IoT Based Secure Communication using Digital Forensic

MORE PRATHAMSH PRAKASH

Department of Information Technology (MSc.IT part II) Chikitsak Samuha's S. S. & L. S. Patkar College of Arts & Science, and V. P. Varde College of Commerce & Economics

Abstract- : Explosive growth of the Internet-of-Things (IoT) due to its widespread applicability, it is imperative that IoT designers and architects must incorporate ensuring security of communication in IoT as a key requirement. This emerging field of study, communication in IoT, is concerned with ensuring secure collaboration between smart sensors, actuators and devices and the external environment that constitute the overarching arena of IoT. The field poses new challenges to security and privacy in communication. Most of the cloud service providers such as Amazon, IBM, Microsoft, and Google facilitate various cloud services at reduced cost. The architecture of IoT must be designed to have many features such as scalability, efficiency, accessibility, availability, and flexibility so that applications can be built that can benefit both public and commercial entities. Key factors in driving the success of the IoT will be an accurate specification of security parameters with various security measures that must be enforced. This paper gives an overview of security and privacy aspects in IoT communications using an advanced digital forensic approach for security enhancement. The researchers face various challenges in the investigation of security breaches in IoT. The challenges get magnified multiple folds as cloud service providers utilize many advanced techniques such as virtualization and a multi-tenant usage model to allocate its resources to users securely. These models and architectures make it difficult for investigators who try identify sources that launched various malicious activities and attacks on cloud services. The investigators resort to advanced digital forensic investigation to analyze such attacks. There exist various digital forensic techniques and tools which are not necessarily applied in the context of security breach in IoT. When any security breach occurs, investigators face challenges in collecting evidence as they cannot physically access the evidence buried in devices connected to a local host. The advanced digital forensic approach consists of identifying the evidence related to the source of the crime, and examining and reporting the results and conclusions. The proposed methodology, which employs an advanced digital forensic approach, describes an improved, efficient, and reliable method to identify the source of the crime and collect evidence responsible for security breach during communication**.**

Keywords- IoT, Digital forensic, Security, Privacy

I. INTRODUCTION

Internet of Things (IoT) is yet another disruptive innovation that empowers small electronic devices, sensors, and actuators to transform as smart products. These electronic devices are connected to each other through various system media, and the sensors play major role in that transformation. The objective of employing IoT is to make lives easier and active. For example, an autonomous vehicle drives on the roads without a driver; a smart light can turn itself off automatically when no one is present in the room; and, a smart climate control system starts working automatically when the room temperature falls to a threshold value. Without a doubt, IoT innovation crosses vertical industry territories, and finds applicability to wide variety of disparate territories such as a smart city, smart healthcare, smart social spaces, smart home and forensic sciences . However, IoT innovation can open the doors to hackers and invite them to commit cyber-crimes that disrupt the routine functioning of these territories and inflict chaos into people's daily lives.

Like most other innovations, IoT innovation had not been planned with security in view, as the primary objective was to economize on the cost of the devices and optimize sizes of devices to foster effectiveness and consumer appeal. This meant sacrificing many functionalities in IoT including security, as they need a specific area and process functions to be run, making the IoT products an obvious target for hackers to commit cyber-crimes.

Most of the IoT device makers readily make available to the users the capabilities of the product. They do not, however, specify the processes and location where the processes are executed that impart 'intelligence' to these devices. For example, an LG smart vacuum, which can clean the room without anyone else's input, carries out its activities with the data collected by sensors which can distinguish the size and the state of the meander at the instant of cleaning. Interestingly, a gathering of analyst found serious security flaws during an LG entry login process that enabled them to take control of the vacuum, giving them access to live-stream video from inside a home

From the viewpoint of the forensic, IoT devices will provide critical history, including any irregularities that occurred that could help in the examination of the run-time behavior of a process. A portion of the history may not become visible except to specialized technical personnel, which implies that the examiners should consider these hidden histories and how they can secure the irregularities that occur from these devices.

