applied sciences

MDPI

Article

Smart Digital Forensic Readiness Model for Shadow IoT Devices

Funmilola Ikeolu Fagbola * and Hein S. Venter

Digital Forensic Science Research Group, Department of Computer Science, University of Pretoria, Pretoria 0002, South Africa; hventer@cs.up.ac.za

* Correspondence: u20732865@tuks.co.za

Abstract: Internet of Things (IoT) is the network of physical objects for communication and data sharing. However, these devices can become shadow IoT devices when they connect to an existing network without the knowledge of the organization's Information Technology team. More often than not, when shadow devices connect to a network, their inherent vulnerabilities are easily exploited by an adversary and all traces are removed after the attack or criminal activity. Hence, shadow connections pose a challenge for both security and forensic investigations. In this respect, a forensic readiness model for shadow device-inclusive networks is sorely needed for the purposes of forensic evidence gathering and preparedness, should a security or privacy breach occur. However, the hidden nature of shadow IoT devices does not facilitate the effective adoption of the most conventional digital and IoT forensic methods for capturing and preserving potential forensic evidence that might emanate from shadow devices in a network. Therefore, this paper aims to develop a conceptual model for smart digital forensic readiness of organizations with shadow IoT devices. This model will serve as a prototype for IoT device identification, IoT device monitoring, as well as digital potential evidence capturing and preservation for forensic readiness.

Keywords: IoT forensics; shadow IoT devices; digital forensic readiness; potential digital evidence

Citation: Fagbola, F.I.; Venter, H.S. Smart Digital Forensic Readiness Model for Shadow IoT Devices. *Appl. Sci.* **2022**, *12*, 730. https://doi.org/10.3390/app12020730

Academic Editors: Gianni Pantaleo and Pierfrancesco Bellini

Received: 1 November 2021
Accepted: 30 December 2021
Published: 12 January 2022

1. Introduction

Internet of Things (IoT) has introduced a vast number of smart 'things' or 'devices' that support various applications, services and platforms. IoT offers a wide range of opportunities to various business sectors and these have a huge impact on society and modern-day interactions. IoT furthermore aims to introduce intelligent collaborations and communications among devices, systems and humans through the use of the internet, different protocols and technologies [1]. For instance, many countries are now seamlessly adopting and integrating IoT solutions into their existing critical health infrastructures for the monitoring, tracking, detection and prevention of the COVID-19 disease [2]. Physically connected thermometers, body temperature sensors, smart wearables, smart clothing and IoT buttons are some of the IoT devices that help provide patients with significant care so they can recover more quickly. Despite having brought ease and convenience by its sensitivity to human needs and digitalization, the high rate of IoT acceptance into the various domains of wellbeing and life has resulted in a huge platform for attacks, threats and security concerns [1,3]. New concerns about the field of forensics have also emerged with the proliferation of IoT and its activities [4,5].

Furthermore, IoT devices such as IP cameras, thermostats, fitness trackers, and wearables can become so-called 'shadow' IoT devices if they use their data link communication privileges to connect to any network, without the prior knowledge of the network administrator. Hence, shadow IoT devices are IoT devices that have the ability to join, interact, perform some activities as well as leave the network without being noticed by the network administrator. Such devices may or may not introduce vulnerabilities or loopholes in a

network. When they do this, attackers or adversaries could exploit them to carry out their criminal activities. According to [6], the varying activities of IoT devices may provide potential evidence for a forensic investigation, although, more often than not, their activities are short-lived and disappear soon after gaining access to the network. These short-lived activities can introduce security breaches, privacy issues as well as crimes that are difficult to trace in forensic investigations, since it is difficult to gather evidence from a shadow IoT device if it is no longer connected to the network. Therefore, the incorporation of digital forensic readiness in such networks is inevitable for the monitoring of shadow IoT devices and their activities.

Conventional digital forensic readiness approaches are not suitable for IoT devices as they are light-weight and resource-constrained. Digital forensic processes are suitable for conventional devices such as computers, servers and smartphones, but IoT forensics needs to counter a far more extensive attack surface compared to conventional digital forensics [7]. For example, numerous shadow IoT devices interact with public interfaces, which makes them highly susceptible to malicious infestation and can become a security trap to enterprise networks. Shadow IoT devices generate vast amounts of digital data and records that become untraceable once they disconnect from the enterprise network. Such digital data and records might be important digital evidence when an unwanted incident occurs, but when the shadow IoT devices are not connected anymore, there is no way to acquire the necessary digital evidence. The preservation of such digital evidence is vital for a digital forensic investigation.

