electronics

MDPI

Article

A Metamodeling Approach for IoT Forensic Investigation

Muhammed Saleh [1,*], Siti Hajar Othman [1], Maha Driss [2,3], Arafat Al-dhaqm [1], Abdulalem Ali [4], Wael M. S. Yafooz [5,*] and Abdel-Hamid M. Emara [5,6]

[1] Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
[2] Security Engineering Lab, College of Computer and Information Sciences Prince Sultan University, Riyadh 12435, Saudi Arabia
[3] RIADI Laboratory, University of Manouba, Manouba 2010, Tunisia
[4] Faculty of Information Technology, City University, Petaling Jaya 46100, Selangor Darul Ehsan, Malaysia
[5] Department of Computer Science, College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia
[6] Department of Computers and Systems Engineering, Faculty of Engineering, Al-Azhar University, Cairo 11884, Egypt
* Correspondence: asmuhammed2@graduate.utm.my (M.S.); wyafooz@taibahu.edu.sa (W.M.S.Y.)

Abstract: The Internet of Things (IoT) Investigation of Forensics (IoTFI) is one of the subdomains of Digital Forensics that aims to record and evaluate incidents involving the Internet of Things (IoT). Because of the many different standards, operating systems, and infrastructure-based aspects that make up the Internet of Things industry, this sector is extremely varied, ambiguate, and complicated. Many distinct IoTFI models and frameworks were developed, each one based on a unique set of investigation procedures and activities tailored to a particular IoT scenario. Because of these models, the domain becomes increasingly complicated and disorganized among those who perform domain forensics. As a result, the IoTFI domain does not have a general model for managing, sharing, and reusing the processes and activities that it offers. With the use of the metamodeling development process, this work aims to create an Internet of Things Forensic Investigation Metamodel (IoTFIM) for the IoTFI domain. Utilizing the metamodeling development process allows for the construction and validation of a metamodel and the verification that the metamodel is both comprehensive and consistent. The IoTFIM is divided into two phases: the first phase identifies the problem, and the second phase develops the IoTFIM. It is utilized to structure and organize IoTFI domain knowledge, which makes it easier for domain forensic practitioners to manage, organize, share, and reuse IoTFI domain knowledge. The purpose of this is to detect, recognize, extract, and match various IoTFI processes, concepts, activities, and tasks from various IoTFI models in an IoTFIM that was established, facilitating the process of deriving and instantiating solution models for domain practitioners. Utilizing several metamodeling methodologies, we were able to validate the generated IoTFMI's consistency as well as its applicability (comparison against other models, frequency-based selection). Based on the findings, it can be concluded that the built IoTFIM is consistent and coherent. This makes it possible for domain forensic practitioners to simply instantiate new solution models by picking and combining concept elements (attribute and operations) based on the requirements of their models.

Keywords: digital forensic; IoT; investigation of forensics; metamodeling

check for updates

Citation: Saleh, M.; Othman, S.H.; Driss, M.; Al-dhaqm, A.; Ali, A.; Yafooz, W.M.S.; Emara, A.-H.M. A Metamodeling Approach for IoT Forensic Investigation. *Electronics* **2023**, *12*, 524. https://doi.org/10.3390/electronics12030524

Academic Editor: Michele Segata

Received: 24 November 2022
Revised: 22 December 2022
Accepted: 10 January 2023
Published: 19 January 2023

1. Introduction

Digital Forensics (DF) was used to identify, acquire, preserve, investigate, and report cybercrimes. The IoT Forensic Investigation (IoTFI) is one of the DF branches used to capture and analyze IoT incidents, as illustrated in Figure 1. Internet of Things Forensic Investigation, often known as IoTFI, is necessary to recognize and locate IoT-related crimes. Additionally, this field is diverse and interoperable because of the many different types of Internet of Things devices and systems and their multidimensionality [1]. The Internet of Things can be broken down into three distinct aspects: IoT device-level forensic environments, IoT network forensic environments, and IoT cloud forensic environments [2–7]. The IoT device-level forensics environments Dimension refers to the area within a crime scene where all hardware, software, and networks related to the crime scene can be found. Following that, the IoT network forensic environments Dimension refers to all the hardware and software at the network's edge that communicates between the internal and external networks and is housed in this zone based on the network type (WSN, WHAN, WPAN, WBAN, WLAN, etc.) to gather the evidence. Lastly, the IoT cloud forensic environments Dimension refers to all the hardware and software that is a part of the cloud and the data from various cloud artifacts, such as DHCP logs, control node logs, interface logs, etc. The IoT devices, IoT network environments, and IoT cloud environments can be used to determine the attack pattern, which can then be used to gather evidence about the source of the attack [5–7]. The varying concepts and terminologies used in the Forensic Investigation process and the unreconciling nature of domain knowledge spread in all directions created additional difficulties for IoTF investigators and practitioners. Models, processes, techniques, tools, frameworks, activities, and approaches are not organized or structured. Thus, generic/standardized models may be limited to unifying concepts and terminologies, reducing confusion, and assisting in the organization and structuring of domain knowledge. Thus, this paper contributes to addressing the interoperability, heterogeneity, and complexity issues of the IoTFI domain through the proposal of an IoTFIM using the metamodeling process approach by developing a Common Investigation Process Model for Internet of Things Forensics to solve the heterogeneity, interoperability, complexity, and ambiguity in the IoTFI field. The developing Common Investigation Process Model identified, recognized, extracted, and shortlisted different IoTFI concepts from other IoTFI models; therefore, this paper contributes to the development of IoTFIM and demonstrates its applicability and effectiveness in the IoTFI field. After development, IoTFIM needs to validate the developed IoTFIM using comparisons against other models and frequency-based selection methods adapted from [8,9]. The validation methods investigate the frameworks, models, methodologies, and so on that address IoTFI criteria for the domain application and whether the metamodel is reasonable and compatible. The common methods of validating metamodels use comparisons against other models and, second, frequency-based selection, which is more effective than other validation techniques [8,9]. For this purpose, 14 models were selected that met the criteria in the IoTFIM for IoTFIM development and 18 models for the verification processes for the first and second validations to develop IoTFIM from the modeling and Digital Forensic Investigation perspectives to ensure its completeness, clarity, logicalness, scalability, interoperability, and usefulness. The proposed metamodel will facilitate structuring, organizing, sharing, managing, and reusing IoTFI domain knowledge. Additionally, this paper is an explicit artifact to describe IoTFI knowledge among domain forensic practitioners. This study assists domain practitioners (incident responders, examiners, investigators, and analyzers) in developing solution models for their problems. Still, it can also provide insight into how to encourage newcomers to use this metamodel as a guideline to investigate drone incidents. [3,10].

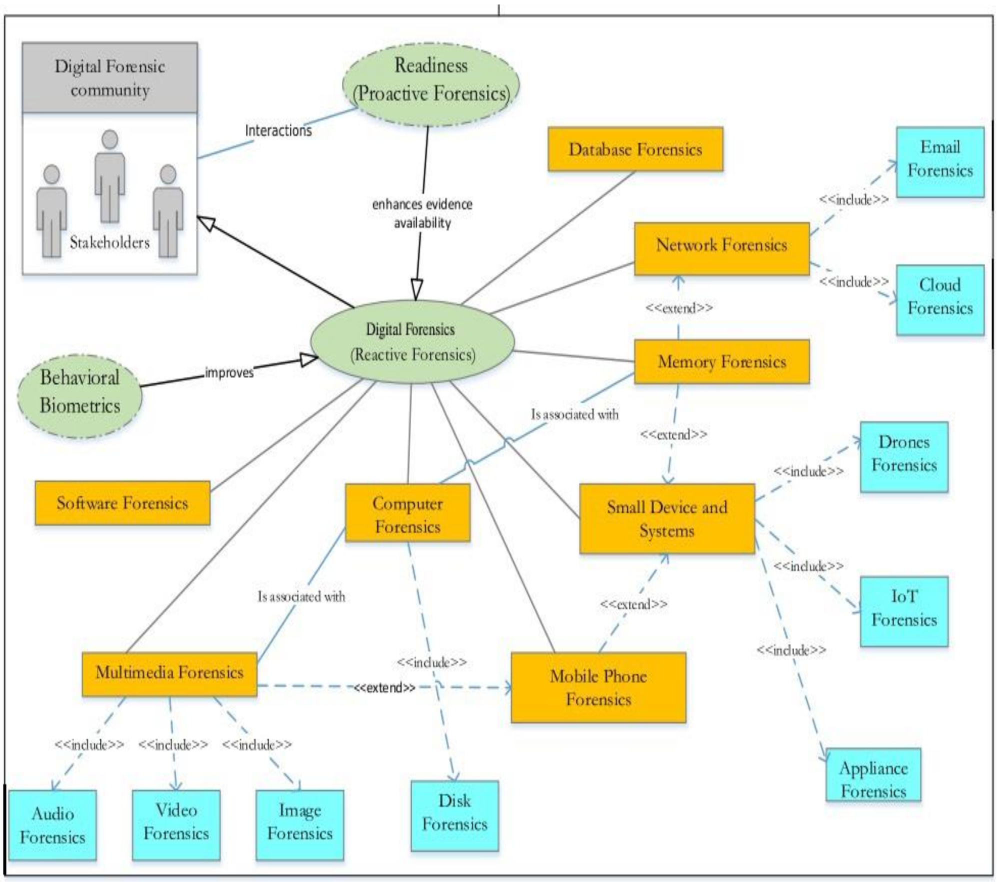

Figure 1. Illustrative example of the many specialized fields that comprise DF [10].

2. Related Works

In the literature, researchers suggested several investigation models for the IoTFI domain. However, the proposed models in the literature are limited in scope and do not encompass the entire IoTFI domain. For instance, Oriwoh (2013) [11] provided a collection of IoT cybercrime scenarios that were carried out by a suspect who used various IoTware to commit cybercrime. The authors used these situations to discover potential sources of evidence in the IoT system. IoT-related DF investigations can be approached in two ways: first, the authors identify prospective sources of evidence within the IoT system using a 1-2-3 Zones method. According to their findings, there are three zones of examination for the Internet of Things: zone 1, zone 2, and zone 3. The first zone represents the internal network, zone two includes all hardware, and zone three includes all software outside of the internal network. The investigators argue that an investigation can be more efficient and faster if the attack area is divided into three zones. A Next-Best-Thing Triage (NBT) model is also introduced, which can be used in conjunction with the 1-2-3 Zones approach when necessary. This study also discussed the introduced a top–down forensic method for the IoT system. They argued it should be used to conduct a successful investigation scenario of the IoT, including inception, interaction, reconstruction, and security. Internal, middle, and external zone networks were created for the investigation space (1-2-3 Zones model). The Triage model and 1-2-3 Zones model are combined in this work to create an integrated model for volatile-based data preservation. To provide or store information, the suggested model would refer to device-to-device communication, which is also known as Machine-to-Machine communication. The base device identifier would refer to this as M2M. There are many different types of M2M communication media to choose from, such as Z-Wave, LTE, Wi-Fi, and Power Line Communication (PLC). It will be necessary to conduct a Triage examination of the big data platform, as it is likely to encounter both structured and unstructured information.

Other studies suggested several approaches. For example, the study by Kebande (2016) [12] proposed an investigation framework for the IoT that includes a Digital Forensic Readiness (DFR) capability. The aim of the proposed framework is to make IoT devices ready for any cybercrimes in the future. The authors proposed an IoT Digital Forensic Investigation Framework (DFIF-IoT) based on this premise. This framework is able to provide a degree of certainty regarding future IoT investigative capabilities. The DFIF-IoT framework comprises three approaches: a proactive process, a reactive process, and a Concurrent Process. It includes defining an IoT scenario, finding an IoT evidence source, spotting a planning incident, gathering possible evidence, preserving digital evidence, and storing possible evidence. IoT forensics consists of three forensic aspects: cloud forensics, network forensics, and device-level forensics and the reactive process. This consists of the following entities: initialization, acquisitive, and investigative. A comprehensive and harmonized Digital Investigation Process Model was developed by Valjarevic and Venter to define Concurrent Processes as concepts that enable effective investigation [12].

The privacy issue of the IoT investigation models was also discussed in previous studies. For example, the work by Nieto (2017) [13] introduced the PRoFIT (Privacy-aware IoT-Forensic Model) approach to making use of the privacy protection elements offered by ISO/IEC 29100:2011 across the phases of an IoT-based Forensic Investigation model. Their proposed approach was evaluated using a malicious software spread scenario in an IoTs-enabled coffee shop. The proposed model consists of six phases: Preparation (planning and setting up the environment), Context-based data collection, data analysis and correlation, Information Sharing (exchange of information), Presentation (presentation of information), and Review.

The study by Bouchaud (2018) [14] proposed a methodology to aid investigators in determining whether evidence data is local or synchronized from a different source. They tested their approach against a set of known circumstances to see if the evidence was generated locally or synchronized from a different source.

Furthermore, the work by Islam (2019) [15] proposed a comprehensive DFI process framework for the IoT environment that can make DFI more efficient and effective. The study's contribution is to provide a comprehensive IoT-Based Forensics Framework in order to lessen reliance on the CSP and network logs while an inquiry is underway. The proposed framework includes the Readiness process (Planning Pre-incident Detection and Collection, Identification of Potential IoT Evidence Sources, and IoT Scenario Definition), IoT forensics (cloud forensics, network forensics, device-level forensics), Initialization process (Planning, Incident Detection, Preparation, Initial Response), Acquisition process (Potential IoT Evidence Identification, Potential IoT Evidence Collection, Potential IoT Evidence Transportation, Storage of Potential IoT Evidence), Investigation process (IoT Evidence Examination and Analysis, Proof and Defense, Presentation, Reporting, Archive and Storage, and Investigation Closure), and Concurrent Process (Obtaining Authorization, Information flow, Chain of Custody, Documentation, Physical Investigation, and Preserving Evidence). The suggested architecture reduces the reliance on CSP or cloud logs for obtaining evidence from the cloud. Furthermore, it eliminates the need for ISP or network records to obtain network proof.

Investigating IoT devices of the IoT is considered one of the important areas due to its role in improving the whole performance of the network. In this regard, a study performed by Scheidt (2020) [16] came up with a new way to identify IoT devices that will improve IoT forensics. They presented a technique to assign a unique identifier for each device in the IoT internationally, which is similar to DNA analysis in terms of IoT forensics. Instead of utilizing standard DNA, they proposed a method to assign a globally unique identifier to all IoT devices. In the case of IoT forensics and the assignment of a unique identification number, these numbers are referred to as the DNA of a device, which is comprised of unique attributes known as Genes. They established the framework of the IoT, its Forensic Investigation and obstacles, as well as the technique of Universal Identification Numbers using Set Theory to elucidate the need for unique device identification. The hierarchical and distributional Hybrid model was proposed in this study to enable main-servers and sub-servers to be in constant communication, as well as to facilitate the global interchange of evidentiary data.

Some issues in the literature are considered crucial and should be given much attention by the IoT experts, such as IoT tracking features. This specific issue was deeply studied by Kang (2020) [17], who described the broad features of fitness tracker analysis and showed how these features are important to experts when performing a tracking analysis. Since both the Xiaomi Mi Band 2 and the Fitbit Alta HR perform as typical fitness trackers, they were selected for this study.

A recent study by Kim (2021) [18] gathered and evaluated wearable user data using a smart device data acquisition framework. This study uses software-based (JTAG and Chip-off) and hardware-based data capture approaches for data extraction. This study used a smart device data gathering framework for wearable devices such as Xiaomi (Amazft Stratos 3 and Mi Band 4), Huawei, LG, and Fitbit for data acquisition and analysis. This could enable wearable gadget crime scene investigations. Xiaomi devices can provide a device name, last charging/connecting time, MAC address, and user input data such as heart rates and workout times. While Huawei and LG smartphones' innards could be accessed via a PC, no useful data could be collected; Chip-off technology was required. Smart bands like the Fitbit Charge 4 and Xiaomi Mi Band 4 have fewer functions than smartwatches, making logical/physical forensics more difficult. Another recent study by Kumar (2021) [19] proposed an IoT forensics framework. Internet-of-Forensics (IoF) solution uses blockchain-based IoT infrastructure for DFs. It provides a comprehensive image of the Investigation process by bringing together all parties (such as heterogeneous devices and cloud service providers). It uses a blockchain-based case chain to handle investigations, including the Chain of Custody and evidence chain. "Consensus" describes a group that tackles cross-border legalization. This study provided a Digital Forensic framework that uses IoT for evidence collecting and transmission and blockchain for evidence management.

