هيكلة التحقيق الجنائي الرقمي لإنترنت الأشياء

نوف الشهراني
قسم الشبكات والاتصالات
جامعة الإمام عبدالرحمن بن فيصل
الدمام, المملكة العربية السعودية
2190001231@iau.edu.sa

مرام النعيم
قسم الشبكات والاتصالات
جامعة الإمام عبدالرحمن بن فيصل
الدمام, المملكة العربية السعودية
2200004532@iau.edu.sa

أسماء العنزي
قسم الشبكات والاتصالات
جامعة الإمام عبدالرحمن بن فيصل
الدمام, المملكة العربية السعودية
2200003137@iau.edu.sa

نوف الزهراني
قسم الشبكات والاتصالات
جامعة الإمام عبدالرحمن بن فيصل
الدمام, المملكة العربية السعودية
2200004376@iau.edu.sa

نور اشرف ال ابراهيم
قسم الشبكات والاتصالات
جامعة الإمام عبدالرحمن بن فيصل
الدمام, المملكة العربية السعودية
2200004369@iau.edu.sa

فرح عامر الرويلى
قسم الشبكات والاتصالات
جامعة الإمام عبدالرحمن بن فيصل
الدمام, المملكة العربية السعودية
2200001369@iau.edu.sa

تحت إشراف : حسين طلال العطاس

نبذة مختصرة:

أحدثت أجهزة إنترنت الأشياء (IoT (Internet of Things)) ثورةً في مجال تقنية المعلومات. هذه الأجهزة لها ميزتان رئيسيتان وهي الاتصال بالإنترنت بالإضافة إلى التقنيات المدمجة كالبرامج وأجهزة الاستشعار. ساهمت هذه المميزات في زيادة عدد المستخدمين بشكل ملحوظ في السنوات الماضية وزيادة في التحديات والتهديدات الأمنية. من منظور علم التحقيقات الجنائية الرقمية، يقدم إنترنت الأشياء تحديات جديدة بسبب الترابط بين الأجهزة والبرامج والسُحب الرقمية والأطراف الخارجية الأخرى التي تدير الأجهزة. في هذا التقرير، نناقش مفهوم إنترنت الأشياء والمصطلحات المرتبطة به وأهميته في التحقيقات الجنائية الرقمية. بالإضافة إلى خطوات التحقيق في أدلة إنترنت الأشياء. وأخيرا، نستعرض تحديات تنفيذ التحريات الجنائية الرقمية على إنترنت الأشياء.

المقدمة:

