

## آینده پژوهی استنادپذیری ادله دیجیتال جرایم سایبری مبتنی بر اینترنت اشیا

حسین سهلانی<sup>۱</sup>

تاریخ دریافت: ۱۴۰۰/۰۸/۲۳

تاریخ پذیرش: ۱۴۰۰/۱۰/۲۴

### چکیده

جهان اطراف ما متشکل از مجموعه ای از اشیای فیزیکی بهم متصل با هویت یکتا می باشند که سرعت فزاینده توسعه آنها صرفاً متکی به الزامات فنی نیست، بلکه در کنار آن لازم است به ابعاد دیگر نظیر ابعاد جنایی و حقوقی نیز توجه شود که در صورت عدم توجه به این ابعاد، باید منتظر چالشهای احتمالی بعدی بود. لذا، در این تحقیق سعی شده به بررسی آینده پژوهی استنادپذیری جرایم اینترنت اشیا پرداخته شود و راهکارهایی را به منظور کاهش اثرات مخرب آن ارائه دهد. روش پژوهش این تحقیق، به صورت ترکیبی، کمی و کیفی بوده که داده های این پژوهش از طریق مصاحبه کیفی عمیق با ۳۲ نفر از خبرگان مراکز علمی و انتظامی مختلف با تحصیلات حداقل کارشناسی و چندین سال فعالیت مدیریتی و علمی مرتبط با این حوزه و با نمونه گیری گزینشی جمع آوری شده است که پس از انجام مصاحبه ها، اشباع نظری حاصل شد. به طوریکه با جمع آوری و کدگذاری اطلاعات در جهت برطرف سازی چالشهای آینده استناد پذیری ادله اثبات دعوی سایبری مرتبط با اینترنت اشیا به سوال اصلی تحقیق که ارائه یک مدل مفهومی برای بررسی چالش های استنادپذیری جرایم اینترنت اشیا بود پرداخته شد که مولفین توانستند یک چارچوب کاربردی در چهار بُعد اصلی استنادپذیری جرایم سایبری مرتبط با اینترنت اشیا، آینده پژوهی جرایم اینترنت اشیا، محدودیت ها و نواقص و ناامنی ها با ۱۰ مؤلفه و ۳۶ زیر مؤلفه ارائه کنند که بر اساس یافته های پژوهش، مهمترین چالش، استنادپذیری جرایم اینترنت اشیا با بار عاملی ۰/۷۷،۹۱ است که برای فائق آمدن بر چالش های اکتساب شده می توان پیشنهادات ذیل را عنوان کرد؛ اتخاذ زود هنگام تدابیر لازم و تجهیز مراکز قضایی، انتظامی و آموزشی برای شناسایی چالش ها و اقدامات صورت گرفته در سایر مراکز علمی، بالا بردن بنیه علمی مراکز قضایی و انتظامی در حوزه کشف جرائم با رویکرد آینده پژوهی با برگزاری مانورهای اجرایی و ارزیابی اقدامات صورت گرفته، عقد قراردادهای بین المللی چند جانبه برای ارائه خدمات زیرساختی و جوابدهی به استعلامات و درخواست ها، آماده سازی و فراهم آوردن زیرساخت های لازم همچون تغییر آدرس دهی از نسخه ۴ به نسخه ۶، الزام ارائه دهندگان خدمات اینترنت اشیا به رعایت استانداردها و لزوم آینده پژوهی برای کشف نظام مند فرصتها و چالش های حال و آینده در حوزه اینترنت اشیا.

واژگان کلیدی: آینده پژوهی اینترنت اشیا، استنادپذیری ادله دیجیتال، استنادپذیری جرایم اینترنت اشیا، جرایم اینترنت اشیا.

## ۱. مقدمه

در سالهای اخیر، با بالا رفتن سرعت اینترنت، پیشرفت فناوریهای بیسیم، بهبود توان محاسباتی و کوچک سازی ادوات الکترونیکی، منجر به تولید نوآوری های وابسته به اینترنت با عنوان اینترنت اشیا<sup>۱</sup> شده است، که تعامل انسان با جهان اطراف خود را دستخوش تغییرات قرار می دهد. اینترنت اشیا مفهومی رایانشی برای توصیف آینده ای است که در آن اشیا فیزیکی یکی پس از دیگری به اینترنت وصل می شوند و با اشیا دیگر بدون نیاز به حضور انسان در ارتباط قرار می گیرند. همچنین اینترنت اشیا همراه با فراگیر شدن اینترنت بی سیم رشد کرد طوری که هر دستگاه فیزیکی قابلیت دریافت یک شناسه ی منحصر به فرد را در یک شبکه دارا شد تا بتواند به تبادل اطلاعات (بدون تعامل انسان) پردازد [۱]. در دنیای امروز اینترنت اشیا از اهمیت خاصی برخوردار است زیرا اشیا وقتی بتوانند خود را به صورت دیجیتالی ارائه کنند در نهایت به پدیده ای بسیار فراتر از کلیتی که در واقعیت هستند، تبدیل خواهند شد [۲]. در چنین شرایطی ارتباط اشیا دیگر محدود به انسان نبوده بلکه آنها با اشیا اطراف نیز در ارتباط هستند و می توانند پایگاه های داده ای را ایجاد کنند که در تصمیمات مدیریتی و امنیتی مورد استفاده قرار گیرد [۳]. محصولاتی که بر اساس این ارتباطات ساخته می شوند اغلب به عنوان محصولات هوشمند روانه بازار می شوند ضمناً می توان با افزودن حس گر به اشیا موجود نیز آن ها را هوشمند کرد [۴] و وقتی اشیا با یکدیگر مرتبط شدند میتوان سخن از یک "محیط هوشمند" به میان آورد [۵]. اینترنت اشیا در زندگی روزمره، به مجموعه ای از اشیا متصل، از لوازم خانگی و اتومبیل ها گرفته تا دستگاه های پزشکی اشاره دارد، که مجهز به حسگرهایی دارای قابلیت های محاسباتی و اتصال به شبکه اند و می توانند داده هایشان را با یکدیگر به اشتراک بگذارند که این امر نوید دهنده فرصت فوق العاده ای برای پیشرفت بسیاری از صنایع است ولی این وضعیت نوپدید، حوزه های گوناگون، از جمله نظام حقوقی را تحت تأثیر خود قرار داده است، بدین صورت که عمده دلایل جهت اثبات جرایم، به دلیل نبود ابزارها و امکانات لازم، محدود و در برخی موارد غیر

ممکن می شد؛ اما با گذشت زمان و با پیدایش و پیشرفت حیرت انگیز فناوری های نو، علومی برای اثبات جرایم کشف گردیدند که علاوه بر افزایش غنای قضاوت های صورت گرفته در اثبات جرایم، نواقص و نارسایی های را نیز رفع می کرد [۶].

در ادامه با تشریح مطالبی در رابطه با آینده پژوهی و اینترنت اشیا به مباحث استناد پذیری ادله دیجیتال استخراجی از آنها پرداخته می شود سپس مدلی را که با مصاحبه ها ایجاد شده بیان می گردد، از مدل، پرسش نامه هایی ایجاد و بین نخبگان میانی توزیع می شود و در نهایت تجزیه و تحلیل پاسخ های داده شده صورت گرفته و راهکارهای پیشنهادی برای داشتن آینده ای بهتر در این حوزه بیان می گردد.

