IOT QURILMALARIDA RAQAMLI DALILLARNI ANIQLASH VA EKSPERTIZA JARAYONINING O‘ZIGA XOS XUSUSIYATLARI

Raxmanova Mohidil Egamberdiyevna
O’zbekiston respublikasi ichki ishlar vazirligi Akademiya
Kriminalistik ekspertizalar kafedrasi katta o’qituvchi
mohidil.rahmonova88gmail.com Tel: 971100203
https://doi.org/10.5281/zenodo.18995789

ARTICLE INFO

Qabul qilindi: 09-mart 2026 yil
Ma’qullandi: 11-mart 2026 yil
Nashr qilindi: 13-mart 2026 yil

KEYWORDS

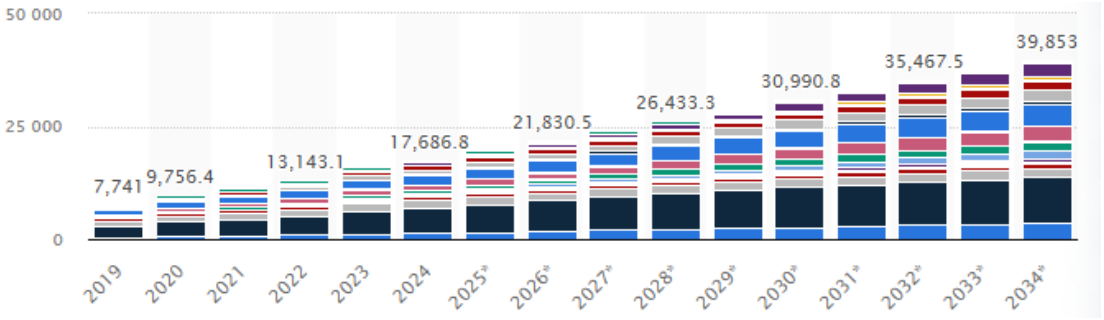
IoT, raqamli dalil, raqamli ekspertiza, xesh qiymat, tezkor xotira, log fayllar, dalil yaxlitligi, bulutli texnologiyalar, tarmoq trafik tahlili.

ABSTRACT

Ushbu maqolada IoT (Internet of Things) qurilmalarida mavjud bo‘lgan raqamli dalillarni aniqlash, yig‘ish, saqlash va tahlil qilish jarayonining o‘ziga xos xususiyatlari yoritilgan. IoT qurilmalarining texnik arxitekturasi, tarmoq orqali ishlash mexanizmi va bulutli muhit bilan integratsiyasi sababli dalillarni aniqlash va mustahkamlash jarayoni an’anaviy raqamli ekspertizadan farq qiladi. Maqolada IoT ekspertizasida uchraydigan muammolar, xesh qiymatlar orqali dalil yaxlitligini ta’minlash, tezkor xotira va log fayllarni tahlil qilish masalalari ko‘rib chiqiladi. Shuningdek, IoT qurilmalariga nisbatan ekspertiza tayinlashning protsessual jihatlari va amaliy tavsiyalar bayon etiladi.

