DESIGN AND DEVELOPMENT OF INTERNET OF THINGS (IOT) TOWARDS DIGITAL FORENSIC INVESTIGATION

DIVYA PREMCHANDRAN

Research Scholar, Dept. of Computer Application,

Sri Satya Sai University of Technology & Medical Sciences,

Sehore, Bhopal-Indore Road, MadhyaPradesh, India

Dr. Jitendra Sheetlani

Research Guide, Dept. of Computer Application,

Sri Satya Sai University of Technology & Medical Sciences,

Sehore, Bhopal Indore Road,Madhya Pradesh, India

ABSTRACT

The Internet of Things (IoT) involves the rapid adoption of smart, adaptive and connected devices and is rapidly being deployed in critical infrastructure areas like heath, utility, homes, transportation and industries. It brings benefits and reliability to consumers, the haste and its large scale connection however poses serious risks to consumers. These risks include new attack vectors, new vulnerabilities and physical destruction through remote access. The IoT brings implications on cyber security as these devices are connected through the internet. Investigating digital crimes in the IoT domain using digital forensic technology is more challenging. Evidence extraction for forensic investigation is difficult since equipment could lose their data if left to operate for a long time; there is also the problem of jurisdictions. In this paper, we review literature related to forensics in the IoT and analyse the various models that have been proposed. The survey revealed the difficulty in digital evidence extraction in the IoT domain.

KEYWORDS: Forensics, Internet of Things, Evidence, Security, IoT forensics challenges, security and privacy challenges

INTRODUCTION

Today is the era of the Internet of Things (IoT). The recent advances in hardware and information technology have accelerated the deployment of billions of interconnected, smart and adaptive devices in critical infrastructures like health, transportation, environmental control, and home automation. Transferring data over a network without requiring any kind of human-to-computer or human-to-human interaction, brings reliability and convenience to consumers, but also opens a new world of opportunity for intruders, and introduces a whole set of unique and complicated questions to the field of Digital Forensics. Although IoT data could be a rich source of evidence,

forensics professionals cope with diverse problems, starting from the huge variety of IoT devices and non-standard formats, to the multitenant cloud infrastructure and the resulting multi-jurisdictional litigations. A further challenge is the end-to-end encryption which represents a trade-off between users' right to privacy and the success of the forensics investigation. Due to its volatile nature, digital evidence has to be acquired and analyzed using validated tools and techniques that ensure the maintenance of the Chain of Custody. Therefore, the purpose of this paper is to identify and discuss the main issues involved in the complex process of IoT-based investigations, particularly all legal, privacy and cloud security challenges. Furthermore, this work provides an overview of the past and current theoretical models in the digital forensics science. Special attention is paid to frameworks that aim to extract data in a privacy-preserving manner or secure the evidence integrity using decentralized block chain-based solutions. In addition, the present paper addresses the ongoing Forensics-as-aService (FaaS) paradigm, as well as some promising cross-cutting data reduction and forensics intelligence techniques. Finally, several other research trends and open issues are presented, with emphasis on the need for proactive Forensics Readiness strategies and generally agreed-upon standards.

The Internet of Things (IoT) is a well-known paradigm that defines a dynamic environment of interrelated computing devices with different components for seamless connectivity and data transfer. Technologies that are often implemented in the IoT domain are machine-to-machine communication (M2M), context-aware computing and radiofrequency identification (RFID). Some typical examples of such proactively sensing and adapting objects include: i) wearable devices like smart watches, glasses or health monitoring systems, ii) smart home appliances like smart locks, sensors for temperature, gas or ambient light, iii) smart vehicles, drones and applications for industrial automation and logistics. IoT devices exchange data with millions of other devices around the globe. Such type of open large-scale communication makes them especially inviting for users with illegal intentions. Only in 2017 there was 600 percent increase in attacks against IoT devices [1]. In many cases, the intruders are not directly targeting the IoT device, but using it as a weapon to attack other websites [2]. As a result, cybercrime has become the second most reported crime globally [3]. IoT systems seem to be easy targets for attackers, mostly due to the fact that when building an IoT device, manufacturers often place great emphasis on cost, size and usability, while security and forensics aspects tend to be neglected. Lally and Sgandurra [4] outline that some producers implement security practices mainly because an eventual exploitation of one of their IoT products will damage the company's image [4].

