پزشکی قانونی ابر: چالش های فنی، راه حل ها و تحلیل مقایسه ای

چکیده

رایانش ابری، مسلماً یکی از چشمگیرترین پیشرفت ها در خدمات فناوری اطلاعات (IT) امروزی است. چندین ارائه دهندگان خدمات ابر (CSPs) خدماتی را ارائه داده اند که تغییرات متحولانه متنوعی را در فعالیتهای محاسباتی تولید کرده اند و فرصتهای فناورانه و اقتصادی فراوانی را ارائه داده اند. با این حال، عمدتاً به دلیل نگرانی های مشتریان ابر در مورد امنیت ابر و تهدیدهای ناشناخته، بسیاری از آنها نسبت به سپردن نیازهای IT خود به ابر، بی میل هستند. به واسطه اینکه مثلاً به مشتریان اجازه داده نمی شود که ببینند که چه چیزی پشت دیوار مجازی ابرشان است، که مانع تحقیقات دیجیتال می شود, CSPها به طور غیرمستقیم نگرانی های آنها را بیشتر افزایش می دهند. علاوه بر این، اختیار قانونی، تکثیر داده ها و چند وجهی بودن در پلت فرم ابر، به چالش موقعیت یابی، شناسایی و تفکیک اهداف مظنون و یا مخاطره آمیز برای پزشکی قانونی دیجیتال می افزاید. متاسفانه, رویکردهای موجود برای جمع آوری و بازیابی شواهد در یک سیستم (سنتی) غیرابر عملی نیستند, زیرا آنها بر دسترسی نامحدود به سیستم مرتبط و داده های کاربر متکی هستند؛ چیزی که به دلیل پردازش غیر متمرکز داده های آن, در ابر دردسترس نیست. در این مقاله, ما به طور نظام مند چالش های پزشکی قانونی در رایانش ابری را بررسی می کنیم و آخرین راه حل ها و پیشرفت های آنها را تحلیل می کنیم. به طور خاص، بر خلاف بررسی های موجود در مورد این موضوع، ما مسائل مربوط به رایانش ابری را با استفاده از فازهای پزشکی قانونی سنتی دیجیتال به عنوان پایه توصیف می کنیم. برای هر مرحله از فرایند پزشک قانونی دیجیتال، ما لیستی از چالش ها و تحلیل راه حل های امکانپذیر آنها را لحاظ می کنیم. توصیف ما به شناسایی تفاوت های بین مشکلات و راه حل ها برای پزشکی قانونی دیجیتال ابر و غیر-ابر کمک می کند. علاوه بر این انتظار می رود که این ارائه به محققان کمک کند تا بتوانند مشکلات در محیط ابر را بهتر درک کنند. مهمتر از همه، این مقاله همچنین شامل جدیدترین توسعه ها در زمینه پزشکی قانونی می باشد که توسط محققان موسسه ملی استاندارد و فناوری و آمازون تولید شده است

کلید واژه ها: رایانش ابری. پزشک قانونی ابر، ارائه دهنده خدمات ابر، مشتری ابر، پزشکی قانونی دیجیتال، شواهد دیجیتالی، توافقنامه سطح خدمات، Amazon EC2

مقدمه

ظهور رایانش ابری در سال های اخیر, پیشرفت های عمده فناورانه را در شیوه تدارک و استقرار خدمات فناوری اطلاعات (IT) به ارمغان آورده است. رایانش ابری، که می تواند توسط افراد و شرکت ها مورد استفاده قرار گیرد، با توجه به بسیاری از ویژگی های مطلوب آن، با نرخ قابل توجه در حال ادامه رشد خود است. در میان موارد دیگر، پذیرش رایانش ابری توسط کاربران می تواند سرمایه گذاری های سرمایه بزرگ را کاهش دهد، و هزینه های کم و مخارج عملیاتی انعطاف پذیرتر را جایگزین آنها کند، و در عین حال استفاده از سرعت، چابکی، انعطاف پذیری، کشسانی بی نهایت و مهمتر از همه, تحرک را به ارمغان می آورد؛ زیرا خدمات در هر زمان از هر نقطه قابل دسترسی خواهد شد. ویژگی های ارائه شده، رشد فوق العاده ای را در بازار خدمات ابری ایجاد کرده اند. مطالعات مستقل انجام شده توسط سازمان هایی مانند آژانس امنیت اطلاعات و شبکه اروپا (ENISA) و Gartner، یک افزایش شدید در پذیرش و اتخاذ خدمات رایانش ابری توسط سازمان های شرکتی، نهادهای آموزشی و ادارات دولتی (Gartner، 2014؛ IEEE، 2014) را پیش بینی کردند. یک مطالعه توسط Media Research Research دریافت که انتظار می رود بازار رایانش ابری جهانی با نرخ رشد سالانه ۳۰٪ رشد کند و تا سال ۲۰۲۰ به ۲۷۰ میلیارد دلار برسد (Zawaod and Hasan، 2013). این رشد به طور عمده توسط صرفه جویی در هزینه ها و مدل پرداخت در هر استفاده که توسط ابر محاسبات ارائه می شود, تغذیه می شود. یک مطالع موردی مشابه که در زمینه مهاجرت ابر انجام شده است، یک متوسط صرفه جویی در هزینه ۳۷٪ را گزارش نمود, زمانی که سازمان ها, زیرساخت های خود را در اختیار ابر آمازون EC2 حرکت دادند، علاوه بر اینکه به طور بالقوه ۲۱٪ از تماس های پشتیبانی را حذف نمودند، که دلایل قانع کننده ای برای اتخاذ رایانش ابری را نشان می دهد. (خواجه حسینی و همکاران، ۲۰۱۰). یک

مطالعه اخیر که توسط گروه Right-Scale در مورد پذیرش و اتخاذ رایانش ابری انجام شد، نتیجه گیری کرد که پذیرش ابر با ۸۷ درصد سازمان های مورد بررسی که از ابر عمومی استفاده می کردند, به همه جا می رسد. Amazon Web Services (AWS) با نرخ ۵۴ درصد باعث جذب ابرها شده است (RightScale، 2014).

از سوی دیگر، Cloud Security Alliance (CSA) (اتحادیه امنیت ابر) یک رشد متناظر در حوادث آسیب پذیری ابر را گزارش داد. به ویژه، گزارش CSA نشان می دهد که حوادث آسیب پذیری ابر در بین سال های ۲۰۰۹ تا ۲۰۱۱ بیش از دو برابر شده است، که سه ارائه دهنده خدمات ابر (CSPها)، یعنی آمازون، گوگل و مایکروسافت در بالای این فهرست، ۵۶ درصد از همه رویدادهای آسیب پذیری غیرشفاف ابر را تشکیل می دهند. این گزارش همچنین اشاره کرد که تعداد حوادث آسیب پذیری در طی پنج سال گذشته به طور قابل توجهی افزایش یافته است (CSA، 2013b). حوادث امنیتی در حال افزایش در ابر، از جمله، به واسطه ثبت آسان حساب کاربری ارائه شده توسط CSPها، دسترسی نامحدود و قدرت محاسباتی عملاً نامحدود ایجاد می شوند. در واقع، مهاجمان می توانند حساب های دروغین را در ابر باز کنند، از آنها برای انجام اعمال خود استفاده کنند، حساب های آنها را ببندند و زمانی که اقدامات مخرب خود را انجام داده اند، به اتر ناپدید می شوند. دسترسی آسان و قدرت تقریباً نامحدود ابر به مهاجمان اجازه می دهد که از ابر به عنوان یک پلتفرم برای انجام حملات قدرتمند خود از هر نقطه در کوتاه مدت استفاده نمایند.

در حالی که جلوگیری کامل تمامی حملات غیرممکن است، مهاجمان باید ردیابی شوند. پزشکی قانونی دیجیتال معمولا برای ردیابی و آوردن مجرمان به محکمه در یک محیط محاسباتی غیر ابر (سنتی) به کار می رود. با این حال، پزشکی قانونی دیجیتالی سنتی نمی تواند به طور مستقیم در سیستم های ابر استفاده شود. به طور خاص، پردازش توزیع شده و ماهیت اجاره ای رایانش ابری، و همچنین محیط بسیار مجازی و پویای آن، شناسایی، حفظ و جمع آوری مدارک دیجیتال، که برای پزشکی قانونی مورد نیاز هستند، را دشوار می سازد. توجه داشته باشید که سیستم های ابر به ندرت با پزشکی قانونی دیجیتال و یکپارچگی شواهد طراحی شده اند، و بنابراین محققان پزشکی قانونی با بسیاری از مسائل فنی، قانونی و منطقی مواجه هستند. سازمان های حرفه ای مانند CSA و موسسه ملی استانداردها

و فناوری (NIST) و محققان, مقالات مربوط به رایانش ابری را در حوزه هایی نظیر مدیریت ابر، امنیت و ارزیابی ریسک منتشر کرده اند (CSA، 2011؛ Iorga and Badger، 2012؛ Jansen و Grance، 2011). با این حال، فقط کار بسیار کمی برای توسعه نظریه و شیوه پزشکی قانونی ابر انجام شده است (Casey، 2012؛ Zawaod and Hasan، 2013)؛ برخی از آنها معتقدند که حوزه پزشکی قانونی هنوز در ابتدای دوران خود قرار دارد (Zawaod and Hasan، 2013).

به تازگی، چندین محقق به چالش ها و مسائل مربوط به پزشکی قانونی ابر پرداخته اند و راه حل هایی برای حل این چالش ها پیشنهاد کرده اند (Damshenas et al., 2012; Daryabar et al., 2013; Grispos et al., 2013; Reilly et al., 2011; Tayloet al., 2011; Zawaod and Hasan, 2013). از آن زمان تاکنون پیشرفت های زیادی در حوزه پزشکی قانونی صورت گرفته است. به طور خاص، NIST, گروه کاری پزشکی قانونی ابر را تشکیل داده است و در ژوئیه ۲۰۱۴ (NIST، 2014a)، نشریات پیش نویس (NIST، 2014a) را تهیه نمود و CSPها, تحویل خدماتی را شروع نموده اند که از پزشکی قانونی پشتیبانی می کند، یعنی, مجموعه امنیتی محصولات Amazon (AWS Security Center 2014) و CloudTrail برای ورود به AWS Cloud (AWS Security Center، 2013a) استفاده شد.

در این مقاله، ما یک تحلیل جامع از چالش های پزشکی قانونی ابر و راه حل های توصیه شده در زمینه فعلی را ارائه می دهیم, زیرا ما از طریق مراحل پزشکی قانونی معمولاً استفاده شده در پزشکی قانونی دیجیتال غیرابر حرکت می کنیم. به طور دقیق، مشارکت ها در این مقاله به شرح زیر است.

- فرآیند پزشکی قانونی را به طور نظام مند ارائه می دهد و چالش ها در مراحل مختلف فرآیند، ابتدائاً برای مدل ابر زیرساخت-به عنوان- یک-خدمت را فهرست می کند. رویکرد نظام مند آن، کارکنان پزشکی قانونی و متخصصان امنیت اطلاعات را قادر می سازد تا به راحتی این مسئله را درک نمایند, زیرا آنها از طریق مراحل مختلف فرایند پزشکی قانونی پیش می روند.
- یک تحلیل جامع از راه ها را فراهم می کند و راه های توصیه شده را ارزیابی می کند.

- حوزه ای را شناسایی می کند که در آن, راه حل ها, هنوز بالغ نیستند یا هنوز به طور کامل توسعه نیافته اند و فرصت ها برای کار آینده را شناسایی می کند.

بقیه این مقاله به شرح زیر سازماندهی شده است: بخش ۲, پیش زمینه فنی فراهم می کند، و جزئیات یک نمای کلی از رایانش ابری و مدل های مختلف خدمات و استقرار آن را فراهم می کند. این بخش همچنین یک مرور کلی از پزشکی قانونی دیجیتال و پزشکی قانونی ابر را ارائه می دهد و فرایند پزشکی قانونی را توصیف می کند. بخش ۳، چالش ها و راه حل های پزشکی قانونی ابر را ارائه می دهد و یک تحلیل انتقادی از راه حل های پیشنهاد شده در مراحل مختلف پزشکی قانونی را ارائه می دهد. بخش ۴ خلاصه ای از یافته ها و کارهای آینده را ارائه می دهد. سرانجام، این مقاله را در بخش ۵ با نتیجه گیری به پایان می رسانیم.

پیش زمینه فنی

رایانش ابری: نمای کلی

NIST رایانش ابری را بدین صورت تعریف می کند: "یک مدل برای توانمندسازی دسترسی شبکه به صورت در همه جا، راحت و به محض تقاضا به یک حوزه مشترک از منابع محاسباتی قابل پیکربندی (مانند شبکه ها، سرورها، ذخیره سازی، برنامه ها و سرویس ها) که می توانند به سرعت تدارک دیده شوند و با حداقل تلاش مدیریتی یا تعامل ارائه دهندگان خدمات "(Jansen and Grance، 2011) فراهم شوند.

به عبارت ساده، رایانش ابری, یک مدل تحویل خدمت است که در آن خدمات IT به عنوان یک خدمت برای مصرف کنندگان ارائه می شوند و بر حسب استفاده صورتحسابدهی می شوند. این خدمات می توانند با استفاده از یک مشتری ظریف از قبیل مرورگر وب، از طریق اینترنت در هر زمان و از هر کجا قابل دسترسی باشند. معماری رایانش ابری دارای ویژگی های اصلی زیر است (IEEE، 2014):

- کشسانی: توانایی مقیاس بندی بالا یا پایین نیازهای محاسباتی همانطور که مشتری نیاز دارد.
- اتصال پذیری: توانایی اتصال و دسترسی به سرویس ها در هر زمان از هر کجا.

- چندین مستاجر: توانایی میزبانی مستاجران متعدد در منابع فیزیکی همانند به اشتراک گذاشتن ذخیره سازی فیزیکی، حافظه و شبکه ها.
- قابلیت مشاهده: توانایی مصرف کنندگان در داشتن دید کامل و کنترل پارامترهای استفاده از ابر، استفاده و هزینه آن.
- خدمت اندازه گیری شده: توانایی سنجش خدمات و صورتحسابدهی در هر استفاده.

ویژگی های مطلوب باعث شده اند که رایانش ابری سریعتر پذیرفته و اتخاذ شوند. منفعت اصلی رایانش ابری, صرفه جویی های به دست آمده از طریق استفاده همه جانبه و کارآمد از منابع و تخصص است. رایانش ابری در چندین مدل استقرار و تحول خدمت مطرح می شود. مدل های استقرار عبارتند از:

- ابر عمومی: زیرساخت و خدمات محاسباتی برای عموم مردم از طریق اینترنت در دسترس هستند. ابر عمومی متعلق و تحت بهره برداری یک ارائه دهنده خارجی است که خدمات ابر را می فروشد.
- ابر خصوصی: محیط محاسباتی منحصراً متعلق و تحت بهره برداری سازمان یا یک شخص ثالث. به دلایلی، ابر خصوصی, کنترل بیشتری بر تمامی منابع محاسباتی فراهم می کند و برای یک مستاجر تنها در نظر گرفته می شود.
- ابر جامعه: مشابه با ابر خصوصی، اما منابع محاسباتی توسط بیش از یک سازمان با قوانین و مقررات امنیتی و قوانین و مقررات مشابه به اشتراک گذاشته می شوند.
- ابر ترکیبی: ترکیبی از دو یا چند ابر که توسط فناوری استاندارد یا اختصاصی متصل می شوند، که قابلیت همکاری داخلی را فراهم می کند.

با توجه به ماهیت سرویس ارائه شده توسط CSP ها، همانطور که در شکل ۱ توضیح داده شده است، سه مدل خدمات ابر شناخته شده وجود دارند (Jansen and Grance، 2011):

- نرم افزار-به عنوان-یک-سرویس (SaaS): یک مدل از استقرار نرم افزار است که در آن یک یا چند برنامه کاربردی و منابع محاسباتی برای اجرای آنها به منظور استفاده بر اساس تقاضا به عنوان یک سرویس کلید چرخش فراهم می شود که توسط یک مشتری ظریف قابل دسترسی است. هدف این مدل, کاهش هزینه کلی توسعه، نگهداری و

عملیات های سخت افزار و نرم افزار است. در این مدل، کنترل برنامه ها و زیرساخت پایه بر عهده CSP ها است؛ مصرف کنندگان دارای امتیازات بسیار محدودی از قبیل مدیریت تنظیمات برنامه و داده های شخصی خود می باشند.

- پلتفرم-به عنوان-یک-سرویس (PaaS): یک مدل استقرار نرم افزاری است که در آن, پلت فرم محاسباتی به عنوان یک سرویس درخواستی فراهم می شود که براساس آن می توان برنامه های کاربردی را توسعه داد و مستقر کرد. هدف اصلی آن، کاهش هزینه ها و پیچیدگی خرید، استقرار و مدیریت سخت افزار و نرم افزار پایه, اجزای پلت فرم، مانند پایگاه داده، سیستم عامل و ابزارهای توسعه می باشد.
- زیرساخت-به عنوان-یک-سرویس (IaaS): یک مدل استقرار نرم افزار است که در آن, زیرساخت محاسباتی پایه سرورها، نرم افزار و تجهیزات شبکه به عنوان یک سرویس درخواستی ارائه می شود که بر اساس آن یک پلت فرم برای توسعه و اجرای برنامه های کاربردی را می توان ایجاد کرد. مشتریان IaaS, از خرید، نگهداری و مدیریت اجزای زیرساخت سخت افزاری و نرم افزاری جلوگیری می کند. در عوض, آنها آن دسته از منابع را به عنوان اشیاء مجازی که از طریق یک رابط سرویس قابل کنترل می باشند، اخذ می کنند.