Raqamli texnologiyalar jadal sur’atlarda rivojlanib borayotgan bir paytda IoT qurilmalaridan foydalanish kundalik hayotning ajralmas qismiga aylanib bormoqda. Aqlli uy tizimlari va sanoat monitoringi kabi IoT texnologiyalari kundan-kunga ko‘proq odamlar va xizmatlar tomonidan qo‘llanilmoqda. Shu bilan birga, IoT qurilmalaridan kelib chiqadigan raqamli izlar jinoyatlarni aniqlashda yangi imkoniyatlar bilan bir qatorda murakkab muammolarni ham yuzaga keltirmoqda. Bugungi kunda O‘zbekistonda ham kiberxavfsizlik va raqamli jinoyatlarga qarshi kurash masalalari keskin dolzarblashmoqda. So‘nggi yillarda respublikamizda kiberjinoyatlar soni keskin oshgani kuzatilmoqda: 2021–2025 yillarda kiberjinoyatlar soni 4 865 tadan 62 440 taga yetib, taxminan 11 barobar ko‘paygan. Bu jinoyatlar fuqarolarga jami 3,73 trillion so‘m zarar keltirgan.[1] 2019-yildan 2034-yilgacha butun dunyo bo'ylab IoT tizimlariga ulangan qurilmalar soni, foydalanish holatlari bo'yicha IoT tizimlariga ulangan qurilmalar soni bo'yicha eng katta foydalanish holati iste'molchi interneti va media qurilmalari bo'lib, 2034-yilda butun dunyo bo'ylab barcha qurilmalarning uchdan bir qismini tashkil qiladi. Qolgan ikkita eng katta foydalanish holati aqlli tarmoq (masalan, aqlli hisoblagichlar) va inventarizatsiyani boshqarish va monitoring qilishdir.[2] Buni quyidagi tahlilda ko’rishimiz mumkin.

[1] https://monitor.kun.uz
[2] Petrok Teylor, 2025-yil 27-noyabr https://www.statista.com/statistics/1194701/iot-connected-devices-use-case/



Ushbu holatlar raqamli dalillarni aniqlash, yig‘ish hamda ularni sudga taqdim etish uchun yangi talablarni keltirib chiqaradi. Ushbu muammolarga qarshi kurashish uchun O‘zbekiston Respublikasi Prezidenti tomonidan 2024 yil 21 noyabrda “Raqamli dalillar bilan ishlash tizimini takomillashtirish”ga qaratilgan O‘RQ-1003-son qonun qabul qilindi. Mazkur hujjat jinoyat, fuqarolik va ma’muriy sud ishlarida raqamli dalillarni aniqlash, rasmiylashtirish, ekspertizadan o‘tkazish va baholash tartibini belgilaydi hamda ularni qonuniy asosda qo‘llash imkonini yaratadi.[3]

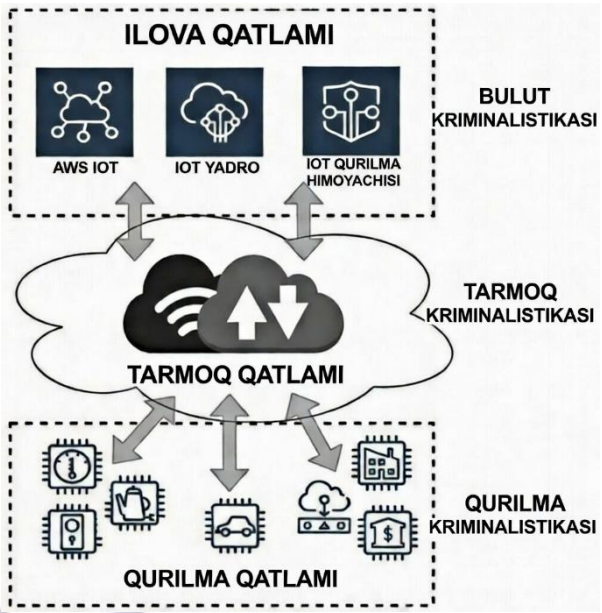
Shuningdek, raqamli kriminalistika sohasida ilmiy izlanishlarni kuchaytirish maqsadida maxsus tadqiqot institutlari tashkil etilib, malakali mutaxassislar tayyorlanmoqda. IoT qurilmalari bilan bog‘liq raqamli izlar va ularning ekspertiza jarayoni, xususan tezkor xotira (RAM), log fayllar, tarmoq trafiklari va bulutli xizmatlardan olingan ma’lumotlarni tahlil qilish dolzarb ilmiy muammo bo‘lib qolmoqda. Shuning uchun ham IoT qurilmalarida raqamli dalillarni to‘g‘ri aniqlash, yig‘ish va tahlil qilish, shuningdek ularni sud jarayonlarida ishonchli dalil sifatida taqdim etish bo‘yicha muammolarni o‘rganish bugungi texnologik va huquqiy muhitda katta ahamiyatga ega.