DIGITAL FORENSIC TOWARDS IOT

IoT forensics has been defined by (Zawoad and Hasan 2015) as one of the digital forensic branches where the main investigation process must suit with the IoT infrastructure. This is important in a way understand the system thoroughly and start to investigate the incident that IoT-related. As the rapid growth of this technology, the IoT forensic must be ready to face the new challenges, especially in the security perspectives. For example, in Europol's The Internet Organized Crime Threat Assessment (iOCTA) 2014, the first death case which is caused by the IoT has been reported. The adversary is expected exploiting the vulnerability of the devices and the

communication channel which initiate malicious instructions to endanger a patient's life. Therefore, the forensic investigation methodology is necessary to be execute in the IoT paradigm.

Digital Forensic Framework

Many digital forensic frameworks has been proposed previously. Most of the framework were developed for the conventional computing. However, none of them are readily and suit for the IoT context.From the table, we can conclude that identification, collection, preservation, examination and analysis is a necessary process in digital forensics procedure. However, these process need to be ready to cater for the Internet of Things characteristic and its environment. The classification of preinvestigation phase, investigation and postinvestigation are being considered based on the process involved in the framework from the previous work.

The Investigation Framework

Clearly, that there are six basic steps in the forensic investigation. The difference now is how to apply these processes according to IoT behaviour. The IoT devices produce a huge measure of information including the conceivable evidence where it will impact the investigation procedure as a whole. It's difficult to identify which device had involved in the incident and it will take more time to find which devices launch the attacks. All the important pieces of evidence need to be collect and preserve to determine the facts about the incident. Collecting and preserving the evidence is the most critical steps of the forensic procedure. Any error at this phase will affect the whole investigation process. In the current practices, the potential devices cannot be switched off in order to preserve the modified, created and accessed times of data. However, this kind of method may not applicable for the IoT devices. The IoT characteristics have made the situation become more complex. New approaches for collecting and preserving IoT evidence is require ensuring all the potential evidence is secure and genuine. The process of evidence extraction also might be complicated than the conventional computing as there are heterogeneous data formats, protocols, and physical interfaces involved. Sometimes the evidence can be partly stored in other devices that shared the same network or in the cloud services. Therefore, the investigator needs to consider to look at the larger dimension or many possibilities of data storage in order to get/extract data.

Diversity of Devices

In the IoT market nowadays, new IoT devices are being created and developed to make our life easier and trendy. Not only the manufacturer, the service provider also has come out with many offers and options to their customers. Technically, these devices are being operated by multiple operating systems and may connect to various network technologies at one time. The characteristic of interactivity and dynamicity makes the IoT become more complex and complicated. This situation may lead to many exploitation or manipulation by the adversary. From the forensic perspective, the up-to-update heterogeneous device, operating system, and communication channel may affect the investigation procedure. Currently, the investigator using dedicated tools either hardware-based or software- based to help the investigation. Typically these tools are created by version sometimes does not support the latest and the

oldest version of the technology in the market. Because of this lack, many attacks has been initiated on top of this problem. The investigator needs to have support tools that can adapt with the latest and the oldest technology.

THE INTERNET OF THINGS (IOT) AND ITS DIGITAL FORENSIC CHALLENGES

Figure 1 depicts an IoT enabled camera that has been mounted in the middle of a city to capture images on traffic situations. Data is transmitted to a central repository and city authorities monitor it for a quick response to restore traffic order where need be.

