Volume 7 Issue 4 (2019) 298-300 ISSN 2347 - 3258
International Journal of Advance Research and Innovation

Novel Perspectives in Forensics Aware Internet of Things

Manas Kumar Yogi, A Srihitha
Department oif Computer Sicence and Engineering, Pragati Engineering College (A), Surampalem, Andhra Pradesh, India

Article Info
Article history:
Received 25 January 2016
Received in revised form
20 February 2016
Accepted 28 February 2016
Available online 15 March 2016

Keywords
IoT, Digital Forensics, Forensics-Aware, IoT Forensics, Digital Forensics Model

Abstract
The Internet of Things involves connecting various things with several communication standards and technologies. While Internet of Things opens accessible opportunities in many fields, it announces new threats in the sphere of forensics investigations. The present day procedures and forensic tools cannot fit the widely distributed infrastructure of the IoT. Forensics investigators will experience threats determining, analyzing and collecting that evidence. This paper comes with the working solution of IoT forensics and consistently evaluates the IoT forensics area to examine the threats and issues in this peculiar field of forensics. We recommend a Forensics-aware IoT (FAIoT) model for approving reliable forensics investigations in the IoT environment.

1. Introduction

The Computer forensics is an uninterrupted evolution. This discipline is adapting its approach, tools and methodologies to cover-up advanced contexts. IoT Forensics is the term to describe a modern branch of forensics devoted to the precise features of investigations in Internet of Things scenarios and its requirements. The adaptation of forensics to consider IoT scenarios is indispensable due to numerous characteristics making forensic analysis in the IoT differentiating from other contexts or paradigms. Actual forensic branches cannot be enforced to the requirements imposed by the IoT, namely: • Increase in numerous devices • Huge development of proprietary protocols • bulk of data, making the identification of particular data complex • Urge for advanced formats to supply evidence in IoT devices • Presence of numerous resource-constrained devices.

These threats results in a consequential effort being made towards the definition and implementation of forensic solutions in the context of IoT paradigm. Despite these efforts, forensics solutions have so far ignored the urge for securing individual privacy throughout investigations. This is true even though devices are known to be capable of collecting and storing large amounts of personal information as they are parts of our lives [1]. Not only are smart-phones utilized and deployed among individuals but also wearable's, smart gadgets, and numerous sorts of context-aware devices.

Forensic mechanisms and tools, similar to those utilized for the seizure of evidence at a crime scene, are prepared for static contexts, in which the voluntary participation of citizens is not required. In such scenarios, the conception of witness is applied to individuals, not to devices, or tools. In scenarios, similar to those envisioned by the IoT, the recovery of evidence is complex and it may be important for the investigator to get help from citizens and devices.

Without a cooperative approach it is complex to understand the whole context, since the information can be distributed and volatile information could otherwise be lost. This is where the conception of digital witness comes into play. Understanding the conceptual background of IoT, evidence and digital forensic are essentially important for conducting a proper investigation and comes-up with a proposal for enhancing the current research milestones in the field of IoT forensic.

1.1 IoT

Conceptual Consideration While the conception of IoT is not relatively very new, its targeted realization and implementation are yet to be done. It is claimed by different references that the term Internet of Things was initially coined by the director of ID-Auto Labs at MIT - Kevin Ashton in 1999[2]. The main concept of IoT is creating an overwhelming "things" with interoperability and communication ability via different suitable protocols such as Radio-Frequency Identification (RFID), Internet and Bluetooth.

This kind of scenario is useful for various applications like smart cities, telemedicine, smart grids, intelligent vehicles and many other applications. Having explained the conception of IoT, it is important to elaborate on the issue of evidence acquisition from IoT. In general cases, the consideration of evidence starts by identifying the crime scene and any directly connected devices to the crime scene.

In IoT, the issue is complex due to sophisticated inter-connectivity where it may seem difficult to reach the exact thing and in worse cases, it may be mistakenly considered. This leads to a numerous ramifications including delaying digital forensic process, misleading the investigation process, further developing the security risks by invading connected surrounding things and finally complicating forensic investigation process by adding a massive amount of exchanged data owing to dense inter-connectivity [3].