پزشکی قانونی دیجیتال: یک نمای کلی

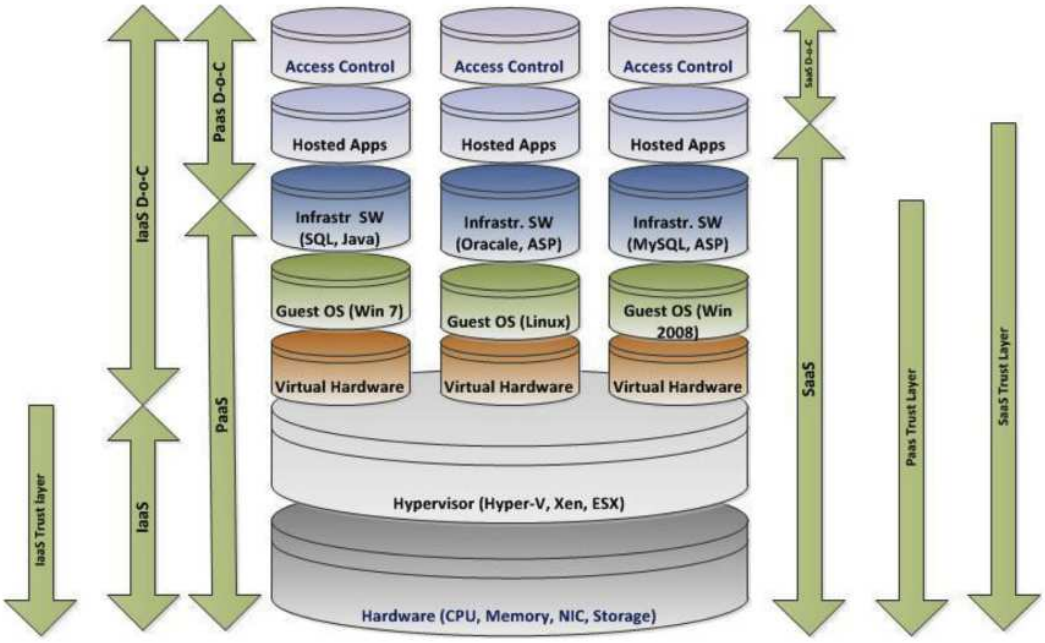
پزشکی قانونی دیجیتال, یک شاخه از علم پزشکی قانونی است که بازیابی و بررسی مواد یا آثار موجود در دستگاه دیجیتالی را در بر می گیرد که اغلب به عنوان یک پاسخ به جرم کامپیوتری انجام می شود. اولین کارگاه تحقیقاتی پزشکی قانونی دیجیتال که در سال ۲۰۰۱ در نیویورک برگزار شد, تعریف کاری زیر از پزشکی قانونی دیجیتال را ارائه داد (Palmer، 2001): "استفاده از روش های استنتاج شده و اثبات شده علمی در جهت حفظ، جمع آوری، تعیین، شناسایی، تحلیل، تفسیر، مستندسازی و ارائه شواهد دیجیتالی استنتاج شده از منابع دیجیتال به منظور تسهیل یا پیشبرد بازسازی وقایع حادثه تعیین شده یا کمک به جلوگیری از اقدامات غیرمجاز که باعث اختلال در عملیات های برنامه ریزی شده می شوند. "

NIST یک تعریف دیگر برای پزشکی قانونی دیجیتال در نشریه ویژه خود در شماره ۸۰۰-۸۶ ارائه داد (Kent et al.، 2006): "*کاربرد علم برای شناسایی، جمع آوری، امتحان و تحلیل داده ها و در عین حال حفظ یکپارچگی اطلاعات و نگه داشتن یک زنجیره سخت برای نگهداری اطلاعات.* "

پزشکی قانونی ابر: نمای کلی

پزشکی قانونی ابر می تواند به عنوان کاربرد پزشکی قانونی دیجیتال در پلت فرم رایانش ابری تعریف شود. این یک حوزه بین رشته ای است. گروه کاری جدید التاسیس پزشگی قانونی ابر NIST (NIST، 2014a)، تعریف زیر را ارائه داد: "علم پزشکی قانونی رایانش ابری، کاربرد اصول علمی، شیوه های فناورانه و روش های استنتاج شده و اثبات شده برای پردازش حوادث رایانش ابری گذشته از طریق شناسایی، جمع آوری، حفظ، بررسی و گزارش دادن داده های دیجیتال به منظور تسهیل بازسازی این حوادث است".

ماهیت پیش فرض محیط ابر مانند چندمستاجر، حوزه قضائی، تکثیر داده ها و درجه بالایی از مجازی سازی، چندین لایه پیچیدگی را به پزشکی قانونی ابر می افزاید. این مقوله زمانی بیشتر افزوده می شود که خدمات تجارت CSPs بین خودشان, پیگیری زنجیره ای از رویدادها را دشوار می سازد. بنابراین، فرایند پزشکی قانونی قابل اجرا در محیط سنتی (غیرابر) در مورد ابر بسیار کاربردی نیست. پزشکی قانونی ابر شامل سه بعد می شود: فنی، سازمانی و حقوقی (Ruan et al.، 2011). بعد فنی شامل روش های اجرایی و ابزارهایی می شود که برای انجام فرایند پزشکی قانونی در یک محیط رایانش ابری مورد نیاز هستند. این کار شامل جمع آوری داده ها، پزشکی قانونی زنده، جداسازی شواهد و اقدامات پیش فعالانه می شود. از طرف دیگر، بعد سازمانی، جنبه های سازمانی پزشکی قانونی را پوشش می دهد. این شامل بازیگرانی مانند CSPs، مشتریان، مشاوران حقوقی، هدایت کننده های حوادث و اشیائی مانند موافقت نامه های سطح سرویس (SLA)، سیاست ها و دستورالعمل های الزام آور می باشد. در نهایت، بعد قانونی، توسعه مقررات و توافقات را برای اطمینان از اینکه فعالیت های پزشکی قانونی, قوانین و مقررات در حوزه های قضایی که داده ها در آنها ساکن یا جمع آوری می شوند، نقض نکنند و به طور همزمان برای اطمینان از محرمانگی مستاجران همزمان که زیرساخت یکسانی را به اشتراک می گذارند، پوشش می دهد.



شکل ۱: مدل ابر، درجه کنترل (D-o-C) و لایه اعتماد.

پزشکی قانونی

فرایند پزشکی قانونی پس از اینکه حادثه به عنوان یک فعالیت پس از حادثه اتفاق می افتد, شروع می شود. این امر از طریق مراحل از پیش تعریف شده دنبال می شود. در رایانش ابری، این فرآیند را می توان به سه حوزه تقسیم کرد، یعنی: (i) پزشکی قانونی مشتری (ii) پزشکی قانونی ابر و (iii) پزشکی قانونی شبکه.

پزشکی قانونی مشتری

جرایم دیجیتال آغاز می شوند و اغلب از سمت مشتری انجام می شود، اما آثار هم در سمت مشتری و هم در سمت سرور می مانند. شناسایی و جمع آوری شواهد از طرف مشتری، یک بخش حیاتی از این فرایند است (Damshenas et al.، 2012). داده های شواهد مانند ثبت وقایع، داده های دما، رجیستری، فهرست های دسترسی, فهرست های چت، داده های جلسه و کوکی های مداوم را می توان در مرورگر وب یافت (Guo et al.، 2012). مهم است که داده ها باید در اسرع وقت در شرایط استریل خود برای مقاصد پزشکی قانونی برای استفاده به عنوان مدرک جمع آوری شوند. یک ریسک بالقوه وجود دارند که داده های هدفمندانه توسط بازیگر یا به طور

غیرمستقیم توسط سیستم به دلیل پیکربندی سیستم قابل پاک کردن است؛ برای مثال، تاریخچه مرورگر وب و فهرست های جلسه را می توان پیکربندی کرد که پس از یک دوره مشخص قابل دوباره نوشتن یا پاک کردن هستند یا زمانی که اندازه فایل به حداکثر حد پیکربندی شده می رسد.

تکثیر نقاط نهایی سمت مشتری، به ویژه نقاط انتهایی تلفن همراه، شناسایی و جمع آوری داده های قانونی را چالش برانگیزتر می سازد (Ruan et al.، 2011). برای پزشکی قانونی ابر، مهم است که نقاط انتهایی شناسایی و به موقع جمع آوری شوند، و یکپارچگی شواهد حفظ شود، به طوری که یک خط زمانی از وقایع را بتوان ایجاد کرد.

پزشکی قانونی ابر (سرور)

بسیاری از آثار دیجیتال که در سرورها ایجاد شده و در دسترس قرار می گیرند، بخش مهمی از داده های پزشکی قانونی را تشکیل می دهند و ضروری است که این شواهد جمع آوری شوند. این آثار شامل فهرست های سیستم، فهرست های مربوط به برنامه، احراز هویت کاربر و اطلاعات دسترسی، فهرست های پایگاه داده و غیره می شوند. عدم دسترسی فیزیکی و موقعیت نامشخص داده ها موجب سخت تر شدن شناسایی شواهد، جداسازی و جمع آوری اطلاعات در پزشکی قانونی ابر می شود. در یک محیط ابر بسیار تمرکززدایی شده و مجازی شده, بسیار معمول است که داده ها ممکن است در مراکز مختلف داده ها در نقاط مختلف جغرافیایی واقع شوند (Hay et al.، 2011). رویکرد سنتی برای تسخیر این سیستم، دیگر عملی نیست، حتی اگر مکان شناخته شده باشد، زیرا می تواند کل مرکز داده ها را پایین بیاورد، که به علت چندمستاجر بودن، دیگر مشتریان را تحت تاثیر قرار می دهد. تعدادی از محققان, این موضوع را ذکر کرده اند و برخی از آنها تا حدودی راه حل های ممکن را پیشنهاد کرده اند (Birk and Wegener، 2011؛ Guo et al.، 2012؛ Hay et al.، 2011؛ Reilly et al.، 2011؛ Wolthusen، 2009).

از دست دادن اداره امور یکی دیگر از مسائل اصلی در پزشکی قانونی ابر است. مشتریان, از نظر اداره امور به ارائه دهندگان اعتماد می دهند. این گزارش همچنین توسط گزارش ارزیابی ریسک ابر رایانه آژانس امنیت شبکه اروپا (ENISA) مشخص شده است که شامل "از دست دادن اداره امور" به عنوان یکی از مهمترین ریسک های رایانش

ابری می شود، به ویژه در زیرساخت ها به عنوان یک سرویس (IaaS) (Catteddu و Hogben، 2009). از دست دادن اداره امور به طور ناگهانی که منجر به از دست دادن کنترل دارایی های اطلاعاتی توسط صاحبان داده ها می شود، تنگنای بزرگ دیگری برای جمع آوری شواهد است. از دست دادن کنترل به مدل ابر بستگی دارد که در شکل ۱ نشان داده شده است. در IaaS, کاربران کنترل بیشتری دارند و دسترسی نسبتاً نامحدودی به فهرست ها و داده های سیستم دارند، در حالی که در مدل PaaS, دسترسی آنها به فهرست های برنامه و آنچه API از پیش تعریف شده فراهم می کند، محدود می شود و در مدل SaaS، مشتریان دسترسی کم یا عدم دسترسی به این داده ها دارند. با توجه به اینکه مشتریان به طور فزاینده بر CSPs برای ارائه قابلیت ها و سرویس ها متکی هستند، آنها به CSP ها, کنترل بیشتری بر دارایی های اطلاعاتی خود می دهند. همانطور که مشتریان کنترل را از دست می دهند، دسترسی به اطلاعات مهم و بنابراین شناسایی و جمع آوری آن ها برای هر گونه نیازهای پزشکی قانونی بعدی را از دست می دهند (Hay et al.، 2011). زمانی که درجه کنترل کاهش می یابد، داده های پزشکی قانونی کمتر برای کاربران ابر در دسترس است و بنابراین وابستگی بیشتر به CSP ها برای دسترسی به چنین اطلاعاتی وجود دارد. این به نوبه خود بستگی به SLA ها و آنچه دارد که CSP مایل به ارائه آن هستند. این مورد در شکل ۱ نشان داده شده است.

علاوه بر این، بر اساس بسیاری از عوامل مانند تعادل بار، پیوستگی کسب و کار و غیره, نمونه های ماشین مجازی (VM) در حال حرکت درون یک مرکز داده، در خارج از یک مرکز داده مختلف در همان حوزه قضائی و یا به طور کامل یک مرکز داده جدید واقع در یک حوزه قضائی جداگانه هستند. این حرکات انجام شده توسط CSPها، کاملا خارج از کنترل مشتری است. این همچنین چالش های اضافی را به پزشکی قانونی سمت سرور ابر اضافه می کند.

پزشکی قانونی شبکه

پزشکی قانونی سنتی شبکه با تحلیل ترافیک شبکه و فهرست های مربوط به ردیابی حوادث که در گذشته رخ داده اند سرو کار دارد. پزشکی قانونی شبکه از لحاظ نظری در محیط های ابر نیز امکان پذیر است. لایه های پروتکل TCP / IP مختلف می توانند چندین مجموعه اطلاعات را در مورد ارتباط بین نمونه های VM درون ابر و نیز موارد خارج از ابر فراهم کنند. CSPها معمولاً مسیرهای شبکه و یا فهرست های ارتباطی تولید شده توسط نمونه های

مشتری یا برنامه های کاربردی را ارائه نمی دهند، بر خلاف این واقعیت که این فهرست ها, عنصر حیاتی داده پزشکی قانونی هستند (Birk and Wegener، 2011). به عنوان یک مثال، اگر کسی از یک نمونه IaaS برای توزیع یک بدافزار استفاده کند، اطلاعات مسیریابی و ورود به سیستم شبکه, بخش حیاتی از جمع آوری داده های پزشکی قانونی هستند، اما به دست آوردن آنها سخت است. این برای مدل های ابر PaaS و SaaS چالش برانگیزتر می شود و قابلیت جمع آوری اطلاعات به شدت به تحقیقات پشتیبانی که از CSPها دریافت می کند بستگی دارد.

پزشکی قانونی: فرایند، چالش ها و راه حل ها

این نه تنها شواهد دیجیتالی است که باید در هر دادگاه قانون حاکم باشند، بلکه فرایند دنبال شده برای انجام تحقیقات نیز باید حاکم باشد. محققان و دست اندرکاران پزشکی قانونی, چندین چارچوب پزشکی قانونی دیجیتال را پیشنهاد کرده اند.

محققان مختلف، فرآیند و چارچوبی که قبلا منتشر شده است را اصلاح نموده اند و موارد جدیدی پیشنهاد داده اند که منجر به مدل های مختلف فرآیند پزشکی قانونی دیجیتالی و اصطلاحات آنها می شود. تعدادی منتخب از مدل های فرایند پزشکی قانونی دیجیتال عبارتند از:

۱. مدل فرآیند تحقیق دیجیتالی (DIP) که توسط اولین کارگاه کنفرانس تحقیقاتی دیجیتال (DFRWS) پیشنهاد شده و شامل مراحل (i) شناسایی (ii) حفظ (iii) جمع آوری (iv) بررسی (v) تحلیل (vi) ارائه (پالمر، ۲۰۰۱) می شود.

۲. مدل McKemmish که شامل یک فرایند خطی مراحل (i) شناسایی (ii) حفظ (iii) تحلیل و (iv) ارائه (McKemmish، 1999) می شود.

۳. مدل پزشکی قانونی NIST که متشکل از مراحل (i) جمع آوری، (ii) بررسی ، iii) تحلیل و گزارش (Kent et al.، 2006) می باشد.

۴. مدل فرایند پزشکی قانونی دیجیتال یکپارچه (IDFPM) که شامل (i) تهیه، (ii) حادثه، (iii) پاسخ حادثه، (iv) تحقیق فیزیکی، (v) تحقیق پزشکی قانونی دیجیتال و (vi) ارائه می شود. در این مدل، نویسندگان, یک فرایند

یکنواخت، یک اصطلاح شناسی مشترک و مدل فرایند پزشکی قانونی دیجیتال استاندارد را پیشنهاد می کنند (Kohn et al.، 2013).

۵. مدل چرخه تحلیل پزشکی قانونی دیجیتال که شامل مراحل (i) شروع (دامنه)، (ii) تهیه و پاسخ، (iii) شناسایی و جمع آوری، (iv) حفظ (کپی پزشکی قانونی)، (v) تحلیل، ((vi، vi)) بازخورد، و (vii) تکمیل یا وظیفه اضافی شناسایی شده می باشد. این یک مدل چرخه ای و تکراری است (Quick and Choo، 2013).

۶. چارچوب پزشکی قانونی دیجیتالی مفهومی یکپارچه برای رایانش ابری که شامل مراحل (i) شناسایی و حفظ منبع شواهد، (ii) جمع آوری، (iii) بررسی و تحلیل، و (iv) گزارش و ارائه (Martini and Choo، 2012) می باشد.

در محیط مبتنی بر سرور سنتی، جایی که مکان های فیزیکی سیستم ها شناخته شده اند، محققان می توانند کنترل کامل بر آثار پزشکی قانونی داشته باشند. ماهیت ذاتی و مشخصات اکوسیستم ابر، چالش های اضافی را برای نقشه برداری از هر چارچوب پزشکی قانونی سنتی برای محیط ابر ایجاد می کند. برای مثال، چارچوب IDFPM به ضبط شواهد دیجیتال (بسته به شرایط) در حین پاسخ حادثه اشاره می کند که در محیط ابر امکان پذیر نیست. مارتینی و چو (۲۰۱۲) یک چارچوب یکپارچه و تکراری برای پزشکی قانونی ابر پیشنهاد دادند. در این مدل در مرحله بررسی و تحلیل، یعنی مرحله (iii)، اگر داده ها یا شواهد بیشتری نیاز باشد، این فرایند دوباره به عقب در مرحله شناسایی و حفظ منبع شواهد تکرار می شود (Martini and Choo، 2012)، یعنی مراحل (i) و (ii) به ترتیب. در یک محیط ابر، این احتمال بالا وجود دارد که شواهد در هر زمان خاص پاک یا اصلاح شوند، زیرا سیستم عامل های ابری دائماً در معرض تغییرات سریع هستند. این امر، اهمیت حفظ شواهد را به محض شناسایی، با استفاده از تکنیک های نگهداری مناسب صرف نظر از منبع شواهد برجسته می کند؛ این گام مهم توسط مارتینی و چو (۲۰۱۴) در کار اخیرشان در مورد پزشکی قانونی سیستم فایل توزیع شده تاکید شده است که به وسیله آن, آنها چارچوب خود را اعتباردهی نمودند.

در این بخش، مدل DIP (Palmer، 2001) را می توانیم در نظر بگیریم که در تمام تحقیقات دیجیتالی و سپس توسط بسیاری از محققین و دست اندرکاران قابل کاربرد است (Grispos et al.، 2013؛ Taylor et al.، 2011).

فرآیند خطی مدل در شکل ۲ نشان داده شده است. مارتینی و چو (۲۰۱۴) از مدل DIP استفاده کردند, آن را گسترش دادند و برای پزشکی قانونی سیستم فایل توزیع شده مورد استفاده قرار دادند. ما از این مدل برای توصیف چالش های هر مرحله از فرآیند و راه حل های پیشنهادی استفاده می کنیم. در مواردی که یک چالش منحصر به یک مرحله خاص نیست، چالش را در تمام مراحل مرتبط قرار می دهیم.

شناسایی

فرایند پزشکی قانونی با شناسایی سیستم ها، رسانه ها، دستگاه های تلفن همراه و غیره که احتمالاً حاوی شواهد بالقوه دیجیتال هستند آغاز می شود. در واقع شناسایی، یک فرایند دو مرحله ای است: (۱) شناسایی حادثه و (۲) شناسایی شواهد لازم برای اثبات حادثه. مرحله (i) نیاز به شناسایی تمام فایل های دستگاه ها و سیستم دارد که مشکوک به داشتن شواهد مربوطه هستند و مرحله (ii) به شناسایی شواهد در رسانه ها نیاز دارد. ردهای شواهد را می توان در رسانه هایی مانند سرورهای ابر، دستگاه های شبکه و دستگاه های تلفن همراه یافت (Brezinski and Killalea، 2002؛ McKemmish، 1999). استاندارد ISO 27037، فرایند شناسایی را به عنوان "فرایند شامل جستجو، شناسایی و مستندسازی شواهد بالقوه دیجیتال" تعریف می کند (ISO 27037، 2012). شناسایی شواهد مناسب مستلزم شناخت مکان، نوع و فرمت فعلی آن است. رایانش ابری، چالش های جدیدی را به فرایند شناسایی مکان می افزاید، زیرا شناسایی مکان فیزیک خاص دارایی دارایی در یک زمان معین دشوار است (Martini and Choo، 2012؛ Taylor et al.، 2011).

