IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Forensics Analysis In The Internet Of Things (Iot): Methods, Difficulties, And Opportunities

Dr. S. Chithra Devi, Assistant Professor,
Department of Digital and Cyber Forensic Science, Sri Ramakrishna College of Arts & Science, Coimbatore.

ABSTRACT

In Digital Forensic investigations, the familiar of Internet of Things (IoT) devices creates special difficulties. Although these appliances enhance speed and utility, they also present security holes that hackers could take advantage of. Collecting, Analyzing, and Preserving digital evidence from IoT environments is the aim of IoT forensics. In order to improve digital investigations in smart ecosystems, this article offers future research areas and provides an overview of current methods, tools, and the primary challenges in IoT forensics.

Keywords

IoT forensics, digital evidence, cybersecurity, data acquisition, smart devices, network analysis.

I. INTRODUCTION

By integrating connectivity into common things, the Internet of Things (IoT) has changed traditional computing platforms. New opportunities and threats arise as a result of the increasing number of devices including smartphones and tablets, CCTV cameras, climate control systems, and agricultural sensors. By 2030, more than 30 billion IoT devices are anticipated to be in operation, per a Statista report. In criminal investigations, these gadgets can frequently be vital sources of digital evidence. However, because of the variety, data instability, and limited nature of IoT systems, conventional digital forensic approaches are inadequate. [1].

II. IOT FORENSICS: DESCRIPTION AND METHODS

The verification, collection, analysis, and submitting of digital evidence from IoT devices is the focus of the newly developing field of digital forensics known as IoT forensics. As IoT devices are rapidly being incorporated into essential systems and daily life, there is a greater chance that these devices will be a part of or impacted by cybercrimes. Forensics for IoT is essential to:

- Examine cyberattacks that target mobile devices.
- To retrieve digital evidence from illegal areas, use integrated IoT technologies.
- Assure legal admissibility in court and information reliability.

The most essential processes are:

- **Identification:** Tracking down possible data information, like detectors or cloud-based networks.
- **Preservation:** Protecting the evidence without compromising its integrity is known as preservation.
- **Analysis:** Developing activities by collecting appropriate information.
- **Reporting:** Outlining results in a way that is acceptable under regulations [2].

III. CHALLENGES IN IOT FORENSICS

In the world of IoT, a forensic investigation encounters a number of difficulties:

- **Device Heterogeneity:** Interoperability is made more difficult by the fact that devices operate on various systems and frameworks.
- **Volatile Data:** Since several devices have a little amount of storage, data can be rapidly altered or damaged.
- **Lack of Physical Access:** It can be challenging to gather evidence since devices may be implanted or positioned far away.
- **Cloud Dependencies:** Restricted access third-party cloud services may house data.
- **Privacy and Legal Barriers:** Managing private user information presents moral and legal challenges [3].

IV. FORENSIC TECHNIQUES AND TOOLS

A. Data Acquisition Techniques

- **Live Acquisition:** Capturing data from active devices.
- **Firmware Analysis:** Dumping and analyzing embedded firmware to uncover traces.
- **Network Sniffing:** Monitoring communications for anomalies and data theft.

B. Tools Used

- **Wireshark:** To record and examine network activity.
- **Autopsy:** An open-source forensic platform for data recovery.
- **IoT Inspector:** Specialized tool for reverse-engineering IoT firmware.
- **FTK (Forensic Toolkit):** Used for analyzing devices and storage [4].

V. A CASE STUDY ON INTELLIGENT HOME ATTACK

IoT gadgets like surveillance systems, refrigerators, digital assistants, and intelligent locks are all integrated into smart homes. Despite the ease they offer, they are at risk for threats. The forensic analysis of a smart home penetration is the main topic of this case study.