أدى التطور المستمر في التكنولوجيا والتوسع في عالم الإنترنت إلى تطور التصاميم المتقدمة بميزات إبداعية كاملة وبنية معقدة تسمى إنترنت الأشياء (IoT). إنترنت الأشياء (IoT) عبارة عن شبكة واسعة تربط العديد من الأجهزة الذكية ببعضها البعض في بنية تحتية عالمية. يمكن استخدام إنترنت الأشياء في مجموعة متنوعة من الصناعات بما في ذلك الزراعة والنقل والمنازل الذكية والرعاية الصحية. على سبيل المثال ، تحتوي أجهزة إنترنت الأشياء على بيانات حساسة وتقوم بمهام أمنية حرجة مثل مراقبة الظروف الصحية للمرضى و السجلات الصحية [1]. يتزايد عدد العقد الذكية المتصلة عبر الإنترنت بشكل كبير بسبب تقدم الشبكات وأنظمة الاتصالات ، والتي يمكن أن تؤدي إلى ربط ملايين الأشياء ببعضها البعض. "وفقًا لـ Statista ، سيكون عدد كائنات إنترنت الأشياء حوالي 75 مليارًا نهاية عام 2025 "[2],[3]. قد تواجه إنترنت الأشياء بعض التحديات. أحد التحديات الخاصة هو الأمن. لذلك ، تعد التقنيات القائمة على إنترنت الأشياء منطقة مثيرة جدًا للاهتمام للمهاجمين. قد يؤدي الوصول غير المصرح به إلى الأنظمة القائمة على إنترنت الأشياء إلى تعريض حياة العديد من المستخدمين للخطر. على سبيل المثال ، يمكن أن يشكل خطرًا على حياة المريض إذا تم اختراق جهاز تنظيم ضربات القلب الخاص بالمريض الذي يدعم إنترنت الأشياء. وبالمثل ، يمكن أن تؤدي الهجمات على سيارة ذكية إلى وقوع حادث. علاوة على ذلك ، يمكن للخصوم اختراق الأجهزة المنزلية الذكية ، مثل كاميرات المراقبة ، للتجسس على سكان المنزل الذكي [3]. يعتبر تأمين أجهزة إنترنت الأشياء مهمة صعبة تستغرق وقتًا طويلاً بسبب هيكلها المعقد. لذلك ، فهي بحاجة إلى طريقة أمنية فعالة ويمكن الاعتماد عليها لضمان سلامتها. سيحمي هذا أكثر خصائص البيانات قيمة ، وهي السرية، الخصوصية، النزاهة والثقة. تم تطوير العديد من الحلول الأمنية لحل مشكلة الأمان. أحد الحلول هو التحليل الجنائي الرقمي. التحليل الجنائي الرقمي هو فرع من فروع علوم الكمبيوتر ويستخدم لجمع وتحليل البيانات من مختلف الوسائط من أجل العثور على أدلة رقمية. يحد من العدد المتزايد للجرائم الإلكترونية ، والتي يمكن أن تحدث بسهولة بسبب تطور الإنترنت ووسائل الاتصال. تساعد هذه التقنية المحققين في الحصول على الدليل الرقمي من أجهزة معينة دون التأثير على بيانات أخرى وتوفير الوقت للمساعدة في تحديد ما إذا كانت هذه البيانات مصابة أو سُرقت من جهاز آخر. من خلال مراجعة أنظمة إنترنت الأشياء وتحديد مكوناتها الحاسمة مثل التهديدات والحلول الأمنية ، تحتاج التحليلات الجنائية الرقمية والعديد من العمليات إلى تقليل التهديد على إنترنت الأشياء [4].

خلفية:

تم اكتشاف مفهوم إنترنت الأشياء لأول مرة في الثمانينات من القرن الماضي من قبل مجموعة من طلاب الجامعات الذين قرروا تعديل آلة بيع مشروبات غازية Coca-Cola ليتمكنوا من مراقبة محتواها عن بُعد، وقد تطورت هذه الفكرة على مر السنين وقد أصبحت مفهومًا معروفًا يتضمن الكثير من الايجابيات. ولكن مع كل ايجابيات إنترنت الأشياء، الا انه هنالك احتمالية سوء استخدامه، وايضًا مخاطر عديده تتعلق بالأمن والخصوصية والجرائم الإلكترونية. مما يجعلنا نتطرق الى أهمية التحقيق الجنائي الرقمي والذي يمكننا من دراسة جميع الأدلة الناتجة عن انتهاكات الأجهزة الإلكترونية في بيئة إنترنت الأشياء. ولكن في الحقيقة إن تقنيات وأدوات التحقيق الجنائي الرقمي التقليدية تواجه الكثير من التحديات في بيئة إنترنت الأشياء والتي ستتم مناقشتها في الأقسام القادمة. [5]

1. ***الحوسبة الضبابية:***

هو هيكل حوسبة لامركزي يقع بين الأجهزة المنتجة للبيانات والسحابة. يسمح هذا للمستخدمين بتوزيع الموارد، بما في ذلك البرامج والبيانات التي تولدها، إلى مساحات افتراضيه لتحسين الأداء. [6]

2. ***نظام كشف الاختراق:***

هو نظام يراقب الشبكة ليكشف اي نشاط غير عادي وينتج إنذارات عندما يكتشف نشاطات مشبوهة. [7]

3. ***نظام منع الاختراق:***

هي تقنية أمان الشبكة (التي قد تكون أجهزة أو برامج) تقوم باستمرار بفحص الشبكة بحثا عن السلوك الضار وتستجيب لها من أجل منعها من الاستمرار، بما في ذلك الإبلاغ عنها أو حظرها أو إيقافها. [8]

أهمية إنترنت الأشياء في التحقيق الجنائي الرقمي:

