Internet of Things

Gowtham Ravi
Griffth Science
Griffth University
Brisbane, Australia
gowtham.ravi@griffithuni.edu.au

***Abstract*— The Internet of Things compromises countless link between various machines through the network allowing information transfer. The Internet of Things is appreciated for precision, systematic and cost-effective — vast development among technology, creating concerns in security and confidentiality of the user's information. While using the Internet of Things system, The Forensic Detective looks up to various threats while searching the needed information. Through this paper, we discuss current and future forensic methods in the Internet of Things and the challenges in the Internet of Things Forensics.**

Keywords—Internet of Things, Digital Forensics, IoT Forensics

I. INTRODUCTION

The popular image of the Internet and digital smart system association created- the Internet of Things (IoT) [1]. The Internet of Things is treated as the ultimate forthcoming assessment of the internet. The elemental concept of the Internet of Things is to grant self-governing, protected network and transfer of information among gadgets and software. These systems can interact immediately with each other or via the Software Interface and can be regulated by taught systems with elevated computing capacities, such as cloud computers, which increase smartness to low computing devices. The Internet of Things carries a considerable commitment to make it possible to regulate all the gadgets we use on our regular grounds. It also holds great hope for cybercriminals who can use home routers, television, refrigerators and other internet-linked devices to start big and dispersed attachments, the Internet of Things presents a range of difficulties from the view of law compliance and digital forensic officers. Therefore, the need for a methodology for forensics to investigate crime related to IoT is relevant. For forensics researchers, the IoT presents some difficulties, including the widespread distribution of data and information, the blurring of boundaries between networks, and the (anticipation of) privacy of consumers with personal networks disappearing progressively into non-personal networks and private networks blurring into government ones. The IoT domain's concentrate is on its advantages and apps as well as applicable safety and privacy issues. There is little in the IoT domain for Digital Forensics respondents by the manner of a devoted incident response methodology.

II. DIGITAL FORENSICS

The chapter discusses a summary of digital forensics and IoT [2]. Next, we describe IoT forensics and show a theoretical case study concerning the IoT atmosphere on digital forensics.

A. Digital Forensics

Before 2006, there was no distinct U.S. Federal law in federal instances to use electronically recorded data (ESI) as proof. In the 2006 amendment, the Federal Rules of Civil Procedure (FRCP) expanded the scope of evidence and included ESI for civil litigation. FRCP defines the content that can be discovered, and all information deposited in the hard disk, RAM, or Virtual Machine (VM) records under this concept can be identified for forensic investigation.

- Identification: There are two primary identifying measures: identifying an event and identifying proof that will be needed for active inquiry of the event, with prospective correlation to other incidents.
- Collection: Digital proof is extracted from multiple sources (e.g. hard disk, cell phone, e-mail, and many other kinds of information) by a researcher during the recording phase. The researcher also retains the evidence's validity.
- Organisation: The organisation process has two main steps: examining and analysing digital evidence. In the examination stage, the information and its features are extracted and inspected by a researcher. The user depicts and interacts the available data in the analytical phase to arrive at a conclusion that can serve to prove or disprove civil, administrative or criminal allegations.
- Presentation: An researcher produces a structured study in this phase to present his or her results on the situation. For submission to the qualified tribunal or trial, this study should be suitable.

In digital forensics, it is compulsory to maintain information privacy and a rigid system of data detention. Several other scientists describe computer forensics as the method for examining the computer system to identify possible legal evidence.

B. Internet of Things

The Internet of Things idea was first put forward by the Auto-ID centre of MIT. The 2005 Internet survey of the International Telecommunications Union (ITU) officially suggested the Internet of Things. The world is heading towards the age of omnipresent network society, according to the report, in which networks and networked devices are pervasive. All of our surrounding things will be connecting things for data exchange through the Internet; these things include personal computers, laptops, tablets, smartphones, insulin pumps, tires, refrigerators, televisions, air coolers/heaters, and much more. By 2020, the people in the world will have ten connected IoT devices and a total of 40 to 80 billion IoT devices. Most IoT devices embed various

sensors and actuators capable of sensing, computing, making smart decisions, and transmitting useful collected information over the Internet. There are many heterogeneous systems involved in the Internet of Things. Among them, the most mature technology is RFID (radio wave recognition) and mobile sensor. There are a large variety of IoT apps, such as command of home appliances, health care management, manufacturing facilities, stock leadership, and many more. The IoT devices generally capture information from the physical setting through various detectors and send data to the cloud for smart decision-making or other information handling activities.