According to the literature in Table 1, there was little research on IoT forensic areas that were utilized to tackle comprehensive problems. Several recent works dealing with the management of IoT/sensor networks threats and vulnerabilities (11-21]) are in dire need of such an investigation framework to identify the security risks and assure proper countermeasures, regulations, and procedures to prevent/avoid them. There are certain unresolved issues in IoT forensics that require more investigation, aiming to boost IoT system adoption rates. This paper may infer that more research is required to develop forensics investigation frameworks for the IoT system that can efficiently manage vast volumes of data generated by heterogeneous IoT devices. Furthermore, IoT device/product makers must address forensics preparedness during the design phase. Moreover, there are no standards or complete formats for IoT device forensics and no standard forensic model or procedure for IoT device forensic testing. Hence, the aim of this work is to propose a high-abstract model for the IoTFI to organize and structure the IoTFI domain. This paper also aims to develop an IoTFIM using a metamodeling approach that specifies all of the tasks that investigators should perform to finish their assignment. A metamodeling technique is utilized to ensure that the end result is satisfying and that the metamodel is completed and consistent.

Table 1. Recent studies gaps and problems.

Year	IoT Forensics Models	IoT Application and Type	IoT Forensic Procedures				Type of the Model		Digital Forensics Readiness		International Standard	Decreases Heterogeneity and Ambiguity		Suppurative Environment		
			Preservation	Acquisition	Analysis	Reporting	Technical	Conceptual	Adopt Pre-Incident Preparation Approach	Provides Mean of Assessing for Forensics readiness	ISO/IEC	Offer Interoperability Environment	Offer Unified Platform	Zone 3: Cloud Forensics	Zone 2: Network Forensics	Zone 1: Device-Level Forensics
2013	[11]	1-2-3 Zones Approaches	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓
2016	[12]	IoT devices	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓
2017	[13]	IoT devices	✓	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✓
2018	[14]	IoT devices	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓	✓
2019	[15]	IoT devices	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✓
2020	[16]	IoT devices	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓

Table 1. *Cont.*

Year	**IoT Forensics Models**	**IoT Application and Type**	**IoT Forensic Procedures**				**Type of the Model**		**Digital Forensics Readiness**		**International Standard**	**Decreases Heterogeneity and Ambiguity**		**Suppurative Environment**		
			Preservation	**Acquisition**	**Analysis**	**Reporting**	**Technical**	**Conceptual**	**Adopt Pre-Incident Preparation Approach**	**Provides Mean of Assessing for Forensics readiness**	**ISO/IEC**	**Offer Interoperability Environment**	**Offer Unified Platform**	**Zone 3: Cloud Forensics**	**Zone 2: Network Forensics**	**Zone 1: Device-Level Forensics**
2020	[17]	wearable IoT devices	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	✓
2021	[18]	IoT devices	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗
2021	[19]	IoT devices	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓
2022	[20]	IoT devices	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✓
2022	[21]	IoT devices	✓	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓

3. Research Methodology and Development Process

As mentioned in the previous section, the main goal of this research is to provide a standardized solution for the IoTF domain, which will be the IoTFI Metamodel. The design science research methodology was adapted in this study [20]. This methodology includes two phases, as shown in Figure 2. The first phase discusses the main gaps and limitations of the IoTF domain. The output of the first phase is used as input for the second phase. At the same time, the second phase was used to develop the IoTF metamodel. The metamodeling approach is a kind of design science method used in well-known benchmarked systems [21–23]. This method is used to develop IoTFIM in the current study. Figure 2 illustrates the research methodology of this study.

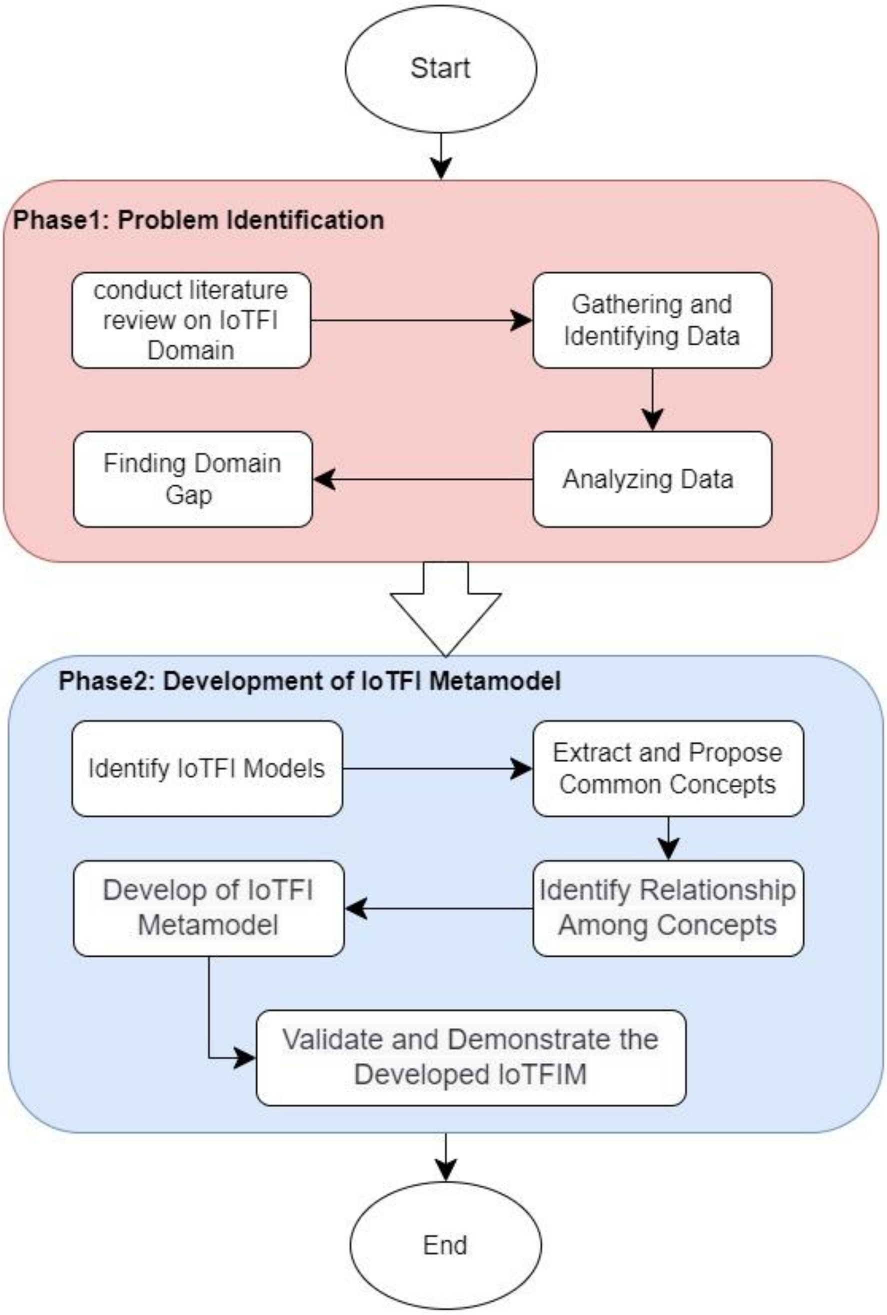
Start
Phase1: Problem Identification
conduct literature review on IoTFI Domain
Gathering and Identifying Data
Analyzing Data
Finding Domain Gap
Phase2: Development of IoTFI Metamodel
Identify IoTFI Models
Extract and Propose Common Concepts
Identify Relationship Among Concepts
Develop of IoTFI Metamodel
Validate and Demonstrate the Developed IoTFIM
End

Figure 2. Research methodology.

3.1. Phase 1: Problem Identification

The aim of this phase is to highlight the main issues in the IoTF domain. This phase includes three steps, as follows:

I. Finding the Existing Solutions in the Database: In this step, the existing solutions are found by using well-known database search engines such as, "Springer Links", "Scopus", "Google Scholar", "Web of Science", and "IEEE Xplore". This research used the search terms "IoT forensics model", "IoT forensics identification", "IoT forensics preservation", "smart de-vices forensics analysis", "IoT forensics acquisition", "evidence extraction of IoT devices", and "IoT forensics examination" to achieve this aim.

II. Gathering and Identifying Data: In this step, the study collected data based on Step 1. The collected data are refined based on the year of publication, relevancy, and quality. Furthermore, only the papers that develop a framework, a model, or a procedure for conducting a Forensic Investigation on IoTF are selected. A further manual filtration approach is used where the title and name of the authors are considered to avoid duplications from multiple sources. Finally, based on the criteria mentioned above, 41 out of 825 articles were selected for use in this study based on IoTFI processes, IoT offenses, concepts, and tasks.

III. Analyzing Data and Finding Domain Gaps: Based on a detailed review, the IoTF domain suffered from several issues, as discussed below:

- Various Forensic Investigation Artifacts: The diverse architectures of smartphone devices resulted in a number of IoTF artifacts with similar names but differing meanings. Therefore, it raises confusion among IoTF investigators.
- Lack of Standardized Investigation Model: Several specific Investigation Process Models were proposed in the literature. Each IoTF has a specific Investigation Process Model, which is largely at variance with other models.
- Redundancy of Investigation Concepts and Terminologies: The diversity of IoT infrastructure resulted in ununified Investigation processes, concepts, and terminologies. The IoTF domain is ambiguous and complex among IoTF practitioners due to the redundancy of concepts and processes in the domain. Therefore, the IoTF domain lacks unified concepts and terminologies.

3.2. Phase 2: Development of IoT Forensic Investigation Metamodel (IoTFIM)

This study used five main steps to develop IoTFIM as follows:

I. Identify IoTF Models: In this study, research articles, books, conference papers, dissertations, and book chapters are taken into consideration while omitting other types of documents. This study demonstrates that researchers and developers deal with the IoTFI domain from three perspectives: (i) IoTFI Dimensions–perspective (IoT device-level forensics, IoT network environments, and IoT cloud environments); (ii) IoTFI Technology–perspective (methods, tools, and algorithms); and (iii) IoTFI Process–perspective (identification, acquisition, analysis, and Documentation). However, they vary in perspective coverage. For example, some models cover most IoTFI perspectives (three perspectives), whereas some others cover two IoTFI perspectives and others cover one IoTFI perspective.

This study categorized these models into two categories based on their coverage: The first category includes models that cover at least two IoTFI Dimensions, IoTFI technology, and at least three Investigation processes, and these are called "full-coverage" models; they cover a wide range of IoTFI perspectives. The second category includes models that cover at least one of the IoTFI Dimensions, IoTFI technologies, and at least two Investigation processes. These are called "partial-coverage" models because they cover only a partial range of the IoTFI perspectives. Based on this categorization, this study found thirty-two (32) models out of forty-one (41) models covered three categories. The first category, full-coverage models (Set1), were used to generate the standard model. The second category is partial-coverage models (SetV1), and the third category is full-coverage models (SetV2). SetV1 and SetV2 were later used for the validation processes. The rest of the models covered a specific IoTFI perspective called "specific-coverage" and are ignored by this study. After that, the models that were gathered were divided into three distinct sets (Set1, SetV1, and SetV2) for the development and validation of the IoTFIM, as illustrated in Table 1. These sets are formed according to how broadly the models cover the three perspectives of IoTF. Set1, which includes 14 full-coverage models, is used to create the initial metamodel, while SetV1 includes 8 partial-coverage models and SetV2 includes 10 full-coverage models. The purpose of this validation SetV1 is to determine whether or not the initial metamodel lacks any concepts because the partial-coverage models provide more information for each perspective of the IoTF domain than provided by full-coverage models. At the same time, SetV2 more comprehensively focuses on generic IoTFI models. Table 2 shows the models in each set.

Table 2. IoTFI models classification sets.

Model	Year	IoT Forensic Investigation						
		Processes				Dimensions		
[11]	2015	✓	✓	✓	✓	✓	✓	✓
[12]	2016	✓	✓	✓	✓	✓	✓	✓
[24]	2017	✓	✓	✓	✗	✓	✓	✓
[25]	2017	✓	✓	✓	✓	✓	✓	✓
[26]	2018	✓	✓	✓	✗	✓	✓	✓
[27]	2018	✓	✓	✓	✗	✗	✓	✓
[28]	2018	✓	✓	✓	✗	✗	✓	✓
[29]	2018	✓	✓	✓	✓	✗	✓	✓
[15]	2019	✓	✓	✓	✗	✗	✓	✓
[30]	2019	✓	✓	✓	✗	✓	✓	✓
[31]	2019	✓	✓	✓	✓	✓	✓	✓
[32]	2020	✓	✓	✓	✗	✓	✓	✓
[33]	2020	✓	✓	✓	✗	✗	✓	✓
[34]	2020	✓	✓	✓	✗	✓	✓	✓
SetV1 (first validation)								
[13]	2017	✓	✓	✓	✓	✗	✗	✓
[35]	2018	✓	✓	✓	✓	✗	✓	✗
[14]	2018	✓	✓	✗	✗	✗	✓	✓
[36]	2018	✗	✓	✓	✗	✓	✓	✓
[37]	2021	✗	✓	✓	✗	✗	✓	✓
[38]	2021	✗	✓	✓	✗	✗	✗	✓
[18]	2021	✓	✓	✓	✗	✗	✗	✓
[16]	2020	✓	✗	✗	✗	✓	✓	✓
SetV2 (second validation)								
[39]	2020	✓	✓	✓	✓	✓	✗	✓
[40]	2020	✓	✓	✓	✗	✓	✓	✓
[41]	2020	✓	✓	✓	✓	✓	✓	✓
[42]	2021	✓	✓	✓	✗	✓	✗	✓
[43]	2020	✓	✓	✓	✓	✗	✗	✓
[44]	2021	✓	✓	✓	✓	✓	✓	✓
[45]	2021	✓	✗	✓	✗	✓	✓	✓
[46]	2020	✓	✓	✓	✗	✓	✓	✓
[47]	2020	✓	✓	✓	✗	✓	✓	✓
[48]	2017	✓	✓	✓	✗	✓	✓	✓
[20]	2022	✓	✓	✗	✗	✗	✗	✓
[21]	2022	✓	✓	✗	✓	✗	✓	✓

II. Extract and Propose Common IoTFI concepts:

At this stage, concepts are manually extracted from each model that is similar to the previous works, such as [10,22,23]. In this laborious process, each model in Set1 is utilized to identify possibly necessary concepts in the IoTFI generic metamodel. The number of concepts from the IoTFI models was chosen and filtered one by one based on their significance and functionality. Concepts should be extracted from the textual contents (primary body) of an IoT forensic model to prevent missing or irrelevant concepts during the extraction process. The created model is housed in the main body. For example, the smart house forensic process model [31] encompassed four processes for the Amazon Echo as a smart home. From each of these processes, we extracted the relevant concepts. The extracted concepts have to be relevant to the IoTF domain, or else they are rejected.

The concept extraction procedure was adapted using [10,22,23]. The concept extraction process may be broken down into two steps: Recognition is the first intellectual model. This step employs a linguistic approach. The notion must have a noun or adjective + a noun or compound noun in order to be recognized. For example, "investigator" is a noun, "chain of custody" is a compound noun, and "data collected" is a combination of an adjective and a noun. The second conceptual metamodel is categories, which may be separated into an actor (active concept) such as (investigator), an object (passive concept) such as (decision, source of potential evidence, and result), and a process (activities) such as (Verification, Documentation). Table A1 displays the notions of extraction from Set1 that yielded a total of 603 concepts (extracted from 14 general models, as shown in Appendix A).