## ۱-۱. بیان مسئله

با توجه به سرعت بالای پیشرفت فن آوری بشر باید خود را برای چنین تغییراتی آماده و مهیا نماید. لذا آینده پژوهی در مراکز قضایی و انتظامی به ویژه در حوزه جرایم سایبری به دلیل ارتباط آن با جامعه و تأثیر کارکرد آن بر نظم و امنیت از اهمیت ویژه ای برخوردار است. پیشگیری، کشف جرائم و برقراری نظم و امنیت متناسب با نیازهای حال و آینده جامعه از وظایف تشکیلات قضایی و انتظامی است. حساس ترین و مهمترین وظیفه آینده پژوهان از نظر تصمیم گیران و مدیران، پیشبینی یک واقعه در شرایط فعلی است. صحت تحلیل و وقوع پیشبینی انجام شده، تأثیر زیادی بر اعتبار آینده پژوهی و اعتماد مسئولان خواهد داشت. بنابراین، آینده پژوهی جرایم سایبری و انعکاس آن به مدیران عالی این مراکز از اهمیت بالایی برخوردار است. از طرفی استناد پذیری ادله دیجیتال هم ضرورت و اهمیت بالایی در مراکز قضایی و انتظامی دارد و اینگونه می توان تعریف کرد که کلیه اقداماتی که منجر به شناسایی شواهد جرایم دیجیتال شود را گویند، به نحوی که اصالت شواهد تضمین گردد. اصالت شواهد باید در مرحله جمع آوری شواهد و بررسی شواهد در نظر گرفته شود تا به استنادپذیری شواهد در مراجع قضایی لطمه ای وارد نشود. یکی از نکات مهم برای تضمین اصالت شواهد، آنالیز و بررسی کپی تصویری دقیق ایجاد

<sup>۱</sup> Internet of Thing

تحقیقات مشابه و مرتبطی که قبلاً صورت گرفته بیان می شود.

در مقاله [۸] مولفین ابتدا در رابطه با اینترنت اشیا و ماژول های اصلی آن (ماژول تشخیص، ماژول پردازشی، ماژول جمع آوری اطلاعات، ماژول های ارتباطاتی و ماژول انرژی) مطالبی را بیان کردند، سپس به برخی از چالش ها، تهدیدات و حملات مربوط به اینترنت اشیا پرداخته اند (جعل اشیا<sup>۱</sup>، وقفه در سرویس<sup>۲</sup>، حملات سرریز بافر<sup>۳</sup>، از بین بردن حریم خصوصی<sup>۴</sup> و ...) و نهایتاً به چالش های استنادپذیری ادله دیجیتال در جرایم اینترنت اشیا پرداخته است (نبود حالت استاندارد برای بررسی های استنادپذیری ادله دیجیتال، برقراری حالت زنجیره حفاظت، تنوع بالای تجهیزات موجود، نبود آمادگی برای بررسی حملات به صورت استنادپذیر، راحت از بین رفتن شواهد).

در مقاله [۹] مولفین ابتدا استنادپذیری ادله دیجیتال در حوزه اینترنت اشیا را در سه سطح استنادپذیری در ابر، استنادپذیری شبکه های اینترنتی و استنادپذیری در تجهیزات مربوط به اینترنت اشیا (سرور و کسی<sup>۵</sup> در [۱۰] وجود برنامه های مربوط به تلفن همراه و چالش های مربوط به آن را نیز در این قسمت بر شمرده اند) تقسیم بندی می کنند و عنوان کرده اند که بسیاری از حملات صورت گرفته به علت وجود نقص در امنیت تجهیزاتی است که به صورت شبکه در کنار هم قرار می گیرند که سبب حملاتی در دسته های مختلف نرم افزاری، پروتکلی، سخت افزاری، رمزنگاری داده ها و سوء استفاده از داده ها می شوند مانند حملات سرریز بافر، حملات باج افزاری و ... در نهایت چالش های فارتزیکتی را در ۶ دسته تقسیم بندی می کنند [۱۱و۱۲]:

مشکلات مربوط به شناسایی تجهیزات: به سبب تغییرات مکان فیزیکی تجهیزات، تعدد و تنوع بالا تجهیزات متصل شده، داده های حجیم ایجاد شده از تجهیزات و ... شناسایی تجهیزات مشکلاتی را به وجود می آورند.

شده از شواهد اصلی بجای خود شواهد است لازم به ذکر است که حفظ اصالت سیستم و حافظه رایانه در زمان انتقال اطلاعات و کپی گرفتن از آنها، از وظایف کارشناس فارتزیک می باشد [۷].

## ۱-۲. اهمیت و ضرورت تحقیق

مهمترین اهمیت آینده پژوهی در خصوص استنادپذیری ادله دیجیتال جرایم اینترنت اشیا این است که یک فرصت ساختاریافته برای نگاه به آینده و بررسی نقش مؤلفه های تأثیرگذار در آینده استنادپذیری فراهم می آورد و زمینه و بستر مناسبی را جهت سیاست گذاری در زمینه های گوناگون فراهم می کند. آینده پژوهی استنادپذیری ادله دیجیتال جرایم اینترنت اشیا در مبانی و اصول خود، سازوکاری منظم را از طریق تحت تأثیر قرار دادن تصمیم گیری های بلندمدت در خصوص تسهیل کردن فرآیند استنادپذیری ادله دیجیتال، ارائه می کند و این شاید مهمترین دلیل بر اهمیت بسیار زیاد این علم نوظهور باشد. علاوه بر این، می توان اهمیت آینده پژوهی استنادپذیری جرایم اینترنت اشیا را در آماده شدن خود و مردم در برابر آینده این نوع جرایم و موارد امنیتی در رابطه با آن؛ کسب نمای کلی از اهمیت و چالش های موجود و در حال ظهور؛ درک زودهنگام خطرات و هشدارها؛ برنامه ریزی و سرمایه گذاری برای به دست آوردن منافع موجود، دانست.

ضرورت پاسخ به استنادپذیری جرایم اینترنت اشیا در سطح مراکز قضایی و انتظامی، به ویژه حوزه جرائم سایبری و چالش های پیش روی این مراکز در حال حاضر توجه و تمرکز به انواع رویکردهای مطرح در آینده پژوهی این چالش ها را اجتناب ناپذیر می کند.

## ۱-۳. پیشینه تحقیق

بررسی تحقیقات انجام شده توسط محققان قبلی نشان می دهد که در حوزه آینده پژوهی جرایم سایبری با رویکرد استنادپذیری در آنها، مطالعه ویژه ای انجام نشده است؛ لیکن

<sup>۲</sup> The Breach of Privacy

<sup>۵</sup> Servida, Casey

<sup>۱</sup> Node Tampering

<sup>۲</sup> Denial of Service

<sup>۳</sup> Buffer Overflow

جمع آوری اطلاعات: به علت نبود استاندارد در نرم افزار و سخت افزار تجهیزات موجود، وجود الگوریتم های رمزنگاری و یا کدینگ اطلاعات استخراجی از تجهیزات، نبود آموزش های لازم برای چگونگی جمع آوری اطلاعات در بررسی صحنه جرم و ... جمع آوری اطلاعات در این مرحله با مشکل روبرو می شود.

مشکلات مربوط به محافظت از داده ها: با توجه به بازنویسی اطلاعات، نبود حافظه به اندازه کافی برای ذخیره اطلاعات، فقدان قوانین لازم و ... محافظت از داده ها را با چالش روبرو ساخته است.

آنالیز: شاید بتوان اشاره کرد که مهمترین چالش مربوط به این قسمت می باشد چراکه چالش هایی مانند دسترسی به داده های ذخیره شده در ابر، عدم امکان بررسی آنها به انتهای تجهیزات به کار رفته و شواهد موجود، عدم همبستگی بین شواهد اکتساب شده، عدم ثبت اطلاعات در سرایند فایل ها و ... سبب مشکل در آنالیز مناسب می شود.

۱- ویژگی حملات: مشکلاتی مانند مخفی سازی IP های به کار گرفته شده، عدم وجود قطعیت برای بیان صاحب اصلی داده ها و چگونگی تغییرات اعمال شده به آنها و ... مربوط به این چالش می شود.