Figure 1 An IoT enabled camera to capture images in the centre of a city

The issue of security is becoming more crucial as IoT devices are becoming more relevant in people's lives. IoT devices may not be as secured as other traditional devices connected to the internet because of their sizes and restrictions on power, the increasing number of connected devices is bound to create challenges that are new and will thus require innovative security approaches [11]. From a legal point of view, there are legal issues associated with the IoT which are not clear and require interpretation, notable amongst them being the impact that location has on privacy regulation and issues associated with ownership of data in the cloud as the data on IoT is stored in the cloud [12]. Other challenges that could be associated with IoT devices include authentication, integrity, access control and confidentiality [11]. Physical threats like theft and tampering, logical threats like denial of service and viruses are threats that can be directed at IoT based devices [13]. As Data is kept on sites in the cloud, it is vulnerable to attacks such as SQL injection, side channel attacks and man in the middle attacks amongst others [14]. Standards and interoperability also pose a challenge [15], in establishing markets for technologies that are new, standards are very vital. Interoperability becomes difficult where different standards are used by different manufacturers of equipment, translating from one standard to another will require added gateways [2]. IoT devices could be hacked to steal data or alter data to the hacker's advantage. These security challenges must be addressed by using computer forensic technology to extract irrefutable evidence that can be relied upon to prosecute offenders in the law court.

Digital Forensics

The application of computer technology to the investigation of computer based crime has given rise to a new field of specialisation known as forensic computing and according to [16] it involves the identification, preservation,

analysis and presentation of computer based evidence in a way which is legally authentic for prosecution in a court of law. To extract data for crime analysis to identify who did what, with whom and at what time, computer forensics is conducted. Digital forensics legally is under the concept of e-discovery or electronic discovery which encompasses the processes involved in the gathering of data from electronic documents to prepare for presentation in a court of law for the trial of offenders [17]. Crime scene is where evidence is gathered and contains physical evidence such as computers, printers and handheld devices. Law suits can be won or lost by investigating the information found in these devices after they have been used to commit crime. Computer forensics involves the identification of digital evidence, its preservation, analysis of the evidence and its presentation in court. In conducting digital forensics, evidence must be managed in a way that meets stringent legal requirements for it to be accepted for tendering in court [16]. It must be proved that the evidence collected has not been tampered with. Specialised computer forensics software and its toolkits must be used in conformity with generally accepted methodologies and guidelines in investigating crimes committed using computers. Digital evidence by its nature is delicate and improper handling or improper examination can change or destroy it rendering it impossible for it to be tendered [18]. Further, digital evidence can easily loose its original form as it can be amended, utmost care must be taken in its collection, preservation and documentation. It is very important for computer forensics investigators to conduct their work properly as all of their actions are subjected to scrutiny by the judiciary should the case be presented in the law court [19]. In the estimation of [17], there are varied number of methodologies and tools that are available for investigations in digital forensics and in their estimation some of the reasons that influence the methodology and tools to be used include the device type, its operating system (OS), application software, type of hardware and legal jurisdictions. Computer forensics process involves seizure, preliminary analysis, investigation and analysis [20]. Tools used for computer forensics include EnCase, Forensic ToolKit, Paraben, FTK, Logicube, Oxygensoftware, Crownhill and InsideOut Forensics. A U.S. Department of Justice special report authored by [21] gave general forensic and procedural principles to be applied when dealing with digital evidence. The report contends that evidence reliability should not be compromised by actions that were taken during the collection and securing of the evidence. Well trained persons in digital forensic technology should be made to conduct examination of digital evidence. Finally, activities relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved and made available for review. In examining digital evidence, it will be better to do it on a copy of the original evidence so that one can revert to the original should the copy be faulty. Digital evidence can be altered or destroyed if not properly handled as it is very delicate.

