌های بسیاری درزمینهٔ پژوهش‌های پزشکی قانونی محیط‌های ابری وجود دارد، با توجه به مزیت‌های استفاده از این محیط، پژوهش‌گران در راستای حل چالش‌های موجود راه‌حل‌های متفاوتی ارائه داده‌اند. در اکثر موارد تمرکز بر ایجاد شرایط مطلوب جهت جمع‌آوری داده از محیط ابر بوده است، به‌نحوی‌که در تمام مراحل «قابلیت اعتماد» حفظ شود. نکتهٔ مشترک تمام راه‌حل‌های پیشنهادی توجه به مسائل قانونی و حفظ محرمانگی کاربران محیط ابری است. در این بخش راه‌حل‌های موجود جهت حل چالش‌های ذکرشده را بررسی خواهیم کرد.

۵-۱- اعتماد

کمبود اعتماد مانع اصلی گسترش محیط ابری است. در [۳۶] پژوهش‌گران به نکات اساسی و چالش‌های دستیابی به اعتماد در محیط ابری اشاره‌کرده‌اند. آن‌ها با استفاده از کنترل‌های پیش‌گیرنده و ارائه چارچوب اعتماد ابری بر مبنای روی‌کردهای مبتنی بر سیاست بر لزوم پاسخ‌گویی در رایانش ابری جهت حفظ اعتماد تأکید کرده‌اند. آن‌ها همچنین سناریوی مربوط به پیاده‌سازی اعتماد را ارائه داده‌اند. این سناریوی اهمیت قابلیت پاسخ‌گویی و قابلیت بازرسی را بیان می‌کند.

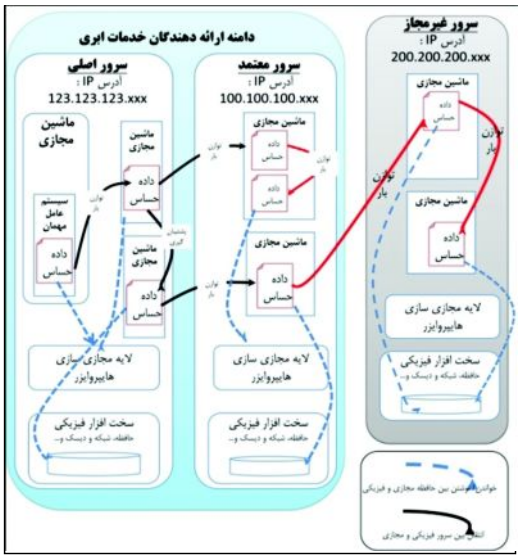
مشتری داده‌های حساس خود را در فایلی ذخیره می‌کند؛ فایل در ماشین مجازی خدمت‌دهنده‌ای که در آن عضو شده بود، بارگذاری می‌شود؛ بعد از فرآیند بارگذاری، از فایل، پشتیبان گرفته می‌شود تا در مقابل شکست‌ایمن شود. از طریق چند خدمت دهندهٔ فیزیکی و مجازی در دامنهٔ اعتماد ارائه‌دهندهٔ ابری، افزونگی‌ای ایجاد می‌شود تا توازن بار برای سیستم آماده شود. ضبط و جمع‌آوری مدارک دیجیتالی گام اولیه و مهم فرآیند پزشکی قانونی است. دو سناریوی ممکن وجود دارد: پژوهش‌گرین راه دور محیط ابری مدارک دیجیتالی را خودشان از منابع موجود جمع‌آوری می‌کنند و یا فراهم‌کنندگان خدمات ابری، مدارک را در اختیار پژوهش‌گرین قرار می‌دهند. هر سناریوی به درجه‌ای از اعتماد در جمع‌آوری داده نیاز دارد.

از زمان ایجاد فایل تا فرآیند پشتیبان‌گیری، تعداد زیادی انتقال داده در خدمت‌دهنده‌های مجازی و فیزیکی و چندین تراکنش خواندن/نوشتن حافظه برای حافظه فیزیکی و مجازی رخ می‌دهد (خط‌چین‌های‌آبی شکل). اگر همهٔ تراکنش‌ها و ایجاد فایل‌های تکراری جدید، همگی به‌درستی لاگ شده باشند و نظارت و حساب‌رسی شوند، آنگاه تاریخچه فایل لاگ قابل‌ردیابی خواهد بود؛ و درنهایت قابلیت پاسخ‌گویی و بازرسی ایجاد می‌شود. (شکل ۶) سناریویی رایانش ابری جهت بیان اهمیت قابلیت پاسخ‌گویی و بازرسی را نشان می‌دهد. علاوه‌براین، هر سناریوی از فن‌های پیاده‌سازی متفاوت برای بازیابی داده استفاده می‌کند. پژوهش‌گران در [۲۴] مدل اعتماد شش‌لایه‌ای را مطابق (جدول ۵) پیشنهاد کرده‌اند.

جدول شامل شش‌لایهٔ «زیرساخت به‌عنوان خدمت»، همراه با فن‌های جمع‌آوری هر لایه و نیز اعتماد موردنیاز برای هر لایه است. همان‌طور که در جدول مشخص‌شده است، هرچه به لایهٔ پایین‌تر نزدیک می‌شویم؛ به اعتماد کمتری نیاز داریم. برای مثال در لایهٔ سیستم‌عامل مهمان به اعتماد در لایه‌های سیستم‌عامل مهمان، هایپرویزور، سیستم‌عامل میزبان، سخت‌افزار و شبکه نیاز داریم. درحالی‌که در لایهٔ شبکه فقط به اعتماد در لایهٔ شبکه نیازمندیم. بازرس پرونده می‌تواند مدارک را در لایه‌های مختلف بررسی کند تا از سازگاری مدارک اطمینان یابد. پژوهش‌گران در این راستا در [۳۷] سه پیشنهاد استفاده از

«ماژول[1] بستر معتمد»[2]، «طرح مدیریت ابری» و «پزشکی قانونی به‌عنوان خدمت» را جهت جمع‌آوری داده‌های محیط ابری برای پژوهش پزشکی قانونی ارائه کرده‌اند. توسعه «ماژول بسترمعتمد» باعث به‌وجودآمدن اعتمادی قوی در سخت‌افزارهای رایانش ابری شده است. TPM صحت اجرای نمونهٔ ماشین مجازی، فایل حاوی لاگ مورد اعتماد و داده‌های پاک‌شده معتمد را برای مشتریان فراهم می‌کند.