چالش در ارائه شواهد به محاکم قضایی: با توجه به ماهیت نوظهور بودن اینترنت اشیاء و تکنولوژی مربوط به ابر نیاز به آموزش های کافی در این خصوص است همچنین با توجه به در دسترس بودن اطلاعات و شواهد برای سایرین نمی توان اصالت داده ها را در تمام شرایط ضمانت کرد.

محققان آینده پژوهی را در حدس حالات ممکن آینده، ارزیابی آیندهی محتمل و انتخاب آیندهی مطلوب می دانند که آینده پژوه برای دسترسی به آینده مطلوب مستلزم بهره گیری از روش های متعددی است. برای مثال، از طریق تحلیل روندهای کنونی فقط می توان در مورد حالات ممکن و محتمل آینده اطلاعات کسب کرد، اما نمی تواند اطلاعات قابل ملاحظه ای پیرامون آیندهی مطلوب در اختیار بگذارد. با تکنیک های پیش بینی آینده می توان به واسطه ی برون ریزی ذهنی طیف وسیعی از آینده های ممکن و نیز تصور گزینه های مطلوب به اطلاعات سودمندی در باب

حالات ممکن و مطلوب آینده دست یافت، این در حالی است که بدون بهره گیری از تکنیک های مختلف نمی توان به اطلاعات کافی در خصوص حالات محتمل آینده های مطلوب دسترسی پیدا کرد. در ادامه برخی از کارهای مرتبط با موضوع تحقیق آورده شده است.

در مقاله [۱۳] تحت عنوان «جایگاه آینده پژوهی در جرم یابی» مولفین باروش توصیفی تحلیلی آینده پژوهی در جرم یابی را مدنظر قرار داده و با مرجع دانستن پلیس در بحث امنیت جامعه مواردی را در جهت داشتن آینده ای بهتر پیشنهاد داده اند از جمله اهداف و سوالاتی که در طرح ایشان بیان شده عبارت اند از: شناسایی جایگاه آینده پژوهی در علوم جرم یابی، شناخت مفاهیم، مبانی و اهمیت آینده پژوهی در علوم جرم یابی؛ شناخت کارکردهای آینده پژوهی در علوم جرم یابی و شناخت اصول آینده پژوهی در علوم جرم یابی.

مولفین مقاله [۱۴] با عنوان «آینده پژوهی و پیشگیری از جرم»، نیز با روش توصیفی به مبانی و اصول آینده پژوهی پرداخته و در نهایت، به ابعاد و مؤلفه های مدیریت پیشگیری از جرم از جمله، تحول در شیوه های مدیریتی، ارتباط کاری مناسب بین مدیران و زیردستان، ارزیابی عملکرد و نظارت بر کارها، آگاه سازی کارکنان، ترویج فرهنگ اسلامی و بهداشت روانی و آرامش با رویکرد آینده پژوهی اشاره کرده است که نهایتاً عنوان کرده اند که مدیران برنامه ریز در حوزه استنادپذیری جرایم دیجیتال باید ضمن تجهیز خود به هنر مدیریت در محیط بی ثبات و پویا و یادگیری چگونگی برخورد با پدیده تغییر و بهره برداری از آن، علم آینده پژوهی را نیز فرا بگیرند.

در مقاله [۱۵] تحت عنوان «آینده پژوهی چالش های سازمانی فرا روی پلیس متأثر از جهانی شدن»، مولفین با اهداف و سؤالاتی از جمله؛ جهانی شدن چیست و روند آن چگونه است؟ با روند فعلی جهانی شدن، جامعه نوین پیش رو (جامعه اطلاعات) چه چشم اندازی خواهد داشت؟ برخی از چالش هایی که ناجا در افق آینده تا ۱۴۰۴ با آن روبه رو خواهد بود کدام اند؟ به بررسی مسئله پرداخته و یافته هایی که برخی از چالش های فرا روی ناجا از دیدگاه خبرگان است در

**۱-۴-۲. سوال‌های فرعی**

(۱) چه راهکارهایی را می‌توان برای رسیدن به حالت مطلوب استنادپذیری جرایم اینترنت اشیا در نظر گرفت؟  
برای ارزیابی وضعیت موجود استنادپذیری جرایم اینترنت اشیا چه مقیاسی را می‌توان مدنظر قرار داد؟

**۱-۵-۵. هدف‌های تحقیق****۱-۵-۱. هدف اصلی**

آینده پژوهی جرایم سایبری مربوط به اینترنت اشیا با رویکرد برطرف نمودن چالش‌های استنادپذیری می‌باشد.

**۱-۵-۲. هدف‌های فرعی**

(۱) شناخت چالش‌های استنادپذیری جرایم مربوط به اینترنت اشیا و ارائه راهکارهایی جهت فائق آمدن بر چالش‌های حال و آینده این جرایم.

ارائه راهکارهایی برای بررسی و ارزیابی وضعیت موجود در استنادپذیری جرایم اینترنت اشیا.

**۱-۶-۶. روش‌شناسی تحقیق**

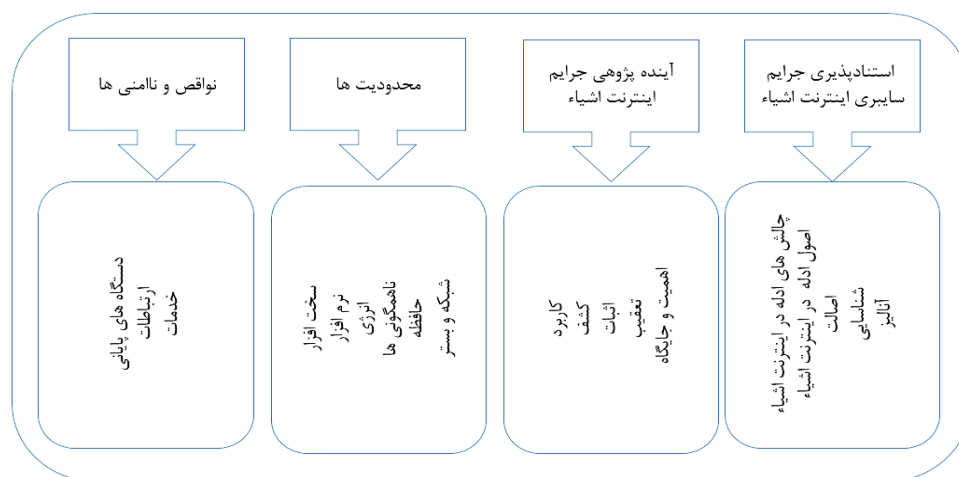
برای انجام این تحقیق هم از مطالعات کمی و هم از مطالعات کیفی به عنوان منبع داده استفاده شد. در این مرحله به بررسی ایده‌ها، رویکردها، نتایج و یافته‌های پژوهش‌های کیفی و کمی پیشین با هدف طراحی و توسعه مدل مفهومی آینده پژوهی استنادپذیری ادله دیجیتال در جرایم سایبری ناشی از اینترنت اشیا پرداخته می‌شود. لذا روش پژوهش در این تحقیق ترکیبی است و در دو بخش کیفی و کمی و در سه گام انجام شد. در گام اول پژوهش با بررسی نظام‌مند متون، جستجو در تحقیقات پیشین و نظریات موجود در خصوص موضوع مولفه‌ها استخراج گردید و یک مدل مفهومی پیشنهادی اولیه از این یافته‌ها ترسیم شد [۷، ۱۷، ۱۸ و ...]. مدل مفهومی اولیه تحقیق، حاصل این گام می‌باشد که در شکل ۱ به نمایش گذاشته شده است.

