International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. **05** Issue **01** | **2020**

A Review on The Relevance of IoT Forensics to Secure the Connected World

Anjana Menon R[1], Dinesh Soni[2], Feon Jaison[3], Dr. Lakshmi JVN[4]
[1,2]*Master student, Department of MCA, Jain Deemed-to-be University, Bengaluru, Karnataka, India*
[3,4]*Assistant Professor, Department of MCA, Jain Deemed-to-be University, Bengaluru, Karnataka, India*

ABSTRACT

Everything in this world is now a 'thing' in Internet of Things (IoT). Even a human being with a heart monitor implant can be called so. From humans to animals and from machines to vehicles, everything is inter-related. In this work, we are discussing about the traces produced by IoT devices that can be utilized to perform digital investigations. This area is termed as IoT Forensics, which is a subset of Digital Forensics. IoT Forensics pertains to IoT related cyber-crimes and also incorporates investigation of inter-connected devices and sensors. Here, we are trying to give a clear image about security challenges and forensic process in IoT in comparison to the traditional approach of Digital Forensics.

Keyword: - Internet of Things, Digital Forensics, IoT Forensics, IoT Devices, IoT Security.

1. INTRODUCTION

The word 'forensics' implies to those scientific techniques that involve examining of properties in a crime scene. This includes areas like DNA profiling and fingerprint detection. Forensics is very important in the court of law as it can prove an individual's guilt or innocence. In 1984, Computer Forensics, a branch of Forensic Science was born due to the demand from the law enforcement communities. They started developing programs to examine computer evidence. Later this became famous as Digital Forensics.

In today's tech savvy world, people across the globe started using gadgets like laptops, tablets and smartphones for socializing and making transactions. In the same way, a hike in the number of IoT devices are also noticeable. IoT devices include smart wearables, sensors and security appliances. Many of the IoT device manufacturers and organizations are implementing security methodologies to secure confidential information. In spite of these security practices, cyber-crimes related to IoT devices are growing day by day. Here comes the importance of IoT Forensics. IoT devices are the ones that provide seamless connectivity and massive data transfer. As a result, massive data breaches are also happening. Based on some sources, 31 billion IoT devices has been installed globally by January 2020.

2. INTERNET OF THINGS: FUNDAMENTALS

Internet of Things is a collection of 'Things' which includes devices, sensors and processes that connects these 'Things'. The Internet of Things is a giant network of connected devices and people – all of which share data about the way they are used and about the environment surrounding them. IoT includes a large number of objects of all sizes – from smart microwaves, which automatically cook food for the exact time period, self-driving cars, whose sensors detect objects and people in their path, to wearables like fitness bands that measure heart rate and the it also includes step counter to count the steps while walking, then use that information to make suggestions and predictions. Using IoT, connected footballs can track how far and fast they are thrown and the findings are recorded for training purpose.

2.1 Evolution of IoT

In 1999, Kevin Ashton coined the term 'Internet of Things' for the first time. Based on the studies conducted in January 2020, 31 billion IoT installations has been done all over the world. It is expected that, by the end of the year, 50 billion installations will be completed.

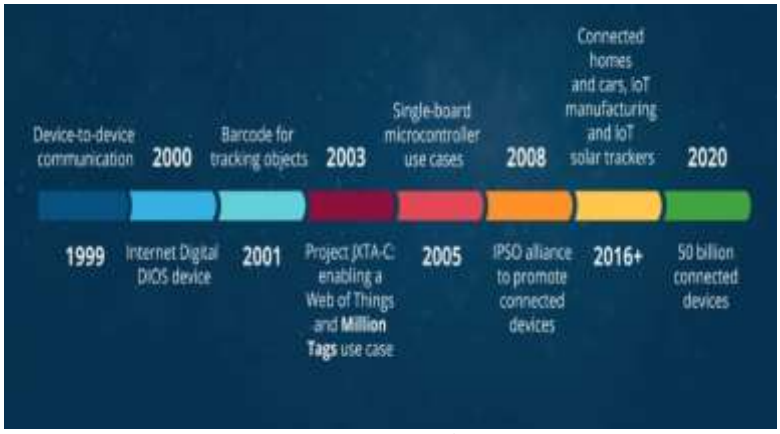

Fig-1: Evolution of IoT

2.2 Working

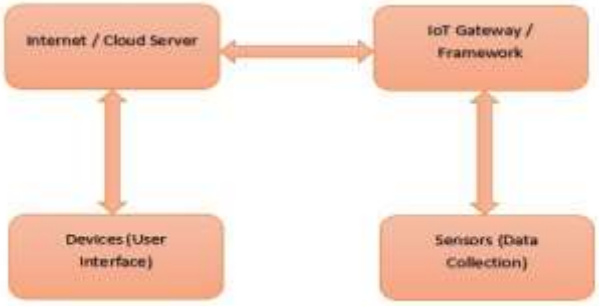

Fig-2: Working of IoT

Sensors: These are the devices that are installed to collect data from the environment. Sensing devices can be installed anywhere and everywhere.
IoT Gateway: IoT Gateway is the way through which we can connect all the things to the internet or cloud server. This is a bridge between the internal sensor network and Internet.
Cloud Server: Data Served by the IoT Gateway is stored and processed within these cloud servers. This creates information required for Data Analytics and decision making.
Devices: The devices provide the user interface for the end users to monitor their devices or things. These devices can access the information from the cloud server. Here, the information is retrieved in human readable format which includes graphs and charts.