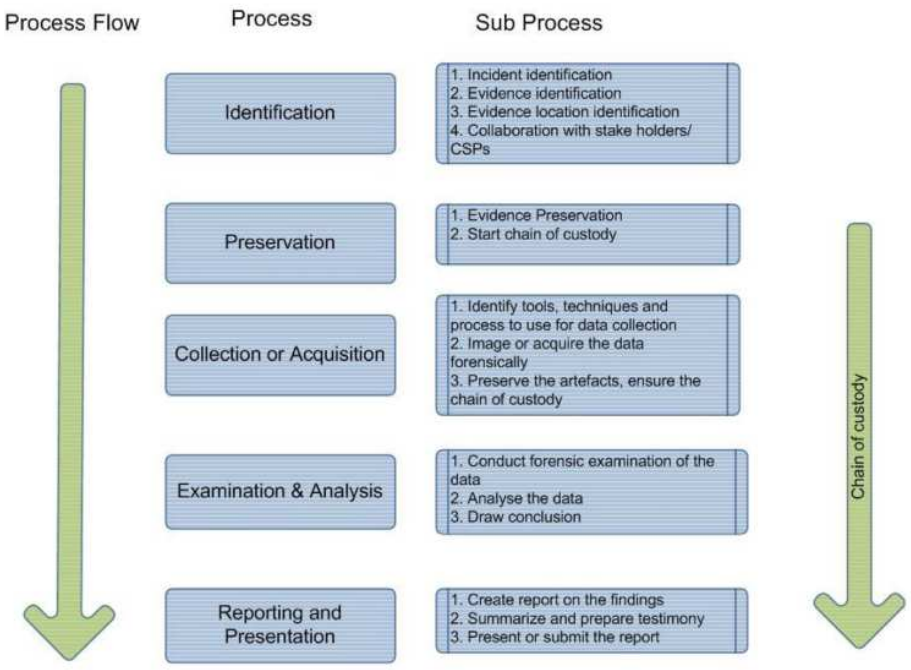
حوزه قضائی و اجاره دادن چندگانه در یک محیط پردازش داده بسیار نامتمرکز، محیط های پیش فرض برای مدل عمومی استفاده از ابر هستند. اغلب CSP ها عمداً مکان داده ها را مخفی می کنند تا تکرار را تسهیل کنند و قابلیت دسترسی به اطلاعات را ارتقا دهند. این محیط ها, چالش های اضافی را در شناسایی داده ها و جمع آوری مطرح می کنند؛ زیرا مکان داده ها ناشناخته است (Birk and Wegener، 2011؛ Hay et al.، 2011؛ Ruan et al.، 2011). فهرست های سیستم و برنامه, بخش مهمی از تحقیقات پزشکی قانونی را تشکیل می دهند و بدست آوردن موقعیت فهرست ها نیز یک چالش یکسان را مطرح می کند (Damshenas et al.، 2012). جدول ۱، چالش های

مرحله شناسایی داده ها و راه حل های پیشنهادی آنها را تشریح می کند، با فرض اینکه شناسایی و مکان یابی موقعیت مکانی مشتری، از جایی که حادثه آغاز شده است، آسان است.

در موارد زیر، چالش های دخیل در مرحله شناسایی و راه حل های ممکن آنها را مورد بحث قرار می دهیم.

مکان فیزیکی نامعلوم

مکان نمونه های مجازی و آثار دیجیتال، مانند فایل های سیستم سرور و فهرست های مرتبط، برای مشتری شناخته شده نیست و بنابراین شناسایی آثار بسیار مشکل است. این می تواند به علت تعدادی از ویژگی های ذاتی رایانش ابری باشد. به عنوان مثال: (الف) داده های ابر را می توان در خارج از حوزه قضائی از تحقیق آژانس اجرای قانون ذخیره کرد یا (ب) داده های مصرف کننده ممکن است در میان تعدادی از دستگاه های ذخیره سازی در محیط ابر تقسیم شوند، بخشی از داده ها همچنان در حوزه قضائی بماند و بخش دیگری در خارج از حوزه قضائی باقی می ماند (Quick et al.، 2013). همه این ها, چالش هایی را در شناسایی آثار شواهد ایجاد می کنند. در زیر برخی از راه حل های چالش را مورد بحث قرار می دهیم.



شکل ۲. فرایند پزشکی قانونی دیجیتال

جدول ۱. مرحله شناسایی: چالش ها و راه حل های پیشنهادی

شماره	چالش ها	راه حل های پیشنهادی	نظرات
1	مکان فیزیکی ناشناخته	برچسب گذاری منبع (Hay et al., 2011)	به طور منفی بر قابلیت CSPs برای تضمین انعطاف پذیری, دردسترس بودن خدمات و قابلیت مدیریت تاثیر می گذارد
		SLA محکم با CSPs (Alhamad et al., 2010;). Birk and Wegener, 2011	بیشتر رهنمودهای SLA عمدتاً بر الزامات امنیت و کمتر بر الزامات پزشکی قانونی متمرکز هستند
		SLA در حمایت از پزشکی قانونی ابر (Ruan et al., 2012)	
		فهرست های سطح سیستم	فهرست های سطح سیستم می توانند حاوی اطلاعات اولیه در مورد دسترسی, خلق و حذف اشیای سطح سیستم باشند.
2	داده های غیرمتمرکز	چارچوب فهرست (Marty, 2011; Sang, 2013)	فهرست های شامل فهرست های سطح فراناظر به فرایند پزشکی قانونی در خط بندی زمان رویدادهایی که می توانند اثر بد بر عملکرد سیستم بگذارند کمک می کند
3	تکثیر داده ها	برچسب گذاری منبع (Hay et al., 2011)	
4	حوزه قضائی	SLA, مشخص می کند که داده ها می تواند به طور منفی بر قابلیت CSPs برای تضمین انعطاف پذیری, دردسترس بودن خدمات در چه جایی می توانند ذخیره شوند و منافع هزینه برای مصرف کنندگان تاثیر بگذارد یا منتقل شوند (Alhamad et al., 2010; Jansen and Grance, 2011; Ruan et al., 2012)	
		جستجوی معکوس برای ادوات شبکه	

به دلیل ماهیت پویای رایانش ابری, این یک اقدام بسیار حیاتی است	بندی شده, توپولوژِ جستجوی معکوس را انجام می دهند (CSA, 2013a).		
فقدان راه حل ها به شکل ابزارهای نرم افزاری, فرایند استاندارد و غیره. دردسترس نیست	هیچ کدام	زنجیره وابستگی	5
رهنمودهای سیاست, اداره امور و فرایند در حال حاضر برای مدیریت کلیدی در ابر وجود ندارد	سیستم مدیریت کلیدی درون ابر (CSA, 2013a) و نهاد قانونی	رمزگذاری	6
SLA خوب, قابلیت دسترسی خدمات و تطابق را تضمین می کند(Pichan et al., 2014)	SLA مشخص کننده خدمات پزشکی قانونی خاص (Alhamad et al., 2010; Kandukuri et al., 2009; Ruan et al., 2012).	وابستگی به CSP	7

- برچسب زدن منابع: مصرف کنندگان منابع ابر، منابع خود را برای نشان دادن محل دارایی های اطلاعاتی خود "برچسب گذاری" می کنند که همچنین می توانند توسط CSP ها برای تعیین اینکه آیا می توان آنها را منتقل کرد و در صورت امکان ارائه مرز مجاز منطقه ای انتقال (Hay et al.، 2011) استفاده کرد. حرکت دادن نمونه های VM و فایل های مربوط به مشتری بین دستگاه های مختلف فیزیکی و گاهاً در سراسر مراکز مختلف داده ها در مکان های مختلف جغرافیایی برای CSP ها امری معمول است. در چنین مواردی، برچسب زدن منابع می تواند برای اطلاع رسانی به CSP ها در مورد اینکه "چه چیزی می تواند باشد" و "چه چیزی نمی تواند باشد" منتقل شده مورد استفاده قرار داد. با دیکته کردن منابعی که انتقال آنها به حوزه قضائیی متفاوت مجاز نیست، این به مسأله قانونی می پردازد. این راه حل ممکن است به طور قابل توجهی, توانایی CSPها برای مدیریت موثر منابع خود و ارائه خدمات اولیه، مانند قابلیت دسترسی و عملکرد قابل قبول را تحت تاثیر قرار دهد.
- SLA قوی: چندین CSP ها، مانند آمازون، گزینه ای برای انتخاب یک مکان جغرافیایی، از فهرستی از مناطق موجود در سراسر جهان برای میزبانی نمونه VM در هنگام ایجاد نمونه برای اولین بار ارائه می کنند. در حال حاضر آمازون,

سرویس های ابر عمومی را در مناطق زیر فراهم می کنند: سه منطقه در ایالات متحده، یکی در اتحادیه اروپا (ایرلند)، سه در آسیا (سنگاپور، توکیو، پکن)، یکی در استرالیا (سیدنی) و یک در آمریکای جنوبی پائولو). آمازون, نمونه های کاربر را حرکت نمی دهد و یا آنها را در مناطق توسط خودش تکثیر نمی کند (AWS Security Center، 2014). این طرح به طور جزئی مسئله حوزه قضائی یا مکان داده ها را برای مشتریان آمازون حل می کند. با این حال، دیگر ارائه دهندگان ابر مانند Google، مایکروسافت، چنین گزینه ای را به عنوان یک ویژگی مشترک ارائه نمی دهند.

گنجاندن این گزینه در SLA توصیه می شود (.Alhamad et al، 2010؛ Jansen and Grance، 2011)، زیرا یک مشتری به CSP خود برای شناسایی موقعیت های مکانی نمونه های VM نیاز دارد که تنها زمانی که توسط SLA اجبار شده باشد, ذخیره خواهد شد. الحامد و همکاران (۲۰۱۰) یک چارچوب SLA مفهومی برای رایانش ابری پیشنهاد داد. محققان دیگر به اهمیت داشتن SLA قوی با CSPهایی که می توانند مورد استفاده قرار گیرند معتقدند (Birk and Wegener، 2011؛ Jansen and Grance، 2011؛ .Kandukuri et al، 2009؛ Patel et al.، 2009؛ .Ruan et al، 2011). Ruan و همکاران (۲۰۱۲) شرایط و ضوابط کلیدی مربوط به فعالیت های پزشکی قانونی در SLA بین ارائه کننده ابر و مصرف کننده را ارائه نمودند.

- ورودی های سطح سیستم: ورودهای سیستم که گزارشات دقیق دسترسی در مورد دارایی های داده هستند، از جمله دسترسی امتیازی کاربران، ایجاد، حذف و اصلاح اشیا در سطح سیستم و غیره. به عنوان مثال، فهرست های تولیدشده توسط AWS CloudTrail Logs (AWS Security Center، 2013b) بخش اول اطلاعات پزشکی قانونی هستند.

داده های غیرمتمرکز

ماهیت غیرمتمرکز پردازش داده ها یکی از ویژگی های کلیدی رایانش ابری است. در نتیجه، هیچ مکان مرکزی برای فایل ها، آثار پایگاه داده، آثار سیستم و فهرست های مربوطه وجود ندارد، که موجب ایجاد چالش های بزرگ برای شناسایی، قفل کردن (برای اطمینان از یکپارچگی) و بازیابی آنها می شود. CSP ها به ندرت جزئیات نحوه ایجاد

فهرست ها و ذخیره سازی آنها را ارائه می دهند. علاوه بر این، CSP ها از فرمت های ورودی شخصی خود به شبکه های خصوصی استفاده می کنند، که منجر به ساختار ورودی نامنظم در رایانش ابری می شود. داشتن یک چارچوب ورود به سیستم یکسان و از نظر پزشکی قانونی قابل اعتماد، یکی از راه های حل مسئله دسترسی به فایل ورودی است. بسیاری از محققان, اهمیت حفظ برچسب های تراکنش جامع و انتها-به-انتها را مشخص کرده اند (Birk and Wegener، 2011؛ Haeberlen، 2010؛ Marty، 2011؛ Sang، 2013). مارتی (۲۰۱۱) یک چارچوب و دستورالعمل های ورود به سیستم کسب و کار را ارائه نمودند که "چه چیزی برای ورود" و "چه زمانی باید وارد سیستم شود" را نشان می دهند و یک رویکرد پیشگیرانه برای ورود به برنامه را پیشنهاد نمودند. با این حال، تاکنون هیچ تحقیقی در مورد یک "ساختار و مکان ورود معتبر از نظر پزشکی قانونی و از پیش تعریف شده" وجود ندارد که قابل مکانیابی، بازیابی و تایید یکپارچگی باشد, که با استفاده از آن محققان پزشکی قانونی بتوانند تحلیل زمانی انتها-به-انتها را انجام دهند (یعنی ، جدول زمانی وقایع).

تکثیر داده ها

تکثیر داده ها به مکان های مختلف یک ویژگی ذاتی رایانش ابری است. CSPها اغلب این ویژگی را برای اطمینان از تداوم کسب و کار و تحمل خطا ارائه می دهند. از دیدگاه پزشکی قانونی، این ویژگی خوبی است، زیرا از بین بردن کامل تمام شواهد از ابر بسیار سخت است (.Ruan et al، 2013). با این وجود شناسایی داده ها به همان اندازه سخت است زیرا داده ها پخش می شوند. با پیروی از زنجیره منطقی فایل ها, می توان از مکانیزم برچسب گذاری منابع (.Hay et al، 2011)، که در بخش ۳,۱,۱ توضیح داده شده است، برای قرار دادن فایل های پاک شده مورد نیاز پزشکی پزشکی قانونی استفاده کرد.

حوزه قضائی

ذخیره سازی داده های مشتری خارج از منطقه قضائی مشتری, در رایانش ابری بسیار رایج است؛ به طور کلی، CSP ها نباید در مورد مکان جزئیات فایل های آنها به مشتریان اطلاع رسانی نمایند. بنابراین، بسته به محل، قوانین مختلف اعمال می شوند که به طور قابل توجهی بر فرایند پزشکی قانونی تاثیر می گذارند. برای دستگاه های شبکه

بندی شده، اگر چه ردیابی یا انجام جستجوی معکوس به منظور تولید توپولوژی کلی و در نتیجه اخذ اطلاعات ضروری از لحاظ نظری امکان پذیر است، این مرحله به دلیل ماهیت سریع پویای سیستم های ابر بسیار دشوار است. اطلاعات توپولوژی (مانند آدرس IP اختصاصی، فضای ذخیره سازی و غیره) تحت تغییرات سریع قرار دارد و بنابراین برای دریافت اطلاعات معنی دار (CSA، 2013a) اغلب پاسخ سریع تر نیاز است. اغلب حرکت نمونه های VM بین دستگاه های مختلف فیزیکی، گسترش آنها در مکان های مختلف قضایی (Hay و همکاران، ۲۰۱۱) و در نهایت ایجاد چالش های پزشکی قانونی در CSPها همچنان ادامه دارد. راه حل های ممکن برای رسیدگی به مساله حوزه قضائی عبارتند از:

- SLA خاص: SLAهایی را ایجاد می کنند که به وضوح مشخص می کنند که داده ها در چه جایی می توانند ذخیره شوند، دوباره مرتب شوند یا کپی شوند (Biggs and Vidalis، 2009؛ .Ruan et al، 2012).
- جستجوی معکوس: پیدا کردن محل ادوات شبکه بندی شده، و انجام یک جستجوی معکوس توپولوژی شبکه (CSA، 2013a).

زنجیره وابستگی

تجارت خدمات را در میان CSP ها بسیار معمول است. برای مثال, یک CSP ارائه دهنده سرویس ایمیل (SaaS) ممکن است به یک CSP شخص ثالث وابسته باشد که PaaS را برای میزبانی فایل های ورودی ارائه می دهند، که به نوبه خود به ارائه دهنده دیگر IaaS برای ذخیره فایل های ورودی بستگی دارد. همبستگی فعالیت ها در سراسر CSP ها یک چالش بزرگ است، که یک زنجیره وابستگی ها در میان CSPها ایجاد می کند. علاوه بر این، ارائه دهندگان مختلف ممکن است خدمات خود را در مکان های مختلف میزبانی کنند. عدم شفافیت, مسئله دیگری است که با سطوح مختلف برون سپاری ارتباط دارد. محققان باید هر پیوند در زنجیره را برای ردیابی لینک و قفل کردن شواهد برای جمع آوری پیگیری و دنبال کنند. با این وجود، هیچ راه آسانی برای انجام این فرایند وجود ندارد. تا به امروز، فرایند، سیاست ها و دستورالعمل های مربوط به معاینه پزشکی قانونی ارائه دهنده, تقریباً وجود ندارد، که به واسطه عدم وجود چارچوب همکاری در میان ارائه دهندگان ابر ادامه می یابد.

رمزگذاری

رمزگذاری به طور فزاینده ای برای رایانش ابری اهمیت دارد. اکثر CSPها, رمزگذاری را به عنوان یک ویژگی در سرویس بسته بندی امنیتی خود ارائه می کنند. CSPها, این سرویس را تنها با ارائه یک API برای رمزگذاری ارائه می دهند، در حالی که مشتریان از سیستم مدیریت کلیدی خود و کلیدهای خود و یا با استفاده از رمزگذاری استفاده می کنند زمانی که داده ها در ابر ذخیره می شود و ذخیره کلید رمزگذاری که اغلب با رمز عبور دسترسی کاربر مرتبط می شود (CSA، 2013a). ارائه دهندگان راه حل ذخیره ابر مانند SpiderOak، قبل از آپلود داده ها به سرورهای ابر، آنها را در محل مشتری رمزگذاری می کنند. این روش, "حریم خصوصی دانش صفر" را ارائه می دهد، به این معنی است که ارائه دهنده هرگز محتوای متن ساده داده های ذخیره شده را نمی داند؛ در نتیجه، تنها مشتری می تواند داده های رمزگذاری شده را با استفاده از رمز عبور خود باز کند. در سرورهای SpiderOak, فایل ها و پوشه ها به عنوان ظروف شماره گذاری شده ترتیبی داده ها ظاهر می شوند (SpiderOak، 2014). صرف نظر از روشی که برای رمزگذاری استفاده می شود، یک داده رمزگذاری شده به عنوان یک جریان بایت پیوسته ظاهر می شود که مرحله شناسایی شواهد و همچنین فازهای بعدی آن را به مشکلات چالش برانگیز تبدیل می سازد.