1.2 DIGITAL EVIDENCE

Digital evidence can be explained as any intended or unintended trace generated by an electronic device due to digital data movement. We use various electronic devices to approach the needed resources and conduct online and offline transactions every day. The idea is all these activities create a trail ranges from log files and browsing history to data movements such as digital files, online transactions and social media activities.

The created evidence may sound unworthy to Internet users and average electronic devices, yet evidence is complex than its counterpart generated from the current cyberspace. The bulk of data can be exchanged between things in IoT, numerous things are available at the crime scene, the second and third connectivity levels and interoperability of things do create a threat for forensic investigators in terms of identifying relative things in IoT, applicable digital forensic techniques and processing time [4].

The challenge may get more complicated here if the thing is implanted and cannot be seized or disposed of and cannot be retrieved for conducting the forensic analysis. Digital Forensic Digital forensic is characterized by the application of forensic science disciplines to electronic-based crime scenes followed by certain legal approaches [5].

The application of forensic goes back in time for multiple decades where it was originally restricted to computer crimes as the cyberspace had not gained its current popularity back then. The tenets of forensic are usually followed as a fundamental procedure of identifying related electronic devices, acquiring evidence in a verifiable manner, analyzing and preserving the acquired digital evidence, and finally presenting the evidence in a readable and organized format to be admissible before law.

The challenge here is applying this standard digital forensic procedure to IoT network where a blend of actuators, sensors, smart phones, embedded computing devices etc. are all interlinked to bulk of data exchanged between them. The issue begins with identifying

Corresponding Author,
E-mail address:

which objects "things" to include while seizing the devices, taking into the account the possibility of an implanted chip for telemedicine purposes.

The next problem is faced if the things are identified and seized, then tracing back the applicable digital forensic procedure considering the possible number of things and the connectivity level. This problem will be further developed considering the possible digital evidence retrieving and tools [6].

2. Challenges in IoT forensics

Crime involving digital technologies is already on high. The emergence of speedy paced Io T transmits data across protected systems.

Most of these devices include some form of cloud service and access through mobile applications. Ten among the popular devices analyzed includes the smart TV, webcam, remote power outlet, door lock, garage remote and hub for managing many devices.

This realizes the basic requirement for seamless digital forensic processes to be in place to trace footprints of perpetrators when the attacks are made. Digital forensics is managed differently that depends on case scenario, organizations, event and type of the system involved. However, the basic objective of any forensic investigation is to acquire evidence which can be utilized in obtaining of an activity in the case under investigation.

There are many digital forensics processes when sequentially applied deliver relative outcomes. The nature of devices in IoT identifying the source of information is a difficult task different from the traditional devices like servers, computers or networks which contain some storage mediums like compact disks, hard disks, flash or thumb drives. In some cases data might not be stored on the device instead it is on a connected service which can be a cloud based system.

After determining source of data, the acquisition type is identified which is normally physical, logical or live acquisition. There are several tools available to help with the evaluation like FT K, En-Case, Os Forensics, Autopsy, Pro Discover [7]. Analyzation is the key component of forensic investigation helps in finding interprets which may lead to a particular conclusion. This step includes clear identification of places, persons, events, and items associated with a specific case. This also includes correlation to various data.

The final phase of the forensics process is reporting where results obtained from the analysis are presented. Sometimes reports may be inclusive. In situations where events have multiple outcomes, each should be explained using a methodological approach which was adopted to reach the outcome [8].

The 10 among popular IoT applications reported by IoT Analytics ranked in popularity from high to low are: Smart Home , Smart City smart grid Industrial Internet Connected Car Connected Health Smart Retail Smart Supply-Chain Smart Farming For the intention of conception our developed system we include the top two applications: Smart Homes, and Smart-City.