Adabiyotlar tahlili

Raqamli kriminalistika sohasida IoT qurilmalari kriminalistikasi alohida yo‘nalish sifatida o‘rganilmoqda, chunki u kompyuter-texnik va mobil kriminalistikadan farqli xususiyatlarga ega. IoT qurilmalari kriminalistikasi — bu IoT qurilmalaridan dalillarni aniqlash, yig‘ish, saqlash va tahlil qilish jarayonlarining bir qismi bo‘lib, asosan tarmoq, qurilma va bulut qatlamlarida tarqalgan ma’lumotlar bilan ishlashga yo‘naltirilgan ilmiy sohadir[1]. IoT qurilmalari turli arxitekturaga ega bo‘lib, ularga, aqlli uy tizimlari, sanoat monitoringi platformalari va maishiy qurilmalar kiradi. Shu sababli, ularni tahlil qilish jarayonida turli xil dalillar paydo bo‘ladi. Bu holat IoT qurilmalari tahlilida dalil manbalarini ajratish va ularni birlashtirish metodlarini yaratishni talab qiladi[2]. IoT qurilmalari ma’lumotlarni qayta ishlashda turli yondashuvlardan foydalanadi. Ba’zi qurilmalar ma’lumotlarni bulutga yubormasdan, ba’zida bir qismini yoki hammasini o‘zida amalga oshiradi. IoT qurilmalarining turli qatlamlarida qanday, qayerda va qachon dalil yig‘ish zarurligini tushunib olish dalillarni yig’ish va tahlil qilishda foydali hisoblanadi.

[3] https://lex.uz

1. Qurilma qatlami kriminalistikasi: IoT qurilmalari juda xilma-xil bo‘lib, barcha qurilmalar uchun bir xil dalil yig‘ish usuli mavjud emas. Dalillar qurilmaning doimiy xotirasidan olinadi, masalan, audio, video, rasm va jurnal fayllari. Shuningdek, foydalanuvchi xatti-harakatlari, sensor ma’lumotlari, yurak urish tezligi, konfiguratsiya va telemetriya ma’lumotlari, hamda qurilma holatlari tahlil qilinadi. Bu ma’lumotlar CCTV kameralar, tibbiy implantlar, aqlli uy jihozlari, tarmoqqa ulangan transport vositalari va dronlardan olinishi mumkin.



2. Tarmoq qatlami kriminalistikasi: IoT qurilmalari bir-biriga va internetga turli tarmoqlar orqali ulanadi, masalan, PAN, BAN, WAN, HAN va LAN. Tarmoqlar tomonidan yaratilgan jurnal yozuvlari va audit funksiyalari yordamida foydalanuvchilarni qonuniy ravishda kuzatish va dalil yig‘ish mumkin.

3. Bulut qatlami kriminalistikasi: IoT qurilmalari ko‘pincha o‘zida yetarli saqlash va hisoblash imkoniyatiga ega emas. Shu sababli, ma’lumotlar bulutga uzatiladi va u yerda saqlanadi hamda qayta ishlanadi. Bulutli hisoblash IoT sud-tibbiy ekspertizasida muhim rol o‘ynaydi, chunki u ma’lumotlarni tiklash, autentifikatsiya qilish va tizim holatini qayta tahlil qilish imkonini beradi. Bulutdan olinadigan ma’lumotlar orasida mijozga yo‘naltirilgan artefaktlar, autentifikatsiya yozuvlari, tizim va ma’lumotlar bazasi jurnallari hamda dastur yozuvlari mavjud. Shu bilan birga, IoT muhitida kriminalistik muammolar juda murakkab bo‘lib, ma’lumotlar tez yo‘qoluvchi, resurslar cheklangan, shuningdek qurilmalar bir necha protokollar orqali ishlaydi. Bu IoT qurilmalari tahlilida ma’lumotni qayta tiklash va huquqiy sud dalili sifatida foydalanish uchun qo‘shimcha metodologiyalar ishlab chiqishni talab qiladi[3].