استنتج العديد من الأكاديميين بأن لا يوجد إجراء واحد في التحقيق الجنائي الرقمي بإمكانه ان يستخدم في جميع أنواع التحقيقات[9]. وعلى الرغم من ذلك، يوفر إنترنت الأشياء مصادر أدلة جنائية أكثر من أي طريقة أخرى تقليدية للتحقيق الجنائي الرقمي، ويعتبر إنترنت الأشياء فرعا مكثفًا منه. يوفر إنترنت الأشياء البيانات المتصلة بالإنترنت والتي تضمن توفرها للمراجعة من قبل الخبراء[10]. في السابق، اعتقد معظم الناس أن الأجهزة الإلكترونية لا يمكن أن توفر سوى بيانات محدودة تحت قيود ضيقة ، مثل الحركة والموقع ودرجة الحرارة وعدد السعرات الحرارية المحروقة... إلخ. ومع ذلك، يمكن أن توفر أجهزة إنترنت الأشياء للمحققين الرقميين أكثر من ذلك بكثير.

أي نوع من الأجهزة المتصلة بالإنترنت يحمل القدرة على جمع البيانات أو معالجتها أو تخزينها أو تبادلها هو مصدر محتمل للأدلة. في الوقت الحاضر تحمل الأجهزة من العديد من الاستشعار، والتي تجمع عديد من المعلومات - بغض النظر عن صغر حجم المعلومات التي تنقلها- تعد أدلة ثرية[11].

عندما يقوم جهاز الاستشعار بجمع البيانات، فإنه سيرسلها تلقائيا إلى السحابة أو إلى أنواع مختلفة من السجلات المخزنة [12], مما يجعل البيانات متصلة ببعضها. يمكن استخدام المعلومات التي تم جمعها من أنظمة إنترنت الأشياء لإنشاء صورة توضيحية لوقت الحادثة[13]. على سبيل المثال، يمكن جمع الأدلة من أجهزة الاستشعار الثابتة الموجودة في المنازل أو المباني، وأجهزة الاستشعار المتحركة في التكنولوجيا أو المركبات القابلة للارتداء، وكذلك أجهزة الاتصال[14].

التحقيق الجنائي الرقمي لإنترنت الأشياء

المراحل التسعة لإطار عمل التحليل الرقمي الموحد هي:

- التحديد: تتضمن هذه المرحلة تحديد الحدث بناءً على المؤشرات ومعرفة طبيعته.
- التحضير: تتضمن هذه المرحلة الاستعداد للمعدات الضرورية والاستراتيجيات وأوامر البحث والتفويض بالمراقبة ودعم الإدارة.
- استراتيجية النهج: تتضمن هذه المرحلة استراتيجية يتم تطويرها ديناميكيًا بناءً على التكنولوجيا المعنية وتأثيرها على المتفرجين.
- الحفظ: تتضمن هذه المرحلة فصل الأدلة المادية والرقمية وحمايتها وحفظها في حالة جيدة.
- التجميع: في هذه المرحلة، يتم التقاط المشهد الفعلي والأدلة الرقمية المكررة باستخدام طرق موحدة ومعتمدة.
- الفحص: تتضمن هذه المرحلة بحثًا شاملاً ومنهجيًا عن المعلومات المتعلقة بالجريمة المشتبه بها.
- التحليل: في هذه المرحلة يتم تجميع أجزاء البيانات معًا، ويتم استخلاص الاستنتاجات بالنظر إلى الأدلة التي تم جمعها.
- العرض التقديمي: تتضمن هذه المرحلة مخططًا وتوفر تفسيرًا للاستنتاجات.
- إعادة الأدلة: تتضمن هذه المرحلة ضمان إعادة كل من الممتلكات المادية والرقمية إلى مالكها الشرعي وتقييم كيف وأنواع الأدلة الجنائية التي يجب إزالتها. [15]

التحديات في تنفيذ التحقيقات الجنائية الرقمية في إنترنت الأشياء:

