A REVIEW OF DIGITAL FORENSIC CHALLENGES IN THE INTERNET OF THINGS (IOT)

Osman Yakubu
PhD Scholar, Faculty of Engineering,
M.S. Ramaiah University of Applied Sciences, Bangalore, India
Faculty of Applied Sciences, Garden City University College, Kumasi, Ghana

Narendra Babu C
Faculty of Engineering, M.S. Ramaiah University of Applied Sciences, Bangalore, India

Osei Adjei
Faculty of Applied Sciences, Garden City University College, Kumasi, Ghana

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 health, 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 includes 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, RFID

http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=9&IType=1
1. INTRODUCTION

In 1990 Kevin Ashton created the term the Internet of Things which is a worldwide dispersed network of objects that are able to connect amongst themselves and other computing devices [1, 2]. The objects are connected via the internet, they share data and are able to sense the environment. Critical areas like weather, security, homes, transportation and healthcare have seen an upsurge in the deployment of IoT enabled devices. Life is made smarter by IoT deployment ensuring that consumers derive highly efficient services from areas that deploy them. Cities, traffic, street lighting and public transport are made more efficient by using IoT devices [2]. Computing is made ubiquitous by the Internet of Things, a concept initially put forward by Mark Weiser in the early 1990s [3]. IoT can be embedded in devices such as thermostat which can be used to sense the weather and adjust temperatures automatically where necessary. An IoT enabled smart fridge can send an alert to its owner in case an essential item for the home like milk is low and needs to be replenished. Sensors and other communication components are currently cheaper and are becoming smaller in size consuming lesser energy and are embedded into objects for everyday use [4]. As these equipment are linked together, users can communicate with their environments utilising the smart things that they are carrying on themselves [5]. The architecture of the IoT is centred on tools for data communication such as items tagged with Radio-Frequency Identification (RFID) [6].

The virtual and physical worlds are connected together by RFID tags [7] and by adding RFID tags to everything, the RFID technology will create an IoT [8]. The storage of data by IoT devices could be local or may be stored by being transferred to another IoT based device, the data could equally be sent to the cloud [9] for processing and storage [10]. The years ahead is expected to witness a boom in IoT growth, a view that is supported by [2]. Gartner Group is cited by [2] to have reported that by the year 2020 devices totalling 26 billion shall be connected to the IoT, a revenue exceeding US$ 300 billion shall also be generated. Further, there will be value addition generated through sales totalling about US$ 1.9 trillion. Notwithstanding the enormous benefits to be accrued from the deployment of IoT enabled devices, it has security challenges which needs to be addressed. They are susceptible to hacks by malicious persons, and perpetrators must be brought to book.

However, evidence acquisition is very difficult as a sizable number of literature perused could not prescribe a comprehensive model that ensures the timely acquisition and reliability of evidence which is very critical for prosecution.

2. 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.
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.

2.1. 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 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, Oxygen
software, 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.

2.2. A Survey of Current Digital Forensics Approaches and Identified Gaps in 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 [22]. 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 [23]. 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 [24]. 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 [25]. 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 [26]. 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 [26]. The Forensics Automated Correlation Engine (FACE) presented by [27] 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, a view shared by [28]. In studying current forensic research directions [28] argues that to move forward the digital forensic community needs to adopt standardised, modular approaches for data representation and forensic processing.
A Review of Digital Forensic Challenges in the Internet of things (IOT)

The size of devices used in data storage have 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 [28]. 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 [29]. 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 by [30] 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 [31]. 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, [32] 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 by [33], 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, [34] 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 [35] 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 [36] there is the urgency to close the gap that exists between rates of processing and volume of data using effective techniques of data reductions.

They further contend that this is done currently on ad-hoc bases using manual techniques that cannot be sustained since the experience of the investigator is what determines the accuracy of the results. An improved forensic examination is suggested by [37] in Wide Area Networks (WANs) where investigators search through large volumes of data which includes data from logging mechanisms that are unreliable possibly with evidence that is missing. The model proposed by [37] gives users who are malicious the chance of tampering with vital evidence. Their model does not automate the process of extracting and analysing evidence.
which will be useful in the IoT. In the estimation of [38] there should be proactive measures to deal with the upsurge in ID theft due to current innovations in technology, this proposal we posit is applicable to forensics in the IoT. The current advancement in technology in the area of cloud, social media and the global usage of mobile technologies have increased the potential of cybercrime, there is therefore the need to consider improving the tools and procedures that can be used in forensic examination. The extended abstract digital forensics model with preservation and protection as umbrella principles were proposed by [40], the model is deficient in protecting privacy and preserving the integrity of digital evidence. Smart TVs which can be part of the IoT sphere have not been factored as capable of being vulnerable to abuse by the owner or being attacked through a network and how the evidence should be extracted [41]. They contend further that devices may lose information when they are switched off so they proposed the consideration of live analysis options. An argument for smart forensics for the smart home was put forward by [42] as extensive research has not yet uncovered a forensics model which takes into account the properties of the smart home as dynamic, largely automated and self-managed. They concede that the proposed model has not been tested or validated within an IoT-based environment with its peculiar characteristics. When a crime is committed the delay between its detection, reporting, arrival of the incidence response team, and commencement of the investigation, may prove too lengthy for any investigation to find any useful evidence, vital evidence may thus be lost.

Forensics in the IoT is classified by [43] as a blend of forensics at the device level, network forensics and forensics in the cloud. They also argue that current forensics tools and its associated techniques are inadequate to deal with IoT infrastructure. A forensic-aware IoT (FAIoT) model which they believed could support trusted forensics investigations in the IoT domain was proposed by them. The drawback of the FAIoT is that it was never implemented in any IoT environment and cannot be verified to be feasible. They propose that the individual IoT application or the IoT infrastructure (e.g., the utility capability) must enforce privacy but they did not explain how that should be done. The connection of billions of IoT enabled devices is expected to produce data in large volumes. Getting evidence to tender in a criminal case becomes challenging when evidence has to be extracted from a large pool of data. IoT equipment are constrained by storage, a lot of the data that IoT devices produce will be kept in the cloud. One of the evidence sources will thus be the cloud so difficulties affecting evidence acquisition in the cloud will also affect forensics in the IoT. The literature reviewed confirms that there is digital evidence challenge in the IoT domain.

3. 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

A Review of Digital Forensic Challenges in the Internet of Things (IOT)


[45] Mr. N. Sampathraja, Dr. L. Ashok Kumar, Mr. K. Vishnu Murthy, Ms. V. Kirubalakshmi and Ms. C. Muthumaniyarasi, Iot Based Underground Cable Fault Detector, International Journal of Mechanical Engineering and Technology 8(8), 2017, pp. 1299–1309.