گروه تحقیقاتی CSA, استفاده از زیرساخت مدیریت کلیدی مناسب و بهترین شیوه های مدیریت کلیدی (مانند زیرساخت کلیدی عمومی) را پیشنهاد کرد به طوری که دارایی های داده ها بتوانند بدون نیاز به اشتراک گذاری کلیدها رمزگشایی شوند (CSA، 2011). با این وجود، هیچ رهنمود منتشر شده ای مشخص نشده است و فرایند استاندارد ISO 27037 هنوز مشخص نشده است.

وابستگی به CSP

با توجه به ماهیت ذاتی رایانش ابری، مشتریان و محققان باید برای شناسایی، موقعیت یابی و قفل کردن شواهد پزشکی قانونی بر CSP ها تکیه کنند. در نظر گرفتن خدمات اساسی پزشکی قانونی مورد نیاز از CSPها در SLA، راه حل کلیدی این موضوع است. CSPها بیشتر از آن آگاه هستند و برخی از این خدمات را ارائه می دهند.

وابستگی به CSP همچنان یک مسئله است، تا زمانی که برحسب تقاضای استفاده از یک پورتال ارائه شده یا برنامه های مشابه, ارائه دهندگان شروع به ارائه ابزارهایی برای جمع آوری آثار پزشکی قانونی نمایند. به عنوان مثال، آمازون, انبارهای حافظه را فراهم می کند و این به معنای انتقال حافظه در هر زمان با پرداخت هزینه، علاوه بر نرم افزار اخیرا منتشر شده Logging CloudTrail است، که بازیابی فهرست های مربوط با استفاده از پورت AWS (AWS Security Center 2014) را میسر می سازد.

حفاظت

ISO 27037, حفاظت را به عنوان "فرآیند حفظ و محافظت از یکپارچگی و / یا شرایط اصلی شواهد بالقوه دیجیتال" تعریف می کند (ISO 27037، 2012). حفاظت شامل تمام فعالیت هایی می شود که از تمامیت شواهد در سراسر فرایند محافظت می کنند. تدابیر باید اتخاذ شوند تا اطمینان حاصل شود که انسجام شواهد در طول چرخه عمر تحقیق، حفظ می شود و زنجیره مناسبی فرایند قانونی آغاز می شود. این کار برای تأمین اطمینان بی چون و چرا به مقامات حقوقی در مورد اینکه داده های موجود, نمایش دقیقی از واقعیت ها هستند مهم است (Grispos et al.، 2013).

حفظ شواهد دیجیتال, بخش حیاتی از فرایند تحقیق دیجیتال را تشکیل می دهد. در رایانش ابری، به دلیل ماهیت توزیع داده ها، این یک گام بسیار پیچیده است (Grispos et al.، 2013). شواهد دیجیتال بسیار شکننده و دارای قابلیت تغییر یا حذف آسان هستند. بنابراین، یکپارچگی شواهد بایستی حفظ شود، تا اطمینان حاصل شود که داده ها در فرم اصلی خود هستند, همان گونه که (یا نزدیک به آن) یافت شده اند و زنجیره دقیق نگهداری از این مرحله تا پایان فرآیند تحقیق ایجاد می شود. علاوه بر این، شواهد باید جمع آوری و به طور ایمن نگهداری شوند تا ثبت شوند (Brezinski & Killalea، 2002؛ Damshenas et al.، 2012).

در حقیقت، حفظ شواهد، یک فرایند یک مرحله ای نیست؛ این فرآیند ادامه می یابد تا زمانی که شواهد در دادگاه ارائه شوند. مرحله نگهداری قبل از مرحله کسب شواهد با قفل کردن یا انجماد شواهد مرتبط است که آماده سازی

برای جمع آوری آنها می باشد. همانطور که پلت فرم ابر بسیار پویا است، این مرحله بسیار حیاتی است. جدول ۲ چالش های موجود در مرحله حفاظت و راه حل های احتمالی آنها را مشخص می کند.

زنجیره نگهداری (امانت)

برای فرایند پزشکی قانونی معمول، زنجیره نگهداری می تواند به عنوان "یک نقشه راه تعریف شود که نشان می دهد که چگونه شواهد جمع آوری، تحلیل و حفظ می شوند تا به عنوان مدرک در دادگاه ارائه شوند" (Grispos et al.، 2013). محققان و دست اندرکاران حقوقی, اهمیت حفظ زنجیره مناسب فهرست نگهداری را برجسته کرده اند. به عنوان مثال، در انگلستان، انجمن افسران ارشد پلیس (ACPO) راهنمایی برای شیوه ها و اصول خوب برای شواهد الکترونیکی مبتنی بر کامپیوتر را ارائه می دهد که در آن اصل ۳, ضرورت حفظ رد حسابرسی یا سابقه دیگر فرایندها را بیان می کند (ACPO، 2012). آدامز (۲۰۱۳) اشاره کرد که نگهداری یک زنجیره نگهداری برای رعایت اصول ACPO ضروری است. Shipley و CFE (2007) اظهار داشتند: "زمینه های اصلی جمع آوری شواهد دیجیتال شامل جمع آوری داده ها به شیوه ای سازگار با قانون، تایید داده های جمع آوری شده و نگهداری یک زنجیره مناسب از نگهداری شواهد جمع آوری شده" می شود. اگر چه هیچ راه منفرد برای اجرای زنجیره نگهداری در پزشکی قانونی دیجیتالی وجود ندارد، استفاده از تکنیک هایی مانند مهرزنی زمانی، هش کردن و نشانه های الکترونیکی, محوریت همه روش ها هستند (Shipley and CFE، 2007).

یکی از راه های ایجاد زنجیره نگهداری برای شواهد دیجیتال, با استفاده از امضای RSA است. امضای RSA یک سیستم رمزنگاری کلید عمومی برای دسترسی امن به داده ها است. لین و همکاران (۲۰۱۲) یک طرح امضاء RSA با کمک ابر برای پلمب کردن و ذخیره شواهد دیجیتالی در ابر پیشنهاد دادند. تکنیک پیشنهادی تا حد زیادی به جمع آوری و ذخیره ایمن شواهد کمک می کند، به ویژه از دستگاه های تلفن همراه که محدودیت های قدرت محاسباتی و ذخیره دارند. امضای دیجیتال نیز می تواند برای اجرای یکپارچگی داده ها استفاده شود و علاوه بر آن ایجاد زنجیره نگهداری از شواهد پس از توقیف نیز می تواند مورد استفاده قرار گیرد. یک محقق می تواند کنترل هایی را بر روی آثار انجام دهد و از طریق کلید خصوصی خود, علامت کنترل را به صورت دیجیتالی امضا کند.

جداسازی شواهد

به طور پیش فرض، رایانش ابری، یک محیط چندمستاجر است. مشخصات چندمستاجر دارای مشکلات در جداسازی و حفظ شواهد بدون ممانعت از دیگر مستاجرین است که منابع مشابه را به اشتراک می گذارند. یک راه حل برای جداسازی شواهد, سندباکس کردن هر نمونه کاربر است

سندباکس کردن یک مکانیزم است که به واسطه آن, برنامه های در حال اجرا به حوزه های مجازی تقسیم می شوند و هر یک از حوزه خاص خود استفاده می کند به گونه ای که هیچ نمونه ای نمی داند که یک همسایگی وجود دارد. همسایگان چنان رفتار می کنند که انگار در میزبان های جداگانه قرار دارند. ضبط کردن کل نمونه های ساندباکس، حالت فعلی نمونه های ماشین مجازی کاربران را در آن لحظه فراهم می کند، که می توان آن را در یک نمونه VM برای تحلیل بارگذاری کرد.

اگر چه مکانیسم فوق به طور جزئی مشکل را حل می کند، ما معتقدیم که راه حل هایی که از سطح ورود فراناظر استفاده می کنند، حاوی اطلاعات سطح سیستم در مورد تمام مستاجران, مانند ایجاد و حذف نمونه های ماشین مجازی هستند، چرا که چنین فهرست هایی مربوط از یک حساب کاربری نرمال دردسترس نیستند و علاوه بر این این فهرست ها به طور بالقوه حاوی اطلاعات در مورد دیگر مستاجرین می باشند.

ذخیره توزیع شده

با توجه به ماهیت توزیع شده و انعطاف پذیر رایانش ابر، اغلب نمی توان تعیین کرد که بخشی از داده ها در کجا ذخیره می شود، زیرا می تواند در بین بسیاری از میزبان ها در چندین مرکز داده توزیع شود. برچسب گذاری نمونه های مجازی (.Hay et al، 2011)، که در بخش ۳,۱,۱ توضیح داده شده، یک راه حل بالقوه برای این است.

فراریت داده ها

ماهیت بسیار فرار داده ها, نگرانی عمده در مورد حفظ و جمع آوری شواهد در یک محیط ابر محسوب می شود. محققان, ذخیره سازی مستمر برای رفع موضوع فراراریت داده ها را پیشنهاد داده اند. ذخیره سازی مداوم و حفظ

ذخیره سازی همگام سازی شده بین نمونه های VM و ذخیره سازی مداوم توسط محققان برای مقابله با مشکلات نوسان سازی پیشنهاد شده است (Birk and Wegener، 2011؛ .Damshenas et al، 2012). با این وجود داده های روی سیستم در حال اجرا که توسط یک دشمن به خطر می افتند قابل کاهش نیستند، اگرچه نشانه هایی از چنین اقدامات نامناسب برای ذخیره سازی مداوم به عنوان یک شواهد در دسترس خواهند بود. توجه داشته باشید که CSP ها معمولاً یک ذخیره سازی ماندگار را به عنوان یک سرویس کلی ارائه نمی کنند، که این کار می تواند در هنگام متوقف شدن یا خاموش شدن VM توسط یک دشمن, موجب از دست دادن داده های حیاتی شود. علاوه بر این، ارائه ذخیره سازی ماندگار در برابر ماهیت برحسب-تقاضا، هزینه کم و الاستیک ابر، پاسخگو است. در حالی که همگام سازی ذخیره سازی داده های فرار به ذخیره سازی غیر ابری، از لحاظ نظری امکان پذیر است، پیاده سازی این کار عملی نیست و ممکن است به شکست در هدف کلی اتخاذ سیستم های ابر منجر شود. بنابراین، به محض اینکه حادثه شناسایی شده باشد، جمع آوری داده های پزشکی قانونی بسیار حیاتی است. این موضوع در بخش ۳,۳ توضیح داده شده است.

شماره	چالش ها	راه حل های پیشنهادی	اظهارنظرات
1	زنجیره نگهداری و انسجام داده ها	امضای RSA (Lin et al., 2012)	می توانند برای اعتبارسنجی زنجیره نگهداری استفاده شوند.
2	جداسازی شواهد	ساندباکس کردن	برنامه های در حال اجرا توسط مکان های مجازی تفکیک می شوند
3	ذخیره توزیع شده	VM در برچسب گذاری نمونه (Hay et al., 2011)	VM برچسب گذاری شده در نمونه ها را می توان برای شناسایی موقعیت مکانی استفاده کرد
4	فراریت داده ها	ذخیره مستمر (Birk and Wegener, 2011; Damshenas et al., 2012)	فراهم نمودن ذخیره پایدار, ماهیت کشسانی رایانش ابری را خراب می کند.
5	انسجام داده ها	الگوریتم های مجموع کنترل (e.g., MD5, SHA1 SHA256)	

یکپارچگی داده

یکپارچگی داده ها اطمینان می دهد که شواهد، یک نمایش دقیق داده های یافته شده در سیستم رایانه ای است. چندین جنبه از محیط ابر روی یکپارچگی داده ها تاثیر می گذارد، اما حفظ یکپارچگی همچنان یک جنبه حیاتی از پزشکی قانونی ابر است. روش شناخته شده برای حفظ یکپارچگی داده ها، استفاده از تکنیک های هش اثبات شده مانند MD5، SHA1 SHA256 است.

جمع آوری یا کسب

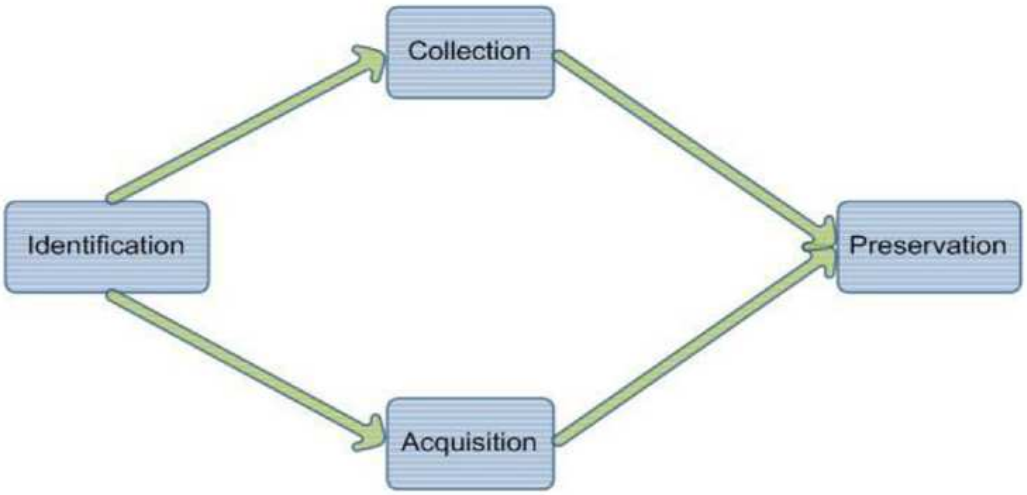
در پزشکی قانونی دیجیتال، جمع آوری به "فرایند جمع آوری آیتم هایی اشاره می کند که حاوی شواهد بالقوه دیجیتالی" هستند، و کسب به "فرایند ایجاد یک کپی از داده ها در یک مجموعه تعریف شده" اشاره دارد (CSA، 2013a). به دلیل ماهیت زودگذر محیط ابر و عدم دسترسی به فایل های سیستم عامل و آثار مانند فایل های موقت اینترنت و رجیستری, جمع آوری شواهد دشوار است. سیستم های ابر عمومی و هیبرید (ترکیبی) می توانند در سراسر حوزه های قضایی عمل کنند، که کسب آثار را تقریباً دشوار می سازند. به استثنای اینکه برنامه های کاربردی رایانش ابر, یک دنباله حسابرسی کامل را فراهم کنند، استخراج شواهد به روش قابل قبول مشکل است، یا ممکن است شواهد کمی برای استخراج وجود داشته باشد (Taylor et al.، 2010).

جمع آوری حقوقی به ضبط شواهد فیزیکی تحت اختیار رسمی یک دستور حقوقی (یعنی حکم تفتیش) اشاره دارد. با توجه به موضوع حوزه قضائی و چندمستاجر بودن مرتبط با محیط ابر، جمع آوری عملی نیست و بنابراین کسب, فرایند توصیه شده است. توجه داشته باشید که جمع آوری نیاز به پشتیبانی CSP دارد در حالیکه کسب می تواند از راه دور با استفاده از روش ها و ابزارهای معتبر انجام شود، که بعداً شرح داده می شود. فرایند کسب (ساخت یک نسخه معتبر حقوقی از تمام آثار پزشکی قانونی) باید با استفاده از یک فرآیند به خوبی تعریف شده، به خوبی آزمایش شده و قابل تکرار، با استفاده از ابزارهای قابل اعتماد انجام شود. بدین ترتیب، کسب فرایند چالش برانگیزتر از جمع آوری است. بر اساس ایزو ۲۷۰۳۷، همانطور که در شکل ۳ نشان داده شده است، جمع آوری و کسب, دو فرآیند موازی است (ISO 27037، 2012).

جدول ۳ خلاصه ای از چالش های موجود در مرحله کسب در رایانش ابری و راه حل های ممکن یا پیشنهاد شده را ارائه می دهد.

عدم قابلیت دسترسی

با توجه به ماهیت رایانش ابری، دسترسی غیرمحدود به ذخیره سازی ابر امکان پذیر نیست، چیزی است که در محیط مشتری-سرور سنتی تضمین شده است. توجه داشته باشید که داده ها در ابر را می توان به چندین مکان تکثیر کرد، که منجر به آثار غیرمتمرکز می شود. برخی از ارائه دهندگان ابر، مانند آمازون، کاربران را قادر می سازد تا موقعیت جغرافیایی خود را در هنگام ایجاد نمونه های VM، انتخاب کنند. حتی اگر مکان شناخته شده باشد، کسب فیزیکی به دلیل ماهیت چندمستاجری ممکن نیست.



شکل ۳. فرایند هدایت شواهد مطابق با ISO 27037 (CSA, 2013a).

محققان, روش های مختلفی برای کسب شواهد از ابر پیشنهاد کرده اند، مانند:

- کسب داده ها از راه دور: این کار به کسب شواهد از راه دور بر روی یک کانال قابل اعتماد و امن اشاره می کند. ابزارهای به طور گسترده استفاده شده پزشکی قانونی مانند Guidance EnCase و Access Data FTK از کسب داده ها از از راه دور پشتیبانی می کنند (Dykstra and Sherman، 2012). Dykstra و Sherman (2012) بازیابی موفق داده فرار و غیرفرار از پلت فرم نمونه کاربر فعال ابر آمازون EC2 با استفاده از ابزارها را گزارش نمودند،

علی رغم اشاره به بسیاری از لایه های اعتماد مورد نیاز. آنها یکپارچگی داده ها را با محاسبه و مقایسه هش ها از تصاویر, قبل و بعد از دانلود داده ها تأیید کردند.