Common concepts with comparable meanings or functions are now grouped together, regardless of their names or synonyms. For example, the source of evidence concept is utilized in models [7,11]. The potential digital evidence from IoT devices [24] and the digital evidence concept in the model [12] have the same meaning. As a result, we combined these notions into a single concept: the source of potential evidence, as illustrated in Table A2. Furthermore, concepts that have a single frequency name, such as investigators in models, are common. Table A2 displays some of the selection of common concepts. We utilized the following characteristics for concepts that had the same meaning: In the models, they used frequency and definition to choose the names of common concepts. Because of this, in the event that two or more concepts have meanings that are comparable to one another, the name of the concept that was defined the most frequently will be selected for inclusion in the metamodel, while the other names will be removed. The shared meaning of the concepts "source of evidence" and "digital evidence," for example, is that "the major source of forensic data is the source of potential evidence, which may be found in IoT devices, and IoT network environments and IoT cloud environments." "Source of potential evidence" was chosen as a common concept since it appears more frequently in more models than digital evidence. As a result, the "source of potential evidence" is included in the metamodel, although digital evidence is not. Indeed, the high frequency (occurrence) of the concept among all models is the major consideration for picking the common concept. This stage results in the selection of common concepts, as illustrated in Appendix B.

III. Identify Relationship Among Concepts

The relationships between the IoTFIM concepts are now established. As depicted in Figures 3–6, three types of common Unified Modeling Language (UML) relationships were discovered: association, specialization/generalization, and aggregation. Typically, an association relationship signifies that one class maintains a relationship with another class in order to accomplish a task.

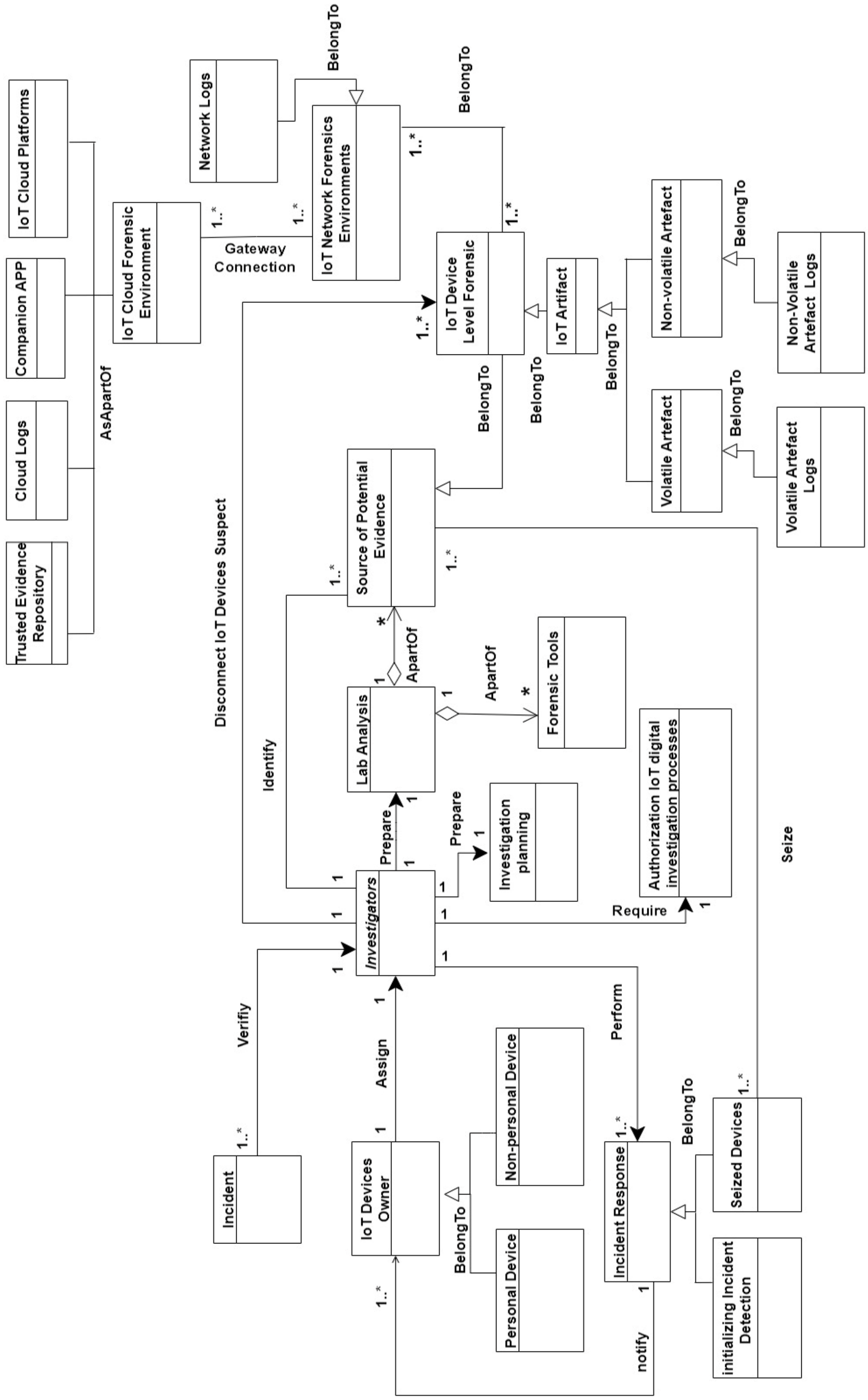

Figure 3. IoT identification process IoTFIM 1.0.

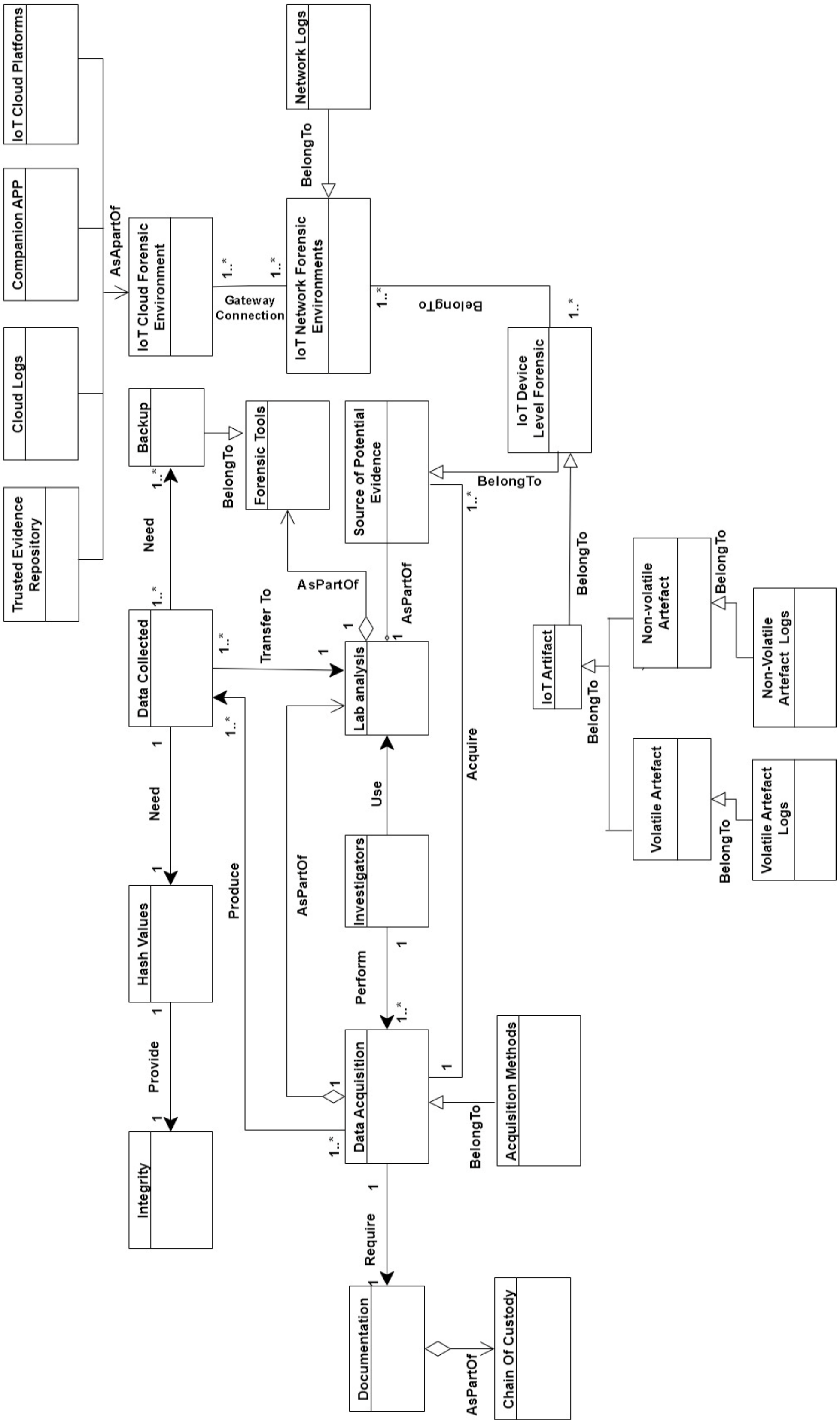

Figure 4. IoT Acquisition process IoTFIM 1.0.

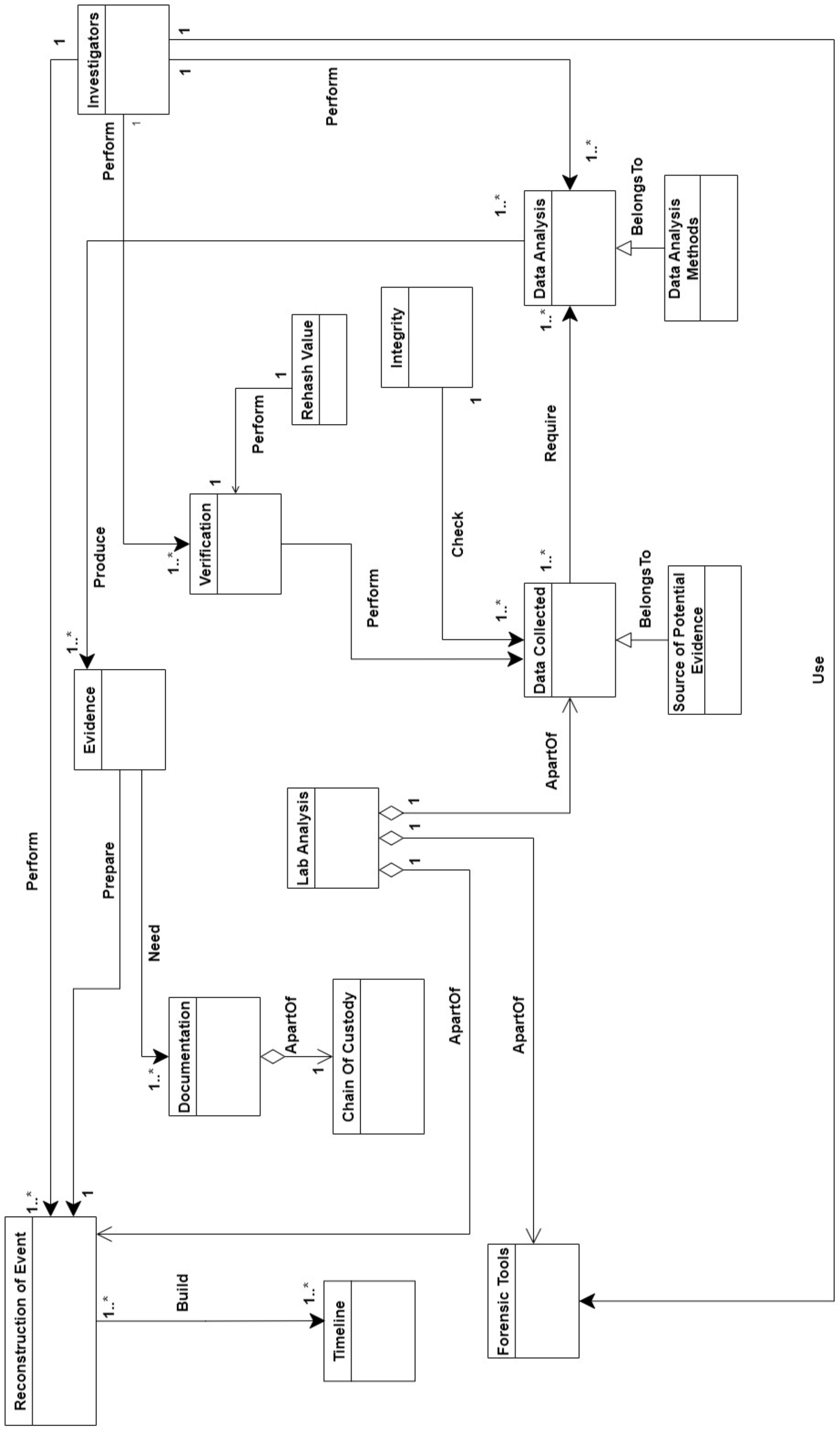

Figure 5. IoT Analysis process IoTFIM 1.0.

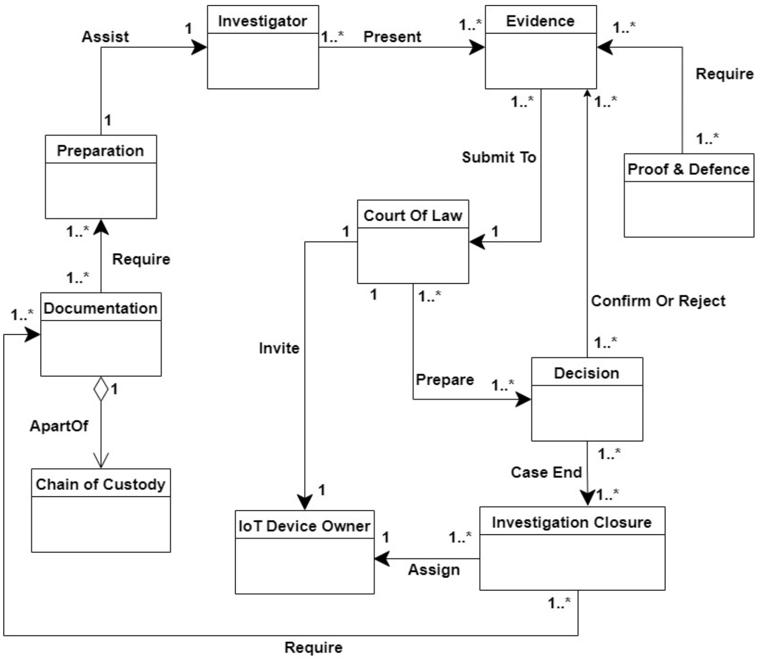

Figure 6. Presentation process IoTFIM 1.0.

There are numerous association symbols that may be used to add information to the model [49,50]. In this study, the symbol used for representing the association link between two concepts is “⟶”. As an example of an association relationship, the concept “assign” between investigators and IoT device owner concepts implies that an owner needs to be assigned and tell the investigators about an incident that occurred in order to begin an investigation. A subclass is related to its superclass via the specialization/generalization connection. It represents attribute and operation inheritance from the superclass to the subclass [50,51]. The symbol “—▷” is used in this study to represent the specialization connection between concepts. For example, the Volatile Artifact concept “BelongsTo” is the IoT Artifact concept. As a result, the actions and properties of the IoT Artifact class may be handed down to the Volatile Artifact subclass. Typically, an aggregate connection indicates ownership [49]. This study used the symbol “—◇” to represent the conceptual aggregation relationship. As an example of an aggregation connection, throughout the identification and artifact-collecting process, the relation “ApartOf” connects Lab Analysis and the source of potential evidence, along with the Lab analysis concept.