C. *Internet of Things Forensics*

The IoT forensics is defined as a special section of digital forensics, where procedures of detection, compilation, organisation, and introduction work with IoT infrastructures to determine the truth of a criminal incident. The IoT forensics identified as a mixture of three electronic forensics systems: device-level forensics, network forensics, and cloud forensics.

- Device-level forensics: A researcher may need to obtain information from the IoT systems ' local storage. It includes the hardware tier forensics when an essential item of proof requires to be gathered from the IoT systems.
- Network Forensics: The forensic is possible to identify the origin of separate assaults from network records. Network records can, therefore, be vital in condemning or exonerating a person. IoT infrastructures include various network types, including Body Area Network (BAN), Personal Area Network (PAN), Home / Hospital Area Networks (HAN), Local Area Networks (LAN) and Wide Area Networks (WAN). It is possible to collect a crucial section of proof from any of these networks.
- Cloud forensics: Cloud forensics will be one of the most significant positions in the IoT forensics domain. Since most IoT phones have small memory and computing capabilities, the cloud stores and processes data produced from IoT phones and IoT networks, this is because cloud solutions offer various benefits including convenience, large capacity, scalability, and on-demand accessibility.

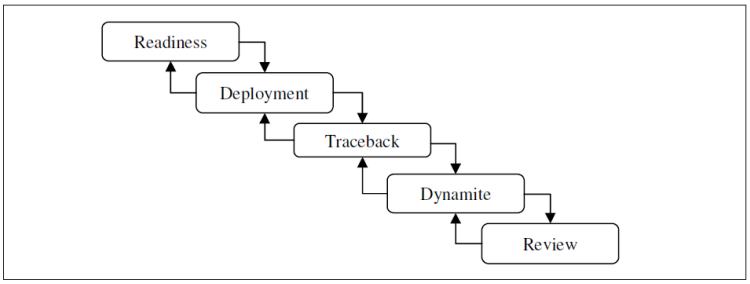
III. PREVIOUS WORK IN IOT FORENSICS

An emerging challenge has been the process of identifying and retrieving information in IoT. Few of the most frequently used IoT forensic models are:

- Digital Forensic Investigation Model
- The Hybrid Model
- 1-2-3 Zones of Digital Forensic

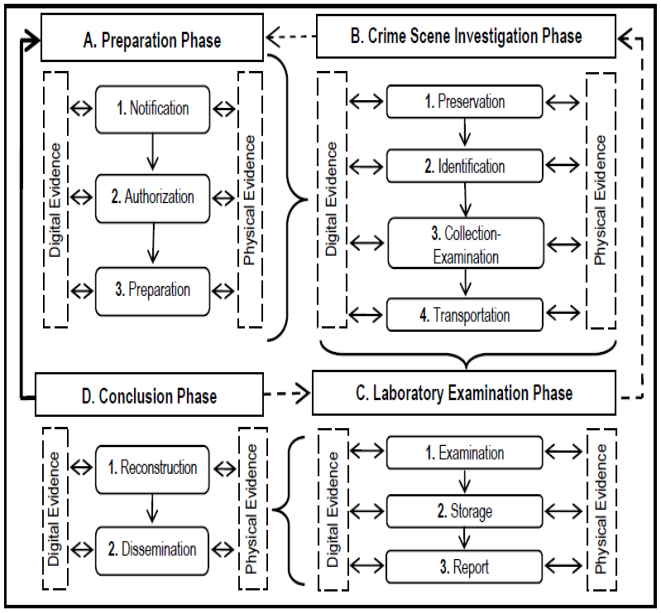
A. *Digital Forensic Investigation Model*

This model presents a major stage called the Traceback phase[3]. This is to allow the researcher to connect the home to the real devices/computer that the criminal uses to execute the crime. The investigation process began with the phase of readiness and the tasks performed are the same as in IDIP. The second phase of deployment provides a mechanism for detecting and confirming an incident. It consists of 5 sub-phases, namely Detection & Notification, Physical Crime Scene Investigation, Digital Crime Scene Investigation, Confirmation, and lastly, Submission. This stage involves surveys of the physical and digital crime scene as well as presenting results to legal entities (through the submission stage). The primary goal is to track the origin crime scene in the Traceback stage, including the gadgets and place.