- **الحصول على البيانات:**

الحصول على البيانات في التحقيق الجنائي الرقمي قد يعتبر اهم خطوة في العملية وهذا لان أي مشكلة قد تحدث في هذه الخطوة بإمكانها التأثير على التحقيق بأكمله، لكن الحصول على البيانات من أجهزة انترنت الأشياء عملية مختلفة عن الحصول على البيانات بشكل تقليدي وهي ليست مهمة سهلة. هذا يعود الى حجم البيانات الذي ينتج من أجهزة انترنت الأشياء. الأجهزة التي تعمل بنظام انترنت الأشياء تنتج كماً هائلا من البيانات. هذا قد يؤثر بشكل كبير على عملية التحقيق عن طريق جعل عملية تحديد الأدلة المهمة والتعرف على جهاز المهاجم أكثر صعوبة واستهلاكا للوقت. بإمكان المحققون أيضا ان يجدوا دقة وموثوقية الأدلة عقبة لهم لان المهاجم لديه القدرة على التلاعب بها [4].

- **قلة أدوات التحقيق الجنائي المناسبة:**

ادوات التحقيق الجنائي المتوفرة لديها العديد من القيود وليس بإمكانها مواكبة التقدمات التكنولوجية الحديثة. هذه الأدوات أيضا ليس لديها قدرة التناسب مع الطبيعة الغير متجانسة واللامركزية للبنية التحتية لأنترنت الأشياء مما يجعل استخدام الأدلة التي تم جمعها وتحليلها من الأجهزة التي تعمل بنظام انترنت الأشياء في المحكمة تحديا الى المحقق الجنائي الرقمي. أيضا، بسبب حجم البيانات المنتجة عن طريق أجهزة انترنت الأشياء وكيفية توزيع البيانات، تزداد الحاجة الى دمج أدوات التحقيق الجنائي للشبكة والكومبيوتر معا لكي تتم عملية تحليل البيانات بشكل صحيح. يمكن جمع البيانات باستخدام أدوات تحليل الشبكة التقليدية المختصة. [4]

- **التخزين والسلطات القضائية المتعددة:**

تحديد موقع البيانات يشكل تحديا آخرا في تحليل أجهزة انترنت الأشياء. هذا لان أجهزة انترنت الأشياء تنقل البيانات الى خدمات السحابة لان التخزين في هذه الأجهزة محدود مما يجعل عملية تحديد موقع البيانات في خادم الويب أكثر صعوبة. غير ذلك، توجد مشكلة عدم القدرة على الوصول المادي الى البيانات والادلة التي تم جمعها من خدمات السحابة عبر أدوات تحليل أجهزة انترنت الأشياء، وبالتالي فمن المهم النظر

في المشاكل المتعلقة بالسلطات القضائية المتعددة قبل دمج انترنت الأشياء مع التحقيق الجنائي الرقمي لأجل تجنب المشاكل القانونية في التحقيق الجنائي الرقمي. التحدي الاخر يكمن في اختيار القانون الذي يجب اختياره من اجل الحكم على القضية المحددة بموجب اختصاص الجهاز والتخزين والمهاجم[4] .

- **تعقب الأدلة:**

الأجهزة التي تعمل بنظام انترنت الأشياء لديها القدرة على نقل البيانات الى مصادر متعددة مثل الأجهزة الخارجية والشبكات والسحابة. هذا يؤثر على القدرة على فحص الأدلة بطريقة صحيحة بسبب ان الأدوات التقليدية الحالية للتحقيق الجنائي الرقمي قد لا يكون ليها القدرة على تعقب الأدلة من المصادر المختلفة التي بدأ منها الهجوم ومن قام بتنفيذ الهجوم[4] .

- **تحديد نطاق التحقيق:**

قد يكون تحديد نطاق مسرح الجريمة في قضية متعلقة بإنترنت الأشياء أكثر تحديًا من الجرائم المعلوماتية المعتادة. ويعود ذلك إلى تعقيد هذه التقنية والبيئة المحيطة بها. قد تقوم أجهزة إنترنت الأشياء بحفظ البيانات على العديد من الأجهزة الافتراضية التي تحذف بياناتها بمجرد إيقاف أو إعادة تشغيلها. يتسبب ذلك في احتمال حذف بيانات قيّمة للتحقيق بما في ذلك السجّلات والملفات المؤقتة.[14]