برای حفاظت از صحت و محرمانگی داده‌ها، با استفاده از TPM می‌توانیم سازوکارهای احراز هویت، رمزنگاری سخت‌افزار، علامت‌گذاری، ذخیره‌سازی کلید امن و تصدیق امضا را به‌دست آوریم.



شکل ۶: سناریویی رایانش ابری جهت بیان اهمیت قابلیت پاسخ‌گویی و بازرسی [۳۶]

البته پژوهش‌گران تأکید کرده‌اند که TPM به‌طورکامل امن نیست و این امکان وجود دارد که فرآیند در حال اجرا بدون اینکه توسط TPM تشخیص داده شود، دچار تغییرات ناخواسته شود. علاوه‌براین در حال حاضر فراهم‌کنندگان خدمات ابری سخت‌افزارهای ناهمگنی دارند و فقط تعداد کمی از آن‌ها دارای TPM هستند. ازاین‌رو فراهم‌کنندگان خدمات ابری نمی‌توانند یک محیط سخت‌افزاری همگن را در آیندهٔ نزدیک تضمین کنند. مشتریان مدارک مجازی را با «طرح مدیریت» کنترل و مدیریت می‌کنند، درواقع کانالی خارج از باند که با زیرساخت محیط ابری رابطه دارد. «طرح مدیریت» چون توسط کاربر اداره می‌شود از جذابیت بیش‌تری برخوردار است. فراهم‌کنندهٔ خدمات، کاربر پایانی و مجری قانون می‌توانند برحسب نیاز فایل‌های حاوی لاگ، تصاویر گرفته‌شده از صفحه و بسته‌های ضبط‌شده را بارگیری کند.

جدول ۴: چالش‌های پزشکی قانونی ابری با توجه به سه مدل خدمت [۱]

چالش‌های موجود در پزشکی قانونی ابری	سه مدل خدمت		
	SaaS	PaaS	IaaS
عدم دسترسی فیزیکی	✓	✓	✓
وابستگی به CSPs	✓	✓	✓
داده‌های فرّار	×	×	✓
مشکل اعتماد	✓	✓	✓
پهنای باند وسیع	×	×	✓
چند مستأجری	×	✓	✓
عدم تمرکز لاگ ها	✓	✓	✓
فرّار بودن لاگ ها	×	×	✓
لاگ ها در لایه‌های مختلف	✓	✓	✓
دسترس‌پذیری لاگ	✓	✓	✓
وابستگی به CSPs برای به دست آوردن لاگ ها	✓	✓	✓
فقدان اطلاعات بحرانی در لاگ ها	✓	✓	✓
زنجیره اعتماد	✓	✓	✓
مشکل ابزارهای کنونی پزشکی قانونی ابری	✓	✓	✓
بازسازی صحنه جرم	×	✓	✓
عبور از مرز قانون	✓	✓	✓
ارائه	✓	✓	✓
مشکل مقبولیت	×	✓	✓

طبق روی‌کرد سوم، پشتیبانی فراهم‌کنندهٔ خدمات ابری از جمع‌آوری داده در فرآیند پزشکی قانونی، گزینه‌ای حیاتی است. درواقع با پیشنهاد ارائهٔ «پزشکی قانونی به‌عنوان خدمت» فراهم‌کنندهٔ خدمات ابری پس از کنترل زیرساخت، داده‌ها را جمع‌آوری و نگهداری می‌کند؛ پس از وقوع جرم، اطلاعات لازم را در اختیار پژوهش‌گر پزشکی قانونی قرار می‌دهد.

مشتریان محیط ابری با انتقال داده‌هایشان در بستر ابر، کنترل داده‌هایشان را نیز به ابر منتقل می‌کنند؛ لذا امنیت و محرمانگی اطلاعات مهم‌ترین مسأله است. کاربران

[1] module
[2] Trusted Platform Module(TPM)

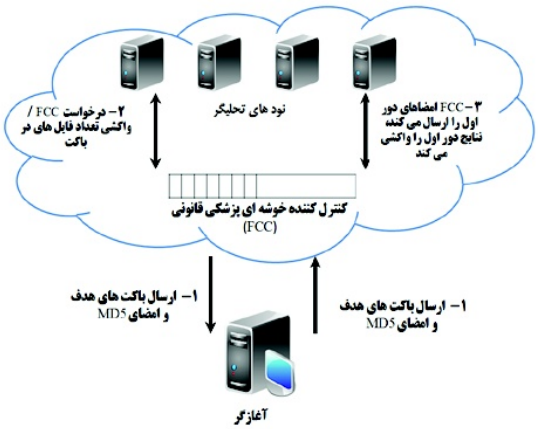
دانش کمی در مورد نحوهٔ ذخیره‌سازی و پردازش داده‌هایشان در محیط ابری دارند؛ پژوهش‌گران در [۳۸] پیشنهاد ارائهٔ شفاف اطلاعات توسط ارائه‌دهندگان خدمت را مطرح کرده‌اند. آن‌ها ارائهٔ «محرمانگی به‌عنوان خدمت» و «پزشکی قانونی به‌عنوان خدمت» را توسط فراهم‌کنندهٔ ابری پیشنهاد داده‌اند. اعتماد کاربران می‌تواند با ایجاد توانایی نظارت بر پردازش و نحوهٔ ذخیره‌سازی داده‌هایشان در محیط ابری حاصل شود. بااین‌وجود، کاربران می‌توانند از اطلاعات حساسشان مراقبت نمایند. این مورد برای کاربران و ارائه‌دهندگان مفید خواهد بود. کاربران کنترل بیشتری بر داده‌هایشان دارند و درصورتی‌که نقض امنیت و محرمانگی وجود داشته باشد، می‌توانند اعلام هشدار کنند. این مسأله می‌تواند نخستین گام برای کسب اعتماد در رایانش ابری باشد. در [۳۹] ارائهٔ مدارک به‌صورت تعاملی و روی‌کرد بصری جهت چیره‌شدن به موضوع اعتماد پیشنهادشده است.

