A Holistic Forensic Model for the Internet of Things

Lakshminarayana Sadineni, Emmanuel Pilli, Ramesh Babu Battula

Chapter 1

A HOLISTIC FORENSIC MODEL FOR THE INTERNET OF THINGS

Lakshminarayana Sadineni, Emmanuel Pilli and Ramesh Babu Battula

Abstract The explosive growth of the Internet of Things offers numerous innovative applications such as smart homes, e-healthcare, smart surveillance, smart industries, smart cities and smart grids. However, this has significantly increased the threat of attacks that exploit the vulnerable surfaces of Internet of Things devices. It is, therefore, immensely important to develop security solutions for protecting vulnerable devices and digital forensic models for recovering evidence of suspected attacks. Digital forensic solutions typically target specific application domains such as smart wearables, smart surveillance systems and smart homes. What is needed is a holistic approach that covers the diverse application domains, eliminating the overhead of employing *ad hoc* models.

This chapter presents a holistic forensic model for the Internet of Things that is based on the ISO/IEC 27043 international standard. The model has three phases – forensic readiness (proactive), forensic initialization (incident) and forensic investigation (reactive) – that cover the entire lifecycle of Internet of Things forensics. The holistic model, which provides a customizable and configurable environment that supports diverse Internet of Things applications, can be enhanced to create a comprehensive framework.

Keywords: Internet of Things forensics, holistic forensic model, forensic readiness

1. Introduction

The Internet of Things (IoT) is a global infrastructure that enables advanced services by interconnecting (physical and virtual) objects based on existing, evolving and interoperable information and communications technologies [14]. The Internet of Things connects electronic, electrical and non-electrical objects to provide seamless communications and contextual services [17]. The explosive growth of Internet of Things devices,

and the nature of services they provide and data they generate have contributed to an increase in security and privacy breaches as well as other abuses [1, 8]. The need to investigate these incidents has led to the new discipline of Internet of Things forensics, which focuses on the identification, collection, organization and presentation of evidence related to incidents in Internet of Things infrastructures [23].

This chapter presents a holistic forensic model for Internet of Things environments that is based on the ISO/IEC 27043 international standard. The forensic model has three phases, forensic readiness (proactive component), forensic initialization (incident component) and forensic investigation (reactive component). These three phases cover the entire lifecycle of Internet of Things forensics. This chapter also discusses the challenges involved in implementing the forensic model, along with feasible approaches and supporting technologies. The holistic model, which provides a customizable and configurable environment that supports diverse Internet of Things applications, can be enhanced to create a comprehensive framework.

2. Related Work

The Internet of Things stretches over several layers comprising heterogeneous devices, interconnected networks and diverse communications protocols and applications. Figure 1 shows a typical Internet of Things layered architecture. The three layers – things layer, edge layer and applications layer – are physically and logically divided according to their functionalities. Ideally, the things and edge layers are part of same network and are physically close to each other. As a result, most Internet of Things forensic approaches consider these two layers; the applications layer is left to cloud forensics [15].

Although much research has focused on computer forensics, network forensics and cloud forensics, limited work has been done in the area of Internet of Things forensics. The main reasons are the heterogeneity of devices, and diverse communications protocols and applications domains. These make it very difficult to identify common attack surfaces and create generic security and forensic solutions.

Nevertheless, several researchers have proposed models or frameworks for security analyses and forensic investigations in Internet of Things environments. Oriwoh and Sant [18] have proposed a model for automating security and forensic services that exclusively targets smart home environments. The layered model has four stages. In stage 1, services such as network traffic monitoring, intrusion detection, data collection, parsing, compression and analysis are configured. Stage 2 automates

