International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

Anti-Forensics Techniques in IoT Devices, Challenges and Countermeasures

Mr. Kousik Maiti
ICTS-Group
CDAC Kolkata
Kolkata, India

Tarun Pandey
E-Security Group
MeitY, Govt. of India
New Delhi, India

***Abstract*—Nowadays IoT devices are present in most criminal activities. Day by day more cyber crimes will be bound to have IoT as a source of evidence. IoT devices have a large spectrum,it can be some small controller of censor devices or can be a huge electro-mechanical device which is controlled by some other system. It can be very challenging for cyber crime investigators to detect, identify, collect, analyse and correlate the evidence from IoT devices. Anti-forensics techniques if applied to IoT that can add more challenges for the investigators. In this paper we are discussing the possible challenges and their countermeasures, which can be faced during the investigations of the cyber crimes related to IoT devices. 'Anti-forensics' is defined by Gary C. Kessler [1] as 'Viewed generically, anti-forensics (AF) is that set of tactics and measures taken by someone who wants to thwart the digital investigation process'.**

Keywords—IoT, Anti-Forensics,

I. INTRODUCTION

Some or all of the following components may be found during the investigations of IoT devices[2]: Sensor, IoT Hardware, Device firmware, Internal memory, External memory, Web Servers including cloud storage, lightweight database and analytics engines, Communication logs, and protocols including proprietary protocol. All collectible logs from all the evidences are very important. It is very hard to collect evidence from IoT devices, as the case may involve a number of devices as well as cloud storage, so some classification [3] has been done, which can help to segregate the motive of the crime.

1. IoT as a target:- Criminal directly targeting the IoT devices for criminal activities. Here Criminals are using the loopholes of IoT devices as well as their skills to get into the targeted devices. Examples: e-Health and m-Health devices[4]

2. IoT as a tool:- Here IoT devices are used for performing the attacks or criminal activities. Here attackers implant some codes by using known vulnerabilities like fixed encryption keys, default passwords and failure to patch or update device firmware of the devices. Examples: Mirai botnet[5].

3. IoT as evidence:- In this class of devices are involved in the process of criminal activities. Here criminals may or may not be aware of the presence of IoT devices. Examples: Kidnapping, bulgering etc[6].

Anti-Forensics Technique may be used by high profile criminals for the some or all of the following reasons:

1. Divert the investigators
2. Hide the criminal activities
3. Delaying the investigations

In the rest of the paper we have discussed as follows: Section II: presented related works done in the anti-forensics of IoT devices. In Section III we have discussed key challenges in IoT devices, in Section IV we have presented countermeasures of the anti-forensics techniques for IoT devices. In Section V we propose a framework for addressing Anti-forensic techniques applied in IoT Devices. In Section VI we draw the conclusion and future work can be done in the field of anti-forensics techniques applicable to IoT devices.

II. RELATED WORK

Some of the common Anti Forensics Techniques [7] with examples, which may be applicable to IoT are:

1. Artifact wiping
2. Data Hiding
3. Trail Obfuscation
4. Attack against forensics tools and method

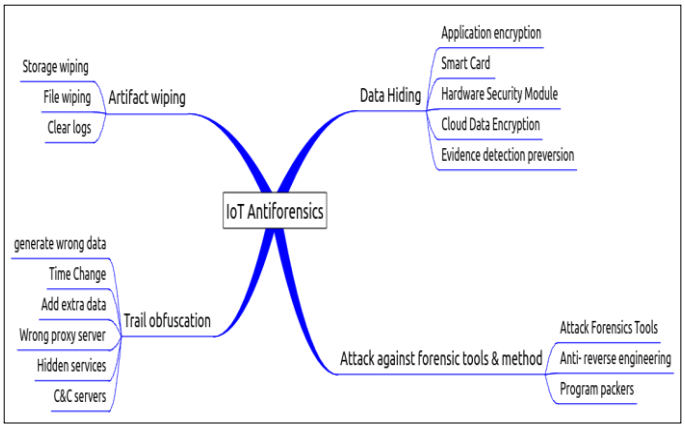


Fig-1 :- IoT Anti Forensics

IoT can be divided into different layers. According to the IoT reference model [8] there are 7 layers.
These are

1. Physical and Device controller
2. Connectivity
3. Edge and Fog Computing
4. Data Accumulation
5. Data Abstraction
6. IoT Application

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

7. Collaboration and Processes

It is possible to perform Anti Forensics Techniques in each of the seven the seven layers.