Two sub-phases, namely Digital Crime Scene Investigation and Authorization (receiving permission to conduct investigations and access data), support it. The dynamite stage follows the Traceback stage. In this stage, the primary homicide site is investigated to identify the prospective culprit. It consists of four sub-phases, Physical Crime Scene Investigation, Digital Crime Scene Investigation, Reconstruction, and Communication. In the sub-phase of Reconstruction, parts of gathered data are placed together in order to build incidents that might have occurred. The sub-phase of the communication is comparable to the earlier stage of the submission. In creating this model, the primary issue was to introduce an increase in the method of digital forensic investigation. The key idea behind the DFIM is to reveal concealed digital evidence. This model is not really going to be concerned about physical evidence. Since this could be a significant drawback if this model were to be regarded as the physical evidence of each IoT case in the IoT forensic analysis.

B. The Hybrid Model



The suggested model could be used to explore hybrid proof crime scenes, but also in cases where there is only digital or physical evidence[4]. The model comprises of four main stages and twelve sub-phases (Fig. 1).

1) Preparation

a) Notification

This first phase involves (a) information about committing a crime. For instance, using the Australian Emergency Number (000) to record a crime, send an email, go to a police station, etc. (b) notification to the appropriate law enforcement agency accountable for conducting the inquiry. The accountable entity can be determined by geographic requirements (place of the accident site) or the type of the accident incident (e.g., theft, murder, etc.). Notification is crucial because the data gathered here is essential to the investigation's next measures.

b) Authorisation

Authorisation to perform an inquiry is acquired from the allocated organisation. The form and details of the authorisation depend on the type of crime and the procedural rules of the nation where the crime happened. Typically, immediately after a crime has been discovered, assigned officers can conduct an investigation at once and inform the attorney on duty as soon as possible.

c) Preparation

Preparation involves the accessibility of the required inquiry instruments, equipment and staff. Preparation is essential not only after a crime or accident notice but also before that, including schooling and instruction, reaction, accessibility and tool and machinery features. The individual accountable for the inquiry will be determined in this sub-phase.

2) Crime Scene Investigation

a) Preservation

It is the responsibility of the head responder at the crime scene to organise several things: first aid, search for witnesses and securing the view from people who are not allowed to approach. Also, it is necessary to recognise and ensure available sources of physical and digital evidence.

b) Identification

The identification is a specific job preferably performed by specialists in the criminal investigation. Their job is to define feasible proof linked physically or digitally to the products in the crime scene. In serious crimes, the research could be conducted by several technicians specialised in different fields. Their level of cooperation and understanding is a significant factor for successful research. This phase also includes documentation which refers to photographing, sketching and mapping the crime scene, taking notes about items or people present at the crime scene etc.

c) Collection – Examination

The collection-examination is one of the model's most significant sub-phases. Fingerprints, crime-related products, biological material and other physical evidence, must be collected by the researcher. The researcher should first check for volatile information in the event; there is digital evidence on the crime scene. Cooperation between the professionals on the digital and physical crime scene is very crucial at this point because gathering physical evidence can ruin digital proof and vice versa. This phase includes examination as well. This is not a thorough examination method in a laboratory setting. Sometimes, however, it is essential to get as much data as necessary for the inquiry. For instance, searching the victim's mobile phone, e.g. last calls or texts or a personal computer for e-mails or latest posts on social networks is highly relevant in a severe crime investigation.

d) Transportation

While transferring proof is generally viewed as a secondary operation, we find it as essential as a compilation. Special measures should be taken during transport to avoid damage to the evidence. In order to prevent any destruction of physical and digital evidence, careful packaging, humidity and temperature should be considered.