جدول ۵: لایه‌های پیشنهادی و اعتماد موردنیاز در هر لایه [۲۴]

لایه	لایه ابر	روش اکتسا	اعتماد موردنیاز
۶	داده برنامه کاربردی مهمان	وابسته به داده	سیستم‌عامل مهمان/ هایپرویزور/سیستم‌عامل میزبان/ سخت‌افزار/ شبکه
۵	سیستم‌عامل مهمان	نرم‌افزارهای پزشکی قانونی راه دور	سیستم‌عامل مهمان/ هایپرویزور/ سیستم‌عامل میزبان/سخت‌افزار/ شبکه
۴	مجازی‌سازی	درون‌نگری	هایپرویزور/ سیستم‌عامل میزبان/سخت‌افزار/ شبکه
۳	سیستم‌عامل میزبان	دسترسی دیسک مجازی	سیستم‌عامل میزبان/سخت‌افزار/ شبکه
۲	سخت‌افزار فیزیکی	دسترسی دیسک فیزیکی	سخت‌افزار/ شبکه
۱	شبکه	گرفتن بسته	شبکه

۵-۲- حفظ صحت

حفظ صحت مدارک دیجیتالی گام سختی در مراحل پژوهش پزشکی قانونی است. بدون حفظ صحت، اعتبار مدارک زیر سؤال خواهد رفت و هیئت‌منصفه می‌تواند این نوع مدارک را رد کند. تولید امضای دیجیتال از مدارک جمع‌آوری‌شده و سپس تأیید اعتبار آن یکی از راه‌های اطمینان از صحت مدارک است. با توجه به این‌که داده‌ها در چندین سرویس‌دهنده توزیع‌شده‌اند، این راه‌حل کار ساده‌ای نیست. البته پژوهش‌گران پزشکی قانونی سازوکارهایی را جهت تولید و تأیید امضای دیجیتال در این شرایط پیشنهاد داده‌اند. در [۴۰] چارچوب تشخیص امضای توزیع‌شده جهت تسهیل پژوهش‌های پزشکی قانونی در محیط‌های ابری پیشنهاد شده است. روی‌کردهای سنتی تشخیص امضا، جواب‌گوی پژوهش‌های پزشکی قانونی و ماهیت توزیع‌شدهٔ رایانش ابری نیستند. مدل کنونی ذخیرهٔ فایل شامل دو مؤلفهٔ سرویس‌دهندهٔ اَبَرداده[1] و دستگاه‌های ذخیره‌سازی اشیا[2] است. مقدار چکیدهٔ هر فایل مانند یک برچسب الکترونیکی در MSD ذخیره می‌شود و صحت آن بعد از هر بارگذاری و بارگیری بررسی می‌شود. در چارچوب پیشنهادشده، ابتدا فهرست باکت‌های هدف همراه با چکیده MD5 به کنترل‌کنندهٔ خوشه‌ای پزشکی قانونی[3] فرستاده می‌شود؛ سپس FCC برای به‌دست‌آوردن تعداد فایل‌های باکت هدف، درخواستی را به نودهای تحلیل‌گر ارسال می‌کند. به‌محض دریافت فایل امضای دور نخست از FCC هر نود تحلیل‌گر برچسب باکت‌ها را بازیابی می‌کند. امضاهای دور نخست فایل با امضای تولیدشده از برچسب توسط نود تحلیل‌گر مقایسه می‌شود. بعد از بازخوردگرفتن از همهٔ نودها، FCC نودهای تحلیل‌گر را متوقف می‌کند. این چارچوب پیشنهادی از دو راه استفاده از Amazon s3 و شبیه‌سازی در بستر ابر مورد آزمایش قرار گرفت. شکل ۷ مراحل تحلیل توزیع‌شده را نمایش می‌دهد.

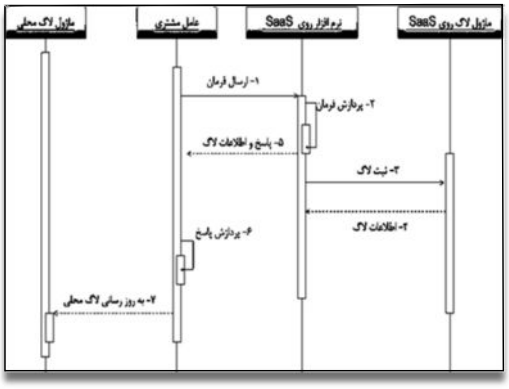


شکل ۷: مراحل تحلیل توزیع شده [۴۰]

[1] Meta data server (MDS)
[2] Object Storage Devices (OSD)
[3] Forensic Cluster Controller(FCC)

۵-۳- ثبت وقایع

اطلاعات لاگ در جریان پژوهش‌های پزشکی قانونی امری حیاتی است. تعداد زیادی از پژوهش‌گران در مورد لاگ در محیط‌های ابری پژوهش کرده‌اند. در [۳۰] راه‌حل مدیریت لاگ پیشنهادشده‌است که می‌تواند چندین چالش لاگ را حل کند. در نخستین مرحلهٔ راه‌حل مطرح‌شده، باید قادر به جمع‌آوری لاگ در همه بخش‌های زیرساخت‌ها باشیم. گام بعدی مربوط به برقراری هم‌زمانی، قابلیت اطمینان، کارایی پهنای باند و لایهٔ انتقال رمزنگاری‌شده برای انتقال لاگ از مبدأ به یک جمع‌آوری‌کنندهٔ لاگ مرکزی است؛ و گام آخر نیز به اطمینان از وجود اطلاعات مطلوب در لاگ‌ها، مربوط می‌شود. حداقل مواردی چون مُهر زمان، نوع برنامه‌های کاربردی، نام کاربر، شناسه نشست، شدت خطا و دلیل را باید به‌عنوان لاگ ثبت کنیم. با ذخیرهٔ این موارد می‌توانیم به سؤالات چه چیزی، چه زمانی، چه کسی و چرا پاسخ دهیم. درحالی‌که در این روی‌کرد مزیت‌های متعددی وجود دارد، امّا این کار هیچ روشی دربارهٔ کاربرد لاگ شبکه، آبَرداده، پردازنده و بسیاری از مدارک مهم دیگر که برای پژوهش‌های پزشکی قانونی مهم هستند، ارائه نمی‌دهد. جهت تسهیل ایجاد لاگ در محیط ابری پژوهش‌گران در [۲] استفاده از ماژول ایجاد لاگ، جهت جمع‌آوری اطلاعات در دو مدل «نرم‌افزار به‌عنوان خدمت» و «بستر به‌عنوان خدمت» را پیشنهاد داده‌اند. آن‌ها با درنظرگرفتن شرایط محیط ابری در این دو مدل فراهم‌کنندهٔ خدمات ابری را ملزم به ارائهٔ لاگ و اطلاعات درخواستی از طرف کاربران می‌دانند. (شکل ۸) روند ارائهٔ لاگ در مدل «نرم‌افزار به‌عنوان خدمت» را نشان می‌دهد.