The contributions of the paper are as follows. This work addresses the challenge of shadow IoT device inclusion in a network by identifying and monitoring shadow IoT device traffic, features and behaviour. It further presents a digital forensic readiness model applicable to organizations with shadow IoT devices. Potential sources of digital evidence that are applicable to IoT networks are also identified in this study. In addition, this paper presents mechanisms on how to capture potential sources of digital evidence within an IoT environement. This paper poses two research questions:

RQ1: What are the risks that shadow IoT devices present to an enterprise network?

RQ2: What are the limitations of existing work in the area of IoT digital forensic readiness?

The first research question (RQ1) was addressed via a review of the risks that shadow IoT devices present to the enterprise network. RQ2 was addressed by a brief survey on existing works in the area of IoT forensics and their limitations in terms of capturing and preserving digital data and records for forensic readiness purposes in the IoT ecosystem (see Section 2). Section 2 also discusses various digital forensic readiness models for IoT as found in literature. Section 3 presents the conceptualized model for shadow IoT device forensic readiness. Section 4 presents an evaluation of the proposed SIoTDFR model and Section 5 concludes this paper and points to our future research.

2. Background

In this section, the authors present an overview of IoT digital forensic challenges, digital forensic readiness (DFR) for IoT and IoT DFR models. The proposed model follows the ISO international standard ISO/IEC 27043:2015 process of carrying out DFR during a digital forensic investigation (DFI). In line with this, the authors advocate the need for shadow IoT device digital forensic readiness.

2.1. IoT Digital Forensic Challenges

IoT forensics is that aspect of digital forensics that is aimed at identifying and extracting legally acceptable and forensically sound digital information from the IoT ecosystem. Unlike the digital forensic field where computers, servers and gateways (among others) act as digital evidence sources, sources of digital evidence in IoT forensics involve things such as fitness trackers, medical implants, smartwatches and infant monitoring systems [8]. The seamless ubiquity of IoT devices and the disparate technologies within the IoT ecosystem

have made digital investigation and forensic readiness processes complex and difficult for the digital forensic community to conduct.

The IoT ecosystem has grown exponentially and there are high expectations of sporadic explosions. For instance, according to CISCO predictions [9], 500 billion IoT devices will be networked and connected to the internet by the year 2030. By 2026, the IoT market cap is expected to extend to 771 billion USD. This explosion in the use of IoT devices has opened up a new area of concern for the forensic community. Since IoT devices engage with the public, the IoT ecosystem has been brought into the limelight of security and privacy risks at a different level. Additionally, any network joined by these devices is subject to their vulnerabilities [8]. IoT technologies and devices have furthermore tainted the cyber-physical space with virtual crimes that may become threats to human life. For example, a group of researchers were able to access a livestream video from inside the house of an owner of a smart vacuum cleaner by using the login portal and so managed to hijack the vacuum cleaner [10]. Smart locks can be configured to either lock or open when a particular condition is satisfied. If such a device is hijacked by a criminal, it can become life-threatening by turning digital risks into cyber-physical threats.

Furthermore, reference [4] suggest that the limited computational resources and memory capability of IoT devices constitute a major limitation and can cause untraceable security concerns to the community. The lifespan of data generated and stored on IoT devices is short-lived and the data that is supposed to serve as digital evidence ends up being deleted or written over easily—thus introducing a security challenge to the forensic evidence gathering community.

According to [4], the amplifying rate at which IoT devices are manufactured and released into society introduces a high level of complexity into forensic investigations as there is so much variation in the functionality and operating systems used by the different IoT devices. The forensic tools in existence at the moment struggle to adapt to the varying characteristics presented by the IoT ecosystem. Another vital point significant to IoT forensics mentioned by [11] is the resilience of IoT devices to physical attacks, theft and natural disaster due to their miniaturized nature. These makes it easy for evidence to be carted away, deleted or erased without trace. The issue posed by these IoT devices would be minimal or controllable if they are known by the network administrator of the enterprise network. Shadow IoT device is liable to introduce greater vulnerabilities, threats and criminal acts to the enterprise network.

The aforementioned challenges need the intervention of the forensic community in terms of digital forensic measures as well as proactive measures in case of any criminal activity.