Sl No	Layer Name	Components	Possible AFT	
1	Physical and Device controller	Physical Hardware	Artifact wiping	External Store wipe
2	Connectivity	Network components and protocol	Trail obfuscation	VPN Tunneling
3	Edge and Fog Computing	Protocol and encryption	Data hiding	VPN Tunneling, Encrypted files at rest
4	Data Accumulation	Application and Logs	Artifact wiping, Trail obfuscation	Log file alteration and or deletion
5	Data Abstraction	Storage and Applications	Artifact wiping, Trail obfuscation	Encrypted files, file alteration and or deletion
6	IoT Application	Authorisation and Application	Trail obfuscation	Encrypted files, file alteration and or deletion
7	Collaboration and Processes	Identity and Application	Trail obfuscation	Encrypted files, file alteration and or deletion

III. KEY CHALLENEGS

As there are a huge number and variety of devices, chances of involvement of IoT devices in crime also increasing. We can have these types of challenges in IoT evidence collection[2]:

1. Devices with limited resources
2. Diversified components
3. Lack of standard
4. Lack of Anti-anti Forensics tools

Devices with limited resources

As the footprint of most of the IoT devices is very small, there are limitations with the IoT devices itself. These limitations are both helpful as well as unaccommodating. Due to low resource constraint encryption & decryption are usually not present. At the same time due to limited resources(i.e. storage) we may only get data from certain windows only. It can vary from seven days to three months.

Heterogeneous Components

During analysis of IoT evidence, we may have faced a wide spectrum of the following components like devices, vendors, sensors, hardware, firmware, networking, communication protocols, infrastructure, databases, analytics, applications and so on. It means we can get both open as well as proprietary hardware, software, protocol etc. So we have to keep these in account during the IoT investigation.

Inadequate Standards

As already mentioned, there are a huge number of devices involved in IoT forensic analysis. But most of the IoT solutions from different vendors are not designed for interoperability, which means there is a lack of standardization. That also creates challenges in IoT investigation as well as anti-forensics technique analysis.

Lack of Anti-anti Forensics tools

Anti-Forensics Techniques for IoT Forensics are quite new, so there are a lack of tools, which can address the challenges created by Anti-Forensics Techniques. This may be a new area which researchers can look into.

IV. COUNTERMEASURES

”Even the cleverest of criminals leave behind clues to their crime.”

Anti-Forensics Techniques discussed in this paper can be addressed by carefully identifying the AF techniques may be applied in the IoT devices. Beauty of the IoT devices are if you miss some traces in one device you can get some traces or logs in other devices for example if the user purposefully removes logs from the IoT controller the counter part of the log can be obtained in other devices like servers to which the IoT controller was connected to.

Most of the countermeasures of Anti Forensics techniques for IoT devices discussed in this paper currently may be limited to researchers only.

We can address the Anti-Forensics issues for IoT devices by the following steps:

1. Preparedness & Identification
2. Analysis
3. Detection
4. Mitigation
5. Correlation and Evaluation

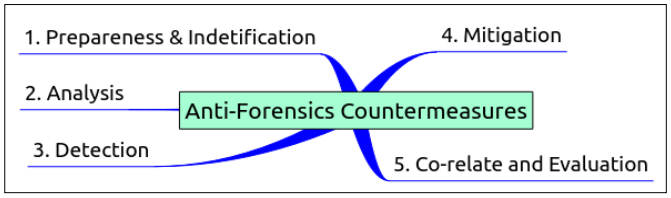


Fig-2: Anti-Forensics Countermeasures

- *Preparedness & Identification:* -When any IoT forensics case is addressed, we have to consider that anti-forensics technique may be applied, though it may not be true all time. It depends upon the technical ability of the criminal, if he/she is capable of applying the anti-forensics technique in IoT devices. If there is any possibility of AFT being found then we have to prepare according to the need of the IoT devices.

  There are some indicators that may hint the presence of anti-forensics technique in IoT evidences[7]. Some of them are

Data Encryption: - The data which should be in normal format, is encrypted then the chance of anti-forensics technique may be present.

Forcefully artifacts wiping:- During investigation if it is found that some artifacts are missing, that may lead to anti-forensics technique.

Trail obfuscation of artifacts:- If there are any changes in logs like date change, some extra data is added forcefully, that also some indicator of anti-forensics technique, it means the attacker might try to apply anti-forensics technique.

- *Analysis :-* If any anti-forensics technique is found then we have to find all the possible ways by analyzing the crime for or of the IoT devices.
- *Detection:-* Proper detection can be done after proper analysis of the case. We have to find the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

possible affected devices, where anti-forensics technique may be applied.

- *Mitigation:* As anti-forensics techniques are highly technical in nature, it is very difficult to mitigate or overcome the changes applied by anti-forensics technique. As already told, IoT devices are connected in various ways, some traces may be found in other components and we have to rebuild the missing link.
- *Correlation and Evaluation:*- Once all or most of the logs and data are collected then we have to co-relate and evaluate all the collected evidence and address the IoT crime case with possible anti-forensics technique findings.