- صفحه مدیریت: کنترل دارایی های مجازی در ابر با استفاده از یک واسطه وب اغلب به عنوان صفحه مدیریت نامیده می شود. با استفاده از واسطه، مانند کنسول مدیریت AWS آمازون، کاربران می توانند کسب داده های آثار پزشکی قانونی مانند تصویر VM، فهرست ها، تصاویر دیسک، اطلاعات دسترسی کاربر و غیره را انجام دهند. میتوان از کنسول مدیریت AWS برای استخراج فهرست های CloudTrail بدون کمک از CSP استفاده کرد (AWS Security Center 2013a). با این حال، یک سطح دیگر از اعتماد، یعنی اعتماد اربرد کنسول مدیریت، مورد نیاز است. به رغم مسئله اعتماد، محققان, استفاده از صفحه مدیریت برای کسب از راه دور داده ها، به ویژه برای مدل IaaS را پیشنهاد نموده اند (Dykstra and Sherman، 2012؛ Zawaod and Hasan، 2013). ظفرالله و همکاران (۲۰۱۱) نشان دادند که امکان جمع آوری فهرست های لازم از زیرساخت ابر با استفاده از ابزارهای منبع باز وجود دارد. برای تأیید هویت کاربر می توان از شناسایی چند-عامل استفاده کرد و تصویر دیسک را از سرور ابر با استفاده از پروتکل تونل زنی رمزنگاری، به عنوان مثال، شبکه خصوصی مجازی (VPN)، برای اطمینان از محرمانه بودن و یکپارچگی داده ها و همچنین حل مسئله زنجیره نگهداری شرح داده شده در بخش ۳,۲,۱ کسب کرد.
- پزشکی قانونی زنده: پزشکی قانونی روی یک سیستم در حال اجرا، به عنوان پزشکی قانونی زنده شناخته می شود، که در آن یک محقق, معاینه پزشکی قانونی یک سیستم را در حالت در حال اجرا انجام می دهد. چنین پزشکی قانونی با یک مزیت اضافه شده همراه است, زیرا قادر به جمع آوری مجموعه ای از اطلاعات، مانند فهرست فرایند، ماژول های کرنل، گزارشات شبکه باز، داده های حافظه فرار و غیره، از سیستم در حال اجرا، علاوه بر اطلاعات ذخیره شده در حافظه ماندگار است. Virtual)درون نگاری (VMI) Machine Introspection) یک روش پزشکی قانونی زنده است که در آن, کاربر می تواند با یک سیستم در حال اجرا از برخی از ماشین های مجازی دیگر، به غیر از آنچه که مورد معاینه است، تعامل داشته باشد. هی و نانس (۲۰۰۸), یک راه حل درون نگاری مجازی را پیشنهاد دادند. آنها راه حل خود را با استفاده از درون نگری مجازی برای مجموعه Xen (VIX) ابزارها به عنوان یک اثبات

مفهوم نشان دادند. این به عنوان یک کتابخانه درون نگاری شناخته شده به نام LabVMI (VMITools) ارتقا یافته است. با این حال، ابزارهای پزشکی قانونی زنده هنوز به عنوان یک سرویس تجاری توسط CSP ثبت و فراهم نشده اند.

- تحلیل عکس فوری: عکس فوری, یک فرآیند گرفتن یک نسخه از تصویر مجازی در حالت در حال اجرا، از جمله تمام حافظه سیستم، و ذخیره این نسخه در یک حافظه ماندگار است. تکنولوژی عکس فوری مشتری را قادر می سازد حالت خاصی از VM را منجمد کند (Birk and Wegener، 2011). بسیاری از فروشندگان فراناظر، مانند Xen، VMWare، ESX و Hyper-V، از ویژگی عکس فوری پشتیبانی می کنند. اگر چه تصاویر عکس فوری, نسخه بیت به بیت از منابع مربوطه خود نیستند، آنها اطلاعات ارزشمندی در مورد وضعیت در حال اجرای یک سیستم ارائه می دهند. تصاویر عکس لحظه ای را می توان با بارگذاری آنها در یک VM هدف برای تحلیل بازگرداند. ویژگی عکس فوری می تواند نمونه VM و همچنین کارها در مناطق غیرمتمرکز زنده را ضبط کند، تا زمانی که نمونه ها در زیرساخت منطقی باقی بمانند. از آنجا که محیط ابر تحت تغییرات سریع قرار دارد، یک سری از تصاویر فوری در طول یک دوره زمانی می توانند اطلاعات ارزشمندی در مورد تغییرات برای دارایی های داده ها فراهم کنند که می توانند برای تحلیل و نقشه برداری بر روی یک خط زمانی رویدادها استفاده شوند. بنابراین، برای آماده بودن یک ابر از پزشکی قانونی، باید یک ویژگی داخلی باید داشته باشد تا تصاویر فوری ماشین مجازی را به صورت اتوماتیک در بازه های قابل پیکربندی انباشت نماید، زیرا دانستن زمانی که نقص امنیتی رخ می دهد مشکل است. در سمت پایین, این ویژگی به فضای ذخیره سازی بیشتری نیاز دارد و می تواند مسائل مربوط به عملکرد را ایجاد کند. با این وجود، مدیران سیستم می توانند از بین بردن تصاویر ناخواسته یا تمیز کردن یا بازنویسی آنها را انجام دهند.

وابستگی به CSP

بسیاری از محققین وابستگی به CSP ها را در طول فرایند تحقیق پزشکی قانونی مورد بررسی قرار داده اند (Dykstra and Sherman، 2011؛ Zawaod and Hasan، 2013). در حالی که شایع نیست، CSP ها برای ارائه ابزارهای مدیریتی حرکت می کنند، به طوری که مشتریان بتوانند آثار را جمع آوری کنند. برای حل مسئله

وابستگی، می توان از مدیریت برنامه ریزی و SLA های خاص استفاده کرد، که در بخش ۳,۳,۱ و ۳,۱,۴ توضیح داده شده است. قطعنامه تهیه شده و اجرای موافقتنامه سطح خدمات بین ارائه دهنده و مصرف کننده یکی از عناصر کلیدی برای رسیدگی به چالش وابستگی CSP است. SLA باید عناصر پزشکی قانونی خاص نظیر نظارت، خدمات پشتیبانی پزشکی قانونی، مالکیت داده (به ویژه داده های تحت بررسی)، مسئولیت، حق نگهداری داده های مصرف کننده را برای هدف تحقیق حل و فصل نمایند، حتی زمانی که مصرف کننده تصمیم به تغییر ارائه دهنده ابر، و تنظیمات انطباق با حریم خصوصی (Alhamad et al.، 2010؛ Ruan et al.، 2012) می گیرد

جدول ۳ مرحله جمع آوری: چالش ها و مراحل پیشنهادی

شماره :	چالش ها	راه حل های پیشنهادی	اظهارنظرات
1	عدم قابلیت دسترسی	کسب داده ها از راه دور (Dykstra and Sherman, 2012)	با ابزارهای تصویربرداری داده ها مانند EnCase, FTK Imager, X-Ways, F-Response, Paladin etc., روی یک لینک شبکه امن
		صفحه مدیریت (Dykstra and Sherman, 2012; Zawaod and Hasan, 2013)	گزینه ترجیحی, وابستگی به CSP را حذف می کند
		پزشکی قانونی زنده (Hay and Nance, 2008)	اطلاعات سیستم در حال اجرا مانند فهرست فرایند, پورت های باز و غیره را فراهم می کند که در پزشکی قانونی آنلاین دردسترس نیستند
		تحلیل تصویر فوری (Birk and Wegener, 2011)	اطلاعات کلی سیستم را در لحظه گرفتن تصویر فوری ضبط می کند
2	وابستگی به CSP	صفحه مدیریت (Dykstra and Sherman, 2012; Zawaod and Hasan, 2013)	گزینه ترجیحی, اما به یک سطح اضافی از "اعتماد" صفحه مدیریت نیاز دارد
		SLA (Alhamad et al., 2010; Kandukuri قوی تر	گزینه ترجیحی برای مشتریان

		)et al., 2009	
تصویر نقطه در زمان سیستم کلی را ارائه می دهد		تحلیل تصویر فوری (Birk and Wegener, 2011)	3
طراحی شده برای کار با سیستم عامل تک, در مقیاس بندی یک محیط ابر مجازی ناموفق است,		مدل پلت فرم مورد اطمینان سخت افزاری (TPM)	4
نمونه های TPM بر حسب تقاضا به دست می آیند, مسئله قابلیت مقیاس بندی را حل می کند		TPMهای مجازی (Dongxi et al., 2010)	
رویکرد ماژولار و قابل گسترش که از ذخیره ماندگار کلیدها حمایت می کند		ماژول محیط مجازی مورد اطمینان (Krautheim et al., 2010)	
یک محیط اجرای جعبه بسته فراهم می کند . محرمانگی و انسجام را تضمین می کند.		پلت فرم رایانش ابر مورداعتماد (Santos et al., 2009)	
رویکرد پیشگیرانه رسمی را تکمیل می کند و می تواند به ریسکی بپردازد که از درون CSPها ناشی می شود.		کنترل های تشخیصی (Ko et al., 2011)	
روش های مختلف بحث شده جداسازی نمونه های ابر.		جداسازی نمونه ابر (Delport et al., 2011)	چندمستاجری بودن 5
محبوب ترین روش جداسازی نمونه ابر و به طور گسترده حمایت شده توسط فروشندگان.		ساندباکس کردن (Delport et al., 2011; Greamo and Ghosh, 2011)	
به طور جزئی بررسی شده در (Alhamad et al., 2010; Kandukuri et al., 2009)	SLA	حوزه قضائی	6
مثلا: معاهده های کمک قانونی متقابل بین المللی (MLAT) (INCSR, 2012)		همکاری بین المللی به شکل توافقات و معاهده ها	
مشکل به دست آوردن و مدیریت ناشی از		تصاویر فوری غالب	داده های حذف شده 7

حجم های برشی تصاویر فوری راه حل های پیشنهادی همچنان باید تجاری سازی شوند.	تصویربردار داده های ابر (Federici, 2014).	فقدان متخصص ابزارهای تجاری	8

ماهیت زودگذر

ماهیت فصلی داده های ابر یکی دیگر از مسائل مهم در دستیابی به اطلاعات است. به عنوان مثال فایل های رجیستری، فایل های موقت، فهرست های تاریخچه دسترسی به اینترنت و غیره، آثار کلیدی پزشکی قانونی هستند؛ با این حال، جمع آوری داده هایی از این دست از یک محیط ابر ممکن است مشکل باشد. در گزارش CSA, اهمیت کسب داده های فرار در ابر ذکر شده است (CSA، 2013a). تصویربرداری دوره ای نمونه های VM که در بخش ۳,۳,۱ توصیف شده است، یک راه حل ممکن است.

اعتماد

به طور کلی، اعتماد به معنای عمل مطمئن با اعتماد و تکیه بر چیزی است که انتظار می رود به صورت وعده داده شده, رفتار کند یا تحویل شود (خان و مالوشی، ۲۰۱۰). در زمینه رایانش ابری، اعتماد، اعتقاد به شایستگی و تخصص CSP ها و معماری ابر و سیستم های پایه ای است که به طور منطقی به دارایی های اطلاعات ارزشمند کاربران احتیاج دارند. *اعتماد* و *کنترل* همراه با هم هستند، مثلا ما به یک سیستم کمتر اعتماد کنیم، اگر دارای کنترل ضعیف باشد. اعتماد نیز تابعی از *مالکیت* است، به عنوان مثال، شما به دارایی داده های شخصی خود اعتماد می کنید. توجه داشته باشید که در یک مدل ابر عمومی، ارائه دهنده خدمات, نگهبان دارایی داده های مشتری است و مشتریان هیچ مالکیت و کنترلی بر محیط ندارند. هنگامی که یک شرکت, ابر را می پذیرد و داده های خود را (متعلق به شرکت و مشتریان آن) به ابر تحویل می دهد، یک آرایه از روابط اعتماد پیچیده را را ایجاد می کند. اولاً، شرکت باید به ارائه دهنده ابر اعتماد کند. دوم، شرکت باید اطمینان حاصل کند که مشتریانش به اندازه کافی دلیلی

برای اعتماد به همان ارائه دهنده دارند. در ابر، فقدان شفافیت و اعتماد منجر به داده های شواهد غیرقابل اعتماد می شود (Birk and Wegener، 2011؛ خان و مالوشی، ۲۰۱۰).

محققان, مساله مربوط به اعتماد در حوزه پزشکی قانونی ابر را برجسته کرده اند (Birk and Wegener، 2011؛ Hay and ،Dykstra and Sherman ،2012؛ Daryabar et al. ،2013؛ Damshenas et al. ،2012؛ Nance، 2008؛ Hay et al. ،2011 ؛ زوائد و حسن، ۲۰۱۳). لایه های مختلف اعتماد برای مدل ابری IaaS عبارتند از: Network، Hardware Physical، OS Host، Virtualization، Guest OS، Application، Guest / Data (Dykstra and Sherman، 2012). معتبر بودن این شواهد به ایجاد اعتماد در لایه های مدل ابر استفاده شده نیاز دارد. لایه های اعتماد به طور جمعی افزایش می یابد زیرا سرویس های بیشتری از CSP مشترک می شوند، یعنی لایه های اعتماد برای مدل SaaS بالاتر هستند و برای مدل IaaS کمترین هستند. شکل ۱ لایه های اعتماد را توصیف می کند.

حل مسئله اعتماد برای پزشکی قانونی ابر همچنان یک چالش بزرگ است. اعتماد را نمی توان به تنهایی با استفاده از فن آوری حل کرد. بلکه راه حل باید ترکیبی از فرآیند، مردم و تکنولوژی باشد. به دنبال یک فرآیند پزشکی قانونی، مانند دستورالعمل های ACPO، داشتن افراد گواهی شده یا باتجربه مناسب برای انجام جمع آوری و ارزیابی پزشکی قانونی و استفاده از نرم افزار یا ابزار سخت افزاری به رسمیت شناخته شده صنعت همراه با تقویت اعتماد به شواهد مفید خواهند بود.

اعتماد نیز می تواند به عنوان یک تابع از امنیت مورد توجه قرار گیرد. مصرف کنندگان به سیستم هایی که بیشتر امن هستند اعتماد می کنند. امنیت, یک عامل اعتماد در یک محیط IT است. در زمینه رایانش پزشکی قانونی محرمانه و اعتماد ابر، در نهایت، ما در جستجوی ابزار، روش ها و افراد قابل اطمینان برای شناسایی، به دست آوردن و تحلیل داده های پزشکی قانونی هستیم، به طوری که شواهد ارزش اعتماد کردن داشته باشند. به عبارت دیگر، شواهد جمع آوری شده از یک سیستم امن تر قابل اعتمادتر خواهند بود. یکی از رویکردهای پذیرفته شده گسترده

برای حل مسائل امنیتی، استفاده از مدل پلت فرم مورداعتماد (TPM) است که به طور خلاصه در زیر شرح داده شده است.

- TPMهای سخت افزاری: فروشندگان سخت افزاری وجود دارند که تراشه TPM را به مادربرد مجتمع می کنند، که قادر به تصدیق هویت پلت فرم است. TPM حاوی یک کلید خصوصی تایید شده با تراشه است که به طور منحصر به فرد سخت افزار (به این ترتیب میزبان فیزیکی) پشتیبانی شده توسط توابع رمزنگاری که قابل اصلاح نیستند را شناسایی می کند. سازنده تراشه, کلید عمومی مربوطه را برای اعتبارسنجی صحت تراشه و اعتبار کلید امضا می کند. با این حال تراشه های TPM معمولاً برای کار با سیستم عامل تک در یک دستگاه طراحی می شوند و معمولاً با مجازی سازی سیستم - مشخصات پیش فرض رایانش ابری مقیاس بندی نمی شوند.
- TPM مجازی (VTPM): TPM مجازی یک رویکرد جدید برای حل مسئله اعتماد است، که در آن, TPMها در ابر به عنوان نهادهای مجازی قرار می گیرند. یک نمونه TPM از ابر TPM بر حسب تقاضا قابل اخذ است، و در نتیجه عملکرد TPM حتی در سیستم عامل هایی که تراشه های TPM ندارند نیز قابل حصول است. این تکنیک برای نمونه های مجازی بسیار مقیاس بندی می شود که در آن می توان به نمونه های مشابه TPM از نمونه ها یا مکان های مختلف VM دسترسی پیدا کرد و کاربران می توانند از قابلیت TPM بدون داشتن تراشه TPM استفاده کنند (Dongxi et al.، 2010).
- ماژول محیط مجازی معتبر (TVEM): با استفاده از یک مدل رابطه اعتماد,TVEM به حل مسئله اعتماد کمک می کند و طرفین را قادر می سازد ارتباط اعتماد بین مالک اطلاعات و محیط مجازی را بر روی یک پلتفرم متعلق به CSP برقرار کنند. مولفه اصلی TVEM, کلید منحصر به فرد محیط مورداعتماد محسوب می شود که اعتماد از مالک اطلاعات و ارائه دهنده خدمات را ترکیب می کند تا یک ریشه اعتماد دوگانه ایجاد کند که برای هر محیط مجازی متمایز است و از اعتماد پلت فرم میزبانی منفک است. معماری TVEM مدولار و قابل انعطاف است که انعطاف پذیری و همچنین ذخیره سازی پایدار برای کلید ها (Krautheim و همکاران، ۲۰۱۰) را میسر می سازد.

- پلت فرم رایانش ابری مورداعتماد (TCCP): با گسترش مفهوم پلت فرم مورداعتماد به محیط IaaS، TCCP, یک محیط اجرای جعبه محدود را فراهم می کند. TCCP, محرمانه بودن و یکپارچگی را تضمین می کند و به کاربران اجازه می دهد که به ارائه دهنده IaaS شهادت دهند که سرویس آن, قبل از راه اندازی VMها امن است. این امر با ارائه یک چکیده از محیط جعبه بسته برای VM مشتری حاصل می شود، که تضمین می کند که هیچ یک از مدیران ممتاز ارائه دهنده ابر نمی توانند محتوای آن را بازرسی و یا تحت تأثیر قرار دهند (سانتوس و همکاران، ۲۰۰۹).
- کنترل های تشخیصی: این یک روش ایجاد اعتماد به ابر را با استفاده از تشخیص (کارآگاهی) است، به جای روشهای پیشگیرانه و به تبع آن موجب ارتقای پاسخگویی می شود. کنترل های تشخیصی بر اساس سیاست و فرآیند است که کنترل های پیشگیرانه را تکمیل می کنند. مزیت این رویکرد اینست که غیر تهاجمی است و نیاز به ساختار سیاست و اداره امور برای هر دوی مصرف کننده و ارائه کننده ابر را اجرا می کند و در نتیجه مسئولیت پذیری و اعتماد را ایجاد می کند (Ko et al.، 2011).

چندمستاجری بودن

یکی از ویژگی های اصلی رایانش ابری اینست که چندین VM، که میزبان چند مستاجر هستند, می توانند یک سخت افزار فیزیکی را به اشتراک بگذارند و می توانند در میان مراکز داده مختلف پخش شوند. این مدل بسیار متفاوت با سیستم تک مالک است، جایی که تصرف سخت افزار آسان می شود. جنبه چندمستاجری به پیچیدگی جمع آوری داده های پزشکی قانونی در ابر می افزاید. اگرچه VMها در سندبکس های خودشان بدون شناخت از وجود همسایگان خود کار می کنند، انجام یک تصرف فیزیکی هرگز عملی نیست، زیرا می تواند داده های دیگر مشتریان را حفظ کند. CSP ها ملزم به حفظ حریم خصوصی مشتریان هستند و از مقررات اطاعت می نمایند. برای مثال, یک گزارش ۲۰۱۲ توسط ENISA تأکید کرد که خدمات برونسپاری شده چندمستاجری باید از حریم خصوصی مستاجران همزمان محافظت کند (Hogben and Dekker، 2012). علاوه بر این Ruan و همکاران (۲۰۱۲) مشخص کردند که SLA ها باید به مسئله حفظ حریم خصوصی پاسخ دهند و اشاره کردند که "*ارائه کننده*

ابر, منابع داده های پزشکی قانونی را که حاوی داده های متعلق به چندین مستاجر می شود, دقیقا و به طور جامع فیلتر کند و فقط داده های مرتبط با یک مستاجر خاص را منتشر می کند".