ابعاد و عناوین سیاسی و تقنینی؛ فرهنگی و مردمی (انسانی)؛ استراتژی و ساختار و خدمات و کالا (اقتصادی) شناسایی، تقسیم بندی و ارائه کرده است که همان طور که مولفین در تحقیق خود اشاره کرده اند تحولات جهانی شدن و پیدایش جامعه نوین و چالش‌های فراروی پلیس ضرورت و نیازمندی در حوزه‌های آینده پژوهی و آینده نگاری در مراکز مطالعاتی پلیس را نشان می‌دهد و نهایتاً، در یافته‌های تحقیق خود مؤلفه‌های سیاسی، فرهنگی و غیره را به عنوان متغیرهای مستقل و چالش‌های فراروی آینده استنادپذیری جرایم دانسته اند. لذا برای حل مشکلات مقابله و کشف جرائم در کشور، به کارگیری مدیران و برنامه ریزان قوی در حوزه استنادپذیری جرایم با رویکرد آینده پژوهانه، تلاش برای شناخت رویدادهای آینده و مؤلفه‌های تأثیرگذار بر آنها، به کارگیری ابزارها و راهکارهای مدیریتی (منطبق با محیط آینده) را پیشنهاد داده اند.

در تحقیق [۱۶] با عنوان «آینده پژوهی پلیس؛ رهیافتی نو برای تحقق امنیت اجتماعی»، مولفین با روش توصیفی-تحلیلی به دنبال پاسخ به این سؤال که آینده پژوهی چه نقشی در کارایی نیروی انتظامی برای برقراری نظم و امنیت اجتماعی داشته و چه سازوکارهایی برای ایفای این نقش وجود دارد، بوده است که راهبردها و سیاست‌گذاری‌ها در حوزه ساختار مدیریتی، آموزشی، پژوهشی و فناورانه در حوزه پیشگیری از جرم و ضرورت آینده پژوهی برای درک سریع متغیرهای محیطی و پیش‌بینی تهدیدها و احراز آمادگی‌های لازم برای پیشگیری از وقوع جرم و حفظ و گسترش رفاه و امنیت جامعه عنوان شده است.

**۱-۴-۴. سؤال‌های تحقیق****۱-۴-۱. سوال اصلی**

چالشها و راهکارهای برطرف سازی آنها در استناد پذیری ادله اثبات دعاوی سایبری مرتبط با اینترنت اشیا در آینده چه خواهد بود؟



شکل ۱. دسته بندی مولفه های موثر در اینترنت اشیا

و حقوقی با استفاده از مقیاس پایایی و روایی مورد بررسی قرار گرفت و نهایتاً داده های حاصل با استفاده از آمار توصیفی و استنباطی (با میانگین آماری و آزمون فریدمن و ارزیابی سطح بلوغ CMMI) مورد تجزیه و تحلیل قرار گرفت.

**جامعه آماری:** جامعه آماری در این تحقیق شامل افسران ارشد و خبرگان در حوزه اینترنت اشیا و استنادپذیری ادله دیجیتال شاغل در قسمت های مختلف پلیس های تخصصی، محققین دانشگاهی در حوزه اینترنت اشیا، صنعتگران و کارآفرینان در حوزه اینترنت اشیا و امنیت شبکه می باشند.

**نمونه و روش نمونه گیری:** از جامعه آماری مذکور ۳۲ نفر از خبرگان، محققین و افسران که مهارت لازم و تجربه کاری بالایی در بخش های مختلف و مرتبط را داشتند، انتخاب و بین همه آنها پرسشنامه توزیع شد و از خبرگان مصاحبه به عمل آمد. از بین این ۳۲ نفر ۸ نفر به عنوان خبره و ۲۴ نفر به عنوان خبره میانی در نظر گرفته شد. خبرگان به روش هدفمند در طول فرآیند تحقیق انتخاب شدند. نمونه گیری هدفمند یکی از روش های شایع نمونه گیری است که گروه های شرکت های کننده بر اساس معیارهای از قبل مشخص شده مربوط به سؤال ویژه پژوهش انتخاب می شوند.

در گام دوم با استفاده از روش تحقیق کیفی و کمی، الگوی اولیه تحقیق از طریق مصاحبه با خبرگان ارشد غنی تر گشت و برخی از اشکالات آن اصلاح شد که مدل ثانویه و تکمیلی پژوهش، خروجی این مرحله می باشد. در مرحله دوم تحقیق، با توجه به این که نظریه یا پژوهش های پیشین درباره آینده پژوهی استنادپذیری ادله دیجیتال جرایم سایبری ناشی از اینترنت اشیا در آنها کامل نبودند لذا محقق از روش کیفی با رویکرد نظرات خبرگان متکی بر نظریه یا پژوهش های پیشین بهره جست. هدف از این کار معتبر ساختن و گسترش دادن چارچوب یا مدل مفهومی مرحله قبلی است. در این مرحله مدل مفهومی برآمده از مرحله اول، توسعه داده شد و بر اساس مدل توسعه داده شده سوالات پرسش نامه تهیه و تدوین گردید مدل توسعه داده شده در شکل (۲) قابل مشاهده می باشد.

در گام سوم به منظور اعتبار سنجی کمی مدل تکمیلی، نظر خبرگان میانی که بصورت هدفمند انتخاب گردیده بودند گرفته شد و پس از تدوین پرسشنامه بر اساس مدل ثانویه، نسبت به بررسی روایی ابزار تحقیق از روایی محتوایی همچنین برای بررسی پایایی ابزار تحقیق از روش آلفای کرونباخ استفاده شد. سپس عملیات جمع آوری اطلاعات از طریق پرسشنامه ۳۶ سوالی با طیف لیکرت ۵ سطحی در ۳ بعد آموزشی، زیرساختی



شکل ۲. مدل مفهومی تحقیق

## ۲. ادبیات و مبانی نظری تحقیق

### ۲-۱. مفهوم آینده پژوهی

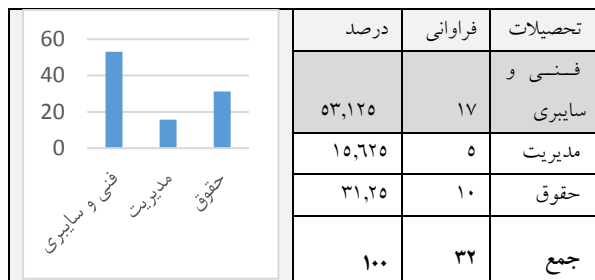
آینده پژوهی مطالعاتی است که به بشر کمک می کند این مسیر را با کمترین ضرر بپیماید. امروزه آینده پژوهی به یکی از ابزارهای مهم سیاست‌گذاران برای کمک به ترسیم چشم‌اندازها و اتخاذ تصمیم‌های میان‌مدت تا بلندمدت تبدیل شده است. "آینده پژوهی مشتمل بر مجموعه تلاش‌هایی است که با استفاده از تجزیه و تحلیل منابع، الگوها و عوامل تغییر و یا ثبات، به تجسم آینده بالقوه و برنامه‌ریزی برای آن‌ها می‌پردازد". باید توجه داشت، اساساً آینده قطعیت ندارد، اگرچه آثار و واقعیت‌هایی که در گذشته و حال ریشه دارند، می‌توانند ما را به آینده رهنمون کنند [۱۹].