II. TRADITIONAL DIGITAL FORENSIC VERSUS IOT FORENSIC

Digital forensic could be characterized as a specialization of forensic that is concerned with the gathering or acquisition of digital evidence in its most unique form, systematically

analyzing the evidence or data, and subsequently reporting the results and conclusions derived. Conventional digital forensic and IoT forensic scene investigation are similar in many respects but they also differ in some aspects. Regarding sources of evidence, in conventional forensic, evidence may be gathered from PCs, cell phones, servers or entryways. In IoT crime scene investigation, the evidence could be gathered from home machines, autos, labels peruse, sensor hubs, therapeutic embeds in people, or other IoT devices

2.1. FORENSIC INVESTIGATIONS IN THE NEW AGE

Digital forensic is gradually evolving as an answer to the issue of cybercrime. At its core, digital forensic is the way toward distinguishing, safeguarding, breaking down and presenting advanced confirmation in a courtroom to support or reject a hypothesis related to a cybercrime investigation. It utilizes standards and licensed instruments in its investigation. IoT forensic has more positive areas than normal criminology. Despite conventional systems such as wired, Wi-Fi, wireless and mobile, the RFID sensor network is also available for IoT. Distinctive IoT programming, for instance, should also be included in the course of the analysis as well as computers, tags and therapeutic tools. The complex concept of IoT approaches poses the basic check in the investigation of an IoT crime. IoT is a blend of many global technology areas, including distributed computing, cell phones, PCs and tablets, sensors and innovations in RFID. Subsequently, legal sciences for IoT will incorporate these previously mentioned zones. Evidence sources on IoT can be divided into three groups:

1. All evidence collected from sensors and smart devices
2. All evidence gathered from hardware and software to communicate between smart devices and the outside world (e.g. machines, modular, IPS, IDS, and firewalls) integrated into traditional forensic computers; and
3. All proof obtained from under review hardware and software outside the system. This collection involves cloud, relational organizations, ISPs, and scalable network suppliers, online virtual characters, and the internet.

III. DIGITAL FORENSIC IN IOT DEVICES

In a cybercrime or data security episode, digital forensic manages digital identification, collection, analysis and introduction of proof from various forms of advanced / electronic capacity media. Typically, from a server machine to a portable de-bad habit, capacity media can be anything. The proliferation of IoT devices and the need for digital security on IoT devices / applications depends on electronic forensic accumulation and investigation. IoT Forensic requires a multifaceted approach to gather evidence from a variety of sources, such as sensor devices, specialized devices, remote storage and even ISP logs. A number of the precedents for IoT devices hacking episodes have been blocking the use of heart devices, for example pacemakers, patient and children's frameworks, launching DDOS assaults using bargained IoT devices (Botnet), hacking / interception of IVI frameworks, hacking of various CCTVs or IP cameras. IoT Forensic is empowered to identify and obtain digital evidence for legitimate and forensic use from IoT phones.

- Extraction of Digital Evidence from IoT Devices When IoT devices join a range of models, work frames, document structures, and restrictive equipment and software, there is no standard approach for identifying and collecting information from a specific IoT system. The following technique is a set of information collection techniques.
- Receiving Flash memory.
- Receipt of a data dump using Linux dd path or net cat.
- Using JTAG and UART procedures to retrieve firmware information. The protocols Telnet, SSH, Ethernet and Wi-Fi have also be en used for accessing and connecting with devices.
- Obtaining a Flash Memory Image: This technology allows an integrated store of the device, using criminological visualization resources such as FTK Imager, X-ways Legal Science or Winshex, when an IoT computer can be paired with a PC. Many sophisticated legal software can be used to analyze the collected criminal image. At any conceivable moment the memorandum-storage gadget is imaging in a bitstream physical mode, for example NAND / NOR Flash chips, SD / CF / MMC cards

.

- Receiving a memory dump using Linux dd command: Indoor utilities such as Linux dd or net cat can be used to protect a criminal image of a selected disk or gadget memory on IoT systems with a working network, e.g. Linux or linux booting in the gadget and accessing the terminal will be needed. To order to recognize and extract significant data from the incident, the resulting visible image may be analyzed.

IV. SECURITY AND PRIVACY REQUIREMENT

In all stages of information gathering, distribution of information, centralized processing and republishing, the police or other associated wrongdoing records of the safety division still exist. The four accompanying requirements should be considered when creating legal Internet security and protection frameworks.

• Data Integrity Data preservation refers to the fact that all data appreciates that semantic measures are taken without unauthorized alteration. Two standards of precision and continuous performance are included. Information respectability can be divided into four classes of information, which can be maintained by remote keypads, limits, principles and triggers, to be specific, substantial uprightness, spatial confidence, and user-specific honesty.

• Data Usability Information is easy to use to ensure that approved users can use information or information frameworks. Huge information brings both great advantages and vital difficulties, such as messy information. In fact, the lack of information or misfortune caused by unapproved data often makes wrecks easy to use.

• Data Auditing The examination of scientific information is a powerful attempt to monitor the use of the assets and to find and follow unusual occasions as a typical measure. Similarly,

cloud specialists typically take on jobs that are not trusted and require sensitive strategies for review. Data analysis involves clients, cloud expert partners, accesses and records of operation.