محققان, استفاده از صفحه مدیریت برای کسب داده های پزشکی قانونی را پیشنهاد نموده اند. Dykstra و Sherman (2012) از ابزارهای پزشکی قانونی مانند EnCase و FTK استفاده کردند تا به طور موفقیت آمیز شواهد را از ابر EC2 آمازون بدون نقض حریم خصوصی سایر مستاجران بازگردانند. برخی از CSP ها، مانند آمازون، در هنگام ایجاد یک نمونه با هزینه های اضافی، یک گزینه مستاجر تک را ارائه می دهند. سایر راه حل های پیشنهادی عبارتند از:

- جداسازی نمونه ابر: دلپورت و همکاران. (۲۰۱۱) یک مفهوم جدید از جدا کردن نمونه ابر را برای تسهیل بررسی های پزشکی قانونی، با استفاده از روش های مختلف مانند مکانیابی دوباره نمونه، مکانیابی دوباره آدرس جابجایی، چارچوب بندی سرور و غیره معرفی کردند. موارد جداشده می توانند مانع از آلودگی یا سوء استفاده بیشتر از شواهد احتمالی شوند.
- سندباکس کردن: ایجاد تصویر سندباکس و نمونه ماشین مجازی، روش دیگری برای جداسازی و حفاظت از شواهد است (Delport et al.، 2011؛ Greamo & Ghosh، 2011). سندباکس کردن یک گزینه به راحتی قابل اجرا است و اکثر فروشندگان از ویژگی سندباکس کردن پشتیبانی می کنند. سپس تصاویر VM سندباکس شده می توانند با استفاده از روش های خرید از راه دور کسب شوند.

حوزه قضائی

CSPها اغلب معکوس نمودن داده ها را برای تضمین قابلیت دسترسی و تداوم کسب و کار می کنند. پایگاه داده های معکوس شده می تواند در حوزه قضائی متفاوت از مکان اصلی باشند، که موجب فقدان اطلاعات زمان واقعی در مورد مکان داده ها و همچنین ایجاد درجه بالا از مشکلات برای کسب داده ها می شود. مسئله قضائی مربوط به موقعیت داده ها, یکی از نگرانی های اصلی مشتریان است. مصرف کننده ابر باید آگاه باشد که انجام تحقیق و بازرسی، زمانی که داده ها در حوزه های قضایی با مقررات مناسب نباشند, دشوار خواهد بود (Ruan et al.، 2013).

یک راه حل ممکن برای حل این مشکل، استفاده از SLA خاص است که در بخش ۳,۱,۴ توضیح داده شده است، که مشتریان می توانند مشخص کنند کجا داده ها می توانند ذخیره یا نقل مکان شوند. ارائه دهنده ابر همچنین باید با دقت صلاحیت قضائی را که در آن داده های مصرف کننده ابر در طول یک دوره معین قرار می گیرند ردیابی کند (Ruan et al.، 2012). اگر دارایی های داده ها در زیرساخت های منطقی در اطراف مکان های مختلف پخش شده باشند، می توان آنها را با استفاده از تکنیک های اثبات شده نظیر کسب داده های از راه دور و یا ابزارهای دردسترس تجاری کسب کرد. علاوه بر این، اگر داده ها از مرزهای جغرافیایی عبور کنند، همکاری و موافقت نامه های بین المللی قوی تر نیز برای جمع آوری آثار شواهد، ایجاد زنجیره نگهداری و غیره مورد نیاز خواهد بود (تیلور و همکاران، ۲۰۱۱). به عنوان مثال، توافقنامه های بین المللی در قالب معاهده های کمک حقوقی متقابل (MLAT) که بین ایالات متحده و سایر کشورها وجود دارد، امکان تبادل اطلاعات و اطلاعات در فعالیت های جنایی را فراهم می کند (INCSR، 2012). کنوانسیون جرایم سایبری، که در نوامبر ۲۰۰۱ در بوداپست برگزار شد، چارچوب پزشکی قانونی مبارزه با جنایات سایبری را مشخص می کند؛ به ویژه ماده ۲۲ تا ماده ۲۵ در مورد حوزه قضائیی، همکاری بین المللی و اصول عمومی مربوط به کمک متقابل به منظور بررسی و یا رسیدگی به جرایم اینترنتی (DOS، 2001) بحث می کند.

پراساد (۲۰۱۲)، نیاز به چارچوب حقوقی بین المللی قوی تر و موثر را بیان می کند، با اشاره به اینکه کنوانسیون ها و معاهدات موجود بین المللی برای مبارزه با جرایم اینترنتی موثر نیستند، به ویژه هنگامی که مجرمان و قربانیان در حوزه قضائی متفاوت از یکدیگر قرار می گیرند. رهبری تشکل های جهان مانند سازمان ملل متحد برای تسهیل توافق میان کشورهای عضو، از جمله جمع آوری و به اشتراک گذاری اطلاعات توسط سازمان های اجرایی (Prasad، 2012) ضروری است.

داده های حذف شده

از دیدگاه پزشکی قانونی، داده های حذف شده و اختصاص دادن داده های حذف شده به یک کاربر خاص، منابع حیاتی از شواهد هستند. به طور معمول، داده های حذف شده را می توان از رسانه ها با استفاده از روش های حکاکی

داده پشتیبانی شده توسط ابزارهای پزشکی قانونی جمع آوری کرد. با این حال، در مورد ابر، فراریت و انعطاف پذیری محیط های ابر، جمع آوری داده های حذف شده را بسیار سخت تر می کند. Dykstra و Sherman 2012)) چگونگی کسب از راه دور سخت افزاری و تصاویر حافظه از ابر آمازون را نشان دادند. آنها همچنین با تحلیل تصویر و همچنین زمان بندی اقدامات انجام شده (در این مورد آنها یک سری از صفحات وب را ایجاد و حذف کردند)، بدون هیچ گونه ناهنجاری و یا چیز غیرعادی تا مشکوک برای یکپارچگی داده ها, کامل بودن داده ها را اثبات کردند. آنها همچنین می توانند ثابت کنند که جمع آوری داده های حذف شده (به شرطی که حجم داده ها توسط یک مستاجر مجددا بازنویسی نشده باشد) توسط همان مستاجر ممکن است، به جز داده ها یا داده های باقی مانده از مستاجر(های) قبلی که احتمالاً دارای یک فضای سخت افزاری مشابه بودند (Dykstra و شرمن، ۲۰۱۲). اگرچه این کار, مقررات مربوط به حفظ حریم خصوصی را رعایت می کند، اما کارکرد آن از دیدگاه پزشکی قانونی منفی است. افراد دارای قصد جنایی می توانند وظایف را با استفاده از ابر انجام دهند و حساب خود را خاتمه دهند، نمونه های VM را حذف کنند و بدون گذاشتن هر گونه رد از خود ناپدید شوند. CSP ها، در تلاش برای ارائه بیشترین احترام به حریم خصوصی، داده ها را زمانی به طور کامل حذف می کنند که توسط کاربران تایید شده باشد. به عنوان مثال، سیاست فعلی گوگل در مورد داده های حذف شده، موارد زیر را بیان می کند:

"پس از آنکه یک کاربر Google Apps یا ادمین Google Apps, یک پیام، حساب کاربری، کاربر یا دامنه را حذف می کند و حذف آن آیتم را تایید می کند (به عنوان مثال خالی کردن سطل آشغال)، داده های مورد نظر حذف می شوند و دیگر از آن واسطه Google Apps کاربر قابل دسترسی نیستند. سپس داده ها از سرورهای فعال Google و سرورهای تکرار حذف می شوند. اشاره گرها به داده ها در سرورهای فعال و تکراری Google حذف می شوند. داده های دوباره مورد ارجاع قرار گرفته با سایر داده های مشتری در طول زمان بازنویسی خواهند شد (Google 2014)».

بدین ترتیب این حقیقت برجسته می شود که بین قوانین حفظ حریم خصوصی و نیازهای پزشکی قانونی در ابر, یک گسستگی وجود دارد. حتی اگر داده های حذف شده در ابر یافت شوند، نسبت دادن آن به یک کاربر خاص به دلیل

حجم مناسبی از داده ها و میزان ارائه پشتیبان ابر, همچنان یک چالش بزرگ است (NIST، 2014b). گرفتن عکس های فوری مکرر از تصویر مجازی, یک راه حل ممکن است که در بخش ۳,۳,۱ توضیح داده شده است.

کمبود ابزارهای تخصصی تجاری

آثار کامل پزشکی قانونی همچنین شامل فراداده ها، تاریخچه بازبینی کامل فایل ها و تغییرات انجام شده برای محتوای فایل، محتویات رجیستری، پارتیشن حذف شده، فهرست های شبکه، الگوهای ترافیک و مهمتر از همه, فهرست های سطح فراناظر می باشد که اطلاعات حیاتی مانند زمان های ایجاد و حذف حساب کاربری نمونه ابر را فراهم می کنند. کمبود ابزارهای تجاری گواهی شده وجود دارند که می توانند برای کشف الکترونیکی و کسب داده ها برای اهداف پزشکی قانونی در محیط ابر به تمامیت آن مورد استفاده قرار گیرند. با این حال، محققان ثابت کرده اند که کسب داده ها از راه دور از یک حساب کاربری فعال (Dykstra and Sherman، 2012) امکان پذیر است. محققان همچنین دریافته اند که گستره وسیعی از آثار پزشکی قانونی در سمت های مشتری و سرور به عنوان بقایای داده ها، مانند فهرست های دایرکتوری، فایل های پیش از واکشی، فایل های لینک، ریزعکس ها، رجیستری، تاریخچه مرورگر و غیره باقی می مانند. علاوه بر این، مراجع فایل لینک هنوز هم وجود دارند حتی پس از آنکه ابزارهای پاک کردن فایل در مطالعات موردی انجام شده روی نمونه های مایکروسافت اسکیدریو و ownCloud گزارش شده اند (Martini and Choo، 2013؛ Quick and Choo، 2013). تمام این بقایای داده ها و مراجع فایل, بخشی از آثار پزشکی قانونی معتبر را تشکیل می دهد.

فدریکی (۲۰۱۴) کار مطرح شده توسط Quick و Choo (2013) را گسترش دادند و یک تصویربردار داده های ابر را ارائه دادند. فدریکی (۲۰۱۴) اشاره کرد که انگیزه این کار این است که رویکرد سنتی نسخه برداری جریان بیت ذخیره انبوه ممکن است در یک تحقیق در مورد اطلاعات مربوط به جرم و میزبانی در پلت فرم ابر امکان پذیر نباشد. برنامه های اختصاص داده شده برای کسب داده های از راه دور با معماری سالم از نظر پزشکی قانونی و الزامات تا به امروز گسترده نیستند و تصویربردار داده ها ابر, این شکاف را پر می کند. تصویربردار داده های ابر یک نرم افزار پزشکی قانونی اختصاصی برای ورود به مکالمه کامل با پلت فرم ابر در سطح برنامه و در متن واضح است که از جمع

آوری داده های از راه دور از ذخیره سازی ابر پشتیبانی می کند، و اصل قابلیت اطمینان و یکپارچگی شواهد دیجیتالی با اجرای خواندن فقط دسترسی (Federici، 2014) تایید می کند.

با این وجود، این نوع ابزارهای جامع و گواهی شده که مجموعه داده های انتها-به-انتهای پزشکی قانونی را فراهم می کنند، از جمله اطلاعات سطح فراناظر، تا به امروز خیلی گسترده نیستند. بنابراین، مصرف کننده یا محققان ابر باید برای ارائه مدارک به CSP ها بستگی دارند.

بررسی و تحلیل

هنگامی که آثار دیجیتالی به دست می آیند و حفظ می شوند، گام منطقی بعدی, فاز بررسی و تحلیل است. بررسی و تحلیل یکی از عناصر مهم رایانش پزشکی قانونی است. با توجه به NIST، *بررسی (معاینه)* به عنوان «*ابزارها و تکنیک های پزشکی قانونی مناسب برای نوع داده هایی که جمع آوری شده اند، برای شناسایی و استخراج اطلاعات مربوطه از داده های جمع آوری شده در حین حفاظت از یکپارچگی آن*» تعریف می شود (Kent et al.، 2006). NIST می گوید که تحلیل "شامل تجزیه و تحلیل نتایج آزمون برای استخراج اطلاعات مفید می شود که به سوالاتی می پردازد که انگیزه ای برای انجام جمع آوری و بررسی هستند" (Kent et al.، 2006). ISO 27037 تحلیل را به عنوان "شناسایی و ارزیابی اقلام شواهد از منبع شواهد بالقوه دیجیتال" تعریف می کند (ISO 27037، 2012).

به طور معمول، در یک مرحله تحلیل، اهمیت آثار اطلاعات ارزیابی شده و یک روایت تولید شده توسط شواهد و جدول زمانی حوادث پشتیبانی می شود. یک روایت کمک می کند تا این مورد بهتر درک شود و به راحتی برای هیئت منصفه توضیح داده شود. با این حال، این اجباری نیست و اغلب حضور شواهد کافی است. جدول ۴, چالش ها و راه حل های توصیه شده در مرحله آزمون و تحلیل در مورد پلت فرم ابر را فهرست می کند.

عدم چارچوب ورود به سیستم

به طور کلی، ارائه دهندگان سرویس ابری از سیاست و قالب شخصی برای ورود به سیستم خود استفاده می کنند (AWS Security Center A، 2013b، 2014، Google، 2014). فقدان چارچوب قابل اجرای ورود معتبر از نظر پزشکی قانونی برای رایانش ابری، چالش هایی را در زمان بندی رویدادها ایجاد می کند. با این حال، فهرست ها

برای بررسی هدف تحقیقی اجباری نیستند و تحقیقات را می توان با بررسی محتویات فایل، دسترسی به تمبرها و بقایای داده ها انجام داد. با این وجود، فهرست ها به یک بررسی کننده کمک می کنند تا نقاط را به هم وصل کند. در بخش ۳ ما در مورد چارچوب های دیجیتالی پزشکی قانونی بحث کردیم. چارچوب ورود یک زیر مجموعه از چارچوب پزشکی قانونی جامع را تشکیل می دهد. توصیه های پیشنهاد شده توسط محققان به طور خلاصه در زیر شرح داده شده است:

- سیستم مدیریت ورود جامع: نیاز به یک سیستم مدیریت ورودی جامع، که حاوی اطلاعات کافی برای رفع نیازهای پزشکی قانونی است، توسط بسیاری از محققین (Dykstra and Sherman، 2012؛ Marty، 2011؛ Sang، 2013؛ Zawoad et al. 2013) مشخص شده است. مارتی (۲۰۱۱) چارچوب ورود به سیستم ابر را پیشنهاد داد و دستورالعمل های دقیق مربوط به زمان ورود، محل ورود و اینکه دقیقا چه چیزی برای ورود به سیستم به منظور فعال کردن بررسی های پزشکی قانونی لازم است، گزارش دهی و همبستگی را ارائه کرد. در ورود-امن- به عنوان-یک-خدمت (SecLaaS)، نویسندگان یک طرح برای ذخیره پیشنهاد دادند که فهرست هایی برای اهداف پزشکی قانونی ایمن ارائه می دهند. این طرح به CSP ها اجازه می دهد که فهرست ها را در ابر ذخیره کنند و در عین حال محرمانه بودن کاربران ابر و یکپارچگی را حفظ کنند و در همان زمان, آن را به شیوه ای امن دردسترس عموم قرار می دهند (Zawoad et al.، 2013).

جدول ۳. فاز بررسی و تحلیل: چالش ها و راه حل های پیشنهادی

شماره :	چالش ها	راه حل های پیشنهادی	اظهارنظرات
1	فقدان چارچوب ورود	سیستم جامع مدیریت ورود (Dykstra and Sherman, 2012; Marty, 2011; Sang, 2013; Zawoad et al., 2013)	یک ورود خوب می تواند به زمانبندی رویدادها و درک بهتر مورد کمک کند
		Amazon AWS CloudTrail (AWS Security Centre, 2013a,	اطلاعات پزشکی قانونی مقدماتی برای کاربران آمازون فراهم می کند

)b			
AWS Cloud Trail, اطلاعات دسترسی جامع را در فرمت UTC فراهم می کند و زمانبندی را میسر می سازد	AWS CloudTrail می تواند یک راه حل جزئی فراهم کند (AWS Security Centre, 2013a, b; 2014)	زمانبندی شواهد	2
فهرست انتها-به-انتها به خلق یک خط زمانی از رویدادها کمک می کند	فهرست های امن با مهرهای زمانی مناسب		
مالکیت و تاریخچه اشیای داده ها را فراهم می کند	منشا امن (Lu et al., 2010))		
پیاده سازی احتمالی آینده به ابزارهای شخص ثالث برای پردازش و تحلیل نیاز دارد	زیرساخت مدیریت کلیدی ابر (CSA, 2013a)	داده های رمزگذاری شده	3
توسط ابزارهایی مانند ArchSight حمایت شده است	AWS CloudTrail از جمع آوری فایل های ورود حمایت می کند (AWS Security Centre, 2013a, b; 2014)	داده های شواهد یکپارچگی	4
ردیابی داده ها در ابر با استفاده از منشا	اطلاعات امنیت و مدیریت رویدادها (SIEM) (Hewlett-Packard, 2012) ردیابی داده ها (Zhang et al., 2011)		

- آمازون AWS CloudTrail: به عنوان بخشی از بهترین شیوه عملیاتی امنیتی و برای رعایت انطباق با صنعت و مقررات، آمازون اخیراً ویژگی ورود به حسابرسی AWS CloudTrail را ارائه داده است. این ویژگی, یک سرویس وب است که تماس های API را برای پشتیبانی از خدمات AWS فراخوانی می کند و فایل ورود را به یک سطل ذخیره خدمات ساده آمازون از پیش تعریف شده Amazon S3 (Amazon S3) تحویل می دهد. اگر چه آمازون, خدمات وب سایت دنباله حسابرسی ابر را با در نظر گرفتن شرایط مختلف ورود و انطباق از PCI DSS v2.0، ISO 27001: 2005 و غیره ایجاد کرده است، همچنین می تواند برای تحلیل پزشکی قانونی مورد استفاده قرار گیرد. فایل های ورودی نوشته شده در فرمت Java Script Object Notation (JSON) نوشته می شوند. فایل های

ورودی را می توان از سطل S3 تعریف شده با استفاده از صفحه مدیریت AWS، بدون نیاز به هیچ گونه پشتیبانی از CSP استخراج نمود. AWS CloudTrail یک مکانیزم جامع برای محدود کردن دسترسی به فایل های ورودی را خودش فراهم می کند, از قبیل پیکربندی دسترسی با استفاده از نقش های IAM یا حتی تقویت کنترل های دسترسی با استفاده از سرویس های تأیید هویت چند فاکتور AWS، و در نتیجه، مسئله مربوط به اصالت یا اعتماد «فهرست های مربوط» را کاهش می دهد. علاوه بر این، فایل های ورود به سیستم با استفاده از رمزگذاری جانبی سرور S3 (AWS Security Center، 2013a، b) رمزگذاری می شوند.