As a result, this study depicts the linkages between concepts based on the semantic UML relationship established and recognized during the survey of the IoTFIs domain. Investigators, for example, conduct at least one Incident Response to acquire incident specifics, such as any information on incident events. The Incident Response concept entails conducting notifications with owners, both personal and non-personal, as well as gathering investigation sources of potential evidence and seized source information [5,9,11]. As a result, three types of linkages, namely association, specialization, and aggregation, were discovered and recognized. Appendix C from Tables A3–A6 depicts several instances of linkages that connect concepts from various IoTFI activities. As a consequence, the second phase produces the initial version of IoTFIM. Figures 3–6 depict the initial edition of IoTFIM, which consists of four (4) IoTFIM 1.0 process classes. We need to mention that relationships in Appendix C from Tables A3–A6 on fields C1, and C2, the symbols meaning are as follows: “*” is many related to concepts, “1” is one related to concepts, and “1..*” is meant one-to-many. The process class’s first version will be improved later in the validation process. The rest of the relationships that link concepts from different IoTFI processes are shown in Appendix C.

IV. Developing IoT Forensic Investigation Metamodel: In this step, the resultant IoTFIM is represented in four different diagrams: the identification process, the Acquisition process, the Analysis process, and the Presentation. The initial version MFM1.0 diagrams are illustrated in Figures 3–6 for each process. Particularly, each figure shows classes that should exist during the corresponding phase of IoTF. The resultant metamodel describes the semantic of the IoTF domain by establishing the relationships between concepts.

The IoT identification process is the first IoT forensic process that is used to prepare the investigation environment by identifying the geographical location of suspect devices using forensic techniques and Incident Detection, as well as allowing the investigators to start planning, developing a digital investigative procedure, and separating the devices from their geographical location.

The IoT Acquisition process is the second IoT Forensic Investigation process involving the collection of potential digital evidence obtained from the IoT environment. Then, the investigators can be transported, stored, maintained, and archived.

The IoT Analysis process is the third IoT Forensic Investigation process that is used to analyze acquired data. This process used the more common Digital Forensic processes, such as Chain of Custody, Lab analysis, results, Archive and Storage, activity reconstruction, data recovery, and geolocation tracking, to reveal who is tampering, when and where the tampering happened, and how the tampering happened.

The presentation process is the fourth IoT Forensic Investigation process that is used to document and present the investigation stages and submit the results to the court.

4. Finding and Discussion

The proposed metamodel uses two validation techniques of metamodel validation known as the comparison against other models and frequency-based selection. In this study, we would like to point out that IoTFIM has several versions, as the metamodel development processes consist of iterative operations to create the final model for IoTFIM. The second phase issues a metamodel that verification processes can develop until the final version of IoTFIM is completed. We will be ready to use IoTFIM 1.2; the last version of IoTFIM will be standardized, robust, coherent, and valuable when used in real-world scenarios. Several recent works dealing with the management of IoT/sensor networks threats and vulnerabilities [52–56] are in dire need of IoTFIM investigation framework to identify the security risks and assure proper countermeasures, regulations, and procedures to prevent/avoid them This section concentrates on the validation of the metamodel and discusses the finding.

4.1. Validation of IoTFIM

This section discusses the validation and development of IoTFIM version 1.0. The validation method is intended to assess the validity and quality of the proposed metamodel [55]. A metamodel must be validated to fulfill the requirements of the item's generality, expressiveness, and completeness. Furthermore, a validation of the suggested metamodel is essential to assure its completeness and validity. Two types of metamodel validation methodologies are used to test the completeness of the IoTFIM. The first validation is carried out by comparing the metamodel against other models to discover any missing concepts in the initial version of the metamodel and ensure its broad coverage. Concepts in the metamodel are verified and compared to concepts in other (valid) existing similar domain models or metamodels using this approach presented in [57]. The IoTFIM validation process then proceeds with the execution of a second validation that assesses the value of individual concepts in the created model [35]. It is widely used and is based on the assumption that the best model is created using the most frequent attributes [30]. It is acknowledged how frequency-based selection is used to validate the importance of IoTFIM concepts. These validation procedures are discussed in the following sections.

4.1.1. Comparison against Other Models

This is the initial validation method. The purpose of comparing the general metamodel to other models is to represent any missing concepts in Set1 of the general metamodel while also ensuring its comprehensive coverage. Concepts from the IoTFIM 1.0 are verified and compared to concepts from other existing related domain models in this method [23]. If a concept in SetV1 was not represented in IoTFIM 1.0, we consider it a strong nominee for inclusion in IoTFIM. Table 3 shows the new concepts in SetV1.

Table 3. Comparison between SetV1 model concepts and IoTFIM 1.0 concepts.

SetV1 (First Validation)		
Model	**Concepts Found**	**New Concepts Found**
[13]	Owner, personal device, non-personal device, investigators, Authorization IoT Digital Investigation Process, data acquisition, Chain of Custody, types of device profiles, victim, suspect, witness, source of potential evidence, forensic tools, data collected, IoT cloud platform, trusted evidence, Integrity, acquisition methods, Documentation, evidence, Proof and Defense, Preparation, evidence.	types of device profiles, victim, suspect, witness
[35]	IoT network forensic environments, source of potential evidence, data collected, Incident Response, Backup, IoT device-level forensic, incident, cloud platform, data analysis, cloud logs, trusted evidence, repository, volatile artifact, non-volatile artifact, evidence, Proof and Defense.	Null
[14]	Investigators, seized device, IoT network forensic environments, source of potential evidence, IoT device-level forensic, trusted evidence repository, non-volatile, volatile, data acquisition, network logs, acquisition methods, data analysis methods, IoT cloud platforms, IoT cloud forensic environment.	Null
[36]	Data acquisition, acquisition methods, forensic tools, data acquisition, IoT network forensic environments, timeline, Reconstruction of events, IoT device-level forensic, IoT network forensic environments, IoT cloud forensic environments, investigators, source of potential evidence, evidence repository, volatile artifact, non-volatile artifact, artifacts, data collected, trusted evidence repository.	Null
[37]	Data collected, Companion App, network logs, data analysis, seized device, non-volatile artifact, Backup, Reconstruction of events, timeline, acquisition methods, data analysis methods, IoT device-level forensic, evidence repository, cloud logs, cloud platform.	Null
[38]	Volatile artifact, volatile artifact logs, non-volatile artifact logs, timeline, data acquisition methods, forensic tools, Backup, data analysis, Reconstruction of events, artifacts, non-volatile, data analysis, data analysis methods.	
[18]	IoT device-level forensic, data acquisition, Companion App, non-volatile artifact, forensic tools, acquisition methods, data analysis methods, Backup, artifacts, non-volatile artifact logs, volatile artifacts log.	Null
[16]	IoT device owner, personal device, non-personal device, IoT device-level forensic.	Null

During this approach, we discovered four new concepts that were not available in IoTFIM 1.0, as shown in Table 3. Device profiles, suspicious, victims, and witnesses are the four new concepts introduced to IoTFIM. The validation changed the first version of IoTFIM 1.0 and generated a second version of IoTFIM 1.1. Figures 7 and 8 show the new concepts with the newly added relationships. Table 4 illustrates the reconciliation shortlisted for the new concepts found.

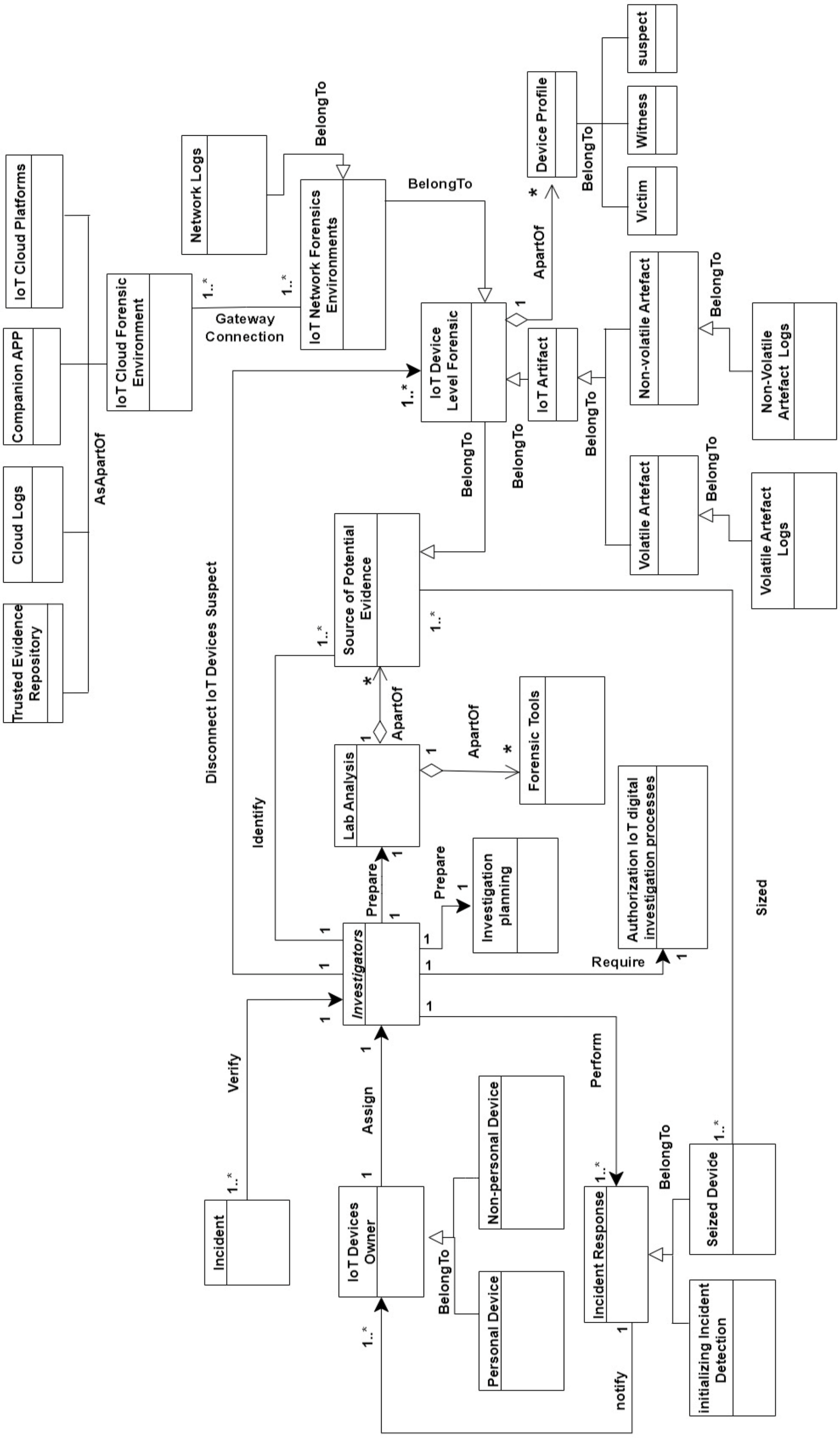

Figure 7. IoT Identification process IoTFIM 1.1.

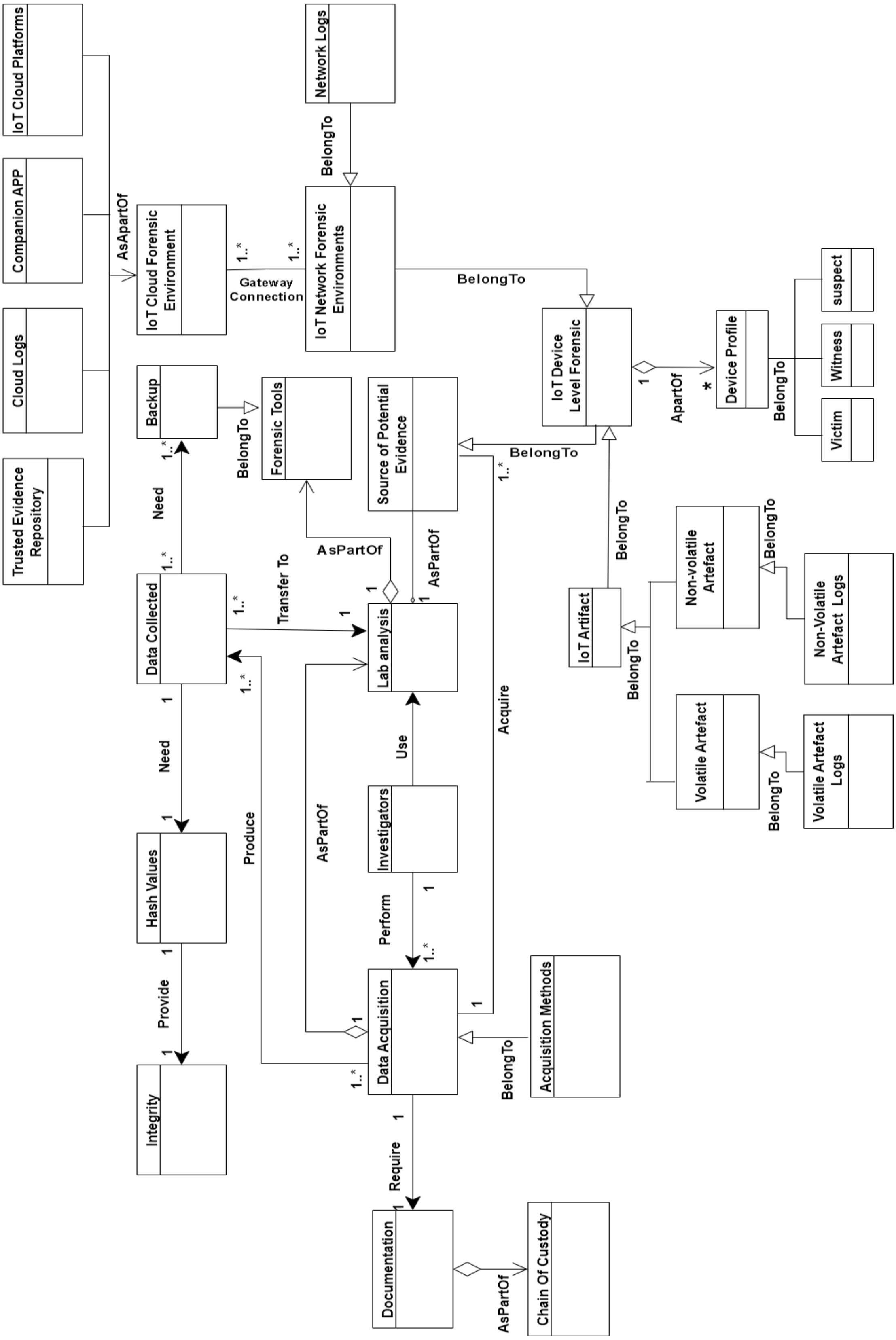

Figure 8. IoT Acquisition process IoTFIM 1.1.

Table 4. New concepts added after validation comparison against other models.

Concept	IoTFIM Process	Definition
Types of device profiles	Preparation, collection	During the course of the investigation, we differentiate between three distinct device profiles: the victim/offender profile, the witness profile, and the suspect profile.
Victim/Offended	Preparation, collection	Belongs to the individual who was the target of the offense. As a result, the owner of the device will want there to be an examination of the data stored on his or her device.
Suspect	Preparation, collection	Is a gadget that may hold digital evidence that either incriminates or exonerates the user.
Witness	Preparation, collection	It offers important digital evidence for the investigation, but these devices are not relevant to the investigation, and they are not the suspect either.