3. Forensic Aware IOT and Opportunities

3.1 Smart Home

Using this technology makes our life easy seems to be the force behind the popularity of Smart-Home IoT application. Smart home applications include quality of air, temperature control, and smart meter to audit power and water consumptions, smoke or gas leakage detection. Consider an example of one application Nest Smart Thermostat [9].

Nest Smart model introduced is of third generation which has enhances the learning capacity to learn family's everyday schedule and adjust the temperatures according to usage varying by area of the house used, number of persons and the temperature level needed in the house. This makes the use of energy consumption efficient and helps in saving the energy bills.

Accompanied mobile application can be used to audit and change the schedule remotely and generate alerts when something goes wrong. Nest Smart contains humidity, temperature and ambient light sensors. Nest Smart works with Wi-Fi connection 802.11b/g/n at 2.4GHz or GHz, 802.15.4 at 2.4GHz, and Bluetooth Low Energy.

3.2 Smart City

As an example for Smart City applications here Intelligent Traffic Management System is considered which is modeled to enhance traffic flow with smart traffic technology using machine-to-machine learning to help drivers decide the efficient route.

The model helps in avoiding traffic stops and roads with congestion and contributes best, real-time, optimizes the overall flow of traffic. Given the short range network within the vehicle and need for long range communication in vehicle-to-vehicle and vehicle-to-infrastructure, various Vehicular Area Networks (VANETs) communication protocols are used.

4. Current Developments to Tackle Iot Forensics Challenge

Many researchers have paid attention to the challenge of conducting IoT forensic. In this regard, Hegarty et al [7], analyzed in their study the challenges face forensics in IoT with the main focus on digital evidence as a key point. In their study, they discussed and displayed the consequence of chain connections and proposed the deployment of Building Information Modeling and the use of cloud-computing investigation to enhance the investigation purposes.

Although the examination presents a general review of mostly quoted ideas and solutions including their own proposed system, it does not send any possible implementation nor does it provide any framework for further implementation. Similar to, Mascarnes et al. addressed a fundamental key point in digital forensic, namely the convenience and time needed for extracting the digital evidence.

In their work, they developed a semantic approach to search through text-oriented digital evidence to sort and search based on certain keywords. The main limitation here is that the approach is applicable only to text-based digital evidence which is seldom to be the case, especially in IoT. Vlachopoulos et al.[10] addressed the similar issue but from a different perspective.

The main idea of their work is derived from a hybrid evidence investigation that simultaneously associates both digital and physical evidence from the crime scene to increase verifiability. Connecting both digital and physical evidence from the crime scene could much improve the outcomes of forensic investigation yet the legal aspect should be precisely tackled with the real experimental testing results aiming to prove the usability of the proposed model.

Besides the digital evidence-based studies, a forensic modeling attempt was displayed in the work of Sanderson et al [5]. Where the authors proposed a model for forensic based on sub-dividing IoT to a numerous zones and included in their model some concepts for base device identification, location finder represented by zones, and triage examination to deal with definitive digital evidence wherever it resides within the zone.

The work forms a serious attempt towards solving IoT forensic modeling, yet it doesn't provide an accurate solution nor does it provide any implementation for the proposed model. The conception of subdividing IoT for forensic applicability was also used by Oriwoh et al [10], where the authors added a new concept to the work of Sanderson et al., which is employing Next Best Thing (NBT).

NBT in their work was proposed to overcome the assumption of the thing's failure or disposal by replacing the thing of interest by NBT. Similarly, Zawoad and Hassan [12] approached IoT forensic by employing a secure centralized trusted repository to overcome the lack of standardizations between IoT entities. This repository is expected to contribute a forensic awareness for modeling IoT forensic and securing the chain of custody which is needed in digital forensic investigation.

Also there were proposals addressing the issues related IoT forensic modeling challenges. For instance, Conroy investigated several challenges related to forensic in large scale systems which implicitly include IoT. Some contemporary and speculated digital forensic challenges were also presented in the work of Lillis et al [11].