2.3 IoT Communication Protocols

Satellite: Wireless communication protocol that enables cell phone communication. This includes GSM, GPRS, CDMA, 2G, 3G, 4G, LTE, EDGE etc.
Wi-Fi: Wi-Fi provides internet access to the devices that are within a small range.
Radio Frequency (RF): Simplest and lowest energy consuming protocol. ZigBee protocol uses a low-power RF radio incorporated into devices.
RFID (Radio Frequency Identification): Widely used protocols that identifies sensors and devices.
Bluetooth: Standard that enables short distance data transfer.
NFC (Near Field Communication): The protocol requires simple setup to enable short distance data transfer.

3. IoT SECURITY

Internet of things involves an abundance of connected devices, but anything that is connected to the internet can be prone to cyber-attacks. IoT security is a domain related to cyber security which is concerned with securing devices, sensors, communication channels and networks in internet of things. IoT devices were not initially built for security purpose. Installing security measures within the device is also not possible in most of the cases. A vulnerable IoT device or sensor can infect the entire network as they can act as attractive targets for hackers.

3.1 IoT Vulnerabilities

The OWASP top 10 list is globally followed by the developers of every kind. The OWASP Internet of Things project was started in 2014 with an intention to throw light on the things to avoid while developing & deploying IoT solutions. OWASP IoT top 10 is a trustable and one-point solution as they are successful in highlighting the high priority issues for safe guiding IoT solutions. Currently, the 2018 release of OWASP IoT top 10 is continuing.

Fig-3: OWASP IoT Top 10

(Image Source: OWASP IoT Top 10 Project)

3.2 IoT Security Solutions

Modern IoT ecosystems are always a complex thing to manage. Preventing vulnerabilities thereby mitigating risks in every nook and corner of the IoT ecosystem is better that jeopardizing the security of the entire network. Many hardware, software and open-source security solutions are available. Among these, software solutions are the most common & popular ones.

Securing IoT Network:

IoT devices are connected to the backend systems using the network. To protect this, endpoint security solutions like antivirus and antimalware software's can be used. Firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can also be used.

Authentication in IoT Devices:

A single IoT device can provide multi-user management features. This requires authentication principles like multifactor authentication, biometrics and digital certificates.

IoT Data Encryption:

The data (at rest & in transit) should be encrypted using cryptographic algorithms and encrypted key throughout its life cycle. This method protects data and user privacy.

IoT Security Analytics:

High profile cyber-attacks including zero the exploits cannot be detected using firewalls. Here comes the importance of analytics. This involves aggregation, monitoring, prediction and even the latest technology like machine learning.

IoT Security Topologies:

This includes PKI and API security methods. PKI- To establish secure connection between the devices and user interface, Public Key Infrastructure methods can be used. This includes X.509 digital certificate, cryptographic key, public/private key generation, distribution, management and revocation. API- Using Rest-based APIs, data integrity is ensured between devices, backend and the user interface. This can also detect and prevent cyber-attacks against APIs.

4. IOT FORENSICS

IoT forensics is the process of forensic investigation of IoT devices, sensors, network, cloud and other backend systems related to Internet of Things. Internet of things forensics process is not confined to examination of IoT devices. As IoT is a combination of many technologies like network, cloud and IoT itself, IoT forensics is also a combination of network forensics and cloud forensics and device level forensics. In IoT forensics, digital evidence can be collected from an IoT device or a sensor, from an IoT network or a routing device, or from cloud.

IoT forensics is a complex process because in most of the IoT ecosystems, the data is stored in cloud. Here, the data acquisition process is done through cloud forensics, which is further more challenging due to the distributed data storage in cloud solutions. IoT networks can be domestic or industrial. It can be a LAN, MAN or WAN. If an accident occurs, all kinds of networks through which the traffic has passed should be examined. Last but not the least device forensics should also be conducted in order to obtain digital evidence. This can be a video footage from CCTV camera or an audio from a virtual home assistant.