3) Laboratory examination

a) Examination

Examining proof in a laboratory setting is essential for any inquiry as it can provide critical evidence linked to the situation to the researcher. While only a portion of the proof gathered can be examined at the crime scene, all proof is carefully inspected and evaluated in this stage according to the type of the proof and the specifics of each situation.

b) Storage

Evidence should be correctly deposited in a locked proof space with strict access controls after the examination. The proof should be marked and separated in order to prevent cross-contamination, to prevent devastation and to allow re-examination if such need arises in a tribunal or any other phase of the inquiry.

c) Report

The report determines the results of the phase of laboratory testing. The laboratory report is one of the investigator's most important documents and all the parties involved in a case (prosecution and defence).

4) Conclusion

a) Reconstruction

Reconstruction of crime is the primary duty of the researcher who evaluates the proof gathered and examined and reflects the truth as described by the assessment of proof. This step would be of value only if the previous steps were followed forensically so that the same results would be obtained by anyone following the same method.

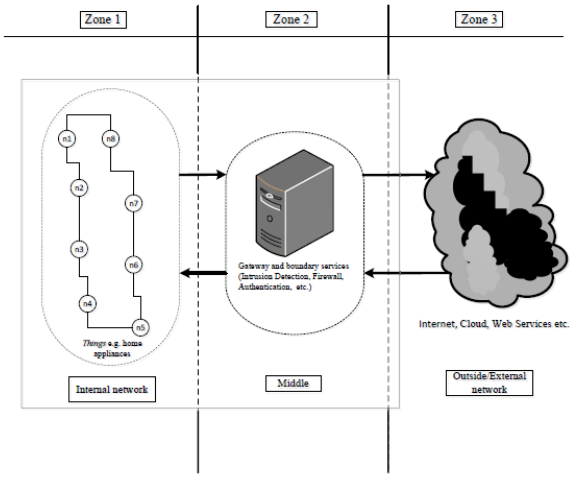
b) Dissemination

Dissemination is the model's final phase. In this phase, a thorough inquiry assessment is performed to maintain the understanding acquired and recognise regions for enhancement. Learned lessons should be documented carefully and disseminated to other sides conducting comparable inquiries.

This digital forensic model created as a result to analyse either physical evidence only or at one moment only digital evidence. This research methodology appears to be very small in aspects of IoT device searching for proof. Whenever IoT crime is concerned, a comprehensive and rapid response is anticipated.

C. Points of Focus - The 1-2-3 Zones of Digital Forensics

Knowing where to search will be involved in the IoT DF. Without this approach to IoT forensics, the precious effort will be lost to look for insignificant proof in the incorrect locations[5]. This article recommends a zone-based approach to inquiries linked to IoT.



Zone 1: As shown in Fig. 1. This is the internal area in which all the hardware, software and networks (e.g. Bluetooth and Wi-Fi) related to the crime scene are catalogued, and a decision is made on what is relevant to the case and what evidence might contain that would be useful to the situation. On these networks, such as smart temperature controllers, the IoTware can be helpful even if only for their tag identification (tag ID) and status, i.e. seated, conscious, and actively transmit, etc.