### ۲-۲. مفهوم اینترنت اشیا

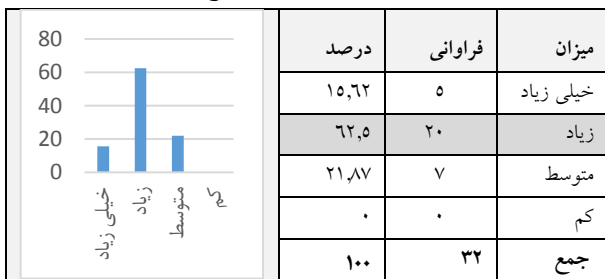
دنیای امروز متشکل از مجموعه‌ای از اشیای فیزیکی است که با شبکه‌ای از حسگرها و عامل‌های هوشمند تجهیز شده‌اند این مفهومی است و زمینه‌ساز یک رویکرد گسترده به دنیایی است که در آن همه چیز از اشیاء و ماشین‌آلات تا افراد به یکدیگر متصل هستند و می‌توانند با یکدیگر به تبادل داده و اطلاعات بپردازند [۲۰]. با وجود مصطلح شدن عبارت اینترنت اشیا در سال‌های اخیر، اما هنوز تعریف واحدی برای آن وجود ندارد. طبق تعریف مؤسسه تحقیقاتی گارتنر<sup>۱</sup>، IoT، شبکه‌ای از اشیای فیزیکی است که دربرگیرنده مجموعه‌ای از فناوری‌های تعبیه شده برای برقراری ارتباط، حس کردن و تعامل با محیط خارجی و یا اجزای داخلی یک شیء می‌باشند. اگرچه عدم وجود یک تعریف واحد از اینترنت اشیا در هنگام گفتگو در مورد مسائل این حوزه، می‌تواند برای ذینفعان و بخش‌های مختلف

<sup>1</sup> Gartner Inc: <http://www.gartner.com/it-glossary/internet-of-things>

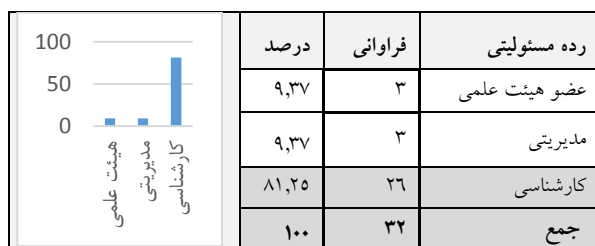
جدول ۳. رشته تحصیلی نمونه آماری



جدول ۴. میزان آشنایی با موضوع نمونه آماری



جدول ۵. رده مسئولیتی نمونه آماری



### ۳-۳. سوالات استنباطی تحقیق

لازم به یادآوری است که سوالات تحقیق ۳۶ مورد در نظر گرفته شده که از طریق آنها نظرات نخبگان میانی درباره شاخص‌های هر سوال جمع‌آوری گردیده است. ابعاد، مولفه و شاخص مربوط به هر کدام از سوالات در جدول (۱۰) آمده است.

### ۳-۴. روایی ابزار تحقیق

در جهت بررسی میزان روایی تحقیق، اقداماتی به شرح ذیل صورت گرفته است:

- ۱- استفاده و اخذ نظر کارشناسان و متخصصان در زمینه اینترنت اشیاء و استنادپذیری ادله دیجیتال.
- ۲- تأمین نظر اساتید و خبرگان این حوزه و تأیید روایی ابزار با بهره‌گیری از روش اعتبار صوری و تنظیم پرسشنامه اولیه.
- ۳- مطالعه پرسشنامه‌های مربوط به کارهای مرتبط.

صنعت باعث سردرگمی شود، اما باید توجه داشت که تعاریف ارائه شده لزوماً با یکدیگر در تضاد نیستند و تنها هر یک این فناوری را از دیدگاه‌های متفاوتی مورد بررسی قرار داده‌اند.

## ۳. یافته‌های تحقیق و تجزیه و تحلیل آن‌ها

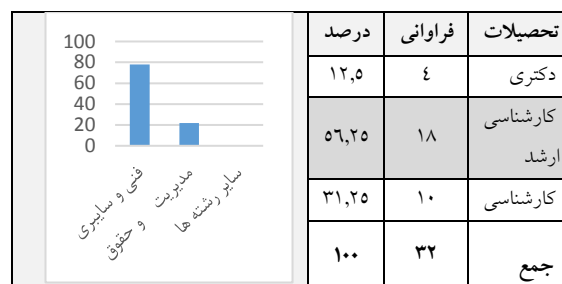
### ۳-۱. تشریح پرسشنامه

همان‌گونه که قبلاً نیز بیان گردید، ابزار اصلی جمع‌آوری اطلاعات در این تحقیق، پرسشنامه است. پرسشنامه مورد استفاده شامل دو قسمت بوده که قسمت اول مربوط به سئوالات جمعیت شناختی خبرگان و قسمت دوم مربوط به سئوالات تحقیق می‌باشد.

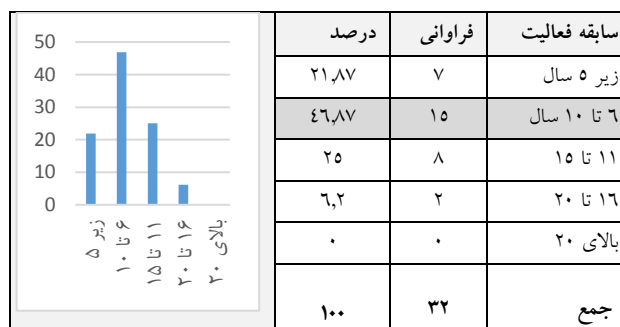
### ۳-۲. سوالات جمعیت شناختی

در این بخش، اطلاعات جمعیت‌شناختی مشتمل بر میزان تحصیلات، رشته تحصیلی، میزان آشنایی با موضوع تحقیق، سابقه یا سنوات خدمتی و رده مسئولیتی بیان می‌گردد که در قالب جداول و نمودارهای شماره ۱ تا ۵ به توصیف ویژگی‌ها پرداخته می‌شود عنوان هر جدول بیانگر یکی از ویژگی‌های پرسش‌شوندگان بوده و مورد با بیشترین آمار به صورت خاص مشخص شده است.

جدول ۱. میزان تحصیلات نمونه آماری



جدول ۲. سابقه فعالیت نمونه آماری





### ۳-۵. پایایی ابزار سنجش

پایایی و اعتبار پرسش نامه این تحقیق با محاسبه آلفای کرونباخ، مورد سنجش قرار گرفته است. مقدار ضریب آلفای کرونباخ کل ۰,۷۸ به دست آمد که نشان دهنده وجود پایایی بالایی برای پرسشنامه می باشد (جدول ۷).

جدول ۷. پایایی جزئی پرسشنامه

متغیر	مقدار آلفای کرونباخ
۱ استنادپذیری جرایم سایبری مرتبط با اینترنت اشیاء	۰,۸۳
آینده پژوهی جرایم اینترنت اشیاء	۰,۷۸
محدودیت ها	۰,۷۴
نواقص و نامنی ها	۰,۷۶
میانگین آلفای کرونباخ	۰,۷۸

۳-۶. تحلیل داده های استخراجی از پرسش نامه ها  
در این مقاله، از روش های توصیفی آماری شامل درصد فراوانی و آزمون فریدمن با بهره گیری از نرم افزار SPSS برای بیان نظرات خبرگان میانی استفاده شده است که برای نمونه نتایج حاصل از شاخص شماره ۱ به نمایش گذارده شده است. شاخص شماره ۱: فاز شناسایی (یکی از مهمترین چالش های استنادپذیری ادله در اینترنت اشیاء شناسایی شواهد موجود می باشد که با توجه به ویژگی های موجود در جرایم سایبری بعضا دسترسی به چنین شواهدی مشکل و یا غیر ممکن می باشد).

مؤلفه ۱: چالش های استنادپذیری در اینترنت اشیاء

بعد ۱: استنادپذیری جرایم سایبری مرتبط با اینترنت اشیاء

جدول ۸. شاخص شماره ۱: فاز شناسایی



### ۳-۷. تحلیل آماری سوالات تحقیق با استفاده از آزمون رتبه ای فریدمن

با توجه به سطح معنی دار  $Asymp.sig = 0$  معنادار بودن آماره آزمون قابل قبول می باشد. تحلیل عاملی اکتشافی این مسئله که شامل ۱۰ مؤلفه است، در جدول زیر درج شده است:

جدول ۹. تحلیل آماری سوالات تحقیق با آزمون رتبه ای فریدمن

N	Chi-Square	Df	Asymp. Sig
تعداد	آزمون خی دو	درجه آزادی	سطح معناداری
10	496.528	113	.000

جدول و نمودار فوق، جایگاه شاخص شماره ۱ را از نظر شرکت کنندگان در ۳ بعد آموزشی، زیرساختی و حقوقی نشان می دهد که نتیجه نظریات خبرگان اهمیت زیاد را به خود اختصاص داده است.