4.1 IoT Forensics Components

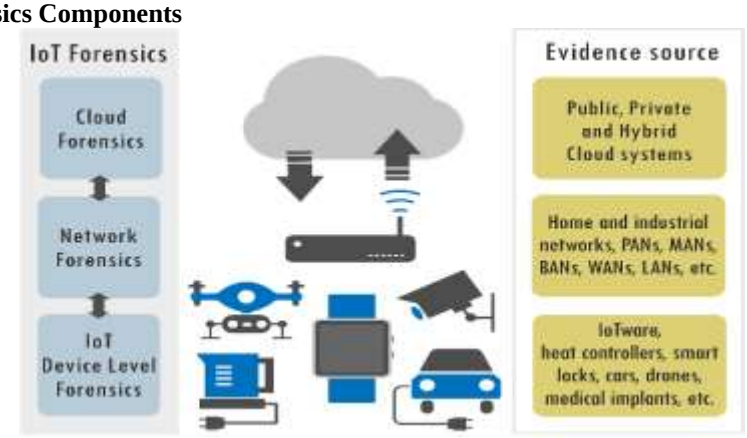

Fig-4: IoT Forensics Components [7]

4.2 IoT Forensics Process

The forensic process in IoT ecosystem is same as that in digital forensics. The only difference is that the source of evidence can be anywhere in the home, home appliances, vehicles, humans or animals with implants or anything across the globe which is IoT enabled.

Steps in Forensics Process:

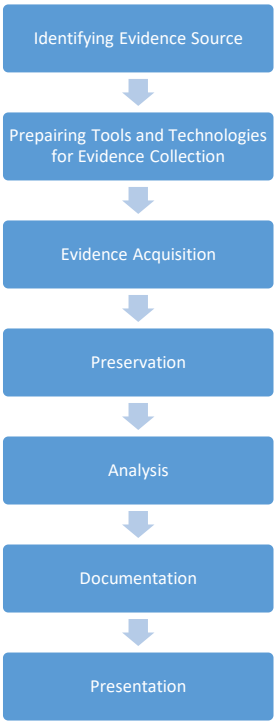

Fig-5: IoT Forensics Process

4.3 IoT Forensics Examining Tools

CAINE (Computer Aided Investigative Environment):

- User friendly interface
- Compiles complete documentation of investigation
- Allows cloning
- Allows preservation, collection, examination and analysis

Wireshark:

- Capturing network packets
- Free and open source
- Display output in readable format

EnCase:

- Recover evidence from seized hard drives
- Conduct depth analysis of files

Bulk Extractor:

- Scans disk image or directory of files
- Extracts credit card numbers, e-mail addresses, web addresses and telephone numbers

NUIX:

- Machine learning enabled e-discovery tool
- Incorporated with Artificial Intelligence & analytics

5. TRADITIONAL FORENSICS V/s IOT FORENSICS

IoT forensics is a subset of digital forensics or traditional forensics which deals with cyber incidents related to internet of things. IoT Forensics is a lot more complex than digital forensics process. In IoT forensics, finding evidence source is the most difficult challenge. When compared to the standard digital forensic methodologies, IoT forensics depicts multiple challenges depending on the versatility and complexity of the IoT devices.

Table-1: Comparison of Traditioal and IoT Forensics

Parameters	**Traditional V/s IoT Forensics**	
	Traditional Forensics	**IoT Forensics**
Evidence	Computers, Cloud devices, Servers, Gateways, Mobile Devices	Home Appliances, Car tags, Readers, Embedded Systems, Nodes
Devices Connected	Billions of devices connected	50 Billion devices by 2020 according to Gartner
Networks	Wired, Wireless, Bluetooth wireless network, Internet	RFID, Sensor network
Protocols	Ethernet wireless (802.11), Bluetooth, Ipv4 and Ipv6	Wi-Fi, RF, RFID, NFC, Bluetooth, Satellite
Size of the digital evidence	Terabytes of data	Exabyte of data

6. CONCLUSION

The paper deals with internet of things, IoT security aspects and IoT forensics. Some existing practices in this context have been reviewed. During the course of this research work, the necessity of IoT forensics process in this digital era is observed and understood.

'Data is the new oil' and it should be safeguarded from cyber incidents. While increasing number of IoT devices are creating wider attack surface, IoT forensics should also be there to cope with these challenges. IoT forensics is a revolutionary footstep of technology which is no more a prediction. It's here and it's now.

7. REFERENCES

[1] https://data-flair.training/blogs/how-iot-works/
[2] https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
[3] https://www.fortinet.com/resources/cyberglossary/iot-security
[4] https://owasp.org/www-project-internet-of-things/
[5] https://www.rapyder.com/blogs/top-10-iot-security-solutions-for-common-iot-security- issues/
[6] https://arxiv.org/ftp/arxiv/papers/1801/1801.10391.pdf
[7] https://www.semanticscholar.org/paper/A-Survey-on-the-Internet-of-Things-(IoT)-Forensics%3A-Stoyanova-Nikoloudakis