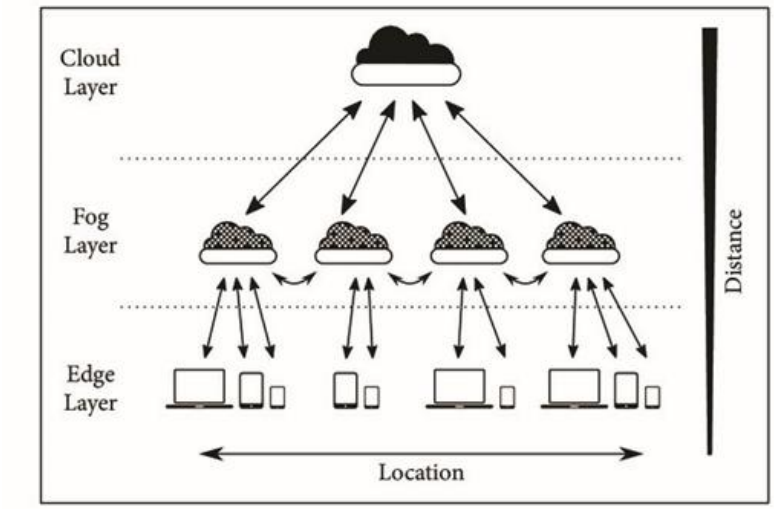
- **نقص في التدريب والمعرفة :**

يلعب العامل البشري دورًا مهما في نجاح التقنيات أو فشلها في حال عدم توفر المعرفة الكافية فيما يتعلق الاستخدام والتنفيذ. في التحقيقات الرقمية، عادة ما يقوم المستجيب الأول للأدلة الرقمية (Digital Evidence First Responder) وأخصائي الأدلة الرقمية (Digital Evidence Specialist)بإجراء التحقيق. وتتمثل مسؤوليتهم في تقييم مسرح الجريمة وجمع الأدلة وتحليلها. يمكن أن يشكل التدريب والتعليم تحديًا كبيرًا خاصة مع التقنيات الجديدة سريعة النمو مثل إنترنت الأشياء. يوصى دائما بتدريب وتطوير مهارات ومعرفة القائمين على التحقيقات الرقمية من أجل الحفاظ على أمان الأدلة وتجنب التغيير في طبيعتها أو فقدان بياناتها القيمة.[14]

- **الخصوصية والاعتبارات الأخلاقية:**

الحفاظ على مصداقية وسرية المعلومات يعتبر عنصر أساسي في نجاح التحقيق. أثناء الحصول على معلومات من جهاز إنترنت الأشياء، يجب على المحققين تجنب انتهاك خصوصية المستخدمين حيث أن معظم أجهزة إنترنت الأشياء تحوي معلومات حساسة عن المستخدمين. لذلك يجب أن تتم عملية جمع الأدلة وتخزينها بطريقة آمنة وجيدة التخطيط. ومن المهم أيضًا جمع البيانات ذات الصلة بالقضية والتحقيق فقط.[14]

إطار عمل التحليل الجنائي القائم على الضباب
تتضمن حوسبة الضباب عادةً ثلاث طبقات رئيسية: طبقة السحابة وطبقة الضباب وطبقة الحافة. شكل أ