شکل ۸: روند ارائه لاگ در «نرم‌افزار به‌عنوان خدمت»[۲]

در [۴۱] ایجاد لاگ از لاگ‌های امن و سیستم‌عامل پیشنهادشده است. آن‌ها به‌منظور انجام پژوهش‌های پزشکی قانونی دیجیتالی در محیط ابری، محیط رایانش ابری را با اکالیپتوس پیکربندی کردند. با استفاده از Snort، Syslog و تحلیلگر لاگ آن‌ها قادر به نظارت رفتار اکالیپتوس و ورودی‌ها خروجی‌های لاگ و تعاملات مؤلفه‌های اکالیپتوس شدند.

جهت آزمایش این روی‌کرد، آن‌ها حمله DDos را در دو ماشین مجازی پ و لاگ پهنای باند و لاگ پردازش‌گر مورداستفاده را برای تشخیص حمله DDos تحلیل کردند. با توجه به لاگ /var/eucalyptus/jetty-request-05-09-xx در ماشین کنترل‌گر ابری، امکان شناسایی آی پی ماشین حمله، نوع بروز و حجم درخواست‌شده و تعداد ماشین‌های مجازی که توسط کاربر کنترل می‌شود و الگوی ارتباطی وجود دارد. این آزمایش نشان داد که اگر ارائه‌دهندهٔ خدمت ابری سازوکار لاگ بهتری را فراهم کند، روند پزشکی قانونی ابری راحت‌تر خواهد شد. جهت ایجاد لاگ با حفظ ویژگی محرمانگی کاربران، صحت لاگ و عدم انکار، پژوهش‌گران در [۴۲] طرح «لاگ امن به‌عنوان خدمت[1]» را پیشنهاد داده‌اند. SecLaaS ابتدا اطلاعات لاگ را از منابع مختلف لاگ استخراج می‌کند. در این مورد از لاگ تهیه‌شده در لایهٔ شبکه استفاده کرده است. لاگ‌های جمع‌آوری‌شده توسط ماژول‌های ارائه‌دهندهٔ خدمت ابری را LE[2] می‌نامد. LE شامل موارد زیر است.

$$LE =< FromIP, ToIP, Port, T_l, UserID > \quad (۱)$$

برای اطمینان از حفظ محرمانگی لاگ کاربران باید برخی از فیلدهای LE را با کلید عمومی آژانس‌های امنیتی (P_{ka}) رمز کنند. برای انجام جستجو در لاگ توسط Csp، بعضی از فیلدها رمزگذاری نمی‌شوند.

$$ELE =< E_{pka}(ToIP, Port, UserID), FromIP, T_l > \quad (۲)$$

برای حفظ ترتیب درست لاگ‌ها زنجیره‌ای از لاگ LC[3] ایجاد کرده است. زنجیره از مقدار درهم‌ساز لاگ‌های جمع‌آوری‌شده توسط ماژول‌های ارائه‌دهندهٔ خدمت ابری

[1] Secure Log As a Service(SecLaaS)
[2] Log Entry
[3] Log Chain

به‌صورت رمزنگاری‌شده (ELE) و زنجیرهٔ قبلی به‌صورت زیر تشکیل می‌شود.

$$LC =< H(ELE, LC_{pre}) \quad (۳)$$

مقادیر ELE و LC درون پایگاه داده پایدار قرار می‌گیرد که DBLE نامیده می‌شود.

$$DBLE =< ELE, LC > \quad (۴)$$

برهان ایجادشده از DBLE را به انباره یک‌طرفه وارد می‌کنند که با نماد AE[1] نشان داده می‌شود. در پایان هرروز ارائه‌دهنده خدمات ابری مقدار AE_D را از داخل انباره بازیابی و به‌صورت PPL[2] منتشر می‌کند.

$$PPL =< H(AE_D), S_{pkc}(AED) > \quad (۵)$$

مقدار AE_D جهت حفظ صحت درهم سازی می‌شود تا با مقدار AE_D های موجود در انباره طی سازوکار تصدیق مقایسه شود. AE_D با کلید خصوصی ارائه‌دهندهٔ خدمات ابری، امضا می‌شود تا مانع از انکار PPL توسط ارائه‌دهنده شود.

برای به‌دست‌آوردن لاگ‌های ضروری در هر سه مدل خدمت پژوهش‌گران در [۲۵] پیشنهاد کردند که ارائه‌دهندهٔ خدمات ابری می‌تواند لاگ شبکه، پردازش و دسترسی را تنها با خواندن API برای مشتریان ارائه دهند. با استفاده از APIها مشتری می‌تواند اطلاعات ارزشمندی را برای پژوهش‌گران فراهم کند. در «بستر به‌عنوان خدمت» مشتریان بر برنامه‌های کاربردی‌شان کنترل کامل دارند و می‌توانند انواع مختلفی از اطلاعات دسترسی را در یک روی‌کرد قابل پیکربندی ثبت کنند؛ ازاین‌رو در «بستر به‌عنوان خدمت» یک خدمت‌دهندهٔ مرکزی لاگ پیشنهادشده است که مشتریان می‌توانند اطلاعات لاگ را ذخیره کنند. به‌منظور حفاظت لاگ از شنودها و عملیات تغییر احتمالی، مشتریان می‌توانند داده‌های لاگ را قبل از فرستادن به لاگ مرکزی رمزنگاری و علامت‌گذاری کنند.