Ko‘plab tadqiqotchilar IoT muhitida raqamli kriminalistikani amalga oshirish jarayoni an’anaviy kompyuter yoki mobil qurilmalar kriminalistikasiga nisbatan murakkabroq ekanligini ta’kidlaydi. Buning asosiy sababi IoT tizimlarining heterojenligi, ya’ni turli ishlab chiqaruvchilar tomonidan ishlab chiqilgan apparat platformalari, operatsion tizimlar va aloqa protokollarining xilma-xilligidir[4]. Bu esa raqamli dalillarni aniqlash va yig‘ish jarayonini sezilarli darajada qiyinlashtiradi. Ilmiy adabiyotlarda IoT kriminalistikasining asosiy muammolari sifatida quyidagilar ko‘rsatib o‘tiladi:

- qurilmalar xilma-xilligi;
- ma’lumotlarning tez o‘zgaruvchanligi (volatile data);
- cheklangan xotira va hisoblash resurslari;
- ma’lumotlarning bulutli servislar va mobil ilovalarda saqlanishi;
- standart kriminalistik metodologiyaning yetarli darajada ishlab chiqilmaganligi[5,6].

Yana bir muhim yo‘nalish – raqamli dalillarni saqlash va ularning yaxlitligini ta’minlash masalasidir. Ayrim tadqiqotlarda IoT muhitida dalillarni ishonchli saqlash uchun blokcheyn

texnologiyalaridan foydalanish taklif etilgan. Bu yondashuv dalillarning o‘zgarmasligini ta’minlash va sud jarayonida ularning haqiqiyligini isbotlash imkonini beradi[7,8].

Yuqoridagi tadqiqotlar IoT qurilmalaridan raqamli dalillarni aniqlash va tahlil qilish jarayoni murakkab va ko‘p bosqichli ekanligini ko‘rsatadi. Shu sababli IoT muhitiga moslashtirilgan yangi kriminalistik metodologiyalarni ishlab chiqish va takomillashtirish ilmiy tadqiqotlarning dolzarb yo‘nalishlaridan biri hisoblanadi.

2. Tadqiqot metodologiyasi

Mazkur tadqiqot IoT qurilmalarida raqamli dalillarni aniqlash va ekspertiza jarayonining o‘ziga xos xususiyatlarini o‘rganishga qaratilgan bo‘lib, unda bir nechta ilmiy tadqiqot metodlaridan foydalanildi.

Tadqiqotning birinchi bosqichida IoT kriminalistikasi bo‘yicha mavjud ilmiy adabiyotlar, xalqaro ilmiy maqolalar va texnik hisobotlar tahlil (analysis) usuli yordamida o‘rganildi. Ushbu bosqichda IoT muhitida raqamli dalillarni aniqlash, yig‘ish va tahlil qilish bo‘yicha mavjud metodologiyalar, modellar va vositalar o‘rganilib, ularning afzalliklari hamda cheklovlari aniqlab olindi.

Keyingi bosqichda taqqoslash (comparative analysis) metodi qo‘llanildi. Bu jarayonda an’anaviy raqamli kriminalistika metodlari bilan IoT kriminalistikasi metodlari o‘rtasidagi farqlar tahlil qilindi. Natijada IoT qurilmalariga xos bo‘lgan quyidagi xususiyatlar aniqlandi: qurilmalar arxitekturasining heterojenligi, ma’lumotlarning tarqoq saqlanishi, tarmoq orqali uzatiladigan ma’lumotlar hajmining katta bo‘lishi hamda real vaqt rejimida ishlash zarurati[9].