4.1.2. Frequency-Based Selection

Frequency-based selection is the second validation approach. This procedure is carried out on the assumption that the best model is created by combining the most generic or common characteristics or attributes. SetV2 is used to validate the metamodel 1.1, which is made up of 10 IoT models, each of which has at least three processes and two Dimensions. We gather concepts from model SetV2 and compare them to concepts from IoTFIM 1.1. With a high level of confidence, this validation builds a high-quality metamodel called IoTFIM 1.2. This approach aims to assess the value of individual concepts in the generated model and score each concept based on its frequency in IoTFIM 1.1. Concepts with a low score are reviewed and may be deleted. The resulting value is known as the Degree of Confidence (DoC) [57]. It computes the number of times the components appear in all SetV2 models. The term "DoC" is defined as follows:

$$\text{Degree of Confidence (DoC)} = \frac{\text{Frequency of Concept}}{\text{Total Model of setV2}} \times 100\% \quad (1)$$

The following five categories of concepts based on their DoC are defined as follows:

1. Very Strong (DoC range: 100–70%);
2. Strong (69–50%);
3. Moderate (49–30%);
4. Mild (29–11%);
5. Very Mild (10–0%).

This study matched each concept from the IoT identification, IoT acquisition, IoT analysis, and presentation processes to the models of SetV2 in Table 2 to determine the concept frequency for each concept in these models. The results suggest that wisdom and investigation planning in the IoT identification process have poor scores, but concepts such as the source of potential evidence, investigator, and incident have good scores. The IoT Acquisition process concepts with intermediate ratings are hash value, Integrity, Documentation, etc. Backup, evidence, data collected, and data acquisition are examples of high-scoring concepts in this process. Table 5 shows that concepts such as the Reconstruction of events and verification analysis have low scores in the IoT Analysis process, but concepts like data analysis, data analysis methods, and timeline have high scores in this process. The concepts of the Court of law have high scores, but concepts such as decision, Preparation, Proof and Defense, and Investigation Closure have low scores in the presentation process. The concepts with a higher score are more important in the IoTFIM domain. On the other hand, concepts with a low score are reviewed and may be deleted.

Table 5. Frequency concepts in IoTFIM 1.1.

IoTFIM 1.1 Preparation Concepts	**Models SetV2**										
	M1	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	**M9**	**M10**	**Frequency**
IoT device-level forensic			✓	✓	✓			✓			4
Volatile artifact	✓	✓					✓				3
Non-volatile artifact	✓		✓			✓	✓				4
Volatile logs			✓				✓	✓		✓	4
Non-volatile logs			✓				✓	✓		✓	4
Investigation planning			✓					✓			2
Device profile		✓	✓							✓	3
Victim			✓					✓		✓	3
Witness		✓	✓								2
Artifacts	✓	✓	✓				✓	✓	✓		6
Suspicious	✓		✓					✓			3
IoT network forensic environments			✓	✓				✓			3
Network logs			✓				✓			✓	3
IoT cloud forensic env.			✓		✓			✓			3
IoT cloud platform		✓		✓	✓				✓	✓	5
Trusted evidence repository		✓	✓						✓		3
Cloud logs		✓	✓							✓	3
Companion App		✓	✓					✓	✓	✓	5
Source of potential evidence	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10
Lab analysis			✓	✓			✓	✓			4
Forensic tools	✓	✓	✓	✓		✓	✓	✓	✓		8
Authorization IoT Digital Investigation Process				✓		✓		✓			3
Investigators	✓	✓	✓	✓	✓	✓	✓	✓		✓	9
Owner			✓					✓	✓		3
Personal device		✓	✓					✓	✓		4
Non-personal device		✓	✓				✓	✓			4
Incident	✓		✓	✓	✓	✓	✓	✓		✓	8
Criminal activities	✓		✓			✓	✓	✓		✓	6
Incident Response	✓			✓	✓						3
Seized device							✓		✓	✓	3
Initializing Incident Detection	✓			✓				✓		✓	4
Backup	✓	✓				✓		✓	✓		5
Data collected		✓	✓			✓	✓	✓		✓	6
Hash values		✓							✓	✓	3
Integrity		✓			✓		✓			✓	4
Data acquisition		✓	✓	✓		✓			✓	✓	6
Data acquisition methods	✓	✓	✓	✓		✓		✓	✓		7
Documentation				✓	✓			✓	✓		4
Chain of Custody	✓			✓	✓			✓			4
Data analysis		✓	✓	✓	✓				✓		5
Data analysis methods	✓	✓	✓		✓	✓	✓			✓	3
History analysis		✓	✓					✓			3
Log data analysis	✓	✓			✓	✓	✓	✓		✓	6
Verification		✓	✓	✓			✓				4
Reconstruction of events	✓	✓	✓							✓	4
Timeline	✓		✓			✓	✓			✓	5
Evidence	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	10
Proof and Defense					✓	✓					2
Court of law	✓			✓	✓	✓			✓		5
Decision					✓						1
Preparation					✓	✓					2
Investigation Closure											0

All the concepts of IoTFIM classified in the DoC classification are presented in Table 6. The classification results are dependent on categorization, as "very strong" is 7, "strong" is 10, "Moderate" is 27, "Mild" is 4, and "very mild" is 2. Decision and Investigation

Closureare two very mild concepts. Including them in the IoTFIM requires a reassessment. Investigation Closure has a zero in the DoC classification, which means this concept is not suitable for IoTFIM. The concept of decision will be kept because it is, in fact, more generic. As the results show, one concept should be deleted (feedback and interview), and one concept should be kept as they are common across varying IoTFI domains. Figure 8 illustrates the deletion concept. Figure 9 illustrates the presentation process after the concept deletion.

Table 6. DoC classification result.

DoC Classification	IoTFIM Concepts Percentage
Very Strong (DoC range: 100–70%)	Source of potential evidence, Investigators, Incident, data analysis methods, acquisition methods, evidence, forensic tools
Strong (69–50%)	Artifacts, IoT cloud platform, Companion App, Criminal activities, Backup, data collected, data acquisition, data analysis, timeline, Court of law
Moderate (49–30%)	IoT device-level forensic, volatile artifact, non-volatile artifact, volatile logs, non-volatile logs, device profile, victim, suspicious, IoT network forensic environments, network logs, IoT cloud forensic, environments, trusted evidence repository, cloud logs, Lab analysis, Authorization IoT Digital Investigation Process, IoT Device's Owner, personal device, non-personal device, Incident Response, seized device, Initializing Incident Detection, Hash values, Integrity, Documentation, Chain of Custody, Verification, Reconstruction of events
Mild (29–11%)	investigation planning, witness, Proof and Defense, Preparation
Very Mild (10–0%)	Decision, Investigation Closure

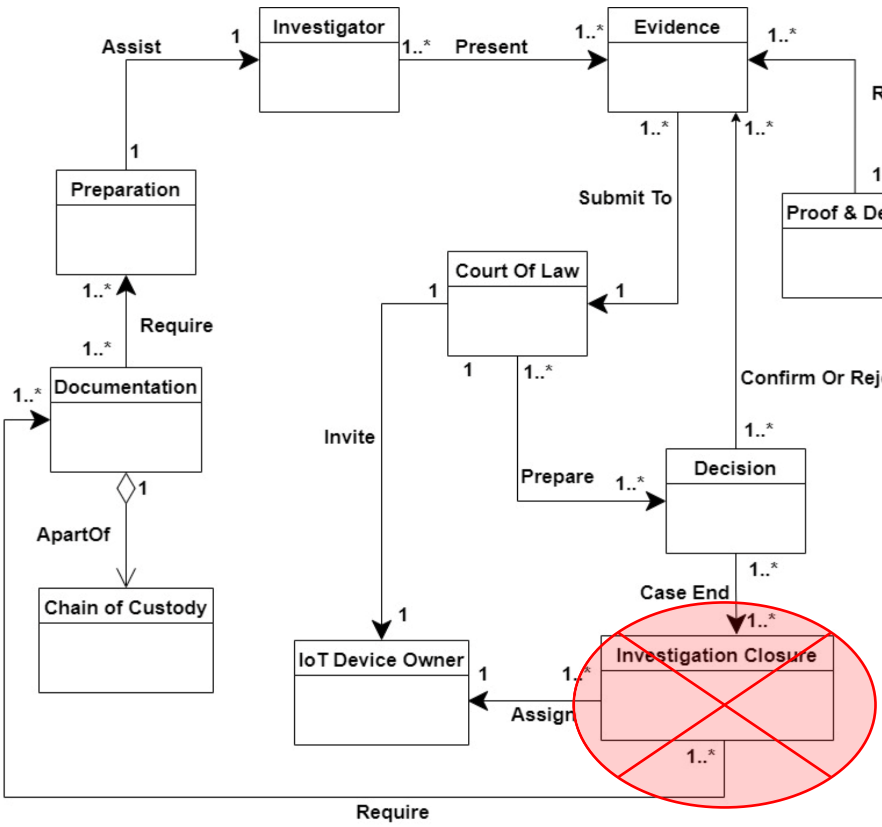

Figure 9. Presentation process in IoTFIM 1.2.

Figures 7 and 8 added new concepts in the IoT identification process and IoT Acquisition process in version IoTFM1.1: device profiles, witness, victim, and suspicious.

"Victim" means that it belongs to the person who suffered an offense. The owner of the device will, therefore, want an investigation of his or her device's data to be opened, while "suspect" means a device that may contain digital inculpatory or exculpatory evidence. Furthermore, the "witness", provides relevant digital evidence for the investigation but is neither the victim nor the suspect.

The IoTFIM 1.2 for four processes, IoT identification, IoT acquisition, IoT analysis, and presentation, are illustrated in Figures 10–13.

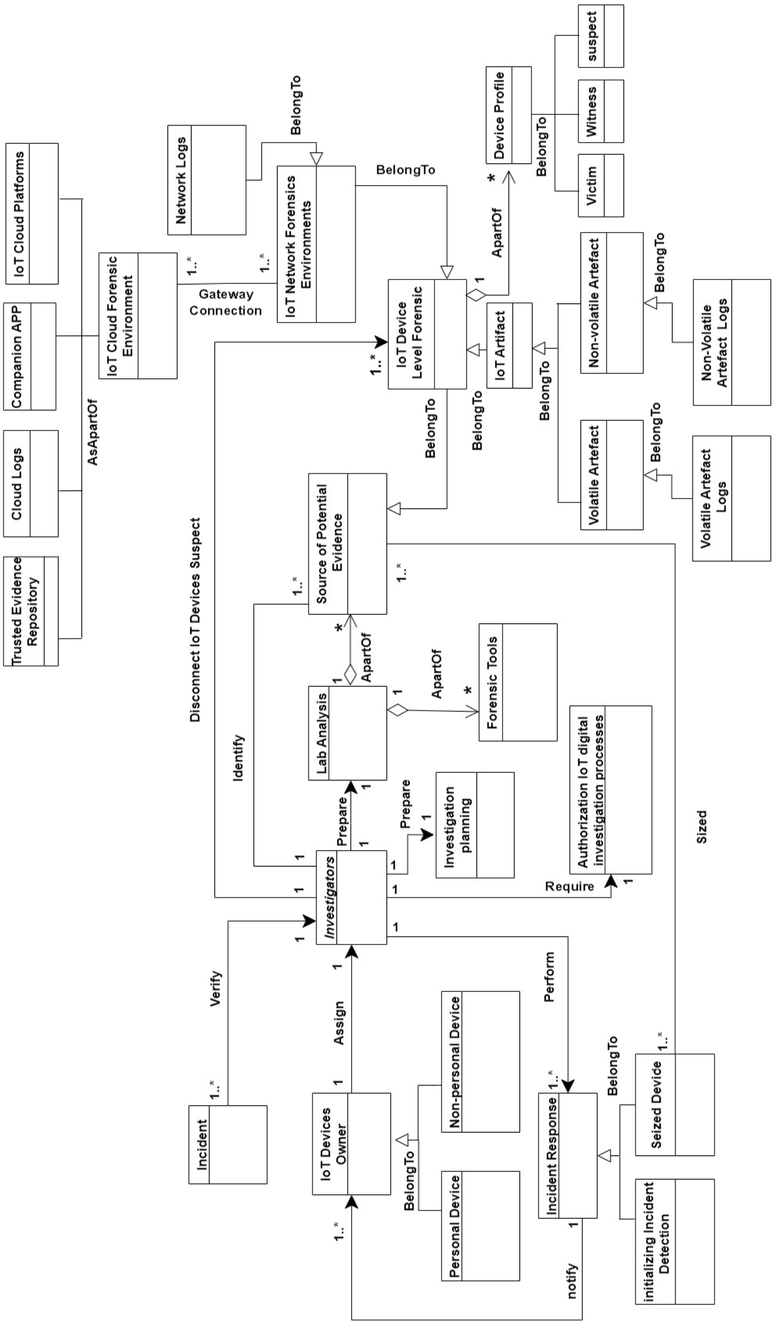

Figure 10. IoT identification process version IoTFIM 1.2.

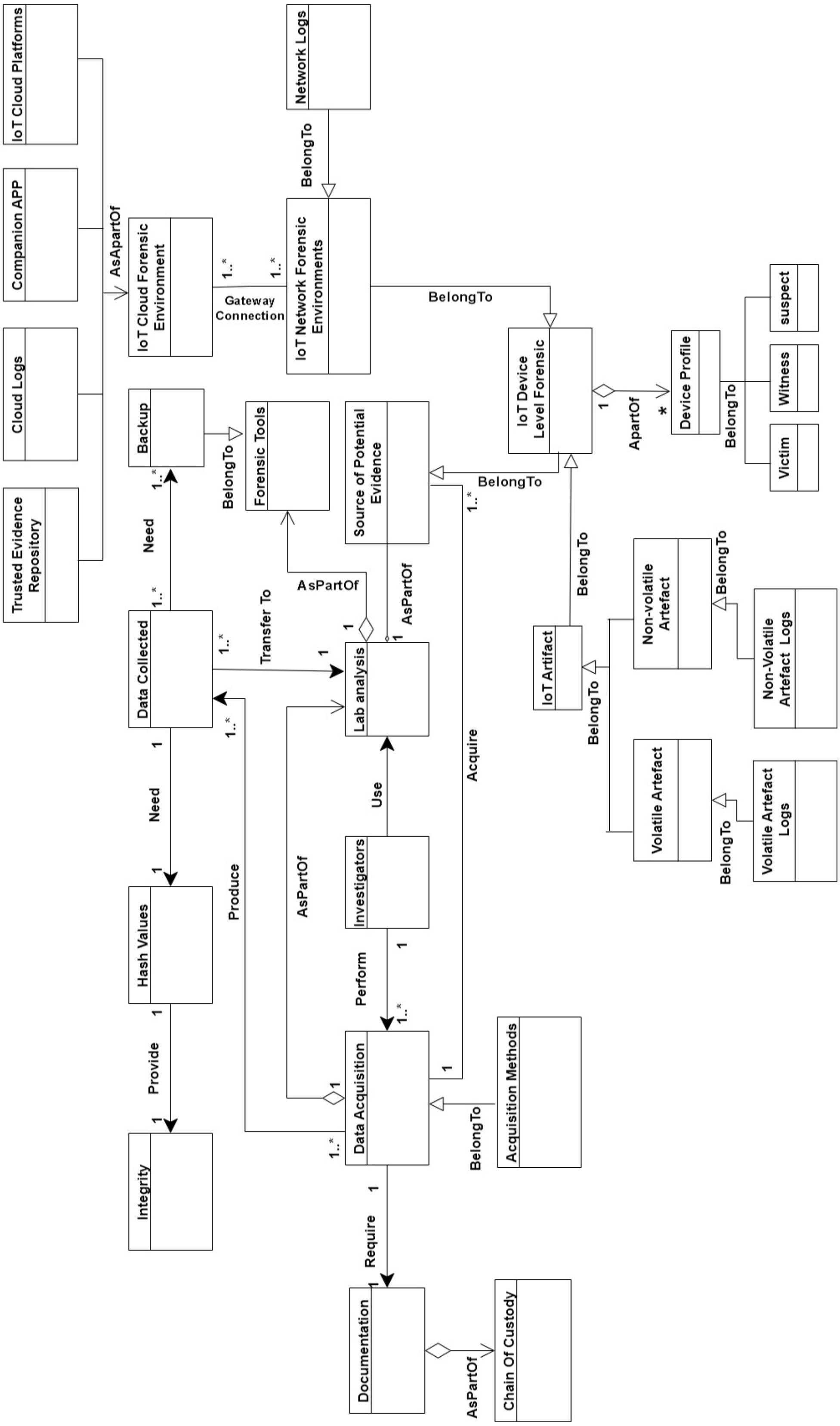

Figure 11. IoT Acquisition process version IoTFIM 1.2.