۵-۴- موارد قانونی

موضوع قانون، یک مانع بزرگ در پزشکی قانونی ابری به شمار می‌آید. عبور از چارچوب قانون‌گذاری، اغلب مانعی برای جریان‌های پزشکی قانونی است. در حال حاضر شکاف بزرگی در توافق‌نامه‌های سطح سرویس وجود دارد؛ که پاسخ‌گوبودن ارائه‌دهندگان خدمات ابری در زمان روی‌داد خصمانه و نقش آن‌ها را در پژوهش‌های پزشکی قانونی مشخص نمی‌کند. پژوهش‌گران بر دقت و توانایی توافق‌نامه‌های سطح سرویس بین ارائه‌دهندگان خدمات و مشتری بسیار تأکید کرده‌اند. برای حل موضوع شفافیت، ارائه‌دهندگان باید یک رابطهٔ اعتماد درازمدت را با مشتریان ایجاد کند. یک توافق‌نامهٔ سطح سرویس قوی باید چگونگی برخورد فراهم‌کنندگان سرویس را با جرایم رایانه‌ای توضیح دهد. برای مثال جزییات پاسخ سؤال «مدارک به وجود آمده از این فعالیت‌ها چگونه و تا چه حدی به جریان پژوهش‌های پزشکی قانونی کمک می‌کنند؟» باید در توافق‌نامه به‌طورکامل مشخص باشد. در این زمینه سؤال دیگری که مطرح می‌شود این است که «چه‌طور می‌شود از کیفیت و دقت لازم توافق‌نامه‌ها مطمئن شد؟» برای اطمینان از کیفیت توافق‌نامه‌ها می‌توان از یک شخص سوم مورد اعتماد کمک گرفت.

برای چیره‌شدن بر مشکل عبور از چارچوب وضع قانون [۴۳] یک واحد بین‌المللی برای معرفی قانون بین‌المللی در پژوهش‌های پزشکی قانونی ابری پیشنهاد کرده است. همچنین پژوهش‌گران در [۲۶] و [۲۵] در مورد چگونگی تنظیم توافق‌نامه و شرایط آن پژوهش کرده‌اند. در راستای بررسی موارد قانونی در مناطق مختلف، پژوهش‌گران در [۴۴] مشکلات قانونی موجود در پژوهش‌های پزشکی قانونی ابری را برجسته کرده‌اند. آن‌ها با بررسی قوانین موجود در ایالات‌متحده، چگونگی دست‌یابی به مدارک الکترونیکی را با توجه به موارد قانونی در جریان پژوهش‌های توضیح داده‌اند.

۵-۵- درون‌نگری ماشین مجازی

درون‌نگری ماشین مجازی درواقع فرآیند نظارت خارجی حالت زمان اجرای ماشین مجازی است که توسط ناظر ماشین مجازی و یا توسط ماشین‌های مجازی مورد بررسی قرار می‌گیرد. از طریق این فرآیند می‌توانیم تحلیل پزشکی قانونی زنده سیستم را اجرا کنیم؛ درحالی‌که هدف سیستم را بدون تغییر نگه می‌داریم. این موضوع نخستین‌بار در سال ۲۰۰۳ جهت تشخیص نفوذ در [۴۵] ارائه شد؛ و در سال ۲۰۰۹ در [۴۶] از طریق هایپرویزور کد ضدویروس با

[1] Accumulator Entry
[2] Proof Of Past Log

استفاده از VMsafe به ماشین مجازی تزریق شد. در همان سال، پژوهش‌گران از درون‌نگری برای نخستین‌بار در پژوهش‌های پزشکی قانونی زنده استفاده کردند؛ و جهت نظارت، مدیریت و امنیت رایانش ابریِ VSphere پیشنهاد شد. این نخستین‌باری است که سعی شد از طریق هایپرویزور ابزار پزشکی قانونی‌ای مانند EnCase به ماشین مجازی تزریق شود؛ از این بابت نوبودن این طرح برای پزشکی قانونی بسیار موردستایش است. البته در سال ۲۰۰۹، گارتنر در [۴۷] مروری بر ابزارهای پزشکی قانونی راه دور، داشته است؛ امّا به‌نظر، ایدهٔ آقای دایکسترا بسیار کاربردی‌تر است. در [۳۰] نشان دادند که اگر یک نمونهٔ ماشین مجازی با نصب برخی روت‌کیت‌ها برای پنهان‌کردن رویدادهای خصمانه به خطر بیفتد، این امکان وجود دارد که این رویدادهای خصمانه با درون‌نگری ماشین مجازی شناسایی شوند. آن‌ها از کتابخانهٔ متن‌باز ماشین مجازی استفاده کردند تا آزمایش خود را اجرا کنند.

۵-۶- ایجاد هم‌زمانی

به‌منظور فراهم‌کردن تقاضاهای محاسباتی و ذخیرهٔ سرویس، فراهم‌کنندگان خدمات ابری امکان ذخیره‌سازی پایدار را برای نمونه ماشین مجازی ایجاد نمی‌کنند. اگر ماشین مجازی را خاموش یا دو بار بارگیری کنیم، تمام داده‌های مستقر در ماشین مجازی را از دست خواهیم داد. برای حل این مشکل پژوهش‌گران در [۲۵] بر امکان همگام‌سازی مداوم داده‌های فرّار با یک دستگاه ذخیره‌سازی پایدار تأکید کرده‌اند. دو روی‌کرد برای همگام‌سازی مداوم وجود دارد: فراهم‌کنندگان خدمات ابری می‌توانند یک همگام‌سازی مداوم API را برای مشتریان فراهم کنند؛ یا با استفاده از API مشتریان می‌توانند داده‌های همگام‌شده را در هر دستگاه ذخیره‌سازی نگهداری کنند. پیاده‌سازی این سازوکار می‌تواند به جمع‌آوری مدارک از ماشین مجازی آسیب‌دیده حتی درصورتی‌که دشمن بعد از فعالیت خصمانه ماشین مجازی را خاموش کند کمک کند؛ امّا باید توجه داشت که اگر دشمن مالک ماشین مجازی باشد، روی‌کرد بالا جواب‌گوی نیاز ما نخواهد بود؛ بدیهی است که او علاقه‌ای به همگام‌سازی فعالیت‌های ماشین مجازی خود ندارد. برای حل این موضوع، فراهم‌کنندگان خدمات ابری می‌توانند سازوکار همگام‌سازی را با تمام ماشین‌های مجازی و داده‌ها را در زیرساخت خود نگهداری کنند.