Tadqiqotning keyingi bosqichida tizimli yondashuv (systematic approach) asosida IoT qurilmalarida raqamli dalillarni aniqlash va ekspertiza qilish jarayonining asosiy bosqichlari shakllantirildi. Ushbu jarayon quyidagi bosqichlarni o‘z ichiga oladi:

1. Dalillarni aniqlash (Identification) – IoT muhitida mavjud bo‘lgan potensial dalil manbalarini aniqlash (qurilma, mobil ilova, bulutli server, tarmoq loglari).
2. Dalillarni yig‘ish (Acquisition) – IoT qurilmalaridan va ular bilan bog‘liq tizimlardan ma’lumotlarni kriminalistik talablar asosida olish.
3. Dalillarni saqlash (Preservation) – olingan ma’lumotlarning yaxlitligi va autentikligini ta’minlash.
4. Tahlil qilish (Analysis) – olingan ma’lumotlarni ekspertiza usullari yordamida tahlil qilish va hodisa rekonstruksiyasini amalga oshirish.
5. Natijalarni taqdim etish (Presentation) – ekspertiza natijalarini huquqiy jarayonlarda foydalanish mumkin bo‘lgan shaklda rasmiylashtirish[8].

Mazkur metodologiya IoT muhitida raqamli dalillarni samarali aniqlash va tahlil qilish imkonini beradi hamda kiberjinoyatlarni tergov qilish jarayonining samaradorligini oshirishga xizmat qiladi.

Muhokama

IoT texnologiyalarining keng qo‘llanilishi raqamli kriminalistika sohasida yangi vazifalar va muammolarni yuzaga keltirmoqda. Tadqiqot natijalari shuni ko‘rsatadiki, IoT qurilmalarida raqamli dalillarni aniqlash va ekspertiza qilish jarayoni an’anaviy kompyuter yoki mobil qurilmalar kriminalistikasiga nisbatan ancha murakkab hisoblanadi. Buning asosiy sababi IoT muhitining heterojen arxitekturasi, ya’ni turli ishlab chiqaruvchilar tomonidan yaratilgan qurilmalar, operatsion tizimlar va kommunikatsiya protokollarining xilma-xilligidir. Ushbu omil dalillarni aniqlash, yig‘ish va tahlil qilish jarayonini standartlashtirishni qiyinlashtiradi.

Tadqiqot davomida aniqlanishicha, IoT muhitida raqamli dalillar faqat qurilmaning o‘zida emas, balki u bilan bog‘liq boshqa komponentlarda ham saqlanishi mumkin. Jumladan, mobil ilovalar, bulutli xizmatlar, tarmoq loglari va gateway qurilmalarida muhim kriminalistik ahamiyatga ega bo‘lgan ma’lumotlar mavjud bo‘lishi mumkin. Shu sababli IoT kriminalistikasi jarayonida ko‘p manbali dalillarni yig‘ish muhim ahamiyat kasb etadi. Bu esa tergov jarayonida kompleks yondashuvni talab qiladi.

Bundan tashqari, IoT qurilmalarining ko‘pchiligi cheklangan xotira va hisoblash resurslariga ega bo‘lganligi sababli, ularda saqlanadigan ma’lumotlar tezda o‘chib ketishi yoki yangilanib borishi mumkin. Bu esa vaqt omilining muhimligini oshiradi va raqamli dalillarni tezkor ravishda aniqlash hamda saqlash zaruratini yuzaga keltiradi. Shu jihatdan IoT kriminalistikasi jarayonida tezkor identifikatsiya va dalillarni saqlash mexanizmlarini qo‘llash muhim hisoblanadi.

Tadqiqot natijalari shuni ham ko‘rsatadiki, IoT muhitida kriminalistik tekshiruvlar samaradorligini oshirish uchun mavjud metodologiyalarni yanada takomillashtirish zarur. Xususan, IoT qurilmalarining turli qatlamlarini – qurilma darajasi, tarmoq darajasi va bulutli infratuzilma darajasini qamrab oladigan integratsiyalashgan kriminalistik modellarni ishlab chiqish muhim ahamiyatga ega. Bunday yondashuv kiberhodisalarni yanada aniq rekonstruksiya qilish va raqamli dalillarning ishonchliligini ta’minlashga yordam beradi.