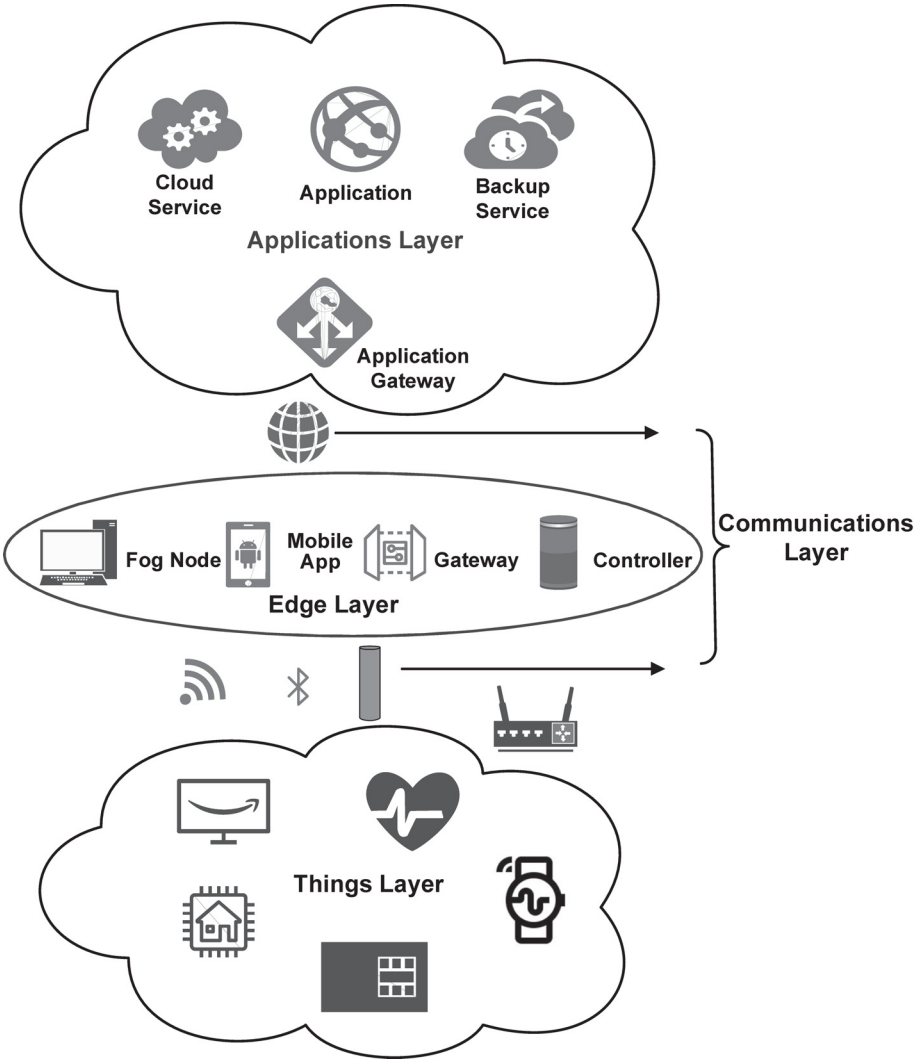

Figure 1. Internet of Things layered architecture.

the configured services to detect incidents and report them to users. In stage 3, users respond to incidents and escalate them to forensic investigators. In stage 4, digital forensic investigators reconstruct the incidents for potential legal action.

Zawoad and Hasan [23] have proposed a forensics-aware model for supporting reliable investigations in Internet of Things environments. Internet of Things forensics has three layers – device level forensics, network

level forensics and cloud level forensics. A secure evidence preservation module monitors registered devices to collect evidence such as network logs, registry logs and sensor readings, and stores them securely in an evidence repository. Hybrid (asymmetric-symmetric) encryption is employed to protect the evidence, making it accessible only to authorized investigators. A secure provenance module ensures chain of custody by preserving the evidence access history. Law enforcement agency personnel may access the preserved evidence and provenance information via secure read-only APIs.

Kebande and Ray [15] have proposed a generic digital forensic investigation framework for Internet of Things infrastructures. The framework, which maps existing digital forensic techniques to Internet of Things infrastructures, comprises three main processes – the proactive process, the Internet of Things forensic process and the reactive process. Other concurrent processes run alongside the three main processes. The proactive process, which is similar to the process defined by the ISO/IEC 27043 international standard, includes scenario definition, evidence source identification, planning incident detection, evidence collection and evidence storage and preservation. The Internet of Things forensic process includes cloud forensics, network forensics and device forensics. The reactive process covers initialization, the acquisition process and the investigation process. The high-level model is holistic and applicable to all Internet of Things environments, but it lacks low-level details that enable it to be customized to specific environments while leaving all the processes unchanged.