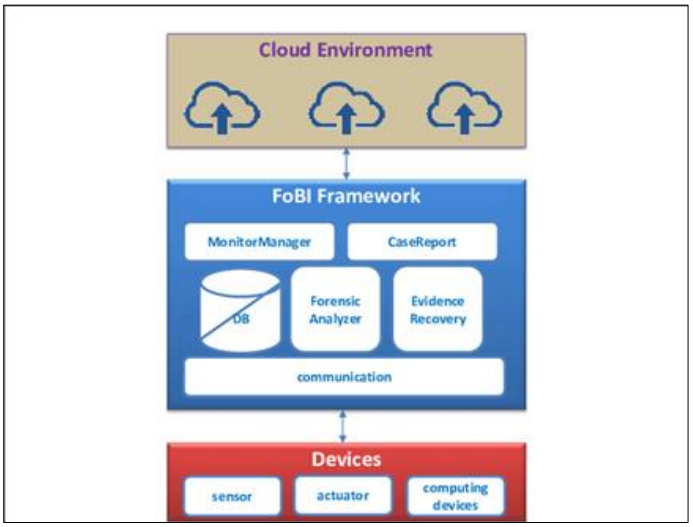
الشكل أ : طبقات حوسبة الضباب

تشكل أجهزة إنترنت الأشياء الطبقة الطرفية الأقرب للمستخدمين. غالبًا ما يمتد إلى مناطق جغرافية أوسع. يتم تنفيذ أجهزة التوجيه والبوابات والمحولات والخوادم التي تتعامل مع الطلبات من الشبكة وتخزنها مؤقتًا في طبقة الضباب. أخيرًا، تتصدر طبقات السحابة هذه الطبقات وتتكون

من خوادم سحابية توفر الكثير من الفوائد، واحدة منها تخزن كمية كبيرة من البيانات بشكل آمن. معظم طرق كشف الطب الشرعي لحوسبة الضباب التي تتضمن مناهج استباقية، حيث يتم نشر الوحدات أو الأجهزة على الشبكة قبل وقوع الحادث، بحيث تعمل في الواقع كمعرف IDS / IPS. من خلال اكتشاف الحالات الشاذة في حركة مرور الشبكة، يمكن إيقاف الهجمات على الشبكة أو أي سلوك ضار آخر. أصبحت قدرة المحققين الشرعيين على الوصول إلى الأدلة المحتملة التي يصعب الحصول عليها عادةً أمرًا ممكنًا من خلال الكشف عن هذه الحركة غير المرغوب فيها وتخزين البيانات ذات الصلة بالحادث. أصبحت قدرة المحققين الشرعيين على الوصول إلى الأدلة المحتملة التي يصعب الحصول عليها عادةً ممكنة من خلال الكشف عن هذه الحركة غير المرغوب فيها وتخزين البيانات ذات الصلة بالحادث. قد تحتوي أنظمة الضباب على مجموعة من الأدلة الرقمية، بما في ذلك مفاتيح التشفير وحركة مرور الشبكة والبيانات الوصفية وثنائيات البرامج الضارة وبيانات المستخدم. تُستخدم أجهزة إنترنت الأشياء والخدمات السحابية عادةً في أنظمة الضباب.[17]

FoBI: يتغلب إطار إنترنت الأشياء الجنائي المستند إلى الضباب على العديد من المشكلات المذكورة أعلاه. يستفيد FoBI من نموذج حوسبة الضباب، والذي يعمل عن طريق استخدام بوابة لدفع البيانات إلى حافة الشبكة، باستخدام FoBI ، ومن الممكن بعد ذلك استعادة الأدلة بناءً على تبادل البيانات بين جهاز إنترنت الأشياء وبوابة أو ضباب العقدة. حالما يتم تحليل البيانات وتحديد النشاط المشبوه بواسطة FoBI ، فإنه سينبه أجهزة إنترنت الأشياء الأخرى بوجود تهديد. بهذه الطريقة، يكون التهديد محدودًا وتقل قدرة المهاجم الإلكتروني على التأثير على أجهزة إنترنت الأشياء الأخرى. يكتشف FoBI خرقًا أمنيًا محتملاً وينبه أجهزة إنترنت الأشياء الأخرى في الشبكة المسجلة عبر بروتوكول مراسلة للنشر (رسالة من خدمة إلى خدمة) للتوقف عن تنفيذ الأوامر عن بُعد حتى يتم الانتهاء من مزيد من التحليل الإضافي أو يتم تنبيه المالك لتوفير وسيلة لمنع الهجوم.

يمكن تشغيل FoBI على عقدة أو بوابة ضباب ويتكون من ست وحدات كما هو موضح في الشكل ب:



الشكل ب: وحدات FoBI

تتمثل مسؤولية نموذج الاتصال في توصيل أجهزة إنترنت الأشياء بإطار عمل وإعداد البيئة الأساسية لمنحهم قدرة جهاز إنترنت الأشياء على إرسال واستقبال البيانات وجعل FoBI يتواصل مع الأجهزة. يتم الاحتفاظ بسجل لجميع الأنشطة المتصلة باتصال أجهزة إنترنت الأشياء بالإطار في التخزين (قاعدة البيانات).