2.2. Digital Forensic Readiness for IoT

Digital forensic readiness (DFR) is a proactive measure employed to capture potential digital evidence ahead of the occurrence of criminal activities or any investigable action. Digital forensic readiness has been employed to salvage countless situations by making available support and safeguarding quantifiable potential digital evidence for digital forensic investigation. References [12,13] suggested six components that should make up the requirements for DFR. These components include capability, resources, operability, strategic planning, knowledge and awareness. According to [14], forensic readiness is attainable in two distinctive ways, namely through employing organizational policies and procedures for data security and through implementing technical methods for tracking and preserving evidence. Some works, including those of [13,15,16], have implemented DFR for IoT via the organizational policies and procedures method. This is because capturing digital evidence is a huge task, especially in the IoT ecosystem. The current research aims to use a technical method for tracking shadow IoT devices as well as for implementing DFR for IoT. The next section discusses the need for digital forensic readiness of shadow IoT devices.

2.3. Risks of Shadow IoT Devices and the Requirements for Digital Forensic Readiness

According to the ISO/IEC 27043 standard [17], the need for digital forensic readiness is four-fold [12,18]. The risk shadow IoT devices poses to the enterprise network necessitates the need for shadow IoT DFR.

- Managing gateway security connections: In a situation where a shadow IoT device joins an enterprise network through an external communication mode such as WiFi or Bluetooth, it will be very difficult for the security gateway to control and manage this connection. Should the IoT device be vulnerable in nature, it could pose a gross impending danger to the network if an adversary leverages on a known vulnerability to sniff out and obtain sensitive data from the enterprise network. It then becomes highly imperative for organizations to proactively employ DFR to identify and gather potential digital evidence. Due to the high risk associated with the presence of shadow IoT devices in the enterprise network, neglecting to gather evidence while the device is still within the network may have catastrophic consequences. For example, shadow IoT devices may premeditate attacks or be used to launch attack(s) on the enterprise network. They quickly become untraceable as their lifespan on the network is always short.
- Managing the possibility of cross-contamination of legitimate IoT devices: The possibility of cross-contamination of legitimate IoT devices connected to the enterprise network is virtually inevitable if vulnerable shadow IoT devices are present. This can pose a great danger to the health and availability of the enterprise network. Hence, the accurate identification of shadow IoT devices, and the monitoring and capturing of their activities as potential digital evidence and as a readiness process in case of any harm to the enterprise network cannot be overemphasized.
- Profiling network activities: The readiness process for shadow IoT devices will serve as a measure to assist cybersecurity incident responders, IoT forensic experts and cybercrime investigators in profiling enterprise networks so as to identify and analyze the network activities of shadow IoT devices that violate an organization's security policies.
- Managing digital forensic investigation (DFI) costs: The DFI process is made easy when potential digital evidence is available. As indicated earlier, the lifespan of shadow IoT devices on the organization's network is short. This may have critical cost implications as potential digital evidence (PDE) may become untraceable when DFI is difficult to conduct. At the occurrence of a crime or breech in the organization's policies involving a shadow IoT device, DFI could become tedious because the device might not leave a trace of its activities on the enterprise network.

The purpose of gathering PDE for shadow IoT devices was discussed in this section. The next section discusses the proposed conceptual model for shadow IoT device forensic readiness to achieve digital forensic readiness.

3. Conceptual Model for Digital Forensic Readiness in Shadow IoT Devices

Despite the existence of a number of IoT digital forensic readiness models, there is not yet any forensic readiness model for shadow-inclusive networks. Therefore, this paper proposes a conceptual digital forensic readiness model for organizations whose networks may become connected to and/or infected by shadow IoT devices. The proposed model presented here complies with the guidelines stipulated in the ISO/IEC 27043:2015. This ISO (International Standards Organization) standard presents incident investigation principles and processes, although not directed at shadow IoT devices.

The proposed Shadow Internet of Things Digital Forensic Readiness (SIoTDFR) model for digital forensics is divided into six distinct stages (A–F) (see Figure 1).