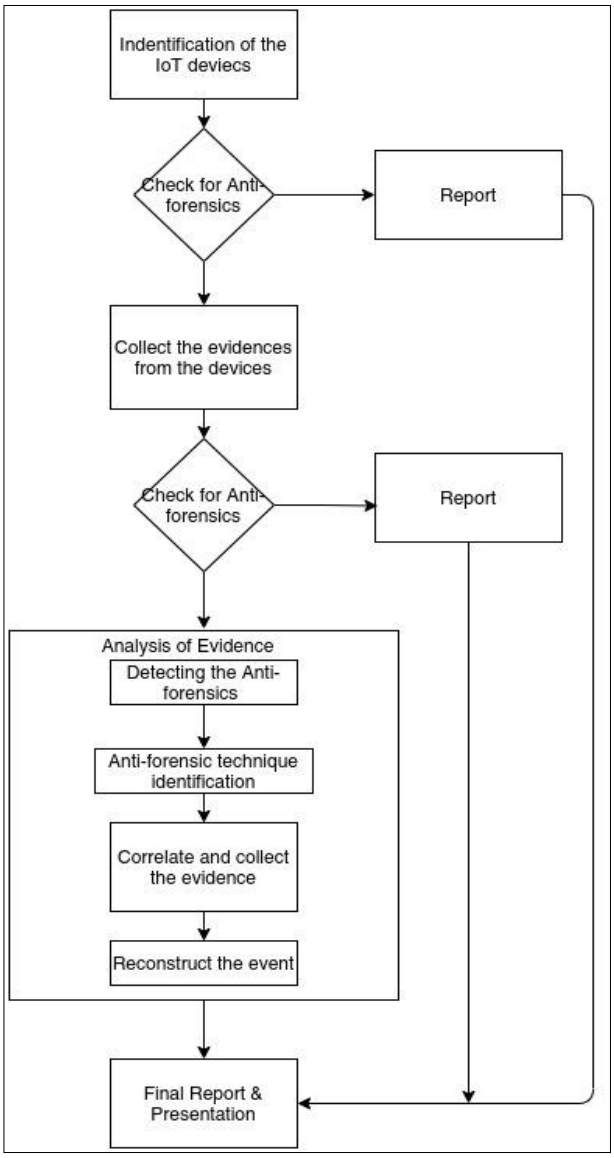
V. PROPOSED FRAMEWORK FOR ADDRESSING ANTI-FORENSICSIN IOT

In IoT Forensics standard steps of Forensics need to be followed[9]:

- Identification:-Identify the devices involved in the incident and what data can be obtained, how that data may help in the investigation and the steps involved to acquire the data.
- Collection:After identification we need to collect the evidence from the available devices or sources. Here some forensic tools may be used.
- Analysis:- Once we collect all the required evidence for IoT related crime, we need to extract,analyse and reconstruct the case to address the 5W (What, WHO, WHERE, When & How)[10].
- Report and presentation:- This is the final step of forensic procedure. Here we have to put every finding, tools used and analysis results for the next course of action.

Here we propose a framework for IoT Anti-forensics investigation process, which can help in addressing the anti-forensic attacks in IoT devices.

During the IoT Forensics investigation, the investigator identifies the source of evidence and collects the evidence from all possible sources. During identification he/she has to check for any possible presence of anti-forensic technique and report it. After identification,the next phase is evidence collection. Also investigators may face some anti-forensic technique. That also needs to be put in a report for final presentation. Analysis phase has been divided into 4 sub-phases: detection of anti-forensic techniques, anti-forensic technique identification, correlating and collecting the evidence from other sources and reconstructing the crime event with the help of missing links available from other sources. The sources may be logs, cloud data or others. In the last phase we have to prepare a final report with the help of all findings and tools involved in the investigation.



ACKNOWLEDGMENT

The authors are grateful to Mr. Debasis Mazumdar, Centre Head and Senior Director C-DAC, Kolkata, India, and MeitY Govt. of India for their valuable guidance and support.

REFERENCES

1. https://www.garykessler.net/library/2007_ADFC_anti-forensics.pdf
2. https://www.hcltech.com/blogs/internet-things-iot-security-key-challenges-their-force-multipliers
3. https://core.ac.uk/download/pdf/301360129.pdf
4. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html
5. https://www.deccanchronicle.com/nation/current-affairs/220419/internet-of-things-based-crime-investigation.html
6. https://www.sciencedirect.com/science/article/pii/S1742287616300378
7. https://www.researchgate.net/publication/333032591_IoT_Forensics_A_State-of-the-Art_Review_Challenges_and_Future_Directions
8. https://hal.archives-ouvertes.fr/hal-02432740/document
9. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
10. http://www.cybercsi.my/download/SOP%20OF%20DIGITAL%20EVIDENCE%20COLLECTION.pdf