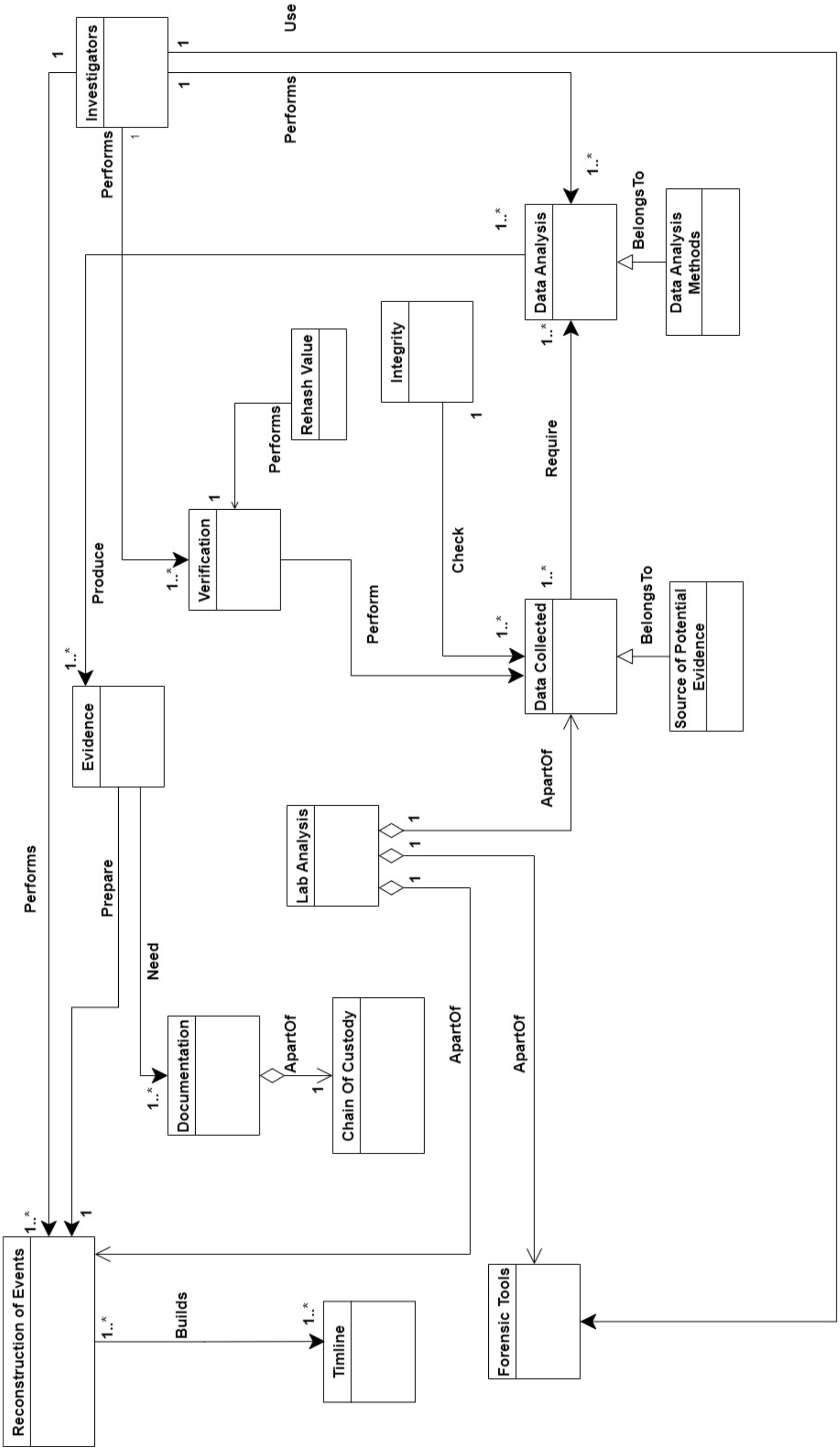

Figure 12. IoT Analysis process version IoTFIM 1.2.

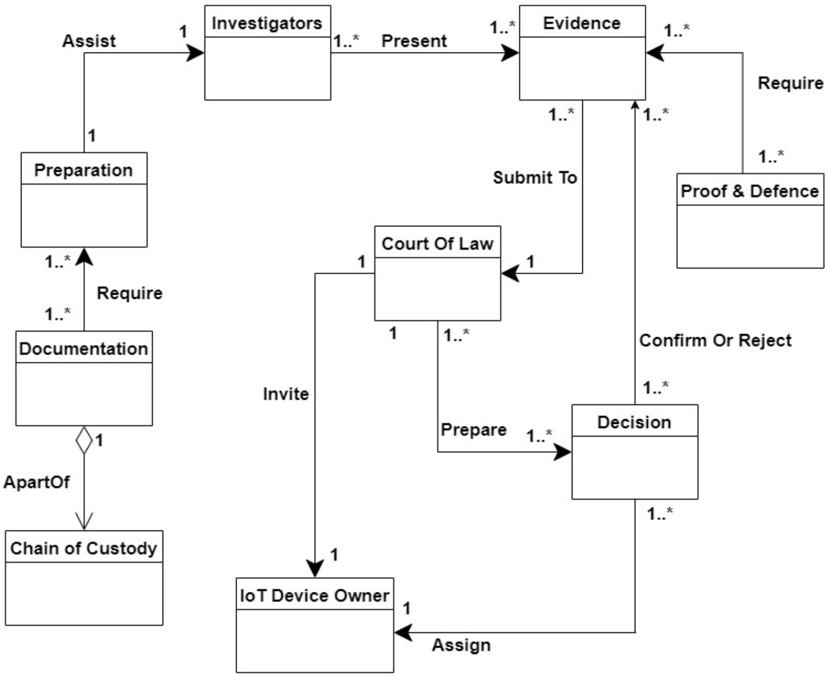

Figure 13. Presentation process version IoTFIM 1.2.

4.2. Discussions

In this study, we focused on the Investigation procedures that were extracted from Set1 models. Common IoTFI procedures emerged from this study. IoT identification, IoT acquisition, IoT analysis, and IoT presentation are the four (4) common processes in the IoTFI process, as shown by the recommended Common Investigation Processes, which are based on a thorough examination of the identified processes and models.In addition, this study identified a number of concepts that were identified and gathered from Set1 IoTFI models. On the other hand, these notions differ and have diverse meanings and synonyms. The semantic meaning (definitions) and concepts with comparable meanings or functions were sorted and organized into distinct and unique clusters. After that, the frequency feature was employed to choose the most prevalent concepts for each category. As a result, a total of 56 common concepts were chosen. Several concept definitions were reconciled using a reconciliation approach.

The IoTFIM was developed using the proposed 4 common processes and 56 common concepts. An IoT Forensic Investigation Metamodel called IoTFIM 1.0 was developed by using Set1 and then performing two validation techniques. The first validation is a comparison against other models using SetV1. The metamodel changed from IoTFIM 1.0 to IoTFIM 1.1. The second validation is a frequency-based selection using SetV2. The metamodel changed from IoTFIM 1.1 to IoTFIM 1.2. The first validation added four new concepts that were missing in Set1: device profile, suspects, witnesses, and victims from eight models in SetV1. The second validation used the Degree of Confidence (DoC) to look at how often concepts appeared in ten models in SetV2. The approach is to assess the value of individual concepts in the generated model and score each concept based on its frequency in IoTFIM 1.1. The concepts with a low score are reviewed and may be deleted. The presentation process deleted the concept of Investigation Closure and the relationship between Investigation Closure and Documentation because the result of the frequency is zero percent. This study discussed the prototype development and validation to demonstrate the applicability of the IoTFIM in the IoTFI domain.

5. Conclusions

The Investigation processes that were retrieved from Set1 models were chosen in this study. The common IoTFI processes were developed as a consequence of this investigation.

Based on a thorough look at the identified processes and models, the suggested Common Investigation Processes show that the IoTFI process has four (4) common processes: IoT identification, IoT acquisition, IoT analysis, and IoT presentation.

In addition, this study identified a number of concepts that were identified and gathered from Set1 IoTFI models. On the other hand, these notions differ and have diverse meanings and synonyms. After that, the frequency feature was employed to choose the most prevalent concepts for each category. As a result, a total of 56 common concepts were chosen. Several concept definitions were reconciled using a reconciliation approach.

The IoTFIM was developed using the proposed 4 common processes and 56 common concepts. An IoT Forensic Investigation Metamodel called IoTFIM 1.0 was developed by using Set1 and then performing two validation techniques. The first validation is a comparison against other models using SetV1. The metamodel changed from IoTFIM 1.0 to IoTFIM 1.1. The second validation is a frequency-based selection using SetV2. The metamodel changed from IoTFIM 1.1 to IoTFIM 1.2. The first validation added four new concepts that were missing in Set1: device profile, suspects, witnesses, and victims from eight models in SetV1. The second validation used Degree of Confidence (DoC) to look at how often concepts appeared in ten models in SetV2. The approach is to assess the value of individual concepts in the generated model and score each concept based on its frequency in IoTFIM 1.1. The concepts with a low score are reviewed and may be deleted. The presentation process deleted the concept of Investigation Closure and the relationship between Investigation Closure and Documentation because the result of the frequency is zero percent. This study discussed prototype development and validation to demonstrate the applicability of the IoTFIM in the IoTFI domain. The developed IoTFIM focused on Forensic Investigation models that deal with IoT Forensic Investigation Readiness. However, several research opportunities still exist and need further research, such as validating the proposed metamodel applicability through several case studies implementations. Furthermore, the study could enhance the developed IoTFIM by adding IoT forensic proactive investigation. Table 7 illustrates the acronyms of this study.

Table 7. List of acronyms.

No.	Nomenclature	Nomenclature Name
1	IoT	Internet of Things
2	IoTFIM	IoT Forensic Investigation Metamodel
3	DF	Digital Forensic
4	DFI	Digital Forensic Investigation
5	ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
6	PRoFIT	PRoFIT (Privacy-aware IoT-Forensic Model
7	CSP	Cloud service provider
8	JTAG	Joint Test Action Group
9	IoF	Internet-of-Forensics
10	SetV1	Set validation 1
11	SetV2	Set validation 2
12	JSON	JavaScript Object Notation
13	DEB	Digital evidence bag
14	API	Application Programming Interface
15	UML	Unified Modeling Language
16	DoC	Degree of Confidence
17	M2M	Machine-to-Machine
18	Z-wave	Wireless communication protocol
19	LTE	Long-term evolution
20	Wi-Fi	Wireless network
21	PLC	Power Line Communication
22	DFR	Digital Forensic Readiness
23	DFIF-IoT	Digital Forensic Investigation Framework
24	DNA	Digital Network Architecture
25	MAC	Media access control address
26	PC	Personal computer
27	Fitbit	A device that people can wear around their wrist to measure their daily steps, heart rate, and more

Author Contributions: Conceptualization, M.S., S.H.O., A.A.-d. and A.A.; methodology, M.S., S.H.O., M.D., A.A.-d., A.A., W.M.S.Y. and A.-H.M.E.; software, M.S., S.H.O. and M.D.; validation, all authors; formal analysis, M.S., S.H.O., A.A.-d., A.A., W.M.S.Y. and A.-H.M.E.; investigation, M.S., S.H.O., A.A.-d. and A.A.; resources, M.S., S.H.O., M.D., A.A.-d., A.A., W.M.S.Y. and A.-H.M.E.; data curation, M.S., S.H.O., M.D., A.A.-d., A.A., W.M.S.Y. and A.-H.M.E.; writing—original draft preparation, writing—review and editing, M.S., S.H.O., M.D., A.A.-d., A.A., W.M.S.Y. and A.-H.M.E.; visualization, M.S., S.H.O. and A.A.-d.; supervision, M.S. and S.H.O. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Concept Extraction

Table A1. Example of concepts extraction from Set1.

Model	Concepts	Total
[10]	Smart Transport, Smart Industry, Smart Health, Smart Living, Smart Energy, Smart Planet, Smart Cities, Smart Buildings, zone 1, zone 2, zone 3, Authorization, Planning, Warrant Obtained, Planning, Base Device Identification, Triage Examination, Fragile Evidence Zone, Server Cluster, Location/Sector, Structured Data, Unstructured Data, Chain of Custody, Proof and Defense, Archive and Storage, Machine-to-Machine (M2M) communication, Lab analysis, Data in the cloud, threats to privacy.	28
[39]	Universal data format, digital evidence bags (DEBs), Advanced Forensics Format (AFF4), forensic case, case loader, case creator, entities, parser matcher, parser pool, selector modules, tagger modules, schema loader module, visualization module, device ID, device name, action, value, time, start time, end time, last accessed time, last modified time, device metadata, case data, INTERPOL/EUROPOL cloud, File Parsing, schema recommendation, JSON files, data Analysis, Schema Application.	27
[31]	Companion App, Web interfaces, APIs, data available, IoT service platforms, correlational analysis, Device activation, Companion App download and device enrollment, identifying functions of devices, Experiment with the devices, identify function of device, experiment with the device, google home data, google home Hub setting, identify path and content of the acquired data, classify the useful data, identify the incidence, analyzed data, incidence response.	18
Internet of Things (IoT) Digital Forensic Investigation Model: Top–Down Forensic Approach Methodology [10]	Smart Transport, Smart Industry, Smart Health, Smart Living, Smart Energy, Smart Planet, Smart Cities, Smart Buildings, zone 1, zone 2, zone 3, Authorization, Planning, Warrant Obtained, Planning, Base Device Identification, Triage Examination, Fragile Evidence Zone, Server Cluster, Location/Sector, Structured Data, Unstructured Data, Chain of Custody, Proof and Defense, Archive and Storage, Machine-to-Machine (M2M) communication, Lab analysis, Data in the cloud, threats to privacy.	28

Table A1. *Cont.*

Model	Concepts	Total
A Generic Digital Forensic Investigation Framework for Internet of Things (IoT) [18]	Examining potential evidence, analyzing potential evidence, ISO/IEC27043: 2015 international standard, security techniques, incident investigation principles, Digital Investigation Processes, generic framework (DFIF-IoT), holistic framework (DFIF-IoT), IoT systems, IoT architectures, IoT domain model, IoT information model, IoT communication stack, Data layer, end-to-end layer, network layer, ID layer, link layer and physical layer, IoT evidence, potential security incident, IoT Scenario Definition, IoT evidence source identification, Planning Incident Detection, PDE collection, digital preservation, storage of potential evidence, VM images, VM logs, hypervisor error logs, activity logs, cloud carrier logs, database activity and application logs, cloud forensics, network forensics device-level forensics, potential acute attack logs, physical device, Initialization, acquisitive, investigative, Incident Detection, first response, planning and preparing for an investigation, PDE identification, collection, transportation, storage, Analysis of the collected evidence, potential incidents, Chain of Custody, Physical Investigation, Documentation, Obtain authorization, minimizing the cost, minimizing the time, law enforcement agencies, forensic practitioners.	55
An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I: A Theoretical Framework [5]	Digital evidence acquisition, digital evidence analysis, available network forensic methods, verified tools, verified methods, admissible digital evidence, log files, browsing history to data movements, digital files, social media activities, online transactions, Things of Interest Identification, LOS algorithm, zone 0, zone 1, zone 2, report on possible tools, digital evidence retrieval, time-relevance matter, produce backup copies, criminal activity, final report, auditing board, authorized members, risk alarm, data privacy laws, international agreements.	26
Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT) [29]	Artifacts of forensics, applications scenarios, Smart Home, Wearables, Smart City, cloud forensics, network forensics, WSN, WHAN, WPAN, WBAN, WLAN, Things Forensics, Evidence, Collection, Examination, Analysis, Reporting, data extraction, EEG, ECG, EMG, Blood Pressure sensors, health data, wireless body area network, vehicular digital system, Nest Smart system.	28
Toward an Integrated Digital Forensic Investigation Framework for an IoT-Based Ecosystem [10]	Analyze Potential Digital Evidence (PDE), ISO/IEC 27043: 2015 international standard, IoT Scenario Definition, IoT Evidence Source Identification, Planning Incident Detection, Potential Digital Evidence Collection, Digital Preservation, Storage of Potential Evidence, cloud forensics, network forensics (NF), device-level forensics (DLF), Initialization, Acquisitive and Investigative processes, interconnection, interoperability, smarter functionality, interconnected sensors, smart object, Things, Device Connectivity, Communication Network, Readiness Process Groups, IoT forensics, Digital Investigation Process, Concurrent Processes, IoT Management Platform, IoT Policy, IoT Standards and Protocols.	27
IoT Forensic A Digital Investigation Framework for IoT Systems [11]	IoT devices, systematic investigation, evidence of attack, interface layer, APIs, support function, content retrieval, Account, finger print collection, service layer, branded service, revenue model, portability, distribution model, SLA inspection, network layer, communities, social network, security, privacy, log analysis, sensing layer, device, sensor, smart object, media, cache and memory analysis, layered architecture, components of IoT ecosystems, possible forensic options, smart device, data storage, data collection, operation log, incident start time, end time.	31