Meffert et al. [16] have proposed a framework and practical approach for Internet of Things forensics through device state acquisition. The proposed approach is based on collecting device state information using a dedicated controller to obtain a clear picture of the events that have occurred. The controller is operated in three modes – device controller, cloud controller and controller controller. The controller acquires state information directly from devices, the cloud and controllers using their respective modes. While the framework can reliably collect state data in Internet of Things environments using the three modes, its limitations include accessing historical and deleted data, physical access requirements and inability to connect to new devices.

Zia et al. [24] have proposed an application-specific investigative model for Internet of Things environments. The model comprises three independent components – application-specific forensics, digital forensics and forensic process. It is conceptualized based on three key Internet of Things applications – smart homes, wearables and smart cities. The

sources of forensic artifacts in the forensic readiness model are smart homes, wearables, smart cities, networks and the cloud.

Shin et al. [20] focus on the reactive process that occurs after an incident has occurred. They applied various digital forensic methods to collect data from an Internet of Things device (Amazon Echo) and network (home area network using the Z-Wave protocol). However, their approach is limited to selected devices and communications protocols.

Babun et al. [5] have proposed a digital forensic framework for smart environments such as smart homes and smart offices, where applications installed on smart devices are used to control sensors and actuators in the environments. The framework has two components – modifier and analyzer. The modifier examines the source code of smart applications at compile time to detect forensically-relevant data and insert tracing logs in the appropriate places. The analyzer uses data processing and machine learning techniques to extract forensic data related to device activity in the event of an incident.

Harbawi and Varol [11] have proposed an improved digital evidence acquisition model for Internet of Things forensics. They highlight the need to identify things of interest that produce initial evidence traces. Perumal et al. [19] have proposed a four-tiered digital forensic investigation model for the Internet of Things. Their model covers the entire investigative lifecycle starting from the authorization of forensic experts in a case to the archival of evidence after the case is closed.

Unfortunately, the forensic models discussed above fail to provide low-level details on how they can be customized to specific application scenarios. In contrast, the model proposed in this chapter engages a holistic approach that emphasizes configurable forensic readiness that is applicable to any Internet of Things domain.

3. Proposed Holistic Forensic Model

The proposed holistic forensic model for the Internet of Things is based on the ISO/IEC 27043 international standard [13]. The standard describes digital forensics as comprising several processes, each incorporating one or more activities. ISO/IEC 27043 processes correspond to phases in the proposed model and activities correspond to modules.

Figure 2 presents the holistic forensic model. The model has three phases: (i) forensic readiness (proactive) phase; (ii) forensic initialization (incident) phase; and (iii) forensic investigation (reactive) phase. Each phase has a number of component modules. Although all the modules focus on Internet of Things devices, their approaches can be mapped to the applications layer if needed.