Where the focus was directed towards forensic investigators consider the expand in evidence in near future. Mostly the area of IoT forensic process is still premature and up to the authors' knowledge, very few research attempts that are conducted and reported in this field. The prominent majority of the conducted

researches lack the proper experimental results owing to unavailability of testing data and/or environment [13].

While the minimum of them are experimentally tested models, is very specialized and cannot be generalized for a comprehensive IoT forensic investigation model challenges.

5. Conclusions

Internet of Things is expanding the capability of internet with hundreds, if not thousands, of things being added each day. In addition to increase in capability has raised concerns about the security of things, the networks and applications adopting the IoT.

One of the major threats is the nature of things which bring inherent security weaknesses hence making them vulnerable to attacks. This has inspired the requirement for unique digital forensics measures which can address the examination, collection, analysis and reports of evidence in application-specific IoT Systems. This paper addresses the need and introduces an application definite forensics investigation model by pointing out the types of artifacts which would be of forensics importance in forensics. We have presented a holistic forensics approach which encompasses existing best practices in digital forensics industry and unique application definitive model to deal with the range of evidence of forensics value in differentiating IoT systems. This paper sets a scene for implementation of application-specific forensics processes, guidelines and tools which would be favorable in corporate high-tech investigations and law enforcement agencies to deal with IoT forensics challenges. As future directions of our research we plan to develop tools to extract data from things and have an applied approach of our developed model. Furthermore, we will also scrutinize the IoT security protocols which are applicable in conjunction with our model to have both strengthened security and efficient digital forensics methods in IoT systems.

References

[1]. ZA Baig, et al. Future challenges for smart cities, Cyber-security and digital forensics, Digital Investigation, volume 22, 2017, 3-13.

[2]. R Adams, V Hobbs, G Mann. The advanced data acquisition model (ADAM), a process model for digital forensic practice. Journal of Digital Forensics, Security and Law, 8(4), 2014, 25–48.

[3]. A Botta, W Donato, V Perisco et al. On the Integration of Cloud Computing and Internet of Things, in International Conference on Future Internet of Things and Cloud (FiCloud), 2014, 23-30.

[4]. U Salama, Smart Forensics for the Internet of Things (IoT), Security Intelligence IBM, 3, 2017.

[5]. T Baker, M Mackay, A Shaheed, B Aldawsari, Security-oriente Cloud Platform for SOA-based Scada, in the proceeding of the 15th IEEE/ACM international conference on Cluster, Cloud and Grid Computing (CCGrid), 2015.

[6]. A Mylonas, V Meletiadis, L Mitrou, D Gritzalis, Smartphone sensor data as digital evidence. Comput. Secur. 38, 2013, 51–75.

[7]. J Grover, Android forensics: Automated data collection and reporting from a mobile device. Digit. Investig. 10, 2013, S12–S20.

[8]. JM De Fuentes, L González-Manzano, AI Gonzalez-Tablas, J Blasco, WEVAN—A mechanism for evidence creation and verification in VANETs. J. Syst. Architecture 59, 2013, 985–995.

[9]. C Moore, M O'Neill, E O'Sullivan, Y Doröz, B Sunar, Practical homomorphic encryption, A survey in Proceedings of the 2014 IEEE International Symposium on Circuits and Systems (ISCAS), Melbourne, VIC, Australia, 6, 2014, 2792–2795.

[10]. W Liu, M Yu, .AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments. IEEE Trans. Veh. Technol. 63, 2014, 4585–4593.

[11]. A Kosba, A Miller, E Shi, Z Wen, Papamanthou, C Hawk, The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 5, 2016, 839–858.

[12]. NP Karvelas, A Kiayias. Efficient Proofs of Secure Erasure, In Proceedings of the International Conference on Security and Cryptography for Networks (SCN 2014), Amalfi, Italy, 9, 2014, 520–537.

[13]. S Peng, S Yu, A Yang. Smartphone malware and its propagation modeling: A survey. IEEE Commun. Surv. Tutor. 16, 2014, 925–941.