جدول ۱۰. تحلیل آماری سوالات تحقیق و رتبه بندی آنها

میانگین بارعاملی	رتبه	حقوقی	زیرساختی	آموزشی	گویه ها	مولفه	بعد
77/91	1	75/35	86	85/25	فاز شناسایی	چالش های ادله در lot	استنادپذیری جرایم سایبری مرتبط با اینترنت اشیا
	6	75/1	80/05	79/15	فاز حفظ و نگهداری اطلاعات		
	2	68/95	88/05	86/85	فاز آنالیز		
	7	87/05	69/5	50/45	فاز ارائه		
	5	69/35	79/3	87/6	اصل اصالت	اصول ادله در lot	
	4	76/1	82/15	78/6	اصل مشابهت(کپی بیت به بیت)		
	3	72/9	82/5	85/35	اصل شبیه سازی		
	8	75/1	80/05	69/15	اصل تبادل		
68	2	65/12	85/23	78/69	احراز آمادگی های لازم	کاربردها	آینده پژوهی جرایم اینترنت اشیا
	1	71/95	85/8	82/4	پیش نگری فناوری های آینده استنادپذیری ادله جرایم		
	7	58/65	66/35	57	کشف جرم	اهمیت و جایگاه	
	5	65/5	69/85	64/9	اثبات جرم		
	6	54/65	71/4	65/75	تعقیب و دستگیری متهمان		
	8	49/7	59/4	54/65	انجام تحقیقات مقدماتی در جهت پیش گیری از جرایم و اعتبار و قطعیت یافته های استنادپذیری ادله جرم		
	3	70/7	75/7	75/97	تعیین نوع جرم ارتكابی		
	4	75/25	63/1	65/65	محاکمه		
64/9	5	37/7	92/35	50/4	انرژی مورد نیاز سخت افزار های به کارگیری شده	سخت افزار	محدودیت ها
	4	55	76/95	63/15	حافظه مورد نیاز		
	8	60/95	70/85	71/3	ایمنی فیزیکی ابزارهای به کار گیری شده		
	1	55/05	78/5	81/35	نرم افزار های تعریف شده(مثال: حمله اکتشافی)	نرم افزار	
	6	35/75	78/3	65/15	محدودیت های برنامه ریزی(به سبب جایگزینی با میان افزارها)		
	7	44	74/6	60/45	توسعه پذیری	شبکه	
	2	62/55	75	68/7	ناهمگونی دستگاه های متصل		
	3	60/85	73/25	65/45	ناهمگونی رسانه های مورد استفاده(مثال: تحریف ساعت، جمینگ)		

70/34	1	74/5	87/6	80/2	دستکاری داده ها در ذخیره سازها	در دستگاه های پایانی	نواقص و ناامنی ها
	2	70/7	82/3	81/1	رمزگشایی و استخراج اطلاعات از ذخیره سازها		
	10	44/95	66/15	65/1	وجود کدک های مخرب به سبب وجود انواع اشیا		
	3	64/18	81/15	84/15	جعل هویت در نرم افزارها		
	4	61/75	81/1	83/6	ایجاد برنامه های مخرب و کنترل از راه دور		
	9	58/21	67/56	65/36	ایجاد خلل در خدمات دهی به اشیا	در خدمات	
	11	57/3	58/27	59/32	تهدید در حریم خصوصی خدمات دهی ابری		
	8	64/75	72/15	65/25	تهدید در خدمات دهی ابری اشتراکی		
	7	63/75	75/45	72/35	وجود تهدیدات در امنیت ارتباطات اشیا(مثال: سو استفاده از مسیریابی)	در ارتباطات	
	6	63/75	75/75	74/15	وجود تهدیدات در امنیت خدمات شبکه ای(مثال: انسداد سرویس)		
	5	61/75	81/1	76/6	وجود تهدیدات در رمزنگاری ارتباطات (مثال: جعل هویت)		

### ۳-۷-۱. نتایج حاصل از تجزیه و تحلیل

بعد آموزش: بعد آموزش اشاره به یاددهی و یادگیری نیروهای تخصصی در جهت مرتفع سازی مشکلات استنادپذیری ادله دیجیتال دارد. برابر تحلیل نظریات خبرگان در این بعد بر اساس ارزیابی سطح بلوغ CMMI با نمره ۵۷,۶۷۵ در سطح سوم بوده یعنی استانداردهای لازم تعریف و استفاده می گردد.

مدل ساختاری تحقیق آینده پژوهی استنادپذیری ادله دیجیتال در اینترنت اشیا برای بررسی در سه سطح آموزشی، زیرساختی و حقوقی با چهار متغیر و بعد معنادار استنادپذیری جرایم سایبری مرتبط با اینترنت اشیا، آینده پژوهی جرایم اینترنت اشیا، محدودیت ها و نواقص و ناامنی ها مورد بررسی قرار گرفت که از بین این چهار بعد، بعد استنادپذیری جرایم سایبری مرتبط با اینترنت اشیا با ۷۷,۹۱٪، بعد آینده پژوهی جرایم اینترنت اشیا با ۶۸٪، بعد محدودیت ها با ۶۴,۹٪ و بعد نواقص و ناامنی ها با ۳۴,۷۰٪ بار عاملی برخوردار بوده اند.

جدول ۱۱. ارزیابی بلوغ استنادپذیری در حوزه اینترنت اشیا

بعد رایانش ابری	آموزشی	زیرساختی	حقوقی
میانگین نمره ارزیابی	۵۷,۶۷۵	۴۱,۹۱	۳۹,۶۱



شکل ۳. سطوح بلوغ در CMMI

### ۳-۷-۲. تحلیل بلوغ بر مبنای CMMI

بر مبنای مدل سطوح بلوغ در CMMI جایگاه بررسی استنادپذیری در حوزه اینترنت اشیا و در سه بعد آموزشی، زیرساختی و حقوقی در (جدول ۱۱) آورده شده است:

طبق ارزیابی صورت گرفته و سطوح بلوغ در CMMI، آینده پژوهی استنادپذیری در حوزه اینترنت اشیا را می توان به این صورت تعریف کرد:

**بعد زیرساخت و تجهیزات:** بعد زیرساخت و تجهیزات اشاره به چالش‌هایی دارد که این بعد کار استنادپذیری جرایم حوزه اینترنت اشیا را مشکل و یا غیر ممکن می‌کند و مربوط به تجهیزات فیزیکی، شبکه‌ای، داده‌ای (اطلاعات مربوط به شناسه هر فرد و ...)، نرم‌افزاری، ذخیره‌سازها و محاسبات و ... می‌باشد. برابر تحلیل نظریات خبرگان در این بعد بر اساس ارزیابی سطح بلوغ CMMI با نمره ۴۱,۹۱ در سطح سوم بوده یعنی استانداردهای لازم تعریف و استفاده می‌گردد.