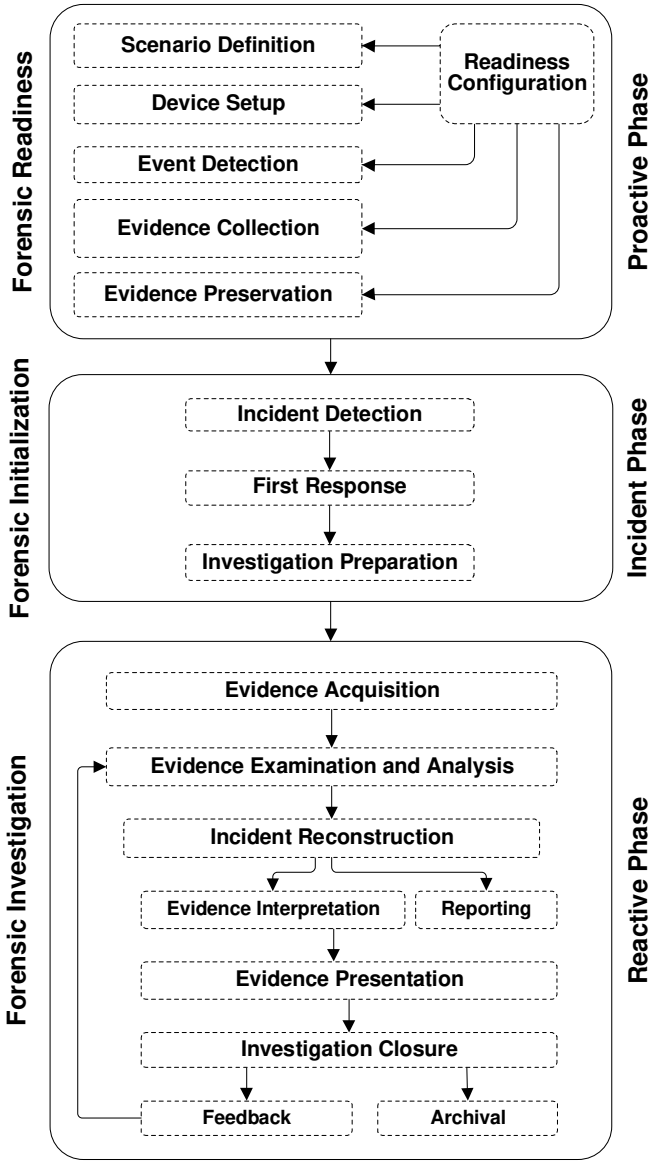

Figure 2. Holistic forensic model for the Internet of Things.

3.1 Forensic Readiness (Proactive) Phase

During the forensic readiness (proactive) phase, digital evidence related to an Internet of Things environment is collected and preserved.

This reduces the time, effort and cost involved in investigating subsequent incidents.

The forensic readiness phase has six modules.

- **Module 1.1 (Readiness Configuration):** This module coordinates all the forensic readiness activities. It provides configurable services to customize the model to different Internet of Things environments, rendering the model holistic. The configuration is performed by administrators and/or security experts to create application-specific, device-specific and context-aware directions for event detection, forensic data collection and preservation.

  The readiness configuration module has the following basic functionality:

  - Provides a mechanism for adding comprehensive information about Internet of Things devices in an environment (e.g., adding information about the smart devices in a smart home). The information about each device includes the device name, device manufacturer, device type, device id, firmware details, device functionality, interactions to be logged (based on defined scenarios) and device description.
  - Guides the device setup module in identifying suitable properties and configuring each device for evidence collection.
  - Guides the event detection module in identifying the specific events that must be logged.
  - Guides the evidence collection module on the data pertaining to specific events that needs to be collected.
  - Guides the evidence preservation module on how the collected data is formatted and stored for future investigations.

  It is important to note the difference between an event and an incident. An event denotes one or more interactions with Internet of Things devices that can change their states (e.g., changes in the sensor readings of a smart watch and a sensor data request sent from a mobile application to a smart watch); an event need not be suspicious. In contrast, an incident is a sequence of suspicious events that disrupts the regular functioning of Internet devices; an incident impacts security and/or privacy.

- **Module 1.2 (Scenario Definition):** This module defines scenarios as sequences of events that are forensically sensitive to specific Internet of Things applications (e.g., unusual interactions with a

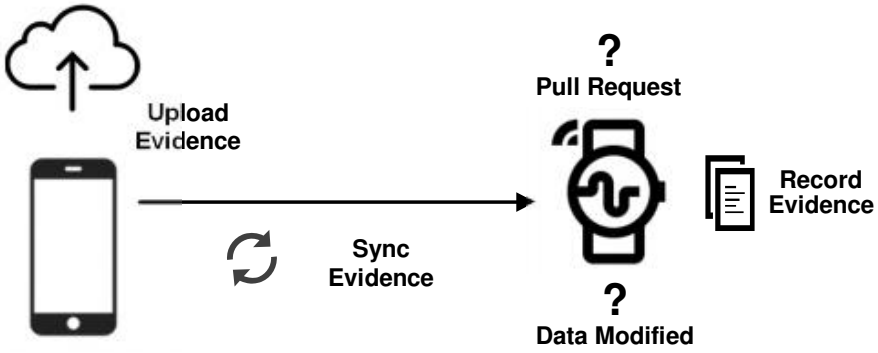

Figure 3. Example event in a smart watch scenario.