Table A1. *Cont.*

Model	Concepts	Total
Adding Digital Forensic Readiness as a Security Component to The IoT Domain [30]	Smart environments, like healthcare, surveillance, energy systems, home appliances, industrial machines, smart grids and smart cities, ISO/IEC 27043: 2015, 27030: 2012 international standards, 27017: 2015 international standards, IoT environment, high-level of the architecture, hypothetical scenario, case scenario, planning processes group, scenario definition, identification of PDE sources, planning pre-incident collection, storage and handling of data representing PDE, planning pre-incident analysis of data representing PDE, Planning Incident Detection, defining system architecture, implementation processes group, implementing system architecture, implementing pre-incident collection, storage and handling of data representing PDE, implementing pre-incident analyses of data representing PDE, implementing Incident Detection, the assessment processes group, assessment of implementation, implementation of assessment results, Device Domain, Local Network Domain, Wide Area Network Domain, Service Enablement Domain, Applications And Data Domain, Enterprise Systems Domain, Machine-to-Machine (M2M) connectivity, send data, receive data, Internet Protocol (IP) addresses, Readiness guidelines, techniques of achieving forensic Readiness, proposed Readiness processes and reporting, IoT Intelligent Network (IoT-IN), IoT Operating System (IoT-OS), IoT Network Functionalities (IoT-NF), IoT Device Functionality (IoT-DF), IoT devices, initialization, acquisitive, investigative part, IoT Sensor Monitoring, IoT Device Monitoring, IoT Network Monitoring, Intrusion Detection Systems (IDS), False Alarm Detection and Notifications, Forensic logging, log parsing, log preservation, log storage, log analysis and log characterization, IoT Operating System, IoT Network Functionalities, IoT Device Functionalities.	59
Functional Requirements for Adding Digital Forensic Readiness as a Security Component in IoT Environments [13]	Physical objects and devices, embedded sensors, IP address for Internet connectivity, objects communications, unique identifiers, Human-to-Human (H2M), Human-to-Computer interaction (HCI), real-time monitoring, IoT environments, basic building blocks, Functional Requirements (FRs), forensic Readiness aspects, ISO/IEC 27043: 2015, IoT Requirements, Proactive Requirements, Extraction of digital evidence, parsing forensic logs, digital preservation, creation of Hash values, evidence storage, log analysis and characterization, Readiness report, Extract Digital Evidence (Logs), log extractor, preservation mechanism, Parsing Forensic Logs (PFL), Create Hash Values, log retrieval, Storage of Evidence, Log Analysis and Characterization, Forensic Readiness Report, Reconstruction of Events, proactive strategies, cloud forensic Readiness model, Possible Crime Scene Hypothesis, Investigation Closure.	35
Digital Forensic Investigation Framework for Internet of Things (IoT): A Comprehensive Approach [38]	Cloud Service Provider (CSP), network logs, IoT Based forensics, cloud forensics, network forensics, Device forensics, IoT Scenario Definition, Identification of Potential IoT Evidence Sources, smart cities, smart city, health devices, cloud services, smart grid, identified Planning, Pre-incident Detection and Collection, IoT based Pre-incident Detection, storage, handling of IoT data, data repository, forensic tools, data integrity, the large volume of data, data diversity, data duplication, high-speed data transmission, data extraction location, data storage on the network devices, data privacy, access to IP addresses, Forensic Monitoring Plane (FMP), forensic tools, network analysis tools, vulnerability assessment tools, network sniffing and packet analyzing tools, network scanning tools, and Network monitoring tools, physical devices, memory (RAM, ROM, or various secondary device), graphics, audio, video, image, files, other IoT devices, evidence storage, history of digital evidence, Application Programming Interface (API), Incident Detection, Initial Response, Planning, Preparation, Potential IoT Evidence Identification, Potential IoT Evidence Collection, Potential IoT Evidence Transportation, Storage of Potential IoT Evidence, IoT Evidence Examination and Analysis, Reporting, Presentation, Proof and Defense, Archive and Storage, Investigation Closure, authorities, users, owners information, Chain of Custody.	60

Table A1. *Cont.*

Model	Concepts	Total
How Do I Share My IoT Forensic Experience With the Broader Community? An Automated Knowledge Sharing IoT Forensic Platform [39]	Universal data format, digital evidence bags (DEBs), Advanced Forensics Format (AFF4), forensic case, case loader, case creator, entities, parser matcher, parser pool, selector modules, tagger modules, schema loader module, visualization module, device ID, device name, action, value, time, start time, end time, last accessed time, last modified time, device metadata, case data, INTERPOL/EUROPOL cloud, File Parsing, schema recommendation, JSON files, data analysis, Schema Application.	27
IoT Forensics: Amazon Echo as a Use Case [28]	Sensing layer, network layer, service layer, interface layer, specialized/customized tools, forensic tools, commercial forensic tools, offense classification stage, IoT as a target, IoT as a tool, IoT as a witness, acquired forensic artifacts, evidence repository, third parties, remote servers, nature of the offense, data acquisition methods, relevant laws, botnet attack, amazon echo, Define device space, Establish the device lifecycle, Establish access, Define data categories, Network access control, Identify the access to devices, middleware, file system, applications, application software development kit (SDK), data extraction tools/methods, manual, logical, hex dumping/JTAG, Chip-off, and micro-read, memory forensics, key evidence items, Live memory evidence extraction, volatile memory extraction, memory acquisition tools, anti-forensics (AF) techniques, timeline of activities, embedded files, Device related data, Connectivity, User data, Application data, other data, device time zone.	49
A Logging Model for Enabling Digital Forensics in IoT, in an Inter-connected IoT, Cloud Eco-systems. [40]	Record sufficient attributes and information, IoT event logging, data collection framework, specifying the log architecture, the parameters to log, log collection design stack, Unique IoT ID, physical identification, Geo-location, Timestamp, chain of events, Application ID/Session ID, embedded application, User Id, external application, Severity, Data, Business records, Operational data events, Error values, Start, stop, re-start events, Configuration data change, State change events, Security events, Authentication and authorization, IoT data and security violation events, Periodic object identification, Physical attack events, Compliance events, Re-certification events, IoT layer, Event layer, Protocol layer, Cloud layer, Application layer, Presentation layer.	34
Holistic Digital Forensic Readiness framework for IoT-enabled organizations [9]	IoT specific, ISO/IEC 27043, digital evidence, forensic data, Planning Process Group, Implementation Process Group, Assessment Process Group, Concurrent Processes, abstract level, organizational processes, data privacy and protection, Chain of Custody, diligence, authenticity, relevance, external organizational processes, internal processes, forensic policy, Reporting, nontechnical stakeholders, technical stakeholders, IoT data management cycle, data production, collection/ delivery, storage/archival, processing/integration, delivery, consumption, key data source, Digital Forensic Tools, Incident Analysis, detection and Monitoring, Integrity, Availability, Access control, auditability, IoT certificate authority (CA), encryption key manager, attribute manager, data transport layer security.	40
Smart Home Forensics—Data Analysis of IoT Devices [31]	Companion App, Web interfaces, APIs, data available, IoT service platforms, correlational analysis, Device activation, Companion App download and device enrollment, Identifying functions of devices, Experiment with the devices, identify function of device, experiment with the device, google home data, google home Hub setting, identify path and content of the acquired data, classify the useful data, identify the incidence, analyzed data, incidence response.	18

Appendix B. Proposed Common Concepts

Table A2. Common concepts used in Appendix B.

Common Concept Suggestion	Concepts	Frequency	Definition	Generality
Source of potential evidence	Source of evidence	3	1	1
	potential digital evidence	1	1	1
	digital evidence	1	1	1
IoT Device's Owner	IoT Device's Owner	2	1	1
	Owner	1	1	1
	Ownership	1	1	1

Table A2. *Cont.*

Common Concept Suggestion	Concepts	Frequency	Definition	Generality
IoT Device-Level Forensics	IoT device-level forensics	6	1	1
IoT network forensic environments	IoT network forensic environments	4	1	1
	Network Forensic	1	0	1
	Network layer	2	1	1
Volatile artifact logs	Device level memory	1	1	1
	artifacts logs	1	1	1
	devices logs	1	1	1
	IoT-based nodes Logs	1	1	1
	Physical devices data	1	1	1
Network logs	Network logs	6	1	1
	Logs attack	1	1	1
Non-Volatile artifact Logs	non-volatile IoT artifact logs	1	1	1
	artifacts logs	1	1	1
	devices logs	0	1	1
	IoT-based nodes Logs	1	1	1
	physical devices data	1	1	1
	device level caches	1	1	1
Cloud logs	Cloud logs	4	1	1
	IoT-based nodes Logs	1	1	1
Forensic tools	Forensic tools	3	1	1
	specialized/ customized tools	1	1	1
Incident	Incident	4	1	1
Investigators	Investigators	3	1	1
	authorized Digital Forensic	1	1	1
IoT cloud forensic Environments	Cloud forensic	3	1	1
IoT artifacts	IoT artifacts	2	1	1
Companion App	Companion App	2	1	1
	Application Programming Interface	1	1	1
Lab analysis	Lab analysis	2	0	1
Trusted evidence repository	Trusted evidence repository	1	1	1
	Trusted repository	1	1	1
	encrypted evidence repository	1	1	1
Non-personal device	Non-personal device	6	0	1
Personal devices	Personal devices	11	0	1
Incident Response	Incident Response	8	1	1
	Initial Response	1	1	1
Seized device	seized device	3	1	1
	Capture	2	1	1
	Seizure	1	1	1
Authorization IoT Digital Investigation Processes	Authorization	4	1	1
	Obtain authorization	1	1	1
Initializing Incident Detection	initializing Incident Detection	1	1	1
	initial trace of the evidence	1	1	1
IoT cloud platforms	IoT cloud platforms	2	1	1
	IoT management platforms	2	1	1
Investigation planning	Investigation planning	3	1	1
	Planning for incident	1	1	1
	Planning group	1	1	1
	Planning Pre-incident Detection and Collection	1	1	1
Backup	Backup	3	1	1
	retrieving the data	1	1	1
Integrity	Integrity	4	1	1
Hash value	Hash value	2	1	1
	Hashes	1	1	1

Table A2. *Cont.*

Common Concept Suggestion	Concepts	Frequency	Definition	Generality
Data collected	Data collected	4	1	1
	Evidence collected	3	1	1
Chain of Custody	Chain of Custody	7	1	1
Documentation	Documentation	2	1	1
Data acquisition	data acquisition	4	1	1
	potential digital evidence collection	1	1	1
	digital evidence acquisition	1	1	1
Acquisition methods	physical methods	1	1	1
	memory data extraction	1	1	1
Timeline	Timeline	3	1	1
Reconstruction of events	Reconstruction of events	3	1	1
Verification	Verification	4	1	1
evidence	Evidence	4	1	1
Data analysis	Data analysis	4	1	1
	Incident Analysis	1	1	1
	Digital Forensic analysis	1	1	1
Data analysis methods	Log analysis	2	1	1
	History analysis	2	1	1
	user behaviors analysis	1	1	1
Preparation	Preparation	4	1	1
Court of law	Court of law	6	1	1
	Court	1	1	1
Proof and Defense	Proof and Defense	2	0	1
	Proof	2	1	1
Decision	Decision	1	1	1
Investigation Closure	Investigation Closure	2	1	1

Appendix C. Relationships between Concepts

Table A3. IoT Identification Process Relationships.

Concept 1	Relation Type	Relation Name	Concept 2	C1	C2
IoT device-level forensic	Specialization/ Generalization	BelongTo	Source of potential evidence	*	1
IoT device-level forensic	Association	M2M communication	IoT network forensic environments	1..*	1..*
IoT artifacts	Specialization/ Generalization	BelongTo	IoT device-level forensic	*	1
Volatile artifact	Specialization/ Generalization	BelongTo	IoT artifacts	*	1
Non-volatile artifact	Specialization/ Generalization	BelongTo	IoT artifacts	*	1
Volatile artifact logs	Specialization/ Generalization	BelongTo	Volatile artifact	*	1
Non-volatile artifact logs	Specialization/ Generalization	BelongTo	Non-volatile artifact	*	1
Network logs	Specialization/ Generalization	BelongTo	IoT network forensic environments	*	1
IoT network forensic environment	Association	Gateway connection	IoT cloud forensic environment	1..*	1..*
Trusted evidence repository	aggregation	AsApartOf	IoT cloud forensic environment	1	1
Companion App	aggregation	AsApartOf	IoT cloud forensic environment	1..*	1
Cloud logs	aggregation	AsApartOf	IoT cloud forensic environment	1..*	1

Table A3. *Cont.*

Concept 1	Relation Type	Relation Name	Concept 2	C1	C2
Cloud platforms	aggregation	AsApartOf	IoT cloud forensic environment	1	1
Source of potential evidence	Association	sizes	Sized devices	1..*	1
Investigators	Association	Identify	Source of potential evidence	1..*	1..*
Forensic tools	Specialization/ Generalization	BelongTo	Lab analysis	1..*	1
Investigators	Association	Prepare	Lab analysis	1	1..*
Source of potential evidence	aggregation	AsApartOf	Lab analysis	1	1..*
Investigators	Association	Verify	Incident	1..*	1..*
Investigators	Association	Perform	Incident Response	1..*	1..*
Investigators	Association	Require	Authorization IoT Digital Investigation Processes	1..*	1
Investigators	Association	Prepare	Investigation planning	1	1..*
IoT Device's Owner	Association	Assign	investigators	1	1
Personal Device	aggregation	AsApartOf	IoT device's owner	1	1
Non-Personal Device	aggregation	AsApartOf	IoT device's owner	1	1
Seized device	Specialization/ Generalization	BelongTo	Incident Response	*	1
Initializing Incident Detection	Specialization/ Generalization	BelongTo	Incident Response	*	1
Investigators	Association	Disconnect IoT Devices Suspect	IoT device-level forensic	1..*	1..*
IoT Device's Owner	Association	Notify	Incident Response	1..*	1..*

Table A4. IoT Acquisition Process Relationships.