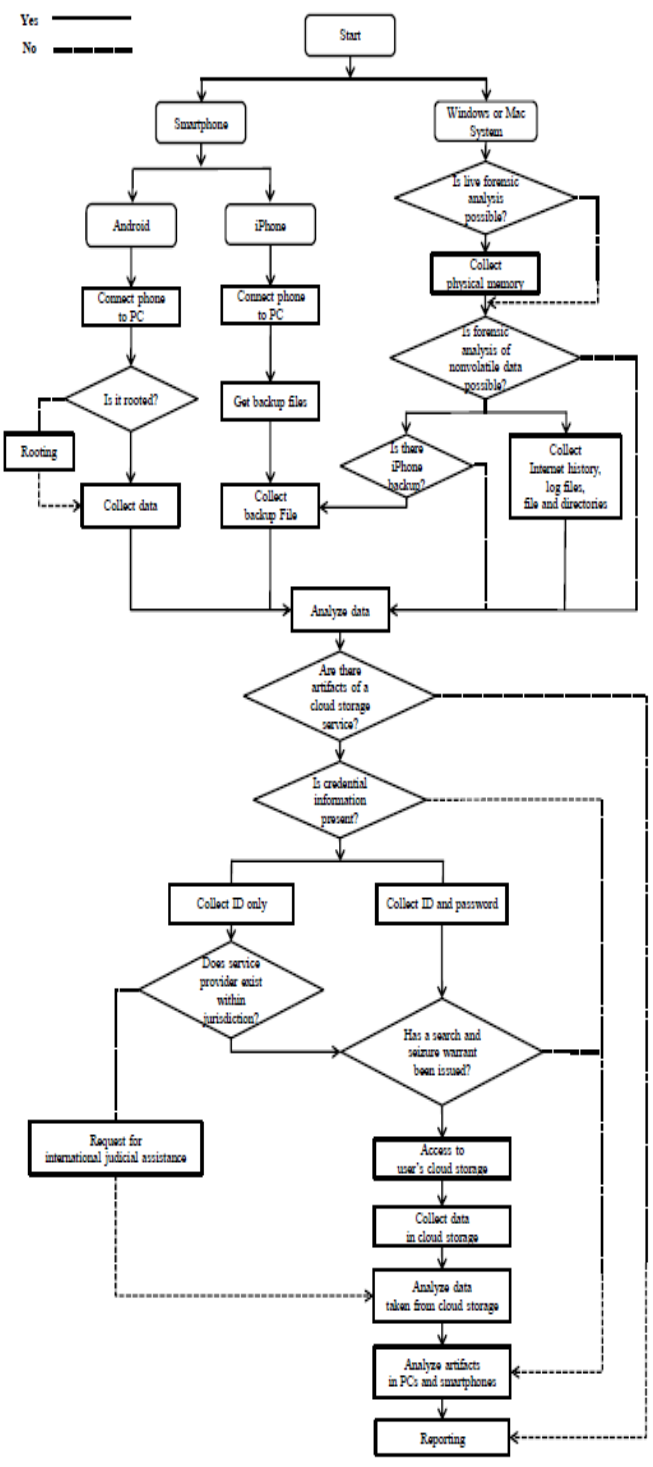
Zone 2: All appliances and software located at the network boundary and providing a medium of communication between internal and external networks reside in this zone. This area contains all of the networks ' public-facing appliances in the issue. Typically, forensics inquiries will require recognising these components, cataloguing them and obtaining from them any relevant proof available. Devices in this area may include Firewalls Network and Intrusion Prevention and Detection Systems (IPS and IDS).

Zone 3: It includes all hardware and software outside the relevant network. This area involves proof from all cloud, social network, Internet Service Provider (ISP) and information from mobile network suppliers; Internet and web-based facilities, digital internet item identification, edge network, Internet proof device-based proof, e.g. RFID tag and reader records; a portal or border phones, etc.

The implementation of this strategy will be at the request of DF researchers and can be achieved in conjunction (all simultaneously studied zones), or the highest target region can be recognized (this can be depending on the depiction of the recorded occurrence and potentially the highest effect region) and a choice can be taken to concentrate on this first. Reacting to IoT-related digital attacks using the described 1-2-3 Zones provides a useful method for DF investigators to plan and systematically approach investigations and to effectively identify potential OOFIs. This strategy decreases the difficulty experienced in IoT settings, and guarantees researchers can concentrate on obviously designated areas and items in preparing for research.

IV. NEW PROJECT

A. *Cloud Services*



Cloud storage facilities, a series of IaaS, provide consumers with processing room. Their use is growing as they also give a range of extra facilities such as printing records and pictures, songs and video playability, and the capacity to submit the correspondence[6]. Most hosting companies provide free storage space, and a user who wants more space can lease extra storage capacity. Using a Web browser, cloud memory facilities can be obtained, and client apps can be provided for easy use. The Providers supply client applications for various platforms to enable people to use their services with multiple devices, such as android gadgets and tablet. A variety of differentiated services are provided by cloud storage facilities. Depending on the particular characteristics of the system, the artefacts they produce in PCs and smartphones vary between distinct facilities.