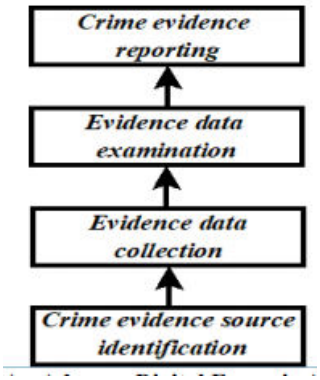
• Forensic departments Information Privacy The data from the Forensic department can be subdivided into two classifications. The psychological condition of crime, sexual introduction, inherited data and personality data are also included in delicate information, which may also be referred to as forensic offices. We must ensure that sensitive data is not distributed to unapproved users, or that the data transmitted can not be comprehended by unapproved users, regardless of whether the information is blocked.

V. FORENSIC IOT CHALLENGES

IoT innovation has introduced a noteworthy move in the examination field; especially by the way it is associated with the information. Be that as it may, there are a few difficulties as far as Forensic IoT. Many IoT data is being distributed in different areas that are not managed by the user. Data Location Such data could be available in the cloud, on a laptop, or on a cell phone. This makes it one of the most difficult in IoT forensic to decommission the field of evidence and take account of the ultimate goal of collecting the proof. In addition, IoT information may be located in different countries and blended with various user data, which includes different nations ' controls . In August 2014, a Microsoft refused to follow the court order to seek information put away outside the United States (nation of warrant) putting forward the appeal for a long time . The case was exceptional. The lifetime expectative limit on digital media is limited and the data can easily be over-composed in view of the limitation of capacity on IoT phones. The probability of lack of evidence. In this way, the time of verification in IoT systems before it is overwritten is one of the difficulties. Exchanging information with something else could be an easy response to the test, for example the neighborhood Hub or the cloud. Another test shows in any case that has not been altered or updated by anchoring the proof chain and how to present the evidence . Most records are hidden users because cloud advantages do not allow the client to consent to their administration with exact information. A criminal could hardly be recognized . As example, given the discovery by agents in the cloud that a particular IoT system in a crime scene is shown to be the reason for the abuse, this finding does not indicate that the criminal could be identified quickly. Security requires evidence of the lack of safety on an IoT system could be altered or removed, so that the evidence is not sufficiently strong for admission to lawyers . For example, in the industry, a few organizations, when focused on another product, don't update their gadgets routinely or at least occasionally, stop supporting the framework of the gadget. Therefore, these devices could remain defenseless as the programmer discovered another weakness. Devices compose the specialized legal experts in the distinguishing proof era to identify a virtual scene of fraud and to receive evidence. Most of the data is a form of PC system such as a PC and mobile telephone. In IoT, however, artifacts like a shrewd cooler or genius espresso maker could be the origin of the verification. The examiners are going to face those obstacles in this way. The IoT-devices in the crime scene are one of these obstacles. It could be the gadget killed because the battery is weak, making it so alarming, particularly if the IoT device is small, in a closed location or looks like a traditional device. The device could be killed because It could be another challenge for the examiners to look to the device composing, to transport the device to the lab and to find a place. In addition, the elimination of the proof form of these devices is also seen as another IoT concern as most vendors are facing distinctive levels, operating frames and phones. The CCTV forensic , in which CCTV producers are organized into their devices to connect the distinctive document framework. It is still a challenge to legally retrieve curiosities from the storage devices of CCTV. We also seem to be working with a restrictive standardized document storage frame in order to reduce the erased image impression. The data created by IoT devices is not configured to co-ordinate with what is not spared in the cloud. In fact, the client does not have immediate access to his or her data in a system different from the information it is stored in. Data could also be prepared to make better use of diagnostic capacities. In light of this, the information framework should be returned to the first set up before investigation, taking into account the final objective which is to be recognized in the court of law

VI. ADVANCE DIGITAL FORENSIC APPROACH

An advance digital forensic approach has following four steps:



Step 1: Crime evidence source identification: In this step, the investigator identifies the source of crime and gather the information about the source of crime evidence.

Step 2: Evidence data collection: In this step, the investigator collects the possible evidence from the crime scene.

Step 3: Evidence of data examination: In this step, all the gather collected information is examined by the investigator using advanced forensic techniques.

Step 4: Crime evidence reporting: In this last step, crime evidence complete report is developed by the investigator.

• Types of Investigation: There are mainly three types of investigations based on the crime type. Public, private, and hybrid investigations.

1. Public: In the public investigation, various government or public agencies involved in crime investigation. The primary objective of the investigator for public investigation is to get the knowledge about the local area first then gather the evidence of public crimes such as murder, burglary or molestation by following all the cyber laws and legal procedures existing for the investigation area. In public investigation, we generally follow the following process:

Step 1: After registering a complaint seize the digital evidence.
Step 2: Launch the digital forensic investigations.
Step 3: Demonstrates the crime evidence report of digital forensic evidence gathered during a digital forensic investigation in court for prosecution.