Shuningdek, IoT kriminalistikasi jarayonida avtomatlashtirilgan tahlil vositalari, sun’iy intellekt asosidagi monitoring tizimlari hamda blokcheyn texnologiyalaridan foydalanish istiqbolli yo‘nalishlardan biri hisoblanadi. Ushbu texnologiyalar dalillarni saqlashning ishonchliligini oshirish, ularning yaxlitligini ta’minlash va ekspertiza jarayonini tezlashtirish imkonini beradi.

Umuman olganda, olib borilgan tadqiqot IoT qurilmalarida raqamli dalillarni aniqlash va ekspertiza qilish jarayonini samarali tashkil etish uchun kompleks yondashuv zarurligini ko‘rsatadi. Shu bilan birga, IoT kriminalistikasi bo‘yicha yangi metodologiyalar va texnik vositalarni ishlab chiqish ushbu sohada olib borilayotgan ilmiy tadqiqotlarning muhim yo‘nalishlaridan biri bo‘lib qolmoqda.

Natijalar

Mazkur tadqiqot doirasida IoT qurilmalarida raqamli dalillarni aniqlash va ekspertiza jarayonining o‘ziga xos xususiyatlari tahlil qilindi. O‘tkazilgan tahlillar natijasida IoT muhitida raqamli kriminalistika jarayoni an’anaviy kompyuter va mobil qurilmalar kriminalistikasiga nisbatan murakkabroq ekani aniqlandi. Bunga asosiy sabab sifatida IoT tizimlarining heterojen tuzilishga ega ekanligi, turli ishlab chiqaruvchilarning apparat platformalari va operatsion tizimlaridan foydalanilishi hamda ma’lumotlarning turli manbalarda saqlanishi ko‘rsatildi.

Tadqiqot natijalari shuni ko‘rsatdiki, IoT muhitida raqamli dalillar faqat qurilmaning o‘zida emas, balki boshqa bog‘liq komponentlarda ham mavjud bo‘lishi mumkin. Jumladan, mobil ilovalar, bulutli xizmatlar, tarmoq infratuzilmasi hamda gateway qurilmalari muhim kriminalistik ma’lumotlar manbasi hisoblanadi. Shu sababli IoT kriminalistikasi jarayonida dalillarni aniqlash va yig‘ish bir nechta manbalarni qamrab oluvchi kompleks yondashuv asosida amalga oshirilishi zarurligi aniqlandi.

Tadqiqot davomida IoT qurilmalarida raqamli dalillarni aniqlash va tahlil qilish jarayonining asosiy bosqichlari tizimlashtirildi. Ular quyidagilardan iborat: dalillarni identifikatsiya qilish, dalillarni yig‘ish, dalillarni saqlash, tahlil qilish hamda natijalarni huquqiy

jihatdan rasmiylashtirish. Ushbu bosqichlarning izchil amalga oshirilishi IoT muhitida yuzaga keladigan kiberhodisalarni samarali tekshirish imkonini beradi.

Shuningdek, tadqiqot natijalari IoT qurilmalarining cheklangan texnik resurslari, ma'lumotlarning tez o'zgaruvchanligi va qurilmalar o'rtasidagi tarmoq aloqalarining murakkabligi kriminalistik tekshiruv jarayoniga sezilarli ta'sir ko'rsatishini ko'rsatdi. Shu sababli IoT muhitida dalillarni yig'ish jarayonida tezkorlik va ma'lumotlarning yaxlitligini ta'minlash muhim ahamiyatga ega ekanligi aniqlangan.