**بعد حقوقی:** بعد حقوقی اشاره به روابط و مقررات داخلی و بین‌المللی، روابط و قراردادهای، وظایف تعریف شده برای نهادها و ارگان‌های داخلی و بین‌المللی و قوانین حریم خصوصی و امنیتی دارد. برابر تحلیل نظریات خبرگان در این بعد بر اساس ارزیابی سطح بلوغ CMMI با نمره ۳۹,۶۱ در سطح دوم بوده یعنی مدیریت یافته‌بوده و فرآیندها اندازه‌گیری و کنترل می‌گردد، البته لازم به ذکر است که چالشی که در بعد حقوقی وجود دارد چالش برانگیزترین مورد می‌باشد و دلیل این مورد هم به قوانین و مشکلات حقوقی داخلی برمی‌گردد و هم به قوانین و مشکلات حقوقی خارجی که برای برطرف شدن مشکلات داخلی باید با توجه به نهادهای ذی‌صلاح مطالعات لازم صورت گیرد، آیین‌نامه‌ها نوشته‌شود و بعد از بررسی تمام جوانب آن قوانین لازم تصویب گردد ولی در مورد موانع بین‌المللی باید کنوانسیون‌های بین‌المللی در این زمینه ایجاد و راهکارهای واحد بین تمام کشورها و یا با توجه به روابط بین کشورهای مختلف روابط دو جانبه بین کشور جمهوری اسلامی ایران و کشورهای دیگر ایجاد شود تا بتوان چالش‌ها و شکاف‌های قانونی بین‌المللی را برطرف کرد.

#### ۴. نتیجه‌گیری

##### ۴-۱. جمع‌بندی

آینده پژوهی و آینده‌شناسی حوزه استنادپذیری جرایم دیجیتال، آینده را به کمک امروز آورده و مبنای تصمیم‌گیری‌ها، سیاست‌گذاری‌ها و برنامه‌ریزی‌ها در ساختار مدیریتی، آموزشی، پژوهشی و فناوری کشور قرار خواهد داد. بنابراین، از اهم

ضرورت‌های کاری کشور و محاکم قضایی که فوت وقت در آن موجب فسادها، خسارتها و تأسفات‌های بسیاری خواهد شد، تربیت آینده‌نگرهایی است که یاد بگیرند چگونه آینده را بررسی کنند و آینده‌پژوهانی که با ارائه تصویری محتمل و بدیل از آینده، نگاه جامعه و مدیران به آینده را واقع‌بینانه و سازنده نمایند. لذا با وجود مرکز استنادپذیری جرایم دیجیتال سایبری در ساختار محاکم قضایی و انتظامی در سطح کشور، میتوان توسعه بنیان معرفتی و دانش آینده‌پژوهی در مجموعه برنامه ریزان و کارکنان نهادهای امنیتی و انتظامی را انتظار داشت.

البته در تحقیقات پیشین به نوعی به موارد اکتساب شده در این تحقیق اشاره شده است که در قسمت مربوط به کارهای انجام شده به این موضوع به صورت کامل پرداخته شده است و بیانگر این می‌باشد که با نتایج و یافته‌های پژوهش حاضر همپوشانی و ارتباط مستقیم دارد.

لذا با توجه به سوال اصلی تحقیق یافته‌های مرتبط با شاخص‌ها و الگوی‌های متجانس با رویکرد استنادپذیری جرایم اینترنت اشیا، با توجه به مطالعات صورت گرفته و نظرات نخبگان، پیشنهادات محققین مقاله در دو مدل مفهومی اولیه و مدل حاصل از نظرات نخبگان در اشکال ۱ و ۲ و در جدول ۵ در ۴ بعد کلی بیان گردید که از بین این چهار بعد، بعد استنادپذیری جرایم سایبری مرتبط با اینترنت اشیا با ۷۷,۹۱٪، بعد آینده‌پژوهی جرایم اینترنت اشیا با ۶۸٪، بعد محدودیت‌ها با ۶۴,۹٪ و بعد نواقص و ناامنی‌ها با ۳۴,۷۰٪ بار عاملی برخوردار بوده‌اند که بیانگر این می‌باشد که از دید پاسخ‌دهندگان مهمترین چالش در آینده مربوط به استنادپذیری جرایم مرتبط با اینترنت اشیا می‌باشد و با توجه به چالش‌های مطرح شده در مدل ارائه شده باید راهکارهایی برای این موارد دیده شود.

با توجه به سوال فرعی اول که به راهکارهای برون‌رفت از چالش‌ها اشاره دارد و با توجه به نظرات اکتسابی از پرسش‌نامه‌ها و نظرات خبرگان راهکارهای فائق‌آمدن بر چالش‌ها در سه قسم برطرف نمودن نیازهای آموزشی، ایجاد بستر و زیرساخت مناسب و تدوین قوانین و آیین‌نامه‌های به‌روز در نظر گرفته شده است برای نمونه در جدول ۱۲ به برخی از چالش‌ها و نحوه برون‌رفت از آنها توضیح داده شده است.

جدول ۱۲. تشریح برخی از چالش ها و رویکردهای پیشنهادی برای برون رفت از آنها

گویه ها	آموزشی	زیرساختی	تشریح چالش و راهکارها
فاز شناسایی	85/25	86	75/35
اصل اصالت	87/6	79/3	69/35
احراز آمادگی های لازم	78/69	85/23	65/12
کشف جرم	57	66/35	58/65
حافظه مورد نیاز	63/15	76/95	55
ناهمگونی دستگاه های متصل	68/7	75	62/55
رمزگشایی و استخراج اطلاعات از ذخیره سازها	81/1	82/3	70/7

در بعد زیر ساخت و تجهیزات که اشاره به چالش های موجود در شبکه های کامپیوتری و سایر زیرساخت ها دارد نمره ۴۱،۹۱ کسب شده است. در بعد حقوقی نیز نمره ۳۹،۶۱ اکتساب گردیده که برای برطرف شدن مشکلات و چالش های مربوط به این حوزه هم باید قوانین داخلی و هم قوانین خارجی مد نظر قرار گیرد. نتیجه به دست آمده حاکی از آن است که ارگان های دخیل در مسیر استانداردپذیری و استفاده از ظرفیت های مرتبط در حوزه

در رابطه با سوال فرعی دوم تحقیق که بررسی وضعیت موجود استانداردپذیری جرایم اینترنت اشیا می پردازد پیاده سازی و سنجش بلوغ متناسب با استانداردپذیری جرایم اینترنت اشیا صورت پذیرفته که متناسب با نمره کسب شده در سطح بلوغ CMMI در سه بعد آموزشی، زیرساختی و حقوقی موارد زیر احصاء گردید: در بعد آموزش برابر تحلیل نظریات خبرگان و بر اساس ارزیابی سطح بلوغ CMMI با نمره ۵۷،۶۷۵ کسب گردیده است.

اینترنت اشیاء در چارچوب ها و استانداردهای بین المللی حرکت نموده و با توجه به نوظهور بودن این فناوری، در سطح بلوغ مناسبی قرار دارند و می توانند با رفع اشکالات و پی گیری هدفمند این موضوع به سطح بلوغ مناسبتری برسند.

#### ۴-۲. پیشنهادها

با توجه به موارد احصا شده در تحقیق پیش رو پیشنهادات ذیل را می توان برای برون رفت و رسیدن به حالات بهتر یک سیستم در نظر گرفت:

برون رفت از چالش های آموزشی:

در حوزه آموزشی، استانداردهای مربوط به استنادپذیری اینترنت اشیاء به صورت جامع و مستمر بررسی و وضعیت فعلی ارزیابی و بر اساس دوره های بین المللی برای رسیدن به حالات استاندارد، آموزش ها و الزامات مربوطه به روز گردد طوری که نگرانی که به بررسی استنادپذیری در جرایم مربوط به اینترنت اشیاء می پردازند به تمام فنون مورد نیاز (علوم مربوط به شبکه های کامپیوتری و حملات مربوطه در سطح شبکه و وب و ...) تسلط کافی داشته باشند و تا تحقق سطح پنجم مدل CMMI یعنی لایه بهینه شده این آموزش ها ادامه یابد. با نگاه جزئی تر می توان موارد زیر را در نظر گرفت.