The investigator is collecting and analysing data from all devices used by a user to access a cloud storage service. Such gadgets include PCs, smartphones, tablet PCs, and PDAs, but this paper only covers PCs and smartphones, the devices most commonly used. Figure 1 shows a procedure to investigate such devices. The researcher can examine storage documents deposited on a PC for the iOS working scheme (iPhone) or retrieve and evaluate information used for iTunes. In other cases, the researcher can evaluate previous information supported up by iTunes on a PC or obtain information for an evaluation straight from the iPhone. Data can be acquired after rooting in the case of an Android phone. Rooting is a method that provides reliable power for Android smartphone customers. It is a crucial method to obtain information from Android smartphones because only after rooting can you enter the file directory and receive data. As described above, the investigator analyses the data collected from PCs and smartphones and then check whether there are traces of a cloud storage service in the data collected. If so, the researcher will check whether the qualifications of a user are available. If the identification and password of a user and any other data allowing entry to the cloud room of a user is discovered, a search and seizure license should be awarded if necessary. The logging into the storage service is steep at this stage and gather evidence even if a user's ID and name are discovered. This is because the space of a user is personal. Since it would not be due practice to log on without a warrant, information gathered without a permit would not be applicable. If a search and seizure order has been given by the researcher, the researcher can enter user files and retrieve information in cloud storage. If the investigator has not issued a search and seizure warrant, only the remaining artefacts in PCs and smartphones can be analysed. If only the user ID is found, the investigator will check whether there is a server that belongs to the cloud storage service used by the customer under the same jurisdiction as the investigator. If this is the case, a warrant for search and seizure should be reissued. The investigator collects the files in the cloud storage of the user after that. In all cases, the investigator analyses the data available from the cloud storage and from artefacts in local devices after the legal proceedings have been completed. Remote storage collecting and analysing data is the reason for examining file contents. The investigator writes a report to complete the procedure.

The cloud environment concept of IoT forensic requires a new mindset in which some data will not be available, some data will be suspicious, and some data will be court ready and can fit into the traditional forensic model of the network. Any forensic investigator is challenged to understand what data collected falls into each of the categories of unavailable, suspected, and ready for court.

V. CONCLUSION

In the coming years, IoT presents an enormous transformation in the entire sector. More precise technology analysis is needed as the digital forensic investigator will face more challenges. In this paper, new IoT based forensic has been proposed. The future of IoT is not only influenced by users. The potential autonomy of IoT or lack of control over IoT by those it impacts will doubtless generate IoT adoption resistance potentially manifested by public protests, negative publicity campaigns and actions by governments.

In the past ten years, many IoT foundation technologies have been influenced by developed concerns that have been labelled as "privacy threats." Privacy is multidimensional in itself. Popular definitions focus on the freedoms of the individual or the right to remain alone. In reality, privacy includes the interests of individuals, informal groups and all forms of organisations and is thus a complex multidimensional subject. Future research work would focus on the methodology of IoT privacy.

REFERENCES

[1]S. Alabdulsalam, K. Schaefer, T. Kechadi and N. Le-Khac, "Internet of Things Forensics – Challenges and a Case Study", in *IFIP International Conference on Digital Forensics*, 2018.

[2]S. Zawoad and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things", in *2015 IEEE International Conference on Services Computing*, New York, NY, USA, 2015.

[3]Y. Yusoff, R. Ismail and Z. Hassan, "Common Phases of Computer Forensics Investigation Models", *International Journal of Computer Science and Information Technology*, vol. 3, no. 3, pp. 17-31, 2011. Available: 10.5121/ijcsit.2011.3302.

[4]K. Vlachopoulos, E. Magkos and V. Chrissikopoulos, "A Model for Hybrid Evidence Investigation", *International Journal of Digital Crime and Forensics*, vol. 4, no. 4, pp. 47-62, 2012. Available: 10.4018/jdcf.2012100104.

[5]E. Oriwoh, D. Jazani, G. Epiphaniou and P. Sant, "Internet of Things Forensics: Challenges and Approaches", in *9th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing*, Austin, Texas, United States, 2013.

[6]H. Chung, J. Park, S. Lee and C. Kang, "Digital forensic investigation of cloud storage services", *Digital Investigation*, vol. 9, no. 2, pp. 81-95, 2012. Available: 10.1016/j.diin.2012.05.015.