Xulosa

IoT texnologiyalarining jadal rivojlanishi raqamli kriminalistika sohasida yangi ilmiy va amaliy vazifalarni yuzaga keltirmoqda. IoT qurilmalarining kundalik hayotda keng qo'llanilishi ularni kiberjinoyatlarni tergov qilish jarayonida muhim raqamli dalil manbalaridan biriga aylantirmoqda.

Mazkur tadqiqot natijalari IoT qurilmalarida raqamli dalillarni aniqlash va ekspertiza qilish jarayoni o'ziga xos murakkabliklarga ega ekanligini ko'rsatdi. Xususan, qurilmalar xilma-xilligi, ma'lumotlarning turli infratuzilmalarda saqlanishi hamda tizimlarning tarqoq arxitekturasi kriminalistik tekshiruv jarayonini murakkablashtiradi. Shu sababli IoT kriminalistikasi jarayonida qurilma, tarmoq va bulutli infratuzilmani qamrab oluvchi kompleks yondashuvdan foydalanish zarur.

Tadqiqot doirasida IoT muhitida raqamli dalillarni aniqlash va tahlil qilish jarayonining asosiy bosqichlari tizimlashtirildi hamda ularning samarali qo'llanishi kiberhodisalarni tekshirish jarayonining aniqligi va ishonchliligini oshirishi asoslab berildi. Shu bilan birga, IoT kriminalistikasi sohasida yangi metodologiyalarni ishlab chiqish, avtomatlashtirilgan tahlil vositalarini joriy etish hamda dalillarni saqlashning zamonaviy texnologiyalaridan foydalanish ushbu sohaning keyingi rivojlanish istiqbollari sifatida baholandi.

Umuman olganda, IoT qurilmalarida raqamli dalillarni aniqlash va ekspertiza qilish usullarini takomillashtirish kiberxavfsizlikni ta'minlash hamda kiberjinoyatlarni samarali tergov qilishda muhim ahamiyat kasb etadi

Foydalanilgan adabiyotlar:

1.Ahmed A. A., Farhan K., Jabbar W. A., Al-Othmani A., Abdulrahman A. G. IoT Forensics: Current Perspectives and Future Directions. Sensors. 2024 Aug. mdpi.com

2.Soni N. IoT forensics: Challenges, methodologies, and future directions in securing the Internet of Things ecosystem. Computer and Telecommunication Engineering. 2024.

3.Comparative study of IoT forensic frameworks. Forensic Science International: Digital Investigation. 2024 sciencedirect.com

4.Mohamed H., Koroniotis N., Moustafa N., Schiliro F., Zomaya A. Y. Harnessing Federated Learning for Digital Forensics in IoT: A Survey and Introduction to the IoT-LF Framework. IEEE Open Journal of the Communications Society. 2024

5. Alazab, A., Khraisat, A., & Singh, S. (2023). A review on the Internet of Things (IoT) forensics: Challenges, techniques, and evaluation of digital forensic tools. IntechOpen. https://doi.org/10.5772/intechopen.109840

6. Shin, D.-H., Han, S.-J., Kim, Y.-B., & Euom, I.-C. (2024). Research on digital forensics analyzing heterogeneous Internet of Things incident investigations. Applied Sciences, 14(3), 1128. https://doi.org/10.3390/app14031128

7. Soni, N. (2024). IoT forensics: Challenges, methodologies, and future directions in securing the Internet of Things ecosystem. Computer and Telecommunication Engineering, 2(4), 3070. https://doi.org/10.54517/cte3070
8. Sayakkara, A., Le-Khac, N.-A., & Scanlon, M. (2019). Leveraging electromagnetic side-channel analysis for the investigation of IoT devices. arXiv preprint. https://doi.org/10.48550/arXiv.1904.02089
9. Mahmood, H., Arshad, M., Ahmed, I., Fatima, S., & Rehman, H. (2024). Comparative study of IoT forensic frameworks. Forensic Science International: Digital Investigation. https://doi.org/10.1016/j.fsidi.2024.301748