Concept 1	Relation Type	Relation Name	Concept 2	C1	C2
IoT device-level forensic	Specialization/ Generalization	BelongTo	Source of potential evidence	*	1
IoT device-level forensic	Association	M2M communication	IoT network forensic environments	1..*	1..*
IoT artifacts	Specialization/ Generalization	BelongTo	IoT device-level forensic	*	1
Volatile artifact	Specialization/ Generalization	BelongTo	IoT artifacts	*	1
Non-volatile artifact	Specialization/ Generalization	BelongTo	IoT artifacts	*	1
Volatile artifact logs	Specialization/ Generalization	BelongTo	Volatile artifact	*	1
Non-volatile artifact logs	Specialization/ Generalization	BelongTo	Non-volatile artifact	*	1
Network logs	Specialization/ Generalization	BelongTo	IoT network forensic environments	*	1
IoT network forensic environment	Association	Gateway connection	IoT cloud forensic environment	1..*	1..*
Trusted evidence repository	aggregation	AsApartOf	IoT cloud forensic environment	1	1
Companion App	aggregation	AsApartOf	IoT cloud forensic environment	1..*	1
Cloud logs	aggregation	AsApartOf	IoT cloud forensic environment	1..*	1

Table A4. *Cont.*

Concept 1	Relation Type	Relation Name	Concept 2	C1	C2
Cloud platforms	aggregation	AsApartOf	IoT cloud forensic environment	1	1
Backup	Specialization/ Generalization	BelongTo	Forensic tools	*	1
Backup	Association	need	Data collected	1..*	1
Data collected	Association	Transfer to	Lab analysis	1..*	1
Data collected	Association	need	Hash value	1..*	1
Hash value	Association	provide	Integrity	1	1
Data acquisition	aggregation	AsApartOf	Lab analysis	1	1..*
Investigators	Association	performs	Data acquisition	1..*	1..*
Data acquisition	Association	Acquire	Source of potential evidence	1..*	1..*
Acquisition methods	Specialization/ Generalization	BelongTo	Data acquisition	*	1
Data acquisition	Association	Require	Documentation	1..*	1..*
Chain of Custody	aggregation	AsApartOf	Documentation	1..*	1
Forensic tools	Specialization/ Generalization	BelongTo	Lab analysis	1..*	1
Data acquisition	Association	produce	Data collected	1..*	1..*

Table A5. IoT Analysis process Relationships.

Concept 1	Relation Type	Relation Name	Concept 2	C1	C2
Data collected	aggregation	AsApartOf	Forensic lab	1..*	1
Data collected	Association	Check	Integrity	1..*	1
Source of potential evidence	Specialization/ Generalization	BelongTo	Data collected	*	1
Data analysis	Association	require	Data collected	1	1..*
Data analysis methods	Specialization/ Generalization	BelongTo	Data analysis	*	1
Investigators	Association	Perform	Verification	1..*	1
Verification	Association	perform	Data collected	1..*	1
investigators	Association	use	Forensic tools	1..*	1..*
investigators	Association	perform	Reconstruction of events	1..*	1
Reconstruction of events	Association	build	Timeline	1	1
Reconstruction of events	aggregation	AsApartOf	Forensic lab	1	1
Chain of Custody	aggregation	AsApartOf	Documentation	1	1
evidence	Association	need	Documentation	1..*	1..*
evidence	Association	prepare	Reconstruction of events	1..*	1
Data analysis	Association	produce	evidence	1..*	1..*
investigators	Association	perform	Data analysis	1..*	1..*
Verification	Association	perform	Re-hashed	1..*	1
Forensic tools	Specialization/ Generalization	BelongTo	Lab analysis	1..*	1

Table A6. Presentation process Relationships.

Concept 1	Relation Type	Relation Name	Concept 2	C1	C2
Chain of Custody	aggregation	AsApartOf	Documentation	1	1
Preparation	Association	require	Documentation	1	1
Preparation	Association	assist	investigators	1	1..*
Investigators	Association	present	evidence	1..*	1..*
Evidence	Association	Submit to	Court of law	1..*	1
Evidence	Association	require	Proof and Defense	1..*	1..*
Court of law	Association	prepare	decision	1	1
Court of law	Association	invite	IoT device owner	1	1
Decision	Association	Case end	Investigation Closure	1	1
Investigation Closure	Association	require	Documentation	1	1
Decision	Association	Confirm or reject	evidence	1..*	1..*
Investigation Closure	Association	assign	IoT device owner	1..*	1

References

1. Kannus, K.; Ilvonen, I. Future prospects of cyber security in manufacturing: Findings from a Delphi study. In Proceedings of the 51st Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 3–6 January 2018. [CrossRef]
2. Lutta, P.; Sedky, M.; Hassan, M. The Forensic Swing of Things: The Current Legal and Technical Challenges of IoT Forensics. 2020. Available online: https://www.researchgate.net/publication/341655454_The-Forensic-Swing-of-Things-The-Current-Legal-and-Technical-Challenges-of-IoT-Forensics (accessed on 1 December 2022).
3. Saleh, M.A.; Othman, S.H.; Al-Dhaqm, A.; Al-Khasawneh, M.A. Common Investigation Process Model for Internet of Things Forensics. In Proceedings of the 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE); 2021. [CrossRef]
4. Conti, M. *Internet of Things Security and Forensics: Challenges and Opportunities*; Elsevier: Amsterdam, The Netherlands, 2018. [CrossRef]
5. Al-Masri, E. A fog-based digital forensics investigation framework for IoT systems. In Proceedings of the 2018 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, USA, 21–23 September 2018. [CrossRef]
6. Alhir, S.S. Understanding the model driven architecture (MDA). *Methods Tools* **2003**, *11*, 17–24.
7. Aljahdali, A.; Aldissi, H.; Banafee, S.; Sobahi, S.; Nagro, W. IoT Forensic models analysis. *Romanian J. Inf. Technol. Autom. Control* **2021**, *31*, 21–34. [CrossRef]
8. Chavez, N. Arkansas Judge Drops Murder Charge in Amazon Echo Case. 2017. Available online: https://apnews.com/article/f66ee9c4e2514d4789a50324860a9c29 (accessed on 1 December 2022).
9. Hauser, C. In connecticut murder case, a fitbit is a silent witness. *The New York Times*, 27 April 2017.
10. Al-Dhaqm, A.; Adeyemi, I.R.; Kebande, V.R.; Razak, S.A.; Grispos, G.; Choo, K.-K.R.; AL-rimy, B.A.; Alsewari, A.A. Digital Forensics Subdomains: The State of the art and Future Directions. *IEEE Access* **2021**, *9*, 152476–152502. [CrossRef]
11. Oriwoh, E.; Jazani, D.; Epiphaniou, G.; Sant, P. Internet of things forensics: Challenges and approaches. In Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, Austin, TX, USA, 20–23 October 2013. [CrossRef]
12. Kebande, V.R.; Ray, I. A generic digital forensic investigation framework for internet of things (iot). In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016. [CrossRef]
13. Nieto, A.; Rios, R.; Lopez, J. A methodology for privacy-aware iot-forensics. In Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, Australia, 1–4 August 2017. [CrossRef]
14. Bouchaud, F.; Grimaud, G.; Vantroys, T. IoT Forensic: Identification and classification of evidence in criminal investigations. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018. [CrossRef]
15. Islam, M.J.; Ray, I. Digital forensic investigation framework for internet of things (IoT): A Comprehensive Approach. In Proceedings of the 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), Dhaka, Bangladesh, 3–5 May 2019. [CrossRef]
16. Scheidt, N.; Adda, M. Identification of IoT Devices for Forensic Investigation. In Proceedings of the 2020 IEEE 10th International Conference on Intelligent Systems (IS), Varna, Bulgaria, 28–30 August 2020. [CrossRef]
17. Kang, S.; Kim, S.; Kim, J. Forensic analysis for IoT fitness trackers and its application. *Peer-to-Peer Netw. Appl.* **2020**, *13*, 564–573. [CrossRef]
18. Kim, S.; Jo, W.; Lee, J.; Shon, T. AI-enabled device digital forensics for smart cities. *J. Supercomput.* **2021**, *78*, 3029–3044. [CrossRef]
19. Kumar, G.; Saha, R.; Lal, C.; Conti, M. Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Gener. Comput. Syst.* **2021**, *120*, 13–25. [CrossRef]
20. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design science in information systems research. *MIS Q.* **2004**, *28*, 75–105. [CrossRef]

21. Atlam, H.F.; Alenezi, A.; Alassafi, M.O. Blockchain with Internet of Things: Benefits, challenges, and future directions. *Int. J. Intell. Syst. Appl. (IJISA)* **2018**, *10*, 40–48. [CrossRef]
22. Ali, A.; Razak, S.A.; Othman, S.H.; Mohammed, A.; Saeed, F. A metamodel for mobile forensics investigation domain. *PLoS ONE* **2017**, *12*, e0176223. [CrossRef]
23. Othman, S.H.; Beydoun, G.; Sugumaran, V. Development and validation of a Disaster Management Metamodel (DMM). *Inf. Process. Manag.* **2014**, *50*, 235–271. [CrossRef]
24. Harbawi, M.; Varol, A. An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. In Proceedings of the 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, Romania, 26–28 April 2017. [CrossRef]
25. Zia, T.; Liu, P.; Han, W. Application-specific digital forensics investigative model in internet of things (iot). In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–1 September 2017. [CrossRef]
26. Kebande, V.R.; Malapane, S.M.G.; Kigwana, I.; Karie, N.M. Towards an integrated digital forensic investigation framework for an IoT-based ecosystem. In Proceedings of the 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), Xi'an, China, 17–19 August 2018. [CrossRef]
27. Sathwara, S.; Dutta, N.; Pricop, E. IoT Forensic A digital investigation framework for IoT systems. In Proceedings of the 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 28–30 June 2018. [CrossRef]
28. Kebande, V.R.; Karie, N.M.; Venter, H.S. Adding Digital Forensic Readiness as a Security Component to the IoT Domain. 2018. Available online: http://hdl.handle.net/2263/66602 (accessed on 1 December 2022).
29. Kebande, V.R.; Karie, N.M.; Venter, H.S. Functional Requirements for Adding Digital Forensic Readiness as a Security Component in Iot Environments. 2018. Available online: http://hdl.handle.net/2263/66569 (accessed on 1 December 2022).
30. Zhang, Z.; Ye, N. Locality preserving multimodal discriminative learning for supervised feature selection. *Knowl. Inf. Syst.* **2011**, *27*, 473–490. [CrossRef]
31. Li, S. IoT forensics: Amazon echo as a use case. *IEEE Internet Things J.* **2019**, *6*, 6487–6497. [CrossRef]
32. Pichan, A. A Logging Model for Enabling Digital Forensics in IoT, in an Inter-connected IoT, Cloud Eco-systems. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020. [CrossRef]
33. Kebande, V.R.; Mudau, P.; Adeyemi, I.R.; Venter, H.S. Holistic digital forensic readiness framework for IoT-enabled organizations. *Forensic Sci. Int. Rep.* **2020**, *2*, 100117. [CrossRef]
34. Kim, S.; Park, M.; Lee, S.; Kim, J. Smart Home Forensics—Data Analysis of IoT Devices. *Electronics* **2020**, *9*, 1215. [CrossRef]
35. Chi, H.; Aderibigbe, T.; Granville, B.C. A framework for IoT data acquisition and forensics analysis. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018. [CrossRef]
36. Dawson, L.; Akinbi, A. Challenges and opportunities for wearable IoT forensics: TomTom Spark 3 as a case study. *Forensic Sci. Int. Rep.* **2020**, *3*, 100198. [CrossRef]
37. Sandvik, J.-P. Coffee forensics—Reconstructing data in IoT devices running Contiki OS. *Digit. Investig.* **2021**, *37*, 301188. [CrossRef]
38. Umamaheswari, K. Botnet attack investigation on Geography of Things (GoT) using INSPECT approach. *INFOCOMP J. Comput. Sci.* **2020**, *19*. Available online: https://infocomp.dcc.ufla.br/index.php/infocomp/article/view/779 (accessed on 1 December 2022).
39. Akinbi, A.; Berry, T. Forensic Investigation of Google Assistant. *SN Comput. Sci.* **2020**, *1*, 272. [CrossRef]
40. Hilgenberg, A. Digital Forensic Investigation of Internet of Thing Devices: A Proposed Model and Case Studies. In *Cyber and Digital Forensic Investigations*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 31–49. [CrossRef]
41. Raman, J.A.; Varadharajan, V. HoneyNetCloud investigation model, a preventive process model for IoT forensics. *Ingénierie Syst. Inf.* **2021**, *26*, 319–327. [CrossRef]
42. Gudlur, V.V.R. Industrial Internet of Things (IIoT) of Forensic and Vulnerabilities. *Int. J. Recent Technol. Eng.* **2020**. [CrossRef]
43. Castelo Gómez, J.M.; Mondéjar, J.C.; Gómez, J.R.; Martínez, J.L. A context-centered methodology for IoT forensic investigations. *Int. J. Inf. Secur.* **2021**, *20*, 647–673. [CrossRef]
44. Salamh, F.E. A Forensic Analysis of Home Automation Devices (FAHAD) Model: Kasa Smart Light Bulb and Eufy Floodlight Camera as Case Studies. *Int. J. Cyber Forensics Adv. Threat. Investig.* **2021**, *1*, 18–26. [CrossRef]
45. Hutchinson, S.; Yoon, Y.H.; Shantaram, N.; Karabiyik, U. Internet of Things Forensics in Smart Homes: Design, Implementation, and Analysis of Smart Home Laboratory. In Proceedings of the 2020 ASEE Virtual Annual Conference Content Access, Virtual, 22–26 June 2020. [CrossRef]
46. Yankson, B.; Iqbal, F.; Hung, P.C.K. 4P based forensics investigation framework for smart connected toys. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual, Ireland, 25–28 August 2020. [CrossRef]
47. Meffert, C.; Clark, D.; Baggili, I.; Breitinger, F. Forensic State Acquisition from Internet of Things (FSAIoT) A general framework and practical approach for IoT forensics through IoT device state acquisition. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–1 September 2017. [CrossRef]
48. Poernomo, I. A Type Theoretic Framework for Formal Metamodelling. In *Architecting Systems with Trustworthy Components*; Reussner, R.H., Stafford, J.A., Szyperski, C.A., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2006; Volume 3938. [CrossRef]

49. Bermell-Garcia, P. A Metamodel to Annotate Knowledge Based Engineering Codes as Enterprise Knowledge Resources. 2007. Available online: http://hdl.handle.net/1826/3169 (accessed on 1 December 2022).
50. Driss, M.; Aljehani, A.; Boulila, W.; Ghandorh, H.; Al-Sarem, M. Servicing your requirements: An fca and rca-driven approach for semantic web services composition. *IEEE Access* **2020**, *8*, 59326–59339. [CrossRef]
51. Sargent, R.G. Verification and validation of simulation models. In Proceedings of the 2010 Winter Simulation Conference, Baltimore, MD, USA, 5–8 December 2010. [CrossRef]
52. Driss, M.; Hasan, D.; Boulila, W.; Ahmad, J. Microservices in IoT security: current solutions, research challenges, and future directions. *Procedia Comput. Sci.* **2021**, *192*, 2385–2395. [CrossRef]
53. Hasan, D.; Driss, M. SUBLμME: Secure Blockchain as a Service and Microservices-based Framework for IoT Environments. In Proceedings of the 2021 IEEE/ACS 18th International Conference on Computer Systems and Applications (AICCSA), Tangier, Morocco, 30 November–3 December 2021; pp. 1–9. [CrossRef]
54. Khan, M.A.; Khan Khattk, M.A.; Latif, S.; Shah, A.A.; Ur Rehman, M.; Boulila, W.; Driss, M.; Ahmad, J. Voting classifier-based intrusion detection for iot networks. *Adv. Intell. Syst. Comput.* **2022**, *1399*, 313–328. [CrossRef]
55. Atitallah, S.B.; Driss, M.; Almomani, I. A Novel Detection and Multi-Classification Approach for IoT-Malware Using Random Forest Voting of Fine-Tuning Convolutional Neural Networks. *Sensors* **2022**, *22*, 4302. [CrossRef]
56. Driss, M.; Almomani, I.; Ahmad, J. A federated learning framework for cyberattack detection in vehicular sensor networks. *Complex Intell. Syst.* **2022**, *8*, 1–15 [CrossRef]
57. Rahayu, J.W.; Chang, E.; Dillon, T.S.; Taniar, D. A methodology for transforming inheritance relationships in an object-oriented conceptual model to relational tables. *Inf. Softw. Technol.* **2000**, *42*, 571–592. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.