2. Private: The private investigation includes private enterprises or civil breaches of the company. The principal purpose of the Private Investigator is to understand the business system in which private offenses such as e-mail bullying, data falsification, bias against sex and age, theft and the selling of client sensitive information should be kept minimally disrupted while investigation. (Fig. 7) We usually follow the following procedure in the private investigation:
Step 1: Electronic information is confiscated after a report has been registered by the management team.
Step 2: Start a digital forensic investigation to try and get disk images for forensic investigation of a suspect laptop or computer terminal.
Step 3: Demonstrate a crime investigation report with electronic forensic evidence for further intervention to the higher management team.

3. Hybrid: The hybrid investigation involves the combination of government or public agencies and private companies or organization's legal violations. The primary objective of the investigator for hybrid investigation is to understand that the local area information and the business process to make sure that there should be a minimal interruption during investigations of hybrid crimes. In the hybrid investigation, we generally follow the following process:
Step 1: After registering a complaint seize the digital evidence.
Step 2: Start the digital forensic investigation and try to acquire evidence for forensic investigation analysis.
Step 3: Demonstrates an investigation crime evidence report to the concerned authorities with digital forensic evidence for further actions.

VII. TOOLS AVAILABLE FOR DIGITAL FORENSIC

There are large numbers of tools available as an open source. A few tools are quite certain and center around one specific protest, though different apparatuses center around a substantially more extensive point of view. There is regularly a jump circumstance happening where another rendition of a specific device outperforms its rivals. A brief span later a contender may present another form and it turns into the pioneer until the following jump circumstance. Hence, we won't attempt to rank specific apparatuses and innovations or give nitty-gritty directions on the best way to play out a particular operation with a device. A portion of the prominent instruments are given beneath.

1. **Digital Forensic Framework** Another prominent stage dedicated to advanced forensic is the Digital Forensic Framework. This tool is open source and is licensed under the GPL. Either experts or non-specialists tend to make it useful without disadvantage. It appears to be useful for a computerized authorisation chain, to access remote or nearby computers, Windows or Linux OS crime scene surveys, lost documents recovery, fast meta-information data scans, and more.
2. **Open Computer Forensic Architecture** Another well-known open-source forensic P computer framework is Open Computer Forensic Architecture (OCFA). This system is based on Linux and uses PostgreSQL for information removal. It was developed for the mechanization of computerized legal research by the Dutch National Police Agency. The GPL permission is available for download.
3. **CAINE** is the Linux for advanced digital forensic (Computer Aided Forensic Framework). This offers a framework for quickly understanding the application of different programming tools as programming modules. It's an open source tool.
4. **EnCase** is another popular scientific stage in many areas of digital forensic with various playing tools.
5. **The Coroner's Toolkit** In addition, the Coroner's Toolkit or TCT is a good technical tool for forensic analysis. It continues to operate under some systems related to Unix. It can be used very well to investigate computer fiascos and recover data.
6. **Oxygen Forensic Suite** is a decent programming to gather proof from a mobile phone to encourage your case. This instrument helps in get-together gadget information (checking producer, OS, IMEI number, sequential number), contacts, (messages, SMS, MMS), re-upset deleted messages, call logs and date-book information. It also allows you to get to and research mobile phone data and records. It makes clear reports for a superior comprehension.

VIII. CONCLUSION

Digital forensic is an area of innovation containing various threats and winds. The doors open is limitless in the field of the prosecution of computerized crime, but are not out of the core for the poor. Bothering is a typical problem, therefore a skilled person should have the capacity and mentality to push through. IoT devices and their data security incidents have developed and developed and analyzed by IoT Forensic. their legal accumulation and analysis is required. Although the standards and procedures of IoT Forensic are not exactly the same as standard computer-based legal research, the methodology, strategies and learning of various work frameworks and documents are unique in their nature. The lawful acquisition and review of IoT gadgets is a key test due to the wide range of gadgets and their multi-faceted reliability. IoT Forensic is continually making strides to adapt to new types of equipment, data processing, and workflows.

IX . REFERENCES

[1] Watson, Steve, and Ali Dehghantanha. "Digital forensics: the missing piece of the internet of things promise." Computer Fraud & Security 2016, no. 6 (2016)
[2] Nieto, Ana, Ruben Rios, and Javier Lopez. "IoT-forensics meets privacy: towards cooperative digital investigation.
[3] A generic digital forensic investigation framework for internet of things.