device and failed authorization attempts when accessing a service). In the applications layer, scenarios are defined to cover how configuration and business data should be managed (e.g., who can access or modify the data). Each scenario specifies events that change the states of Internet of Things devices. The state changes are identified along with the properties of the associated devices.

- **Module 1.3 (Device Setup):** This module identifies each new device added to the environment and its forensic properties before the device becomes operational. It consults the readiness configuration module for device-specific settings and stores all the setup information in a secure database for use by other modules. Also, it keeps track of when a device is detached from the environment.

- **Module 1.4 (Event Detection):** This module identifies forensically-sensitive events based on scenarios defined in the scenario definition module. Rules may be specified for validating device interactions and network traffic, and identifying potential events. In the applications layer, an autonomous module may be designed to monitor the security aspects of system configurations and requests for authentication and data access.

  Figure 3 presents an example event in a smart watch scenario. When sensor data is updated or a pull request is sent from a mobile application to the smart watch, the associated data is recorded as potential evidence. The data is periodically synchronized with a mobile application and may be uploaded to cloud storage for subsequent processing.

- **Module 1.5 (Evidence Collection):** This module covers the collection of potential evidence from Internet of Things devices, controllers and network devices. An example is logging the commands issued to an Internet of Things device along with their timestamps. The sources of commands to the devices are recorded (including multiple possible sources for a device such as a smart TV – TV remote, direct push button and remote user over a network).

  Evidence collection is easier when a device operating system supports forensic interactions to collect relevant information via system calls. Otherwise, an autonomous software layer on top of the operating system has to be created for evidence collection from programmable devices. In both cases, an edge controller issues commands to the device software for evidence collection and preservation. For all other devices, an external collection mechanism is implemented at the controller node.

  When devices execute real-time applications, it is important to know the kind of data that is generated and how it is stored; this helps develop advanced data collection mechanisms [21]. In the applications layer, the sources of all failed interactions (e.g., configuration changes, authentication and access requests, and suspicious API calls) are logged for future investigations. All the collected evidence is formatted according to the storage and processing requirements.

- **Module 1.6 (Evidence Preservation):** This module covers the secure storage of evidence for future investigations. Many Internet of Things devices have on-board flash memory that stores the operating system and real-time executable files. This memory can be used to store forensic data, which could be sent periodically to a central server for longer-term storage and subsequent processing. Alternative storage may be provided by fog nodes. The evidence should be stored securely and protected from accidental modification and intentional tampering. Potential evidence from the applications layer may be preserved in secure cloud storage.

3.2 Forensic Initialization (Incident) Phase

The forensic initialization (incident) phase has three modules: (i) incident detection; (ii) first response; and (iii) investigation preparation.

- **Module 2.1 (Incident Detection):** This module covers the continuous monitoring of an environment for harmful behavior using

appropriate techniques and tools. All user interactions are validated against rules defined by administrators or security experts. In the device and controller levels, the rules are implemented as intelligent scripts that identify malicious interactions (e.g., a script would detect a number of failed authentication requests by an Internet of Things device that exceed a threshold). In the network level, intrusion detection systems and other security tools are used to monitor live traffic. In the applications level, cloud security techniques and tools are used to detect incidents. After an incident is detected, it is reported for further action.

- **Module 2.2 (First Response):** This module covers the transmission of prioritized alerts to users or administrators for immediate action. In the case of an incident, an alert is escalated to a digital forensic professional. If required, devices, controllers and software are suspended to prevent additional damage to the environment. All the relevant components should be disconnected from the production environment until the forensic investigation is completed.