وحدة إدارة المراقبة تراقب أي بيانات أو حركة مرور تذهب إلى أو تأتي من أجهزة إنترنت الأشياء. على سبيل المثال، يبحث في بيانات حركة المرور لتحديد أي أنشطة مشبوهة، بما في ذلك المنافذ أو الهويات أو حجم حركة المرور الغريبة، من بين أشياء أخرى.

يبدأ المحلل الرقمي في جمع المعلومات لمزيد من الاستفسار إذا رفع مدير المراقبة علمًا بشأن أي سلوك مشبوه. ضع في اعتبارك السيناريو الذي يتم فيه ربط العديد من أجهزة إنترنت الأشياء معًا باستخدام رقم منفذ مسجل. عندما يحاول طلب وارد الاتصال بمنفذ غير مألوف، يقره مكون المراقبة. سيتم رفع علم في هذه الحالة، مما يدفع محلل الرقمي إلى استرداد البيانات المتطايرة (أي البيانات الموجودة في الذاكرة والعمليات الحالية) وتخزينها في مكان دائم. يعتمد الموقع على إعداد النظام ويمكن أن يكون محليًا أو على السحابة. علاوة على ذلك، يبدأ محلل الرقمي في إعادة إنتاج البيانات الموجودة على أجهزة إنترنت الأشياء في تخزينها المحلي (البيانات غير المنتهكة). تفصل وحدة تحليل الرقمي الجهاز وترسل إشارة إعادة التشغيل إذا وجدت دليلاً على سلوك مشبوه على جهاز إنترنت الأشياء.

تشرف وحدة استرداد الأدلة على الحصول على المعلومات من أجهزة إنترنت الأشياء المتأثرة. وبعبارة أخرى، فإنه يبني لقطة تدفق بت لجميع بيانات أجهزة إنترنت الأشياء (على سبيل المثال، يقوم بعمل نسخة شرعية). بالإضافة إلى ذلك، يحاول تحديد العمليات النشطة على جهاز إنترنت الأشياء عن بُعد.

تقوم وحدة تقرير الحالة بإنشاء تقرير بعد تحليل جهاز إنترنت الأشياء لتحديد ما إذا كان قد حدث هجوم إلكتروني أو تهديد. إذا تم اكتشاف تهديد محتمل، يمكن لهذه الوحدة إرسال إخطارات بناءً على الأدلة التي تم جمعها.[18]

الخاتمة:

أصبحت تقنيات إنترنت الأشياء جزءًا رئيسيًا من حياتنا اليومية. فهي متواجدة في منازلنا وكذلك في أماكن عملنا. ومع التقدم التقني الذي نشهده، تزداد المخاوف الأمنية، ويزداد عدد الهجمات بسرعة. تحمل تقنيات إنترنت الأشياء قيمة مهمة في التحقيقات الجنائية الرقمية لأنها تولد كثيرًا من الأدلة، ويمكنها تخزين أنواع مختلفة من البيانات المفيدة. تختلف الجرائم الأمنية التي تحتوي على أجهزة إنترنت الأشياء عن الجرائم التقليدية. لذلك يتم التعامل مع هذه الجرائم بشكل مختلف من خلال إطار التحقيق في إنترنت الأشياء. يتكون هذا الإطار من تسع خطوات: التحديد، التحضير، استراتيجية النهج، الحفظ، التجميع، الفحص، التحليل، العرض التقديمي، وأخيرا إعادة الأدلة. يمكن أن يواجه إجراء التحقيق الرقمي في إنترنت الأشياء بعض التحديات المتعلقة بطرق الحصول على البيانات والأدوات المستخدمة في معالجة تلك البيانات والتحقيق فيها، بالإضافة إلى بعض المخاوف المتعلقة بخصوصية وسريّة البيانات. يتم التغلب على بعض الصعوبات التقنية لتنفيذ التحقيق الرقمي لإنترنت الأشياء من خلال إطار fog-based. يعمل هذا الإطار على مراقبة الخطر للحد من أضراره. يمكن أن يوفر تواجد إنترنت الأشياء في التحقيق الرقمي فرصًا وتحديات جديدة بسبب تعقيدها وكمية البيانات المخزنة وقيمتها. ويعد الحفاظ على هذه التقنيات بجانب توفير التدريب والمعرفة المناسبين عنصرين رئيسيين في التغلب على التحديات في التحقيق سواءً كان للقطاع العام أو الخاص.