۵-۷- قرنطینه‌سازی نمونهٔ ابری

این گزینه راه‌حل مسألهٔ چندمستأجری در محیط‌های ابری است. یک نمونهٔ ابری باید در صورت بروز حادثه در آن قرنطینه شود. ایزوله‌بودن بدین‌جهت ضروری است که به محافظت از مدارک از آلوده‌شدن کمک می‌کند. البته اگر چندین نمونه در یک گره قرار داشته باشند، این مورد خود به‌عنوان چالشی جدید مطرح می‌شود. در [۴۸] برخی از فن‌های ممکن در قرنطینه‌سازی نمونه ابری ارائه‌شده است. قرنطینه‌سازی به حفاظت از مدارک احتمالی در مقابل آلودگی و عدم تداوم کمک می‌کند. اگر هرگونه آلودگی اتفاق بیفتد یا پیوستگی آن از بین رود، مقبولیت تمامی مدارک جمع‌آوری‌شده ناشی از پژوهش‌های از بین می‌رود. به‌منظور حفاظت از مقبولیت مدارک، صحنهٔ جرم، به بخش‌های مختلفی تقسیم می‌شود تا عمل قرنطینه‌سازی راحت‌تر انجام شود. هرکدام از این بخش‌ها تنها توسط کارکنان مجاز که از روش مجاز استفاده می‌کنند، ثبت می‌شود. پژوهش‌گران در این راستا فن‌های جابه‌جایی نمونه، خوشهٔ سرور، جابه‌جایی نشانی، دگرگزینی و سند باکسینگ را معرفی کرده‌اند.

۶- زمینه‌های کاری آینده

همان‌طور که در بخش ۵ و ۶ نیز ذکر شد. راه‌حل‌های بیان‌شده برای چالش‌های امنیتی و پزشکی قانونی محیط ابری با ماهیت مجازی‌سازی و الاستیک‌بودن رایانش ابری منافات دارد؛ و تمام راه‌حل‌های پیشنهادی تنها به یک یا درنهایت چند مورد از چالش‌های مطرح‌شده، فائق آمده‌اند و در تسکین چالش‌های دیگر ناکارآمد به نظر می‌آیند. تصور ما این است که ارائهٔ راه‌حلی جامع که بتواند بر همه چالش‌ها فائق آید، به یقین در کارایی محیط ابری تأثیر منفی خواهد گذاشت. ساختار محیط‌های ابری در مقابله با چالش‌های امنیتی ناتوان است؛ و فراهم‌کنندگان خدمات ابری نیز برای حفظ کارایی، مایل نیستند تا تمهیدات امنیتی بیشتری لحاظ کنند و همواره یکی از مشکلات پژوهش‌گران پزشکی قانونی عدم همکاری فراهم‌کنندگان خدمات ابری در جمع‌آوری داده‌هاست؛ حتی درصورت وجود همکاری، به‌علت اتکای پژوهش‌گران به فراهم‌کنندگان، مشکلاتی چون تبانی و عدم حفظ محرمانگی و صحت داده‌ها و حفظ‌نشدن زنجیرهٔ اعتماد وجود دارد. معماری SDN[1] و پروتکل OpenFlow

[1] Software- Defined Networking

باعث می‌شود، سطوح داده و کنترل از یکدیگر جدا شده و شبکه هوشمندتر و کنترل‌پذیرتر و زیرساخت اصلی شبکه از برنامه‌های کاربردی جدا شود [۴۹]. فراهم‌کنندگان خدمات ابری و پژوهش‌گران پزشکی قانونی قادر به برنامه‌نویسی، خودکارسازی و کنترل بیشتر مراکز داده خواهند بود؛ و همین امر می‌تواند وابستگی به فراهم‌کنندگان خدمات ابری جهت جمع‌آوری مدارک پزشکی قانونی را به حداقل برساند. با جداسازی کنترل از داده در بستر شبکه می‌توان گام بزرگی در امنیت محیط‌های ابری برداشت.

با بازنگری رایانش ابری می‌توان معماری مراکز دادهٔ آن را با استفاده از شبکهٔ نرم‌افزار (SDN) به‌گونه‌ای تغییر داد که بستر رایانش ابری منطبق با نیازهای امنیت و پزشکی قانونی گردد و بدین‌صورت چالش‌های مربوط به ماهیت محیط ابری برطرف شود. به نظر می‌رسد محیط ابری هوشمند، در آیندهٔ نزدیک راه‌حلی جامع در این حوزه خواهد بود.

۷- جمع‌بندی و نتیجه‌گیری

افزایش استفاده از رایانش ابری و محبوبیت آن در کسب‌وکارهای بزرگ و کوچک و از طرفی افزایش جرایم سایبری در محیط ابری، ما را بر این داشت تا چالش‌هایی را که پژوهش‌گران در این حوزه آورده‌اند و راه‌حل‌هایی که برای تسکین این چالش‌ها آورده شده است، با نگاهی عمیق‌تر مورد بررسی قرار دهیم. در این مقاله، چالش‌های موجود و راه‌حل‌های پزشکی قانونی ابری را برای پاسخ به سؤال «پزشکی قانونی ابری در کجا قرارداد؟» به‌طور خلاصه بیان کردیم.