- **Module 2.3 (Investigation Preparation):** This module covers activities that support the investigative process. The activities include:

  - An incident management (investigative) plan is prepared. The plan specifies how to proceed with an investigation. It also covers evidence provenance and formatting.
  - An incident response team of available experts is created to implement the incident management plan. Each incident is investigated by a dedicated team.
  - Technical and other support, including organizational and operational support, are provided to the team.
  - The incident response team is briefed about and trained on incident management.
  - The incident management plan is reviewed and improved using techniques such as paper tests, tabletop exercises and simulations.
  - The improved incident management plan is documented for practical implementation.

3.3 Forensic Investigation (Reactive) Phase

The forensic investigation (reactive) phase implements the investigative plan to reconstruct the sequence of events. Potential evidence collected during the readiness phase is acquired and analyzed to prove or disprove that an attack or breach occurred and to identify the victim devices. The insights gained during the investigation are used to improve security and forensic techniques and tools used in the environment.

The forensic investigation phase comprises the following five modules:

- **Module 3.1 (Evidence Acquisition):** This module covers the identification of evidence pertaining to the reported incident and its acquisition from secure storage. It may be necessary to visit the physical location and acquire forensic images of the Internet of Things devices in question. Various techniques may be used to extract the firmware and memory images in order to identify malicious behavior. In the applications layer, artifacts related to the cloud environment such as virtual machine images and logs, hypervisor logs, user activity logs, database access logs and application logs are collected.

- **Module 3.2 (Evidence Examination and Analysis):** This module covers the formatting of the acquired logs and evidence to render them suitable for analysis. Machine learning techniques may be applied to identify attack patterns in Internet of Things networks. Techniques and tools must be updated or augmented periodically in order to identify new attacks. Analytic tools may be used in the applications layer to identify suspicious behavior related to computing, storage and data access requests.

- **Module 3.3 (Incident Reconstruction):** This module covers the reconstruction of an incident as a sequence of suspicious events based on the results of the evidence examination and analysis module. The incident reconstruction module comprises the following two activities:

  - The evidence interpretation activity analyzes results based on predefined postulates to reconstruct an incident (e.g., identify the sequences of events in the devices and edge layer and map them to the applications layer to understand what has occurred). The postulates may be adapted from standard security policies or defined by security experts for specific Internet of Things application scenarios (e.g., a security policy may be defined to limit the number of unsuccessful authentication or

access requests). Some policies may define the standard behavior of Internet of Things devices or the environment to avoid unwanted communications between extraneous devices.

– The reporting activity generates a formal report covering the incident findings related to attacks and victims and their timelines.

- **Module 3.4 (Evidence Presentation):** This module covers the preparation and presentation of evidence to comply with the requirements imposed by legal proceedings. The final report may incorporate graphics and animations to enhance clarity.

- **Module 3.5 (Investigation Closure):** This module covers the post-investigation activities, especially providing feedback and archiving the evidence. Feedback is provided to the evidence examination and analysis module, and evidence traces and records are archived. Case studies may be created to inform and enhance future investigations.

4. Forensic Technologies

This section discusses two emerging technologies, fog/edge computing and blockchains, that can enhance Internet of Things forensic processes.

4.1 Fog/Edge Computing

The terms fog computing and edge computing are used interchangeably to describe the layer between end-devices and the cloud that leverages the storage and processing of intermediate devices (fog nodes). Fog computing can be considered to be an implementation of edge computing [9]. Edge computing brings down services from the cloud to the edges of Internet of Things networks. Since these services include device authentication, access control, and data processing and storage, most of the forensic readiness modules can be implemented using fog computing. Al-Masri et al. [3] have proposed a fog-based digital forensic investigation framework for Internet of Things environments.