AWS Cloud Trail یک سرویس منطقه ای است، اما جمع آوری فایل های ورود در سراسر مناطق مختلف و چندین حساب در یک سطل S3 تک را میسر می سازد. CloudTrail رویدادها را با استفاده از فرمت UTC وارد می کند، علی رغم زمان سیستم در حال اجرا، و اطلاعات جامعی فراهم می کند از جمله "چه کسانی فعالیت را انجام دادند، چه کاری انجام می دادند، چه زمانی و از کجا انجام شد"، که در تحقیقات حادثه و همچنین در زمانبندی شواهد بسیار مفید خواهند بود (AWS مرکز امنیتی، ۲۰۱۳a).

زمانبندی شواهد

زمانبندی شواهد، پیوندی از نشانگرهای زمانی با هر رویداد یا آیتم داده مورد نظر را به منظور بازسازی دنباله ای از وقایع فراهم می کند. زمانبندی از این واقعیت کمک می گیرد که اکثریت اقدامات انجام شده بر روی جسم دارای مهر زمانی هستند. در این مرحله، برخی از الزامات مدارک دیجیتال شایان ذکر هستند. شواهد دیجیتال باید همان الزامات حقوقی را به عنوان شواهد معمول برآورده سازند، یعنی باید (i) معتبر ، (ii) قابل اطمینان باشد، (iii) کامال، (iv) قابل اعتماد و (v) قابل قبول باشند (.Reilly et al، 2010، 2011). علاوه بر این، Reilly و همکاران (۲۰۱۱) توضیح دادند که چگونه دنباله ای از حوادث در یک حملات هک کردن بین دستگاه نهایی، هدف، قربانی و واسطه ها در یک سناریوی ابر بازسازی می شوند. زمانبندی به درک شواهد و داده ها، قرار دادن اطلاعات در متن که به طور بالقوه ساده تر درک می شود, کمک می کند. علاوه بر این، زمان بندی به توضیح بهتر یک مورد برای هیئت منصفه کمک می کند. محققان روش های زیر را برای کمک به زمانبندی شواهد پیشنهاد کرده اند:

- فهرست های امن با مهرهای زمانی مناسب: مانند فهرست های AWS CloutTrail یا Logging Secure همانند سرویس پیشنهاد شده توسط Zawoad و همکاران. (۲۰۱۳) یا فهرست های مربوطه که می توانند برای ایجاد خط زمانی رویداد انتها-به-انتها استفاده شوند
- منشا امن: Lu و همکاران (۲۰۱۰)، منشا ایمنی را پیشنهاد کردند، با اشاره به اینکه این منبع تغذیه پزشکی قانونی داده ها در رایانش ابری است. منشا امن, مالکیت و تاریخچه فرایند را ثبت می کند و شواهد مورد اعتماد اشیاء داده را فراهم می کند؛ بنابراین، نقش کلیدی در پزشکی قانونی ابر ایفا می کند. یک منشا ایمن به درستی پیاده سازی شده به زمان بندی شواهد کمک می کند، زیرا مالکیت و ویژگی های تاریخچه فرایند, اطلاعات مربوط به اینکه "چه کسی" مالک شی داده ها در زمان معین است و "چه کسی" اشیاء را به روز رسانی نمود ارائه می کند.

داده های رمزگذاری شده

رمزگذاری به طور گسترده ای توسط مشتری ابر به عنوان یک معیار تامین امنیت داده ها یا برای برآورده سازی الزامات پزشکی قانونی و انطباق استفاده می شود. با این حال، مجرمان می توانند از رمزگذاری برای هدف غیرقانونی نیز استفاده کنند. McKemmish (1999) اشاره کرد که استفاده گسترده از رمزنگاری توسط مجرمان برای پنهان کردن تصاویر غیرقانونی پنهان است. Biggs و Vidalis (2009) اشاره کردند که ۷۰ تا ۸۰ درصد از حجم کار محقق در سازمان اجرای قانون انگلستان برای نظارت بر استفاده از رایانش ابر توسط پسربازان صرف می شوند. بنابراین، از دیدگاه پزشکی قانونی، رمزگذاری, یک مانع مهم برای یک بررسی کننده ایجاد می کند. گزارش Cloud Security Alliance نشان می دهد که "زیرساخت های کلیدی مدیریت مورد استفاده در ابر (توپولوژی، فرآیند، فن آوری ها) می توانند گزینه ای برای دردسترس ساختن کلید" برای معاینه کنندگان پزشکی قانونی (CSA، 2013a) به عنوان یک راه حل ممکن آینده خلق کنند. با این حال، چنین گزینه ای باید توسط مقررات و ساختار حکومتی مناسب برای جلوگیری از نقض حریم خصوصی و سوء استفاده مورد حمایت قرار گیرد.

جدول ۵. مرحله گزارش دهی و ارائه: چالش ها و راه حل های پیشنهادی

اظهارنظرات	راه حل های پیشنهادی	چالش ها	شماره:
توافقات قانونی)مثلا: MLAT ((INCSR, 2012)	قانون مرز عرضی , روابط بین المللی	حوزه قضائی	1
برای ایجاد اعتماد به شواهد ضروری است	اصول و رهنمودهای خوش تعریف (Biggs and Vidalis, 2009; Grispos et al., 2013; Taylor et al., 2011)	زنجیره نگهداری	2
فقدان این ابزارها وجود دارد	چارچوب, فرایند و رهنمودهای پشتیبانی شده توسط ابزارها و فناوری	بازسازی صحنه جرم	3
توضیح پیچیدگی ابر برای هیئت منصفه مشکل است	زمانبندی حوادث	پیچیدگی ابر	4
	اصول, فرایند و رویه های ایجاد شده (مثلاً رهنمودهای ACPO در انگلستان) (e.g., ACPO guidelines in UK)	انطباق	5

ادغام داده های شواهد

در ابر، داده های شواهد در سراسر بسیاری از دستگاه های گسترده در سراسر مکان های مختلف گسترش می یابد، از جمله نقاط پایانی تلفن همراه، سرورهای پروکسی میان لایه و خود محیط مجازی ابر. علاوه بر این، همانطور که عنوان Ruan و همکاران (۲۰۱۱) اشاره کرده اند، CSPها اغلب خدمات را در میان خودشان تجارت می کنند، و آرایه ای از زنجیره وابستگی درون ابر را ایجاد می کنند. تجارت کردن، چالش های اضافی را نه تنها برای به دست آوردن شواهد از منابع متعدد، بلکه همچنین در جمع آوری و ادغام داده های شواهد ایجاد می کند, زیرا محققان باید هر لینک در زنجیره وابستگی را دنبال کنند.

ادغام تمام این قطعات داده ها و ایجاد دنباله ای از حوادث, بخش های مهمی از فرایند پزشکی قانونی هستند. روش های پیشنهادی زیر مورد بحث قرار می گیرند:

- AWS CloudTrail از جمع آوری فایل های ورود به یک سطل Amazon S3 تک (AWS Security Center، 2013a)، که فقط برای مشتریان آمازون مفید است اما نیاز به ابزارهای شخص ثالث برای تحلیل اطلاعات کسب و کار دارد, پشتیبانی می کند. با توجه به پزشکی قانونی، هر لایه اضافی از ابزارهای شخص ثالث استفاده شده, یک لایه از مسئله "اعتماد" را اضافه می کند.
- ابزارهای امنیتی و مدیریت رویداد (SIEM)، مانند ArchSight، یکپارچگی ورودی را از چندین منبع ارائه می دهند و می توانند برای پوشش دادن شواهد استفاده شوند (Hewlett-Packard، 2012)
- ردیابی داده ها: ژانگ و همکاران. (۲۰۱۱) یک مکانیزم ردیابی داده ها در ابر را با استفاده از ابزارهای نرم افزاری منشا داده ها که با استفاده از اصول ردیابی داده ها پیاده سازی می شوند و به ادغام آثار کاربر و رسم خط زمان رویدادها کمک می کند, فراهم نمود.

گزارش دهی و ارائه

شواهد جمع آوری شده در طول مرحله جمع آوری یا کسب و گزارش های تحلیلی در این مرحله از پزشکی قانونی به دادگاه ارائه می شوند. NIST, گزارش دهی را به عنوان فرایندی تعریف کرد که "شامل توصیف اقدامات انجام شده، تعیین اینکه چه اقدامات دیگری باید انجام شود، و توصیه هایی برای بهبود خط مشی ها، رهنمودها، رویه ها، ابزارها و سایر جنبه های فرایند پزشکی قانونی" می باشد (.Kent et al، 2006). تخصص و صلاحیت ارائه دهنده و اعتبار فرایند تولید گزارش ها می تواند در دادگاه به چالش کشیده شود. بنابراین، گزارش دهی و ارائه برای تعیین ارزش اثبات پذیری مدارک ضروری است.

جدول ۵ فهرست چالش ها و راه حل های توصیه شده در این مرحله را نشان می دهد.

حوزه قضائی

در بخش ۳,۳,۶ ما در مورد موضوع حوزه قضائی مربوط به کسب شواهد در ابر بحث کردیم. حوزه قضائی, در حالی که پرونده را ارائه می دهد، یک چالش است، زیرا قانون زمین, از مکانی به مکان دیگر متفاوت است. به عنوان مثال، پراساد (۲۰۱۲) بیان نمود که طبق قانون استرالیا, مجرم باید در استرالیا باشد یا یک شهروند استرالیایی در خارج از

کشور برای جرایم سایبری باشد که توسط دادگاه استرالیا پذیرفته شود. اگر مجرم در خارج از کشور باشد، اما یک شهروند استرالیایی نباشد، و هیچ پیمان استرداد بین کشور میزبان و استرالیا وجود نداشته باشد، پس دادگاه استرالیا صلاحیت قضائی ندارد، که بحث بیشتر را برای یک چارچوب بین المللی تقویت می کند (Prasad، 2012). علاوه بر این، یک مطالعه انجام شده بر روی معیارهای حیاتی برای توانایی پزشکی قانونی ابر نشان داد که فقدان همکاری بین المللی و مکانیزم پزشکی قانونی در دسترسی و مبادله داده های ملی، تاکنون, اصلی ترین چالش های پزشکی قانونی در ابر هستند (. Ruan et al، 2013). پزشکی قانونی ابر، که یک مسئله چند بعدی است و شامل حوزه های فنی، سازمانی و پزشکی قانونی می باشد، به همکاری بین آژانس های اجرای قانون بین المللی و چارچوب پزشکی قانونی برای انجام و ارائه جرائم با استفاده از رایانش ابری نیاز دارد (.Ruan et al، 2011). چارچوب حقوقی مانند MLAT به کشورهایی که صاحب امضا هستند کمک خواهد کرد.

زنجیره نگهداری

اثبات زنجیره نگهداری در حوزه پزشکی قانونی ابر، یک فرآیند پیچیده تر در مقایسه با پزشکی قانونی سنتی دیجیتال می باشد. علاوه بر این، در یک مطالعه نظرسنجی، Ruan و همکاران. (۲۰۱۳) دریافتند که "یک رویه و مجموعه ای از ابزارهای لازم برای ضبط و حفظ زنجیره نگهداری در تحقیقات برای مصرف کنندگان بسیار مهم است". به دنبال دستورالعمل های تعیین شده، مانند موسسه افسران ارشد پلیس (ACPO) در انگلیس، یکی از راه های ایجاد زنجیره نگهداری است. این دستورالعمل ها, تمام اطلاعات مربوطه را با استانداردهای بالا فراهم می کنند تا پرونده در دادگاه حاضر شود و اعتماد به شواهد ارائه شود (Biggs and Vidalis، 2009؛ .Grispos et al، 2013؛ Taylor et al. 2011)

بازسازی صحنه جرم

به علت فقدان ابزار قابل اجرا و حمایت از فرآیند و دستورالعمل ها, بازسازی صحنه جرم در ابر همچنان یک چالش به شمار می رود. الگوریتم ها و ابزارهای نرم افزاری برای بازسازی ذخیره سازی ابر و شواهد هنوز باید مورد تایید و توسعه قرار گیرند (NIST، 2014b).

پیچیدگی ابر

هیئت های منصفه در نظام حقوقی عرف از فرد تا دادستان، اغلب با درک بسیار محدود یا عدم شناخت از تکنولوژی رایانش ابری تشکیل شده اند. بنابراین، شاهد متخصص با وظیفه ی دلگرم کننده تضمین که اعضای هیئت منصفه از درک کامل اصول و تکنولوژی رایانش ابری مواجه خواهد شد (Grispos et al.، 2013). در زبان ساده، زمان بندی حوادث ، به تشریح بهتر پرونده برای هیئت منصفه و درک راحت آن کمک می کند.

انطباق

برای معتبر شدن شواهد از نظر قانونی در دادگاه، پیروی از یک رویه مشخص استاندارد در سراسر فرایند پزشکی قانونی ضروری است. چند نمونه از این رویه های مشخص عبارتند از: (۱) راهنمای شیوه مناب ACPO برای شواهد الکترونیک مبتنی بر کامپیوتر و (ii) سازمان بین المللی در مورد شواهد کامپیوتری (IOCE). راهنمای ACPO, تعاریف و چهار اصل شواهد الکترونیکی مبتنی بر کامپیوتر را فراهم می کند (ACPO، 2012). به طور کلی, قواعد ACPO توسط IOCE در رهنمودهای پیشنهادی آن نشان داده شده است. اما این رهنمودها قبل از ظهور رایانش ابری توسعه یافته اند (Adams، 2013). آدامز (۲۰۱۳) اصول راهنمایی ارائه شده از سوی ACPO، کاربرد آن در محیط ابر و مشکلات مربوط به پیروی از اصول را مورد بحث قرار داد، با وجود اینکه نویسندگان بر اهمیت پیروی از دستورالعمل ها تاکید نمودند. در غیاب مدل فرایند خاص، چارچوب سطح بالایی مانند ISO، این چارچوب اعمال خواهد شد. اگر سازمان, رویه های عملیاتی استاندارد خاص خود را ایجاد و پیاده سازی نماید، ممکن است در دادگاه حاضر نشود.

خلاصه و کار آینده

پزشکی قانونی دیجیتال به عنوان یک خدمت

ما چندین مدل پزشکی قانونی دیجیتالی را مورد بحث قرار داده ایم، که بیشتر آنها برای اهداف پزشکی قانونی سنتی توسعه یافته بودند. محققان تلاش کرده اند تا این مدل ها را به حوزه های پزشکی قانونی ابر گسترش دهند. با وجود اینکه مدل فرایند پزشکی قانونی دیجیتال استانداردسازی نشده است، درمورد سطح ذهنی مدل دیجیتالی پزشکی

قانونی هماهنگی وجود دارد. با این حال، برای ساخت مدل هایی که برای همه طرفداران رایانش ابری شناخته شده و قابل قبول باشد، کار بیشتر باید انجام شود.

پزشکی قانونی دیجیتال در ابر, یک حوزه در حال ظهور است و پزشکی قانونی دیجیتال به عنوان یک سرویس, یک رویکرد مبتنی بر سرویس برای پردازش و بررسی متن دیجیتالی است که توسط بسیاری از محققان مورد بحث قرار گرفته است (ون بار و همکاران، ۲۰۱۴؛ ون و همکاران ،. ۲۰۱۳). ون بار و همکاران (۲۰۱۴) تحلیل پزشکی قانونی دیجیتال را به عنوان یک مدل سرویس (DFaaS) در هلند ارائه کردند. در مدل DFaaS، محقق دیجیتال به طور مداوم بر روی برداشت داده های پزشکی قانونی تمرکز می کند و داده ها را به یک سیستم متمرکز ارسال می کند. کارآگاهان با تخصص حوزه خاص و دانش عمیق (به جای محققان) دسترسی به زیر مجموعه داده های برداشت شده ای را دارند که آنها را تحلیل می کنند. وظایف کارآگاهان به عنوان تحلیلگران و وظایف محققان بیشتر به عنوان یک برداشت کننده داده های پزشکی قانونی است. با استفاده از برنامه های کاربردی هوش تجاری، تکنیک های جستجوی و فیلترکردن، نویز در مجموعه داده ها بسیار کاهش می یابد و کارآگاهان می توانند به راحتی تحلیل را به مجموعه های کوچک محدود تقلیل دهند که برای تعیین فرضیه و نتیجه گیری اهمیت دارد. این مقاله نتیجه گیری می کند که این مدل در هلند با موفقیت بزرگی به یک استاندارد تبدیل شود (van Baar et al.، 2014).

در اثر Wen و همکاران (۲۰۱۳) روی پزشکی قانونی-به عنوان-یک- سرویس (FaaS), از پلت فرم ابر برای انجام معاینات پزشکی قانونی و تحلیل استفاده شد و مدیریت جریان کار پزشکی قانونی و پردازش آن با استفاده از ابر اثبات شد. با قدرت پردازش و ذخیره سازی بسیار در ابر، یک محیط ایده آل برای ذخیره سازی و پردازش داده های دیجیتالی می باشد و قابلیت همکاری در میان بسیاری از نرم افزارهای پردازش داده های پزشکی قانونی را فراهم می کند. Wen و همکاران (۲۰۱۳) ثابت کرد که مدیریت و پردازش جریان کار پزشکی قانونی مبتنی بر ابر می تواند تا ۸۷ درصد زمان تحلیل را در سناریوهای آزمایش شده، در مقایسه با روش های سنتی، صرفه جویی دهد.

خلاصه یافته ها

مکان فیزیکی ناشناخته آثار پزشکی قانونی و کپی های تکراری داده ها که در سرورهای مجازی مختلف، احتمالاً در کشورهای مختلف در یک محیط ابر گسترش می یابد ، موانع مهمی نه تنها در مرحله شناسایی شواهد، بلکه در مراحل حفاظت و خرید نیز ایجاد می کند. برای شناسایی منابع کارآمد بدون نیاز به هزینه زیاد, باید کار بیشتری انجام شود. اغلب آژانس های اجرای قانون (LEA) و مشتریان باید برای بازیابی کامل داده ها به CSP ها بستگی داشته باشند و به SLAهای قوی نیاز دارند. کارهای بیشتری برای رسیدگی به دستورالعمل های SLA قضایی باید انجام شوند.

ماهیت غیرمتمرکز و کوتاه مدت محیط ابر، نه تنها یک چالش فنی، بلکه یک مسئله حقوقی است که نیاز به حمایت کشورهای دیگر دارد، زیرا ممکن است قربانی، عاملان و پلتفرم ابر در حوزه های مختلف قضایی قرار داشته باشند. اگر چه چارچوب پزشکی قانونی برای همکاری میان برخی از کشورها وجود دارد، نویسندگان کمبود طرح های بین المللی و توافق نامه ها را نشان دادند.