تلاش پژوهشی جاری بیان‌گر این است که پزشکی قانونی ابری هنوز در دوران طفولیت خود به سر می‌برد. مشکلات زیادی وجود دارد که در بخش ۵ ذکر شد. با تحلیل چالش‌ها و راه‌حل‌های موجود، به این نتیجه رسیدیم که ارائه‌دهندگان خدمات ابری باید برای حل مشکلات موجود اقدام کنند. راه‌حل‌های دیگر نیز به ارائه‌دهندگان و سیاست‌های سازنده وابسته است. برای جمع‌آوری دادهٔ پزشکی قانونی، ارائه‌دهندگان خدمات ابری توانسته‌اند ضمانت پاسخ‌گویی‌شان را با استفاده از API یا «طرح مدیریت» به مدرک جمع‌آوری‌شده منتقل کنند؛ امّا بازهم به‌علت عدم دسترسی فیزیکی، هنوز هم برای جمع‌آوری داده پزشکی قانونی به ارائه‌دهندگان وابسته‌ایم. برای مثال، جمع‌آوری لاگ‌های ثبت‌شده، شناسایی فایل‌های پاک‌شده از صفحهٔ سخت و مسائلی از این قبیل، اگرچه وابستگی به ارائه‌دهندگان کم‌تر شده است، ولی همچنان این مشکل، حل نشده باقی مانده است. دیگر مسألهٔ بحرانی محدودیت پهنای باند است. اگر انبارهٔ محیط ابری خیلی بزرگ باشد؛ آن‌گاه پهنای باند برای موردی که زمان در آن بحرانی است، چالش بزرگی خواهد بود، این مسأله تاکنون حل‌نشده است. پژوهش‌گران یک‌پارچگی جهانی قوانین را برای تسکین مسألهٔ تداخل چارچوب قانون پیشنهاد داده‌اند؛ امّا هیچ دستورالعملی برای عملی‌کردن این موارد وجود ندارد. علاوه‌براین، هیچ راه‌حلی برای مسألهٔ بازسازی صحنه جرم یا ارائه وجود ندارد. اصلاح ابزارهای پزشکی قانونی موجود یا ایجاد ابزارهای جدید برای کنارآمدن با محیط‌های ابری مشکل بزرگ دیگری است که تاکنون حل نشده است. وضع مسائل قانونی همچنین از اجرای بدون اِشکال فرآیند پژوهش‌های پزشکی قانونی جلوگیری می‌کند. در بحث راه‌حل‌ها معیارهایی برای لاگ مناسب، جمع‌آوری داده، موضوع اعتماد و موارد قانونی، حفظ صحت، قرنطینه‌سازی و درون‌نگری ماشین مجازی در پزشکی قانونی را بیان کردیم؛ امّا کماکان چالش‌هایی در این زمینه باقی مانده است که در (جدول ۶) آورده شده است.

به‌یقین به یک کار اشتراکی از سازمان‌های خصوصی و عمومی جهت چیره‌شدن بر این مشکلات نیاز داریم؛ و این امر نیازمند همکاری تمام دستگاه‌هاست.

جدول ۶: مشکلات حل‌نشده پزشکی قانونی ابری

مشکلات حل نشده
چیره شدن بر وابستگی به CSP
جمع آوری حجم زیاد داده از راه دور برای موارد بحرانی زمانی
وضع مقررات و پیاده‌سازی وحدت جهانی برای چیره شدن از مرز چارچوب قانونی
بازسازی صحنهٔ جرم در محیط ابری
سازگارکردن ابزارهای پزشکی قانونی موجود برای الگوها ابری
شناسایی محل و قلمرو دقیق داده‌ها
تحلیل خط-زمانی پزشکی قانونی لاگ‌ها
بررسی لاگ، تصحیح و نظارت سیاست‌گذاری لاگ

۸- مراجع

[1] S. Zawoad and R. Hasan, "Cloud forensics: A meta-study of challenges, approaches, and open problems", *CoRR*, vol. abs/1302.6312, 2013.

[2] T. Sang, "A log based approach to make digital forensics easier on cloud computing," in *Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on*, Jan 2013, pp. 91–94.

[3] "Gartner says cloud-based security services market to reach $2.1 billion in 2013."

[4] F. Gens. (2008, Oct.) IT Cloud Services Forecast,2008, 2012: A Key Driver of New Growth. http://blogs.idc.com/ie/?p=224.

[5] Cisco Global Cloud Index : Forecast and Methodology, 2013 – 2018," 2014.

[6] L. Columbus, "Computerworld's 2015 Forecast Predicts Security, Cloud Computing And Analytics Will Lead IT Spending," 2014.<http://www.forbes.com/>

[7] D. Peterson, "Evolution of the cloud: The future of cloud computing in government," GovWin, Tech. Rep., 2009.

[8] G. Grispos, T. Storer, and W. B. Glisson, "Calm before the storm: The challenges of cloud computing in digital forensics", *International Journal of Digital Crime and Forensics*, Vol. 4, 2012.

[9] S. Almulla, Y. Iraqi, and A. Jones, "Cloud forensics: A research perspective," in *Innovations in Information Technology (IIT), 2013 9th International Conference on*, March 2013, pp. 66–71.

[10] A. W. Services. Amazon Security Bulletin. http://aws.amazon.com/security, 2012.

[11] IT Cloud Services User Survey, Part 2.www. clavister.com/documents/resources/white-papers clavister-whp-security-in-the-cloud-gb.pdf.

[12] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: An overview," 2011. [Online]. Available: http://cloudforensicsresearch.org/-publication/Cloud_Forensics_An _Overview_7th_IFIP.pdf

[13] K. Ruan, J. Carthy, T. Kechadi, and I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results", *Digital Investigation*, vol. 10, no. 1, pp. 34 – 43, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/-pii/S1742287613000121

[14] G.Palmer, "A road map for digital forensic research," DFRWS, First digital forensic research workshop, Tech. Rep., 2001.

[15] M. M. Pollitt, "Computer forensics: An approach to evidence in cyberspace", *Proceeding of the National Information Systems Security Conference*, vol. 2, pp. 487–491, 1995.

[16] M. M. Pollit, "An ad hoc review of digital forensic models", *Proceeding of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2007.

[17] D. S. R. X. Wang and S. F. Wu, "Inter-packet delay based correlation for tracing encrypted connections through stepping stones", *Proceedings of the 7th European Symposium on Research in Computer Security*, Oct 2002.

[18] E. S. B. Carrier, "Getting physical with the digital investigation process", *International Journal of Digital Evidence*, pp. 1–20, 2003.

[19] F. T. V. Baryamureeba, "The enhanced digital investigation process model", *Proceedings of the fourth digital forensic research workshop*.

[20] G. G. M. Reith, C. Carr, "An examination of digital forensic models", *International Journal of Digital Evidence*, vol. 1, pp. 1–12, 2002.

[21] G. P. E. Casey, "The investigative process", *Digital evidence and computer crime, Elsevier Academic Press*, 2004.

[22] P. HC. Lee, TM and M. Miller, "Henry leeâ€™s crime scene handbook", *San Diego: Academic Press*, 2001.

[23] R. N. E. Pilli, R.C. Joshi, "Network forensic frameworks: Survey and research challenges", *Digital Investigation the International Journal of Digital Forensics & Incident Response, 2010, Pages:* 14–27.

[24] J. Dykstra and A. T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques", *Digital Investigation*, 2012, Vol. 9, Pages: 90–98.

[25] D. Birk and C. Wegener, "Technical issues of forensic investigations in cloud computing environments," in *Proceedings of the 6th International Workshop on Systematic Approaches to Digital Forensic Engineering SADFE,* Oakland, CA, USA: IEEE, 2011.