4.2 Blockchains

The distributed and immutable characteristics of blockchains suit the demands of Internet of Things forensics. Fernandez-Carames and Fraga-Lamas [10] have presented a comprehensive decision model that checks whether or not a blockchain-based solution applies to a particular Internet of Things scenario. In the decision model, evidence collected from

Internet of Things devices, controllers and applications in the cloud are treated as the ledger. An ideal solution for Internet of Things forensics is a private-permissioned blockchain where the number of nodes is restricted and access is only provided to selected users.

The distributed nature of a blockchain dovetails with fog computing to provide services such as evidence collection and storage. Evidence can be collected by any node and updated in the ledger. The immutability of a blockchain ensures that the evidence is not tampered with and is always valid. A blockchain also supports the verification of the provenance of evidence. These two properties enable forensic investigators to access evidence reliably from any node at any time. Ali et al. [2] have presented a global naming and storage system secured by blockchains.

In summary, blockchains can be used to timestamp and store evidence collected from Internet of Things devices [10]. Banerjee et al. [6] have presented an interesting blockchain application that tracks changes made to Internet of Things device firmware and automatically restores the original firmware in the event of tampering. Similar approaches can be used to maintain the integrity of Internet of Things evidence.

5. Research Challenges

Internet of Things forensics is challenging due to the complexity of devices and applications, and the lack of uniform standards across device manufacturers and system developers. Most tools are designed to work with conventional systems with significant storage and computing capabilities instead of small, specialized devices [21]. Challenges are also imposed by the heterogeneity of devices, applications and communications technologies. As a result, the stored data has diverse formats and requires custom acquisition methods.

Another challenge is extracting volatile data from Internet of Things devices before it is overwritten. Sophisticated mechanisms are needed for swift collection. Collection can be sped up by storing data on the device itself, but the data must be moved periodically to supplementary storage to free up device memory. The data may also be synchronized to fog nodes or cloud storage at regular intervals. This approach is safer in the long term because Internet of Things devices can be tampered with or even destroyed. The transfer and aggregation of evidence also make it more difficult to maintain the chain of custody [12]; fortunately, this can be addressed using blockchain technology.

Some challenges are specific to the phases of the proposed holistic forensic model. The principal challenge in the readiness phase is applying forensic processes to devices and their firmware when the devices are

operating. Separate hardware devices with automated forensic scripts may have to be developed to support forensic readiness activities. Challenges in the incident phase include taking control of devices deployed at remote locations (software-defined networking could help) and communicating alerts about incidents. Challenges during the investigation phase include formatting heterogeneous evidence into a uniform structure for examination and analysis, and employing machine learning algorithms to detect new attacks (e.g., cross-layer attacks) [4].

6. Conclusions

Due to the diversity of devices, networks and applications, a number of *ad hoc* digital forensic solutions have been developed for specific Internet of Things environments. A holistic digital forensic model that covers diverse Internet of Things environments is required to eliminate the overhead imposed by the *ad hoc* solutions.

The Internet of Things forensic model presented in this chapter is holistic and covers the entire forensic lifecycle. The model, which is based on the ISO/IEC 27043 international standard, is customizable and configurable, and supports diverse Internet of Things applications.

Future research will focus on the implementation and testing of the model in selected application domains, with the ultimate goal of creating a comprehensive framework for Internet of Things forensics.

References

[1] F. Alaba, M. Othman, I. Hashem and F. Alotaibi, Internet of Things security: A survey, *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[2] M. Ali, J. Nelson, R. Shea and M. Freedman, Blockstack: A global naming and storage system secured by blockchains, *Proceedings of the USENIX Annual Technical Conference*, pp. 181–194, 2016.

[3] E. Al-Masri, Y. Bai and J. Li, A fog-based digital forensics investigation framework for IoT systems, *Proceedings of the Third IEEE International Conference on Smart Cloud*, pp. 196–201, 2018.

[4] V. Asati, E. Pilli, S. Vipparthi, S. Garg, S. Singhal and S. Pancholi, RMDD: Cross-layer attack in Internet of Things, *Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, pp. 172–178, 2018.

[5] L. Babun, A. Sikder, A. Acar and A. Uluagac, IoTDots: A Digital Forensics Framework for Smart Environments, arXiv:1809.00745 (`arxiv.org/abs/1809.00745`), 2018.