CURRENT DIGITAL FORENSICS APPROACHES AND IDENTIFIED GAPS IN THE IOT

The nature of the processes involved in computer forensics is complex as it deals with irrefutable evidence and as a result a number of forensic models have been proposed. A comprehensive forensic model can provide a common reference framework for investigation. These models can support the development of tools, techniques, training

and the certification/accreditation of investigators and tools. The outcome of digital forensics investigation depends largely on the methodology adopted. Overlooking one step or interchanging any of the steps may lead to incomplete or inconclusive results, resulting in wrong interpretations and conclusions. IoT forensics shall include forensics in mobile devices, the cloud, computers, sensors and RFID technologies and many other areas [14]. In a traditional digital forensic landscape, evidence is got from computers, mobile phones, printing devices, websites and emails amongst others. These devices are still relevant in investigations relating to IoT devices. Amongst the industries to have adopted IoT are industries that are very vital in national security and national infrastructure. The United Kingdom for instance has implemented a modern system for flood defence that utilises sensors and satellites to enable them gather information to communicate warnings automatically and promptly. In conducting forensics in the IoT domain, forensics in the cloud will be relevant since data got from IoT devices will be increasingly stored on locations in the cloud. The IoT will generate enormous volume of data so the procedures that have been developed to deal with forensics in big data will still be applicable in the IoT. A lot of devices will be introduced from the implementation of the IoT, forensic investigators must be equipped to receive digital data from sources that are unfamiliar and diverse. The First Digital Forensics Research Conference (DFRW) made an initial effort at explaining the processes to follow in conducting digital forensics; they proposed a model known as the DFRW Investigative process (DIP) which in their estimation could be used in all digital forensic examinations. The model identifies a sequential process to follow in investigations which involves identifying, preserving, collecting, examining, analysing and presenting the evidence. Members at the conference unanimously agreed that the model was incomplete and there was the need to do more work on it. It however became bases for the development of subsequent models. Since it required further work, it has a narrow focus and cannot be applied to the IoT . The Forensics Automated Correlation Engine (FACE) presented by demonstrates completely automatic relationship of different sources of evidence. For the future they suggest there should be more work for an improved correlation, they suggest that rigorous logical methods should be employed. There should also be improved data visualisation as forensic data is large and standard means of data exchange is non-existent. In studying current forensic research directions argues that to move forward the digital forensic community needs to adopt standardised, modular approaches for data representation and forensic processing.

The size of devices used in data storage has grown exponentially, creating an image of these devices in contention and processing all their data takes a long time. Single devices were analysed in cases formerly, current cases are more sophisticated and therefore require that numerous devices should be analysed and the evidence found are linked. The scope of investigations in digital forensics is also restricted by legal tussles. Terrorists and other criminals use mobile phones in their operations, it is important that forensic investigators should retrieve data from these phones in a highly principled way. Procedures to retrieve data from these phones have not been standardised. Researchers do not have a logical method for reverse engineering even though a lot of resources have been spent in researching into it, forensic tools are not well automated and data cannot be exchanged. These drawbacks affecting traditional forensics will also affect forensics in IoT devices. In analysing new security threats and issues

related to privacy in the IoT domain there is an argument for attacks to be intercepted, data authenticated, access controlled and the privacy of customers guaranteed. This view holds for IoT smart energy devices as we are of the opinion that intercepting attacks as they occur will ensure that evidence acquired will be reliable and irrefutable. There is the need for a common legal framework to deal with items in different jurisdictions also. The model proposed results in forensic investigation taking a longer time to complete and so cannot produce effective and reliable results. Due to volatility this model cannot be applied in IoT forensics. There shall be two major challenges in order to guarantee seamless network access, the first issue relates to the fact that today different networks coexist and the second issues being the number of connected IoT devices. They further contend that the information technology landscape as it exists currently has little experience in implementing a system that connects to IP based networks with a huge number of objects. As a recommendation for future work, proposed for the development and implementation of a system that is proactive and reactive utilising domain-specific modelling language and code that is automated. They believe their proposed method will result in the creation of novel digital investigative tools and its associated techniques to optimise the capacity to foresee an attack proactively providing timely feedback. A range of forensic examination models on physical and digital evidence were surveyed, they introduced the term hybrid evidence to represent physical and digital evidence and proposed a model for its investigation. This model aims to separate the process of investigation to physical and digital crime scene. The problem with this approach is that the time needed to collect physical evidence could lead to loss of volatile data or other digital evidence related to the crime and so is not applicable to the IoT. In studying the research challenges in the IoT, argued that the development of concrete approaches for building privacy-preserving mechanisms for IoT applications still presents a number of challenging aspects. In the estimation of it is impossible sometimes to get access to items like pacifiers that are of forensic interest. The next best evidence source has to be identified and considered. They proposed a model known as the Next Best Triage (NBT), they however did not explain how to get this alternative evidence. There is the assumption that devices will continue to hold evidence for a long time which may not always be true in the IoT domain. In the estimation of there is the urgency to close the gap that exists between rates of processing and volume of data using effective techniques of data reductions.