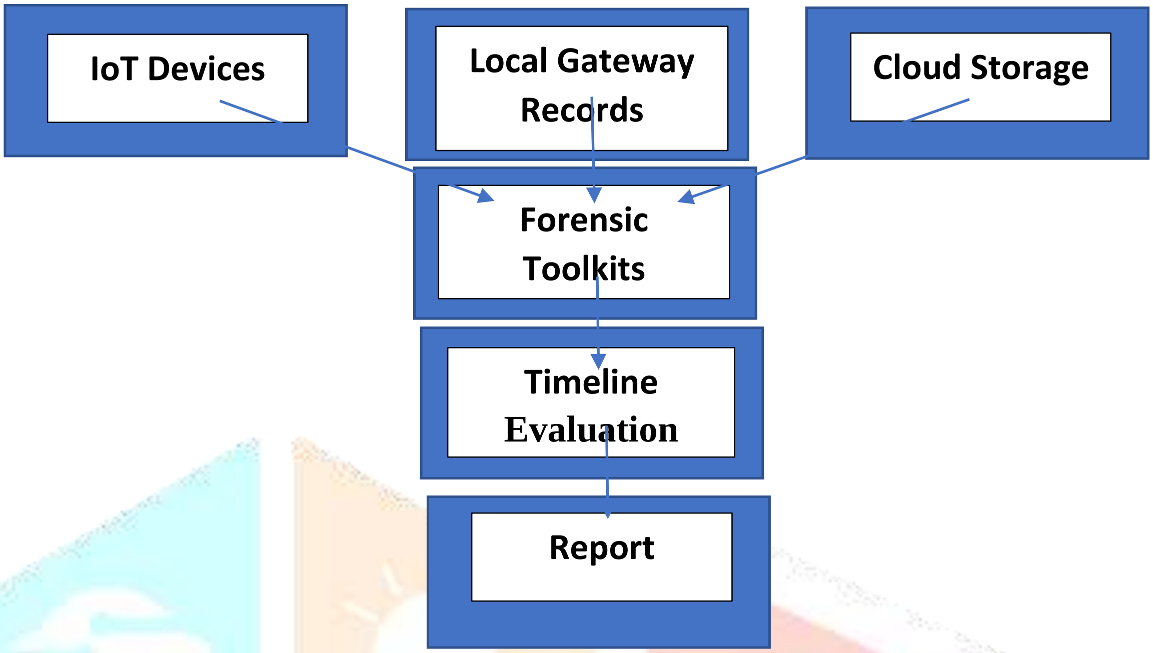

Fig:1 Forensic IoT workflow in Intelligent Home Attack

IoT Devices

IoT devices (Speech assistants, refrigerators, surveillance cameras, and intelligent locks) are the main sources of forensic evidence and possible points of entry for a crimes.

Local Gateway Records

Device records, such as those from a wireless router or intelligent hub, which document:

- History of device connections
- Attempts at login
- Commands for access

Cloud Storage

A lot of digital gadgets send video streams and records to cloud platforms. Among these records are:

- History of remote access
- Alerts from the system
- Media files, such as footage from security cameras

Forensic Toolkits

An application or system for gathering, storing, and examining digital evidence from the Internet of Things. Relevant files and metadata are extracted for examination using tools like FTK, Autopsy, or custom scripts.

Timeline Evaluation

In this step, the events are recreated:

- When every gadget was accessed
- Unusual actions
- Multiple logs are correlated to determine the intrusion time.

Record

Final records discussing:

- Point of entry for the attack
- Utilization of vulnerabilities
- Attacker's technique and agenda
- Suggestions to avoid similar events in the future

An intrusion into an intelligent house was found to be caused by a hacked IoT door lock. Investigators examined recordings from cloud storage, collected recordings from the lock, and examined communication packets using Wireshark. A flaw in the lock manufacturer's API that permitted unauthorized access was discovered by the study. Forensic procedures ensured the integrity of the evidence and facilitated legal investigation.

VI. FUTURE DIRECTIONS

The following lines of investigation are suggested in order to improve IoT forensic capabilities:

- Structured Guidelines: Creation of international forensic standards and norms.
- Edge Forensics: Analyzing data at the edge to save latency and protect information.
- AI: Using machine learning to identify and categorize irregularities.
- Blockchain: Maintaining chain-of-custody through distributed ledgers [5].

VII. CONCLUSION

Digital forensic investigations are significantly hampered by the complexity and diversity of IoT environments. Although conventional forensic techniques can be modified, new approaches are needed to handle the particular problems that smart devices provide. In order to develop strong investigative solutions, this study emphasized the necessity of interdisciplinary collaboration while highlighting present practices, significant challenges, and potential future developments in IoT forensics.

REFERENCES

[1] S. Zawoad and R. Hasan, “FAIoT: Towards building a forensics-aware eco system for the Internet of Things,” IEEE International Conference on Services Computing, 2015.

[2] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, “Internet of Things forensics: Challenges and approaches,” 2013 International Conference on Emerging Security Technologies, 2013.

[3] A. Alabdulatif, I. Khalil, and X. Yi, “Privacy-preserving digital forensics model for IoT evidence using blockchain,” Future Generation Computer Systems, vol. 110, pp. 675–687, 2020.

[4] M. Ahmed, F. Ahmad, H. Abbas, and M. A. Khan, “Forensic Investigation of Smart IoT Devices: Current Techniques, Limitations, and Future Trends,” IEEE Access, vol. 9, pp. 75693–75713, 2021.

[5] D. Berman, J. Iannacone, and K. Jones, “The future of digital forensics in IoT,” Digital Investigation, vol. 26, pp. S96–S103, 2018.