[26] J. Dykstra and A. T. Sherman, "Understanding issues in cloud forensics: Two hypothetical case studies", *Journal of Network Forensics*, vol. 3, no. 1, Autumn 2011, Pages: 19–31.

[27] H. Guo, B. Jin, and T. Shang, "Forensic investigations in cloud environments," in *Computer Science and Information Processing (CSIP), 2012 International Conference on*, Aug 2012, pp. 248–251.

[28] P. D. M. Slusky, Ludwig; Partow-Navid, "Cloud computing and computer forensics for business applications", *Journal of Technology Research*, 2012.

[29] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: Exploring information leakage in third-party

compute clouds," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 199–212.
[30] R. Marty, "Cloud application logging for forensics," in *Proceedings of the 2011 ACM Symposium on Applied Computing*, ser. SAC '11. New York, NY, USA: ACM, 2011, pp. 178–184. [Online]. Available: http://-doi.acm.org/10.1145/1982185.1982226
[31] N. Thethi and A. Keane, "Digital forensics investigations in the cloud," in *Advance Computing Conference (IACC), 2014 IEEE International*, Feb 2014, pp. 1475–1480.
[32] C. W. D. Reilly and T. Berry, "Cloud computing: Pros and cons for computer forensic investigations", *International Journal Multimedia and Image Processing, 2011, Vol.1, Pages: 26-34*
[33] S. Zawoad and R. Hasan, "I have the proof: Providing proofs of past data possession in cloud forensics," in *Cyber Security (CyberSecurity), 2012 International Conference on*, Dec 2012, pp. 75–82.
[34] K. PopovicÃŒï¿½ and Z. Hocenski, "Cloud computing security issues and challenges," in *MIPRO, 2010 Proceedings of the 33rd International Convention*, May 2010, pp. 344–349.
[35] C. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati, "Privacy-enhanced location-based access control," in *The Handbook of Database Security: Applications and Trends*, M. Gertz and S. Jajodia, Eds. Springer-Verlag, 2007, pp. 531–552.
[36] R. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "Trustcloud: A framework for accountability and trust in cloud computing," in *Services (SERVICES), 2011 IEEE World Congress on*, July 2011, pp. 584–588.
[37] J. Dykstra, "Digital forensics for infrastructure-as-a-service cloud computing," Ph.D. dissertation, UMBC Univercity, May 2013.
[38] S. Zargari and A. Smith, "Policing as a service in the cloud," in *Emerging Intelligent Data and Web Technologies (EIDWT), 2013 Fourth International Conference on*, Sept 2013, pp. 589–596.
[39] S. D. Wolthusen, "Overcast: Forensic discovery in cloud environments," in *Proceedings of the 2009 Fifth International Conference on IT Security Incident Management and IT Forensics (IMF '09.*(Washington, DC, USA: IEEE Computer Society, 2009, pp. 3–9.
[40] *Forensic Analysis of Distributed Data in a Service Oriented Computing Platform*.
[41] Z. Zafarullah, F. Anwar, and Z. Anwar. Digital forensics for eucalyptus. In Frontiers of Information Technology (FIT), 2011, pages 110–116.
[42] S. Zawoad, A. K. Dutta, and R. Hasan, "Seclaas: secure logging-as-a-service for cloud forensics," in ASIACCS, 2013, pp. 219–230.
[43] S. Biggs and S. Vidalis, "Cloud computing: The impact on digital forensic investigations," in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, Nov 2009, pp. 1–6.
[44] J. Dykstra, "Seizing electronic evidence from cloud computing environments," in *Cybercrime and Cloud Forensics: Applications for Investigation Processes*, K. Ruan, Ed. IGI Global, 2013.
[45] S. L. GARFINKEL, "Digital forensics research: The next 10 years", *Proceedings of the Tenth Annual DFRWS Conference*, vol. 7, p. S64â€"73, August 2010.
[46] M. SANTANA. (2009. September) Cloud security: Beyond the buzz. [Online]. Available: http://www.linuxworldexpo.com/storage/i۰ documents/CI7 20Mario%20Santana.pdf
[47] J. HEISER. (2009) Remote forensics software. Gartner RAS Core Research Note G00171898.
[48] W. Delport, M. Kohn, and M. S. Olivier, "Isolating a cloud instance for a digital forensic investigation," in *Proceedings of the 2011 Information Security for South Africa (ISSA 2011) Conference*. ISSA, August 2011.
[49] White paper, Software-Defined Networking: The New Norm for Networks, Open Networking Foundation, April 13, 2012. Retrieved August 22, 2013

هاله نجفی دیارجان مدرک کارشناسی و کارشناسی ارشد خود را به‌ترتیب در دانشگاه خوارزمی تهران، ایران و دانشگاه گیلان، ایران در شهریورماه سال ۱۳۹۰ و شهریورماه سال ۱۳۹۳ دریافت کرده است. زمینه‌های پژوهشی وی شامل رمزنگاری، رایانش ابری، پزشکی قانونی، شبکه‌های نرم‌افزارمحور است.

رضا ابراهیمی آتانی مدرک دکترای خود را از دانشگاه علم و صنعت تهران، ایران در سال ۱۳۸۹ دریافت کرد. ایشان هم‌اکنون استادیار گروه فنی مهندسی دانشگاه گیلان هستند. زمینه‌های پژوهشی موردعلاقهٔ ایشان شامل طراحی، تحلیل و پیاده‌سازی الگوریتم‌ها و پروتکل‌های رمزنگاری و کاربردهای آنها در امنیت شبکه‌های رایانه‌ای و ارتباطات سیار است. از

ایشان تاکنون بیش از ۱۲۰ مقاله در مجلات و همایش‌های بین‌المللی و ملی به چاپ رسیده است.

سجاد زیبافر

مدرک کارشناسی و کارشناسی ارشد خود را به‌ترتیب در دانشگاه خوارزمی تهران، ایران و دانشگاه گیلان، ایران در شهریورماه سال ۱۳۹۰ و شهریورماه سال ۱۳۹۳ دریافت کرده است. زمینه‌های پژوهشی وی شامل رمزنگاری، رایانش ابری، پزشکی قانونی، شبکه‌های نرم‌افزارمحور است.