اغلب سرویس تجاری CSPs در میان خودشان، یک مجموعه ای از وابستگی ها و مسئله اعتماد را ایجاد می کند. محققان باید به دنبال هر لینک در زنجیره برای جمع آوری شواهد باشند. با حرکت به جلو، یک نیاز قوی برای یک چارچوب ورودی یکنواخت معتبر از نظر پزشکی قانونی وجود دارد، از جمله توانایی ضبط ورودهای سطح فراناظر که در هر سطح حساب کاربری جدا جمع می شوند (برای محافظت از حریم خصوصی مستاجران همزمان)، و توانایی ردیابی حرکت فایل های کاربر در داخل ابر. این مکانیزم ورود تا حد زیادی به قابلیت ردیابی کمک خواهد کرد و شفافیت را فراهم می کند. رهنمودها و یا فرآیندهای پیگیری, زمانی که CSPs خدمات را بین خودشان معامله می کنند, راه های دیگری برای کار تحقیقاتی دیگر هستند.

مشتریان ابر از رمزگذاری برای تضمین محرمانه بودن و یکپارچگی داده ها یا برای برآورده نمودن الزامات سیاست یا مقررات استفاده می کنند. با این حال، رمزگذاری باعث بزرگترین چالش در شناسایی شواهد و جداسازی شواهد می شود. پزشکی قانونی زنده و ضبط مکرر عکسهای فوری از سیستم در حال اجرا, قابلیت های پزشکی قانونی را افزایش می دهد، اما به هزینه ها افزوده می شود، و باعث ایجاد سربار و مشکلات فراوانی می شود. به همان اندازه مهم است

که مقادیر حشره مصنوعی پزشکی قانونی، همچون فایلهای ایمن را حفظ کنید. باید برای ایجاد یک روش عملیات استاندارد و حمایت از دستورالعمل های موجود در دست اقدامات بیشتری برای دسترسی به کلید رمزگشایی بدون نقض قوانین حریم خصوصی, کار بیشتری انجام شود.

منشا ایمن پیاده سازی شده مناسب می تواند بخش مهمی در آینده پزشکی قانونی داشته باشد؛ زیرا مالکیت، تاریخچه پردازش و ویژگی های امنیتی جامع را فراهم می کند و در نتیجه بخشی از شواهد معتبر را تشکیل می دهد (لو و همکاران، ۲۰۱۰). مکانیزم ردیابی داده که توسط ژان و همکاران (۲۰۱۱) ارائه شده است. می تواند گسترش یابد تا نگاهی فراتر از یک محیط به میان-ابر به ابعاد بین ابر، ابر-به-اینترنت و انتقال داده ها به اینترنت و مدیریت سیسکو به عنوان کارهای آینده داشته باشد.

ما همچنین دریافتیم که تضمین اعتماد برای شواهد ابر همچنان یک چالش بزرگ در زمینه پزشکی قانونی است. همچنین جمع آوری داده های پاک شده از یک پارتیشن ابر بسیار سخت تر است. به طور کلی، الزامات پزشکی قانونی و قواعد حریم خصوصی اغلب با یکدیگر و ارائه دهندگان ابر تضاد و تناقض دارند، و این کار در تلاش برای اارئه حداکثر احترام به قوانین حفظ حریم خصوصی، پلت فرم ابر را امن تر می سازد و به طور ناخواسته انجام وظایف پزشکی قانونی را بسیار سخت تر می سازد. همچنین مشاهده ما اینست که CSP های اصلی, ارائه قابلیت های پزشکی قانونی در پیشنهادات خدمات خود (مانند Amazon CloudTrail) را شروع کرده اند.

در مطالعه موردی اخیر با استفاده از ابزار XtremeFS، در سیستم فایل توزیع شده که معمولًا در محیط های رایانش ابری استفاده می شوند، مارتینی و چو (۲۰۱۴), اهمیت فرایند صحیح پزشکی قانونی را برجسته نمودند. چنین فرآیندی می تواند یک راهنمایی واضح برای دست اندرکاران پزشکی قانونی دیجیتال در تحقیق خود، اعم از شناسایی و حفاظت از منابع شواهد و مدارک، جمع آوری داده های فرار، غیرفرار و شبکه، برای بررسی و تحلیل داده ها، و در نهایت گزارش و ارائه در دادگاه قانون (مارتینی و چو، ۲۰۱۴) فراهم نماید.

نتیجه گیری

رایانش ابری، نحوه تحویل و مصرف IT را تغییر داده است. رشد چشمگیری در پذیرش و اتخاذ ابر صورت گرفته است و انتظار می رود این روند ادامه یابد. به همین ترتیب مصرف کنندگان در مورد امنیت و حریم خصوصی اطلاعات ذخیره شده در ابر، نگران کننده هستند. از سوی دیگر، نگرانی های رو به رشد در مورد امکان استفاده از ابر به عنوان یک پلت فرم برای انجام جرائم اینترنتی وجود دارد. با قدرت محاسباتی بسیار زیاد و ذخیره سازی ارائه شده توسط ابر، حملات بزرگی می توانند در دوره های کوتاه تر و با هزینه کم انجام شوند. مجرمان می توانند حساب را به طور کامل خاتمه دهند و بدون جا گذاشتن اثر از خود ناپدید شوند. این موضوع با مشکلات و چالش های پزشکی قانونی دیجیتال در محیط ابر تشدید می شود. در این مقاله، ما تحلیل منظم چالش های پزشکی قانونی، راه حل های احتمالی مربوط به مراحل مختلف پرونده پزشکی و تحلیل دقیق راه حل های توصیه شده را ارائه کرده ایم. ما بلوغ راه حل ها را شناسایی کرده ایم و فرصت هایی را برای تحقیق و توسعه بیشتر نشان داده ایم. ما همچنین خلاصه ای کوتاه از مدل های پزشکی قانونی به عنوان یک سرویس را ارائه کردیم.

References

ACPO. ACPO good practice guide for digital evidence (Version 5.0). 2012. Available at, http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf [Accessed 02.12.14]. UK.

Adams R. The emergence of cloud storage and the need for a new digital forensic process model. In: Ruan K, editor. Cybercrime and cloud forensics: applications for investigation processes. IGI Global; 2013. p. 79–104.

Alhamad M, Dillon T, Chang E. Conceptual SLA framework for cloud computing. In: 4th IEEE International Conference on Digital Ecosystems and Technologies (DEST); 2010. p. 606–10.

AWS Security Centre A. AWS cloud trail, user guide. 2013. Available at, https://aws.amazon.com/documentation/cloudtrail/ [Accessed 12.12.14].

AWS Security Centre A. Logging in AWS. 2013. Available at, http://aws.amazon.com/whitepapers/security-at-scale-logging-in-aws/ [Accessed 12.12.14].

AWS Security Centre A. Amazon web services: overview of security process. 2014. Available at, https://aws.amazon.com/security [Accessed 11.12.2014].

Biggs S, Vidalis S. Cloud computing: the impact on digital forensic investigations. In: Proceedings of the 2009 International Conference for Internet Technology and Secured Transactions, (ICITST). London, UK: IEEE; 2009. p. 1–6.

Birk D, Wegener C. Technical issues of forensic investigations in cloud computing environments. In: Proceedings of the 2011 IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE). Oakland, CA, USA: IEEE; 2011. p. 1–10.

Brezinski D, Killalea T. Guidelines for evidence collection and archiving. Req For Comments 2002;3227.

Casey E. Cloud computing and digital forensics. Digit Investig 2012;9:69–70.

Catteddu D, Hogben G. Cloud computing risk assessment. European Network and Information Security Agency (ENISA); 2009. Available at, http://wwwenisaeuropaeu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment [Accessed 17.07.14].

CSA. Mapping the forensic standard ISO/IEC 27037 to cloud computing. 2013. Available at, https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf [Accessed 10.08.14].

CSA. Security guidance for critical areas of focus in cloud computing V3.0. Cloud Security Alliance; 2011. Available at, https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/ [Accessed 10.09.14].

CSA. Cloud computing vulnerability incidents: a statistical overview. Cloud Security Alliance; 2013b. Available at, https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/ [Accessed 10.11.14].

Damshenas M, Dehghantanha A, Mahmoud R, bin Shamsuddin S. Forensics investigation challenges in cloud computing environments. In: Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). IEEE; 2012. p. 190–4.

Daryabar F, Dehghantanha A, Udzir NI. A survey about impacts of cloud computing on digital forensics. Int J Cyber-Secur Digit Forensics (IJCSDF) 2013;2:77–94.

Delport W, Kohn M, Olivier MS. Isolating a cloud instance for a digital forensic investigation. In: Proceedings of the 2011 Information Security South Africa (ISSA) Conference. Johannesburg, South Africa: ISSA; 2011.

Dongxi L, Lee J, Julian J, Nepal S, Zic J. A cloud architecture of virtual trusted platform modules. In: Proceedings of the 2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC). IEEE; 2010. p. 804–11.

Kohn MD, Eloff MM, Eloff JH. Integrated digital forensic process model. Comput Secur 2013;38:103–15.

Krautheim FJ, Phatak DS, Sherman AT. Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing. In: Acquisti A, Smith SW, Sadeghi A-R, editors. Trust and trustworthy computing. Berlin Heidelberg: Springer; 2010. p. 211–27.

Lin C-H, Lee C-Y, Wu T-W. A cloud-aided RSA signature scheme for sealing and storing the digital evidences in computer forensics. Int J Secur Appl 2012;6.

Lu R, Lin X, Liang X, Shen XS. Secure provenance: the essential of bread

DOS. Convention on cyber crime. Department of State, United States of America; 2001. Available at, http://www.state.gov/s/l/treaty/tias/2001/131597.htm [Accessed 08.12.14].
Dykstra J, Sherman AT. Understanding issues in cloud forensics: two hypothetical case studies. J Netw Forensics 2011;3:19–31.
Dykstra J, Sherman AT. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques. Digit Investig 2012;9:S90–8.
Federici C. Cloud data imager: a unified answer to remote acquisition of cloud storage areas. Digit Investig 2014;11:30–42.
Gartner. Forecast: public cloud services, worldwide, 2012–2018, 1Q14 update. 2014. Available at, https://www.gartner.com/doc/2696318?ref=clientFriendlyURL [Accessed 08.09.14].
Google. Google's approach to it security, a google White paper. 2014. Available at, http://www.google.com/enterprise/apps/business/resources/docs/security-whitepaper.html [Accessed 12.12. 2014].
Greamo C, Ghosh A. Sandboxing and virtualization: modern tools for combating malware. Secur Priv IEEE 2011;9:79–82.
Grispos G, Storer T, Glisson WB. Calm before the storm: the challenges of cloud. In: Emerging digital forensics applications for crime detection, prevention, and security; 2013.
Guo H, Jin B, Shang T. Forensic investigations in cloud environments. In: 2012 International Conference on Computer Science and Information Processing (CSIP). IEEE; 2012. p. 248–51.
Haeberlen A. A case for the accountable cloud. SIGOPS Oper Syst Rev 2010;44:52–7.
Hay B, Nance K. Forensics examination of volatile system data using virtual introspection. ACM SIGOPS Oper Syst Rev 2008;42:74–82.
Hay B, Nance K, Bishop M. Storm clouds rising: security challenges for IaaS cloud computing. In: Proceedings of the 2011 44th Hawaii International Conference on System Sciences (HICSS); 2011. p. 1–7.
Hewlett-Packard. Security information and event management. Big data big security (White paper). 2012.
Hogben G, Dekker M. Procure Secure: a guide to monitoring of security service levels in cloud contracts. In: ENISA; April 2012. At, http://www.enisa.europa.eu/activities/Resilienceand-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-incloud-contracts [Accessed: 10.06.14].
IEEE. IEEE cloud computing. In: IEEE cloud computing Premiere issue may 2014. IEEE; 2014. pp. 4–7, 10–9.
INCSR. International narcotics control strategy report (INCSR): treaties and agreements. United States of America: Department of State; 2012. Available at, http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm [Accessed 08.12.2014].
Iorga M, Badger L. NIST: challenging security requirements for US government cloud computing adoption (Draft). 2012. p. 54–6. NIST Special Publication.
ISO 27037. Guidelines for identification, collection, acquisition and preservation of digital evidence. 2012.
Jansen W, Grance T. Guidelines on security and privacy in public cloud computing. 2011. p. 1–38. Available at; http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf [Accessed 21.12.2014]. NIST special publication.
Kandukuri BR, Paturi VR, Rakshit A. Cloud security issues. In: Proceedings of the 2009 IEEE International Conference on Services Computing, SCC '09 Bangalore, India; 2009. p. 517–20.
Kent K, Chevalier S, Grance T, Dang H. Guide to integrating forensic techniques into incident response. 2006. p. 800–86. NIST Special Publication.
Khajeh-Hosseini A, Greenwood D, Sommerville I. Cloud migration: a case study of migrating an enterprise it system to IaaS. In: Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD). Miami, USA: IEEE; 2010. p. 450–7.
Khan KM, Malluhi Q. Establishing trust in cloud computing. IT Prof 2010; 12:20–5.
Ko RK, Jagadpramana P, Mowbray M, Pearson S, Kirchberg M, Liang Q, et al. TrustCloud: a framework for accountability and trust in cloud computing. In: Proceedings of 2011 IEEE World Congress on Services (SERVICES). IEEE; 2011. p. 584–8.
Martini B, Choo K-KR. An integrated conceptual digital forensic framework for cloud computing. Digit Investig 2012;9:71–80.
Martini B, Choo K-KR. Cloud storage forensics: ownCloud as a case study. Digit Investig 2013;10:287–99.
Martini B, Choo K-KR. Distributed filesystem forensics: XtreemFS as a case study. Digit Investig 2014;11:295–313.
Marty R. Cloud application logging for forensics. In: Proceedings of the 2011 ACM Symposium on Applied Computing. ACM; 2011. p. 178–84.
McKemmish R. What is forensic computing?: Australian Institute of Criminology. 1999.
NIST. NIST cloud computing collaboration site. 2014.
NIST. In: Group CFSW, editor. NIST Cloud Computing Forensic Science Challenges (Draft NISTIR 8006); 2014.
Palmer G. A road map for digital forensics research, Report from the first Digital Forensics Research Workshop (DFRWS). In: Palmer G, editor. DFRWS Technical Report DTR – T1001-01 FINAL. New York: DFRWS; 2001.
Patel P, Ranabahu AH, Sheth AP. Service level agreement in cloud computing. 2009.
Pichan A, Lazarescu M, Soh ST. Can Nuclear Installations and Research Centres Adopt Cloud Computing Platform? Available at: http://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014-papers/000075.pdf. Symposium on International Safeguards Linking Strategy, Implementation and People Available at: http://wwwiaeaorg/safeguards/symposium/2014/home/eproceedings/sg2014_eproceedings_onlinepdf. Vienna: IAEA; 2014. p. 1–9.
Prasad K. Cyberterrorism: addressing the challenges for establishing an international legal framework. In: Proceedings of the 3rd Australian Counter Terrorism Conference, Perth, Australia. Perth, Western Australia: SRI Security Research Institute, Edith Cowan University; 2012. p. 9–14.
Quick D, Choo K-KR. Digital droplets: Microsoft SkyDrive forensic data remnants. Future Gener Comput Syst 2013;29:1378–94.
Quick D, Martini B, Choo R. Cloud storage forensics. 1 ed. Massachusetts, USA: Syngress; 2013.
Reilly D, Wren C, Berry T. Cloud computing: forensic challenges for law enforcement. In: Proceeding of the 2010 International Conference for Internet Technology and Secured Transactions (ICITST). London, UK: IEEE; 2010. p. 1–7.
Reilly D, Wren C, Berry T. Cloud computing: pros and cons for computer forensic investigations. Int J Multimed Image Process (IJMIP) 2011;1:26–34.
RightScale. State of the cloud report. RightScale; 2014. Available at, http://assets.rightscale.com/uploads/pdfs/RightScale-2014-State-of-the-Cloud-Report.pdf?mkt_tok=3RkMMJWWfF9wsRonuqvAd%2B%2FhmjTEU5z17%2BokW662glkz2EFye%2BLIHETpodcMRMFgN6%2BTFAwTG5toziV8R7fBL81u3c8QXRjq [Accessed 20.1.15].
Ruan K, Carthy J, Kechadi T, Baggili I. Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results. Digit Investig 2013;10:34–43.
Ruan K, Carthy J, Kechadi T, Crosbie M. Cloud forensics. In: Peterson G, Shenoi S, editors. Advances in digital forensics VII. Berlin Heidelberg: Springer; 2011. p. 35–46.
Ruan K, James J, Carthy J, Kechadi T. Key terms for service level agreements to support cloud forensics. In: Peterson G, Shenoi S, editors. Advances in digital forensics VIII. Berlin Heidelberg: Springer; 2012. p. 201–12.
Sang TA. Log based approach to make digital forensics easier on cloud computing. 2013. p. 91–4.
Santos N, Gummadi KP, Rodrigues R. Towards trusted cloud computing. In: Proceedings of the 2009 conference on Hot topics in cloud computing: San Diego, California; 2009. p. 3.
Shipley TG, CFE C. Collecting legally defensible online evidence. 2007. Available at: http://veresoftware.net/uploads/CollectingLegallyDefensibleOnlineEvidence.pdf [Accessed 17.12.14].
SpiderOak. SpiderOak cloud storage storage solutions. 2014.
Taylor M, Haggerty J, Gresty D, Hegarty R. Digital evidence in cloud computing systems. Comput Law Secur Rev 2010;26:304–8.
Taylor M, Haggerty J, Gresty D, Lamb D. Forensic investigation of cloud computing systems. Netw Secur 2011:4–10.
van Baar R, van Beek H, van Eijk E. Digital forensics as a service: a game changer. Digit Investig 2014;11:S54–62.
VMITools. LibVMI: An Introspection Tools.
Wen Y, Man X, Le K, Shi W. Forensics-as-a-Service (FaaS): computer forensic workflow management and processing using cloud. In: CLOUD COMPUTING 2013, The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization; 2013. p. 208–14.
Wolthusen SD. Overcast: forensic discovery in cloud environments. In: Fifth International Conference on IT Security Incident Management and IT Forensics. IEEE; 2009.
Zafarullah Z, Anwar F, Anwar Z. Digital forensics for eucalyptus. In: Frontiers of Information Technology (FIT), 2011. IEEE; 2011. p. 110–6.
Zawaod S, Hasan R. Cloud forensics: a meta study of challenges, approaches and open problems. Distrib Parallel Clust Comput 2013. arXiv: 1302.6312v1 [cs.DC].
Zawoad S, Dutta AK, Hasan R. SecLaaS: secure logging-as-a-service for cloud forensics. In: Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. ACM; 2013. p. 219–30.
Zhang OQ, Kirchberg M, Ko RK, Lee BS. How to track your data: the case for cloud computing provenance. In: Proceedings of the 2011 IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom). IEEE; 2011. p. 446–53.