المراجع:

[1]. Islam, Md & Mahin, Md & Khatun, Ayesha & Debnath, Biplab & Kabir, Sumaiya. (2019). Digital Forensic Investigation Framework for Internet of Things (IoT): A Comprehensive Approach. 1-6. 10.1109/ICASERT.2019.8934707.

[2] . S. Vailshery, "IOT devices installed Base Worldwide 2015- 2025," Statista, 27-Nov-2016. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-ofconnected-devices-worldwide/

[3] Hossain, Mahmud & Karim, Yasser & Hasan, Ragib. (2018). FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger. 33-40. 10.1109/ICIOT.2018.00012.

[4] Atlam, Hany & Alenezi, Ahmed & Alassafi, Madini & Alshdadi, Abdulrahman & Wills, Gary. (2020). Security, Cybercrime and Digital Forensics for IoT. 10.1007/978-3- 030-33596-0_22.

[5] A. Castle, "IOT Technologies explained: History, examples, risks & future," Vision of Humanity, 22-Apr-2022. [Online]. Available: https://www.visionofhumanity.org/whatis-the-internet-of-things/ . [Accessed: 19-Oct-2022].

[6] "What is fog computing? definition and facts," What is Fog Computing? Definition and FAQs | HEAVY.AI. [Online]. Available: https://www.heavy.ai/technical-glossary/fogcomputing [Accessed: 25-Oct-2022].

[7] B. Lutkevich, "What is an intrusion detection system (IDS)? ," SearchSecurity, 07-Oct-2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/intrusio n-detection-system [Accessed: 24-Oct-2022].

[8] "What is intrusion prevention system?," VMware, 20-Oct2022.[Online].Available:https://www.vmware.com/topics/glo ssary/content/intrusion-prevention-system.html. [Accessed: 25-Oct-2022].

[9] H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi, and G. B. Wills, "Security, cybercrime and digital forensics for IOT," Intelligent Systems Reference Library, pp. 551–577, 2019. 6

[10] J. M. Castelo Gómez, J. Carrillo Mondéjar, J. Roldán Gómez, and J. Martínez Martínez, "Developing an IOT forensic methodology. A concept proposal," Forensic Science International: Digital Investigation, vol. 36, p. 301114, Apr. 2021.

[11] S. Perumal, N. M. Norwawi, and V. Raman, "Internet of Things(IOT) Digital Forensic Investigation Model: Top-down Forensic Approach Methodology," 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), 2015.

[12] F. Bouchaud, T. Vantroys, and G. Grimaud, "Evidence gathering in IOT criminal investigation," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 44–61, 2021.

[13] A. MacDermott, T. Baker, and Q. Shi, "Iot forensics: Challenges for the ioa era," 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018.

[14] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191-1221, Secondquarter 2020, doi: 10.1109/COMST.2019.2962586.

[15] Janarthanan, Tharmini & Bagheri, Maryam & Zargari, Shahrzad. (2021). IoT Forensics: An Overview of the Current Issues and Challenges. 10.1007/978-3-030-60425-7_10.

[16] V. Moysiadis, P. Sarigiannidis, and I. Moscholios, "Towards distributed data management in Fog Computing," Wireless Communications and Mobile Computing, 02-Sep-2018. [Online]. Available: https://www.hindawi.com/journals/wcmc/2018/7597686. [Accessed: 29-Oct-2022]

[17] J. H. Gundersen, "Digital forensics on fog-based IoT devices," 01-Jun-2022. [Online]. Available: https://ntnuopen.ntnu.no/ntnuxmlui/bitstream/handle/11250/3006996/no.ntnu%3Ainspera%3A106263136%3A68627142.pdf?sequence=1 . [Accessed: 29-Oct-2022].

[18] Al-Masri, Eyhab & Bai, Yan & Li, Juan. (2018). A Fog-Based Digital Forensics Investigation Framework for IoT Systems. 196-201. 10.1109/SmartCloud.2018.00040.