توسعه دانش در زمینه تجهیزات و امکانات سخت افزاری و نرم افزاری موردنیاز واحدهای استنادپذیری جرایم دیجیتال سایبری نوظهور و تولید دانش و ادبیات بومی استنادپذیری جرایم دیجیتال سایبری در کشور؛

به کار گیری مدیران برنامه ریز در حوزه استنادپذیری جرایم دیجیتال که باید ضمن تجهیز خود به هنر مدیریت، علم آینده پژوهی را نیز فرا بگیرند؛ زیرا داشتن نگرش عمیق از تحولات به آینده، نیاز مبرم مدیران در این بخش است.

افزایش قابلیت های علمی واحدهای استنادپذیری جرایم دیجیتال سایبری در زمینه تجزیه و تحلیل چالش ها و مشکلات پیشروی استنادپذیری جرایم دیجیتال سایبری در رسیدگی های قضایی و چگونگی رویارویی و برخورد با این چالش ها و موانع علی الخصوص در جرایم نوظهور؛

برون رفت از چالش های زیرساختی:

در حوزه زیرساخت نیز همانند بعد آموزش نیاز است تا ابعاد زیرساختی اعم از تجهیزات فیزیکی، شبکه ها، داده ها و... با

سطح عمیق تری مطالعه و شاخص های آن برای کارشناسان و ممیزین امنیتی تبیین و تشریح گردد و استانداردهای لازم و آمادگی های فارتزیکتی تا دستیابی به سطوح سوم و چهارم مدل CMMI محقق گردد طوری که در صورت بروز مشکل بتوان شواهد لازم را استخراج و مورد بهره برداری قرار داد.

با نگاه جزئی تر می توان به تدوین مدل معماری اطلاعات ملی و همچنین مهاجرت به زیرساخت آدرس دهی اینترنتی نسخه ۶ از نسخه ۴ جهت استنادپذیری ادله دیجیتالی جرایم مرتبط با اینترنت اشیاء اشاره کرد.

فائق آمدن بر خلاهای قانونی:

در حوزه چالش های حقوقی با توجه به نوظهوری فناوری اینترنت اشیاء و تفاوت های بنیادین آن با فناوری های قبلی، ملازمات و استانداردها به صورت هدفمند ایجاد گردد و تا رسیدن به سطح سوم و یا چهارم مدل CMMI باید این روند ادامه داشته باشد که با نگاه جزئی تر می توان به موارد زیر اشاره کرد:

تدوین و یا بومی سازی استانداردهای تبادلات ماشین به ماشین از طریق سازمان ملی استاندارد با همکاری وزارت ارتباطات و فناوری اطلاعات و در نتیجه اصلاح آیین نامه استنادپذیری ادله دیجیتال و تکلیف آن به دستگاه های مرتبط؛

تهیه و تنظیم استانداردها و قوانین لازم در رابطه با فرمت و مدت ذخیره سازی داده ها و اطلاعات هم در سمت کاربر و هم در سمت ارائه دهنده سرویس؛

با توجه به موارد بیان شده و لزوم آینده پژوهی لازم است مراکز با محوریت آینده پژوهی برای مدیریت حوزه استنادپذیری ادله دیجیتالی توسط مبادی ذی ربط مانند پلیس و قوه قضائیه به عنوان مسئولان اصلی اثبات جرم در کشور ایجاد گردد که برای این مهم می توان از قطب های پژوهشی و دانشگاهی استفاده کرد. به غیر از مراکز دانشگاهی باید مطالعات مستمری در این زمینه در مراکز نظارتی و قضایی صورت پذیرد که ماحصل این مطالعات باید به صورت پیش نویس قوانین مرتبط با فناوری های نوین سایبری تهیه و تنظیم گردد.

## ۵. مراجع (References)

Hashem, Arif Ahmed, SM Ahsan Kazmi, and Choong Seon Hong. "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges." *Future Generation Computer Systems* 92 (2019): 265-275.

[12] Atlam, Hany F., Ezz El-Din Hemdan, Ahmed Alenezi, Madini O. Alassafi, and Gary B. Wills. "Internet of things forensics: A review." *Internet of Things* 11 (2020): 100220.

[۱۳] هندیانی، عبدالله و مرشدی، مسعود (پاییز ۱۳۹۶)، جایگاه آینده پژوهی در جرم یابی. فصلنامه پژوهش های اطلاعاتی و جنایی، ۱۲(۴۷)، صص ۱۳۵-۱۵۶.

[۱۴] عرب انصاری، مهدی (بهار ۱۳۹۴). آینده پژوهی و پیشگیری از جرم. فصلنامه دانش انتظامی سیستان و بلوچستان. ۶(۱۴)، صص ۴۳-۶۴.

[۱۵] رستگار، علی و رضایی، صادق (زمستان ۱۳۹۲). آینده پژوهی چالشهای سازمانی فرا روی پلیس متأثر از جهانی شدن. فصلنامه دانش انتظامی. ۱۵(۴)، صص ۷۹-۱۰۶.

[۱۶] نعیم یآوری، مجید و تقی زاده علیرضا(۱۳۹۱)؛ آینده پژوهی پلیس؛ رهیافتی نو برای تحقق امنیت اجتماعی. همایش ملی آینده پژوهی.

[۱۷] قاسمی یوسف، قلی مرتضی، (۱۳۹۵)، مستندات پروژه تنظیم مقررات و چالشهای حقوقی اینترنت اشیا در کشور.

[۱۸] سازمان فناوری اطلاعات ایران، (۱۳۹۴)، طرح مهاجرت به IPv6

[19] Bell, W. (2003). *Foundations of futures studies: History, purposes, and knowledge* (Vol. 1). Transaction books.

[20] Kechiche, S., George D. and Jain, N., "From concept to delivery: the M2M market today," *GSMA Intelligence*, February 2014.

[1] Tham, Pei En, et al. (2022) "Sustainable smart photobioreactor for continuous cultivation of microalgae embedded with Internet of Things." *Bioresource Technology*, 346: 126558.

[2] Pandey, Neeraj Kumar, and Ajitesh Kumar. (2022), "New Frontiers in Managing and Controlling Industrial Processes Through IoT." *Smart IoT for Research and Industry*. Springer, Cham, 49-68.

[3] Ponnalagarsamy, Sivagami, et al. (2022), "Impact of IoT on Renewable Energy." *IoT Applications Computing*: 107.

[4] Altowajjri, Saleh M. (2022), "Efficient Next-Hop Selection in Multi-Hop Routing for IoT Enabled Wireless Sensor Networks." *Future Internet* 14.2: 35.

[5] Doshi, Nishant. (2022), "Cryptanalysis of authentication protocol for WSN in IoT based electric vehicle environment." *Materials Today: Proceedings*.

[۶] جلالی فراهانی امیرحسین، (زمستان ۱۳۸۶)، استنادپذیری ادله الکترونیکی در امور کیفری، فقه و حقوق، سال چهارم، شماره ۱۵.

[۷] سهلانی حسین، صادقی راشد رضا، (۱۳۹۶)، استنادپذیری ادله دیجیتال، تهران، دانشگاه علوم انتظامی امین.

[8] Zulkipli, Nurul Huda Nik, Ahmed Alenezi, and Gary B. Wills. "IoT forensic: bridging the challenges in digital forensic and the internet of things." In *International Conference on Internet of Things, Big Data and Security*, vol. 2, pp. 315-324. SCITEPRESS, 2017.

[9] Stoyanova, Maria, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis. "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues." *IEEE Communications Surveys & Tutorials* 22, no. 2 (2020): 1191-1221.

[10] Servida, Francesco, and Eoghan Casey. "IoT forensic challenges and opportunities for digital traces." *Digital Investigation* 28 (2019): S22-S29.

[11] Yagoob, Ibrar, Ibrahim Abaker Targio