[6] M. Banerjee, J. Lee and K. Choo, A blockchain future for Internet of Things security: A position paper, *Digital Communications and Networks*, vol. 4(3), pp. 149–160, 2018.

[7] M. Chernyshev, S. Zeadally, Z. Baig and A. Woodward, Internet of Things forensics: The need, process models and open issues, *IT Professional*, vol. 20(3), pp. 40–49, 2018.

[8] M. Conti, A. Dehghantanha, K. Franke and S. Watson, Internet of Things security and forensics: Challenges and opportunities, *Future Generation Computer Systems*, vol. 78(2), pp. 544–546, 2018.

[9] K. Dolui and S. Datta, Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing, *Proceedings of the Global Internet of Things Summit*, 2017.

[10] T. Fernandez-Carames and P. Fraga-Lamas, A review of the use of blockchain for the Internet of Things, *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[11] M. Harbawi and A. Varol, An improved digital evidence acquisition model for Internet of Things forensics I: A theoretical framework, *Proceedings of the Fifth International Symposium on Digital Forensics and Security*, 2017.

[12] R. Hegarty, D. Lamb and A. Attwood, Digital evidence challenges in the Internet of Things, *Proceedings of the Ninth International Workshop on Digital Forensics and Incident Analysis*, pp. 163–172, 2014.

[13] International Organization for Standardization and International Telecommunication Union, ISO/IEC 27043:2015: Information Technology – Security Techniques – Incident Investigation Principles and Processes, Geneva, Switzerland, 2015.

[14] International Telecommunication Union, Recommendation ITU-T Y.2060: Overview of the Internet of Things, Geneva, Switzerland, 2012.

[15] V. Kebande and I. Ray, A generic digital forensic investigation framework for Internet of Things (IoT), *Proceedings of the Fourth IEEE International Conference on Future Internet of Things and Cloud*, pp. 356–362, 2016.

[16] C. Meffert, D. Clark, I. Baggili and F. Breitinger, Forensic state acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition, *Proceedings of the Twelfth International Conference on Availability, Reliability and Security*, article no. 65, 2017.

[17] R. Minerva, A. Biru and D. Rotondi, Towards a Definition of the Internet of Things (IoT), Revision 1, IEEE Internet Initiative, Piscataway, New Jersey (iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf), 2015.

[18] E. Oriwoh and P. Sant, The Forensics Edge Management System: A concept and design, *Proceedings of the Tenth IEEE International Conference on Ubiquitous Intelligence and Computing and the Tenth IEEE International Conference on Autonomic and Trusted Computing*, pp. 544–550, 2013.

[19] S. Perumal, N. Norwawi and V. Raman, Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology, *Proceedings of the Fifth International Conference on Digital Information Processing and Communications*, pp. 19–23, 2015.

[20] C. Shin, P. Chandok, R. Liu, S. Nielson and T. Leschke, Potential forensic analysis of IoT data: An overview of the state-of-the-art and future possibilities, *Proceedings of the IEEE International Conference on the Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing and IEEE Smart Data*, pp. 705–710, 2017.

[21] S. Watson and A. Dehghantanha, Digital forensics: The missing piece of the Internet of Things promise, *Computer Fraud and Security*, vol. 2016(6), pp. 5–8, 2016.

[22] K. Yeow, A. Gani, R. Ahmad, J. Rodrigues and K. Ko, Decentralized consensus for edge-centric Internet of Things: A review, taxonomy and research issues, *IEEE Access*, vol. 6, pp. 1513–1524, 2017.

[23] S. Zawoad and R. Hasan, FAIoT: Towards building a forensics aware ecosystem for the Internet of Things, *Proceedings of the IEEE International Conference on Services Computing*, pp. 279–284, 2015.

[24] T. Zia, P. Liu and W. Han, Application-specific digital forensics investigative model in Internet of Things (IoT), *Proceedings of the Twelfth International Conference on Availability, Reliability and Security*, article no. 55, 2017.