CONCLUSION

From the literature surveyed, it is evident that IoT forensics is different from other forensics. Evidence must be produced timely and must be able to withstand rigorous cross examination in court. A significant number of literatures were reviewed for the purpose of finding gaps in current IoT Forensics. The review confirmed that none of the forensic models that have been proposed is able to extract evidence timely and reliably. From these studies it is amply clear that there is enough scope to continue research to investigate procedures that can be used for the detection and analysis of attacks in the IoT as soon as they occur.

REFERENCES

[1] ASHTON, K. (2009) That 'Internet of Things' Thing, RFiD Journal, 22 (), pp. 97–114.

[2] Davies, R (2015) The Internet of Things Opportunities and challenges, European Parliamentary Research Service, PE 557.012(), pp. [Online]. Available at:http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf(Accessed: 15th September 2015).

[3] Weiser, M (1991) The Computer for the 21st Century, Scientific American, 265, pp. [Online]. Available at:https://www.ics.uci.edu/~corps/phaseii/WeiserComputer21stCentury-SciAm.pdf (Accessed: 30th September 2015).

[4] Mattern, F., Floerkemeier, C. (2010) from the internet of computers to the internet of things, Springer-Verlag, pp. 242-259.

[5] Coughlin, T (2014) Digital Storage and The Internet Of Things, Available at:http://www.forbes.com/sites/tomcoughlin/2014/11/30/digital-storage-and-the-internetof-things/(Accessed: 25th September 2015).

[6] Weber, R.H. and Weber, R. (2010) Internet of Things: Legal Perspectives, Zurich: Springer.

[7] Dlamini, M., Eloff, M. and Eloff, J. (2009) Internet of things: emerging and future scenarios from an information security perspective, Southern Africa Telecommunication Networks and Applications Conference, pp. 6.

[8] International Telecommunication Union (ITU), (2005) International Telecommunication Union (ITU), Available at: http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf (Accessed: 5th September 2015).

[9] Hegarty, R.C. Lamb, D.J. and Attwood, A. (2014) Digital Evidence Challenges in the Internet of Things, International Workshop on Digital Forensics and Incident Analysis , pp. 163-172.

[10] Pereira, P., P.,Eliasson, J., Kyusakov, R., Delsing, J., Raayatinezhad, A. and Johansson, M. (2013) 'Enabling Cloud Connectivity for Mobile Internet of Things Applications',Proceedings of the 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, (), pp. 518-526.

[11] Fremantle, P. and Scott, P., 2015. A security survey of middleware for the Internet of Things.PeerJPrePrints, 3, p.e1241v1.

[12] Sen, J. (2013) Security and privacy issues in cloud computing, Architectures and Protocols for Secure Information Technology Infrastructures, pp. 1-45.

[13] Bos, H., Ioannidis, S., Jonsson, E., Kird, E. and Kruegel, C. (2009) Future Threats to Future Trust, Proceedings of the First International Conference Future of Trust in Computing Springer, pp. 49-54.

[14] Oriwoh, E., Jazani, D., Epiphaniou, G., Sant., P. (2013) Internet of Things Forensics: Challenges and Approaches, Proceedings of the 9th IEEE International Conference on Collaborative Computing:

[15] Kvochko, E., O'Halloran (2015) Industrial Internet of Things: unleashing the potential of connected products and services, Geneva: World Economic Forum.