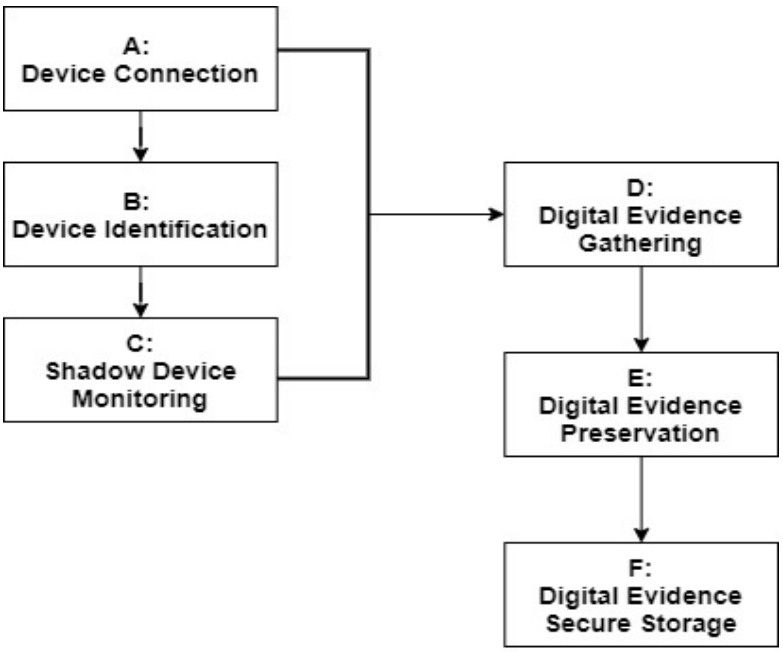

Figure 1. High-Level Overview of SIoTDFR.

Stage A is the device connection stage, while stage B addresses device identification to detect when a shadow IoT device connects to an enterprise network. Stage C deals with the monitoring of the identified shadow IoT devices. Stage D presents the digital evidence collection process that guides how potential digital evidence can be gathered from shadow IoT devices. Stage E describes the potential digital evidence preservation stage for the SIoTDFR model. Lastly, stage F focuses on a secure storage of digital evidence to ensure the integrity of the gathered digital evidence for the purpose of forensic readiness. Each of the components is discussed in detail next.

3.1. Stage A: Device Connection

The SIoTDFR model involves the connection of known (legitimate) or shadow (illegitimate) IoT devices to the enterprise network. In this Bring Your Own Device (BYOD) dispensation, organizations have indirectly opened up their network to both legitimate and shadow IoT devices. Hence, the first stage of the SIoTDFR manages the connection of both shadow and legitimate IoT devices to an enterprise network. Examples of such IoT devices are fitness trackers, smart watches, biosensors and smart thermometers. The flow diagram of the SIoTDFR model device connection stage is depicted in Figure 2.

It is crucial that organizations put in place security measures for their network to ensure that the activities on the network are properly monitored and to enforce compliance with organizational policy. At step 1 of this stage, the researchers assume that each organization puts in place a proprietary network activity monitoring system as a security measure. Step 2 implies that the proprietary network is also able to detect devices as they connect. At step 3, any attempt of an IoT device—be it shadow or known—to join an enterprise network is inspected to confirm the status of the connection as either successful or otherwise. Steps 1–3 serve as the input to this stage. After step 3, it becomes possible to determine the devices that are connected to an enterprise network. Step 4 represents the gathering of potential digital evidence (PDE) artefacts. Three (3) PDE artefacts are gathered at this stage, which are timestamp of device, connected device name, device type.

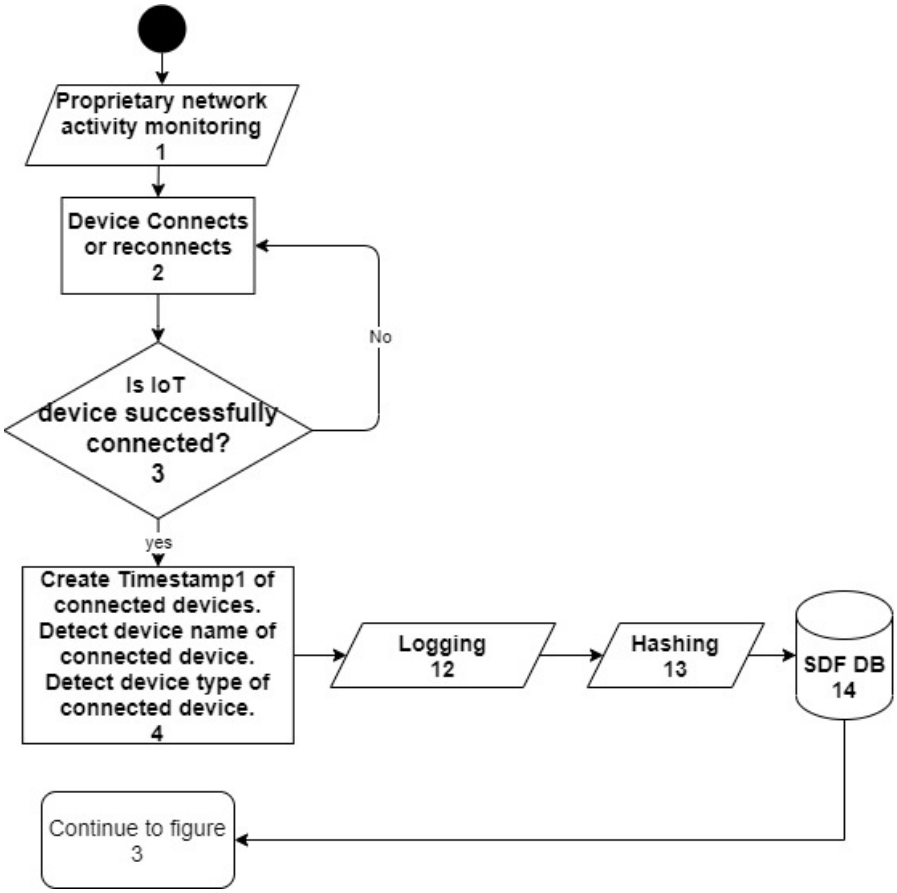

Figure 2. Stage A: Flow diagram of the device connection component.

The PDE gathered is passed to stages D, E and F of the SIoTDFR model, as the respective input and output of these stages are indicated by steps 12–14. For the sake of clarity, these stages (D–F) are already discussed at this point.

Stage D is the digital evidence-gathering stage and it is represented as step 12 in all the flow diagrams shown in this article. Stage D serves as the collector of the PDE for the SIoTDFR model. It involves the logging of potential evidence while ensuring there has occurred no alteration of the digital evidence. The input to stage D is therefore the PDE discovered at each stage of the SIoTDFR model. The process involved here includes the logging of the PDE as strings of characters, while the output involves passing the strings to stage E.

Stage E is the digital evidence preservation step, presented as step 13 in all the flow diagrams in this article. In order to secure the integrity of the logged PDE collected in stage D, hashing is introduced to the logged PDE at stage E. As mentioned above, the input of stage E involves accepting the strings from stage D and transforming them into hashed values. The hashed values are then passed to stage F as the output of stage E.

Stage F, the last stage of the SIoTDFR model, enforces the secured storage of the PDE gathered during the previous stages of the model. Stage F is therefore named digital evidence secure storage, and it is the 14th step in the entire SIoTDFR model process. The hashed values from stage E are the input into this stage, and the process involves a two-factor authentication of the database as well as enforcing access control to the database. The next section explains the concept of identification of connected devices and how they are sorted into either known or shadow device categories.

3.2. Stage B: Device Identification

As discussed above, there is a need to categorize connected Internet of Things (IoT) devices as either shadow or known IoT devices. The SIoTDFR model aims to address the

unavailability of a digital forensic readiness model for shadow IoT devices. In gathering potential evidence from shadow IoT devices, a distinction is to be made between devices that are already known to the enterprise network, and not-known IoT devices. The flow diagram of the device identification stage is presented in Figure 3.

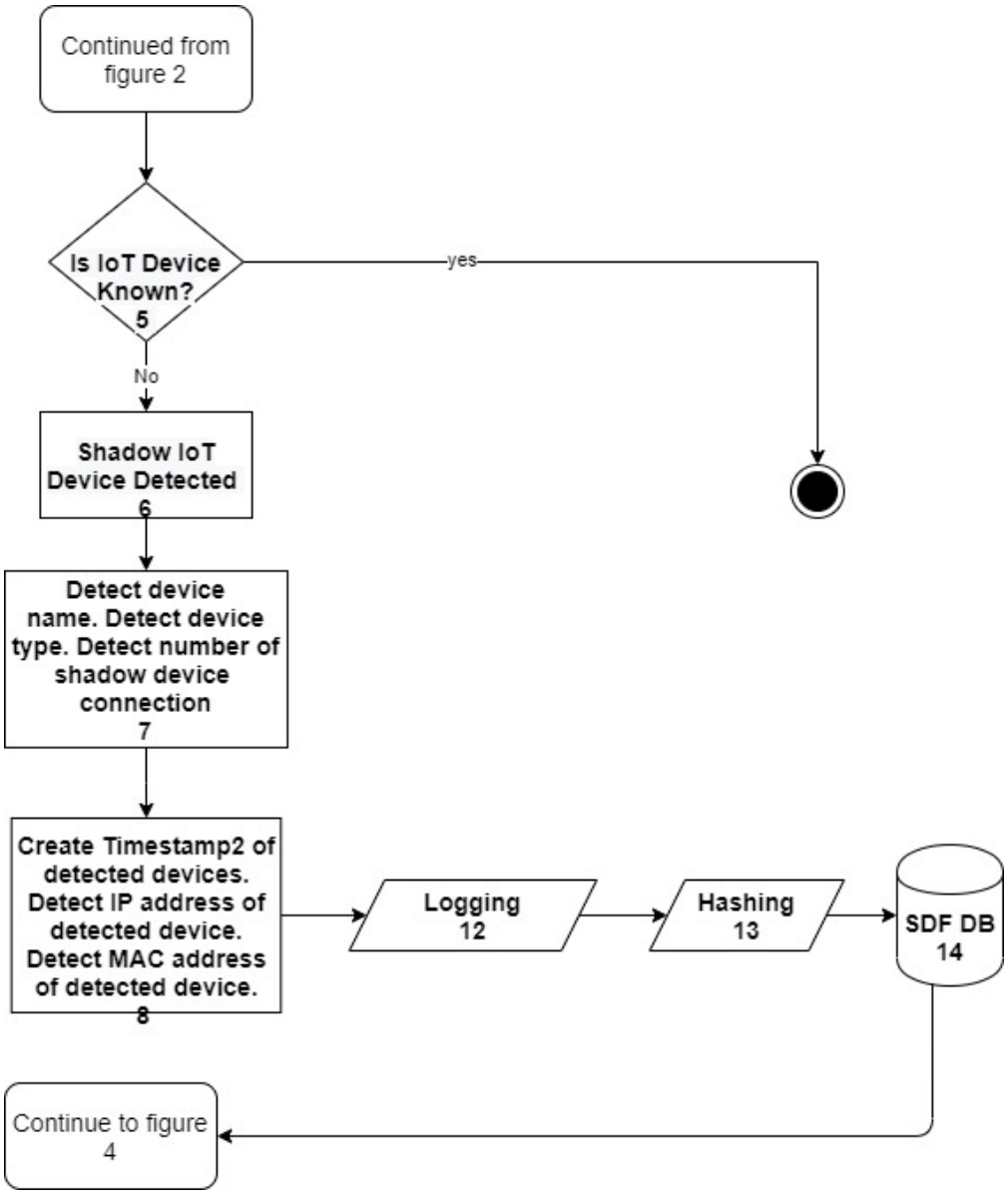

Figure 3. Stage B: Flow diagram of the device identification component.

In the previous stage, the connection of IoT devices (whether shadow or known) was detected, as both categories of IoT devices are able to join the enterprise network (see steps 1–4 in Figure 2). The name of the connected IoT device, as well as other needed attributes of the connected device, is extracted from the SIoTDRF model database. This information serves as the input to the shadow device identification stage and helps to sort the connected devices into either of two categories: shadow or known devices (step 5). The IoT devices that are known to the enterprise network (i.e., not shadow devices) are excluded from further scrutiny because they are legitimate. Any unknown IoT device is identified and detected as a shadow device (see step 6). When a shadow device is detected, PDE for such device such as its name, type and the number of connections that have occurred via such shadow IoT device is gathered (step 7). At steps 7 and 8, five (5) PDE artefacts are

gathered at this stage which are timestamp of device, connected device name, device type, IP address, and the number of shadow IoT device in the network.

All the PDE that has been captured then serves as input to stage D (step 12) which follows through to stage F (step 14). The same process as discussed in the previous section is followed for the purpose of logging, preservation and future reference. It is important to note that detecting an IoT device as shadow does not connote that it is a rogue device. Before a shadow IoT device can be categorized as rogue or not, the activities of such device must be monitored. The monitoring process is presented and discussed in the next section.

3.3. Stage C: Shadow IoT Device Monitoring

The monitoring of the detected devices is of key importance to the enterