International Journal of Pharmaceutical Research and Applications
Volume 10, Issue 2 Mar–Apr 2025, pp: 2269-2272 www.ijprajournal.com ISSN: 2456-4494

Monitoring, Managing and Automating task of IoT Forensics Discussing Real time case studies (past seven years): A Review

1.Khushi Brij Gopal, 2.Aaryan Sathe

1. 3rd year B.Sc. Forensic Science , Kalinga University, Raipur 5R8C+R76, near Mantralaya, Kotni, Atal Nagar-Nava Raipur, Chhattisgarh 492101

2. 3rd year B.Sc. Forensic Science , Kalinga University, Raipur 5R8C+R76, near Mantralaya, Kotni, Atal Nagar-Nava Raipur, Chhattisgarh 492101

Date of Submission: 20-04-2025 Date of Acceptance: 30-04-2025

ABSTRACT

With the introduction of the Internet of Things(IoT), smart monitoring, automating tasks, and even management has greatly advanced. The objective of this paper is to examine insights of IoT analog 12 alongside the controls and hurdles that come with IoT ecosystem. From a capturing standpoint, capturing of data without affecting the operation of the machine can be done with effective monitoring methods, whereas intelligent management methods ensure data is accurate throughout the processes by IoT. As for the low resource expenditure through high reliability tasks, AI units such as Google Alexa allow collection and examination of evidences which significantly lowers the manual work and errors. Homes with AI have revealed the gaping void that forensic IoT systems have, needing fast paced shifting which emphasize coevolution. Understanding evolving IoT networks is deeply needed. The absence of human error is obtainable throughout the appropriate implementation of learning forensic tools, therefore carefully constructed methodologies and other legalistic scaffolding are critical. This review tackles the gaps and broadens mobile forensic, network forensics, and the other branches of the complex system that are needed to enable thorough forensic investigations.

Keywords: IoT, Data, Reliability, Monitoring, Scaffolding, Evolving, Significantly.

I. INTRODUCTION

The sheer growth in Internet of Things (IoT) devices, including smartwatches, has changed the paradigm of personal data generation, collection, and transmission. This innovation poses tremendous challenges to forensic investigators to extract and analyse data. Smartwatches tend to synchronize data with cloud services, and their incorporation into larger IoT systems makes it difficult for traditional forensic practices. This review of literature integrates current research evidence on challenges to forensic investigators in this field, identifying knowledge gaps and areas for future study. Complexity of IoT Environments Forensic investigation in IoT environments, such as smartwatches, is dominated by a dense network of devices that are interlinked. MacDermott et al.,(2018). Illustrate the difficulties arising from the edgeless nature of network topology, in which the borders of devices are indistinct, making it difficult to demarcate and collect pertinent evidence. The researchers must navigate numerous interconnected devices, each of which can hold vital details, making it essential to deploy effective data collection methods that address both logical and physical extraction problems. Smartwatches tend to sync information with cloud services, presenting yet another layer of complexity for forensic examiners. Alabdulsalam et al.,(2018) emphasize the necessity of an integrated solution to client-side and cloud-native forensics. Examiners need to be competent in interpreting local data storage practices and the complexity of cloud data recovery processes. The challenge is to create exhaustive forensic standards that cover both dimensions to improve investigation capabilities.

IoT Forensics

Internet of things (IoT) in terms of digital investigation, forensic refers to the application of scientific approach used in Identification, Collection and Preservation, Documentation and Analysis of electronic evidences. This process is crucial for investigations involving the electronic devices, specially our world is increasingly integrates the Internet-of-Things (IoT) – a network comprised of various interconnected devices, ranging from household gadgets to sophisticated wearable like smartwatches, fit bands, etc. As millions of devices digitally interconnected, the potential implications for criminal activities and privacy invasion have escalated, demanding sophisticated understanding of forensics in this new

International Journal of Pharmaceutical Research and Applications
Volume 10, Issue 2 Mar–Apr 2025, pp: 2269-2272 www.ijprajournal.com ISSN: 2456-4494

landscape. It can pursue innovative function such as:

- ✓ **Monitoring** – This task is helps in monitoring the user real life activity via capturing real time data from IoT sensors (communication records, sensor logs) also tracks device behaviour and network trafficking to detect unauthorised access or tampering . By giving information of Weather, climatic change , Health metrics-blood pressure, heart rate ,oxygen saturation etc., steps count tracking this personal activity and creating logs of day to daily life. Preserve volatile evidence makes use in early detection of incidents.
- ✓ **Managing** – this task perform organising, controlling and securing the IoT devices data they produce. In terms of forensic they produce huge amount of data in Device setting like creates loggings to data retention policy levels to enhance the forensic readiness. This serves to ensure a proper collection, storage and maintaining the chain of custody. Since IoT includes everything from smartwatches to other electronic gadgets.
- ✓ **Automating Task** – allows forensic teams to efficiently access and analyse huge volumes of IoT (spotting patterns , anomalies, or evidence faster) data correlation and timeline building link event in multiple IoT Devices. Implement smart alerts that notifies team of suspect activity .

Methodology-

This research adopts a multiple phase forensic investigation framework to the diverse and complex nature of IoT devices. A systematic designed addresses evidence collection, analysis and interpretation across variety of digital environment , integrating real life case scenario (past seven year cases). This review full fill the real life case study and learned various kinds of IoT devices used in the field of forensics.

Methods

- ✓ **Identification**: identifying Iot devices, electronic gadgets and uses of network service protocols (cloud forensic) at crime scene. Ensures the prevention by isolating devices and seizing the target sources to prevent remote tampering or data losses.
- ✓ **Collection and Preservation**: Acquiring physical, logical and hybrid methods depend on device type (smartwatch, smartphones, home appliances, surveillance, etc). extract GPS navigation history, communications logs and serve legal warrants (e.g. Amazon echo, Fitbit) Smart speaker recording serve as "invisible witness" [10], and flows to detect unauthorised activities. Fitbit activity data uncovering inconsistencies in homicide investigation[8].
- ✓ **Analysis**: by analysing such cases we found that analysing of metadata , call logs ,cross checks data timestamps on various IoT devices, smartphone app [11](such as Whatsapp , SMS exchanges) and cloud records to mitigate synchronized issues identified in forensic cases . Pacemaker data setting precedents in medical devices used in forensic [9][6]. By checking Multi device smart home data correlation supporting timeline reconstruction. Smartwatch forensic providing timeline evidence despite device heterogeneity

Challenges of Forensic IoT: -

- **Device variety: -** IoT devices are produced by many manufacturers, in which they use different types of technologies, protocols, and data formats and because of those difficulty it lacks standardized evidence collection. [1]
- **Size of data volume and relevance: -** the amount of data created by IoT devices complicates identifying, collecting and selecting to help relevant evidence for investigations. [2][1]
- **Limited device Resources: -** many of the IoT devices have less storage, processing power and memory. Which give less data in the investigation process while extracting data from IoT devices. [3][1]
- **Privacy and legal issues: -** some of the IoT devices frequently handle sensitive personal data (e.g. health Metrics, call logs, images) and it raise privacy concerns and complex jurisdictional/legal considerations during forensic investigations. [2][1]
- **Network complexity: -** The IoT networks can be broadly categorized into four main types cellular, LAN/PAN, LP-WAN, and mesh protocols and these categories are primarily distinguished by their coverage area, bandwidth, and power consumption requirements. [5][4][2]

Scope of Forensic IoT: -

- **Evidence collection: -** in case of digital evidence collection from wide range of IoT devices, networks, companion devices

International Journal of Pharmaceutical Research and Applications
Volume 10, Issue 2 Mar–Apr 2025, pp: 2269-2272 www.ijprajournal.com ISSN: 2456-4494

(smartphones, laptops and computer), cloud services and call logs. (Ahmed et al.,2024)

- **Mobile forensics: -** Acquiring and analysis of digital evidence directly from IoT devices, for example such as smart home appliances, wearables, CCTV(Closed Circuit Television) cameras and vehicles. This can include user device logs, images, audio. [3]
- **Network forensic: -** investigating the communication between IoT devices and networks (e.g. PANs, LANs, WANs). This involves analysis of the network traffic, logs and metadata to trace actions and integrations within the IoT ecosystem (e.g. Samsung and apple are most use ecosystem). (Ahmed et al.,2024)
- **Emerging domains: -** using forensic techniques to new IoT domains such as smart healthcare, smart cities, industrial IoT and autonomous vehicles, each device have its own data types and investigative needs.[3]

Drone and Autonomous vehicle: - Extracting data from navigation systems, collision logs and remote-control interfaces to investigate accidents or unauthorized surveillance. (Ahmed et al.,2024)

Real life case study

1. Smartwatch forensics case study**: -** forensic analysis of smartwatches revealed things such as heart rate, GPS, and activity logs. These data points helped investigators to get evidence together timelines and suspect movements, despite challenges from device heterogeneity and synchronization issues [6].

In **2015** Arkansas case, victor Collins was found dead in a hot tub. Police served warrants for Amazon Echo data and collected logs from a nest thermostat and a smart water meter. The thermostat's temperature and humidity records, combined with water-usage spikes, helped confirm timeline inconsistencies and possible cleanup activities, illustrating multi-device correlation in smart home forensics[10].

2. In **2015** Sheena bora's murder case. In-depth knowledge of mobile device forensic was useful to the investigation. The police were able to identify the plot and determine Sheena's last known with the assistance of forensic analysis of call data records and SMS exchanges between the accused, who included Indrani Mukerjea, her husband peter Mukerjea, and other individuals. The arrest and charging of the suspects were made possible in large part by help of digital evidence. [11]
3. In **December 2015**, Connie Dabate was found shot in her home. Her husband, Richard Dabate, claimed a marked intruder was responsible. Investigators used Fitbit data showing connie's movement and heart rate spikes that contradicted his timeline, leading to his arrest. The case dubbed the "Fitbit murder" was upheld by Connecticut's supreme court in 2025 despite noting prosecutorial missteps[8].
4. In **2017**, Ross Compton's house caught fire under suspicious circumstances. Prosecutors obtained cardiac rhythm logs from his internet-enabled pacemaker data as evidence in case of arson and insurance fraud, it is setting a precedent for implantable medical device forensics[9].
5. **In July 2019**, police investigating the stabbing death of silvia galva in hallandale beach, Florida issued a warrant for amazon Echo recordings hoping Alexa captured ambient audio and voice activity from the crime scene. Although it remains unclear what data were ultimately obtained this case underscores law enforcements growing reliance on smart speaker logs as "invisible witnesses." [7]
6. **on 17 April 2018**, the Bhima Koregaon case, forensic investigation revealed that incriminating evidence was planted on the computers of several activists, including stan swamy and Rona Wilson. Arsenal consulting, a U.S.- based digital forensics firm, discovered that the net wire malware was used to remotely access and control the activist's device over extended periods. This malware enabled attackers to deposit fabricated documents, which were later cited as key evidence in the arrests. The timing of the malware activities and subsequent police actions suggested possible collusion between the hackers and law enforcement agencies. [12,13,14]

II. RESULT

The review indicates that smartwatches and IoT gadgets are becoming crucial in forensic science, offering new methods for evidence collection and analysis. However, their widespread use across domains like healthcare, education, industry, home automation, and business are hindered by significant security challenges, impacting their full adoption.

International Journal of Pharmaceutical Research and Applications
Volume 10, Issue 2 Mar–Apr 2025, pp: 2269-2272 www.ijprajournal.com ISSN: 2456-4494

III. DISCUSSION

Even though their benefits, the security of IoT device remains a major concern due to the variety and resource constraints of these devices, which pose unique challenges for forensic investigation. There is an urgent need for developing advanced tools, methodologies, and legal framework to effectively address these issues.

IV. CONCLUSION

To manage these challenges, in the field of IoT forensics must grow rapidly and uphold continuous innovation. This will ensure that forensic investigation can keep the momentum with the evolving of IoT technologies and their applications, enhancing the reliability of digital evidence.

REFERENCE

1. https://indiaforensic.com/iot-forensics-and-critical-considerations/
2. https://doi.org/10.1051/shsconf/202317703002
3. Ahmed, A.A.; Farhan, K.; Jabbar, W.A.; Al-Othmani, A.; Abdulrahman, A.G. IoT Forensics: Current Perspectives and Future Directions. Sensors **2024**, 24, 5210. https://doi.org/10.3390/s24165210
4. https://euristiq.com/types-of-iot-networks/#:~:text=What%20are%20the%204%20types,of%20IoT%20networks%20operate%20wirelessly.
5. https://researchonline.ljmu.ac.uk/id/eprint/7865/1/PID1206230.pdf
6. https://arxiv.org/pdf/1801.10391v1
7. Police Want Your Smart Speaker—Here's Why | WIRED
8. Inside Connie Dabate's 2017 'Fitbit Murder,' and How Husband Was Caught
9. https://doi.org/10.1177/1365712720930600
10. ip_2022_27-2_ip-27-2-ip211541_ip-27-ip211541.pdf
11. The Power of Mobile Device Forensics: Investigating Digital Footprints in 2024 - Karnavati University
12. https://caravanmagazine.in/politics/bhima-koregaon-case-rona-wilson-hard-disk-malware-remote-access?utm_source=chatgpt.com
13. https://www.washingtonpost.com/world/2021/07/06/bhima-koregaon-case-india/?utm_source=chatgpt.com
14. https://www.thehindu.com/news/cities/mumbai/bhima-koregaon-violence-case-digital-forensic-analysis-debunks-electronic-evidence-against-jailed-activist-rona-wilson/article61752748.ece?utm_source=chatgpt.com
15. Alabdulsalam, Saad & Schaefer, Kevin & Kechadi, Tahar & Le-Khac, Nhien-An. (2018). Internet of things forensics: Challenges and Case Study. 10.48550/arXiv.1801.10391.
16. 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), Paris, France, 2018, pp. 1-5, doi: 10.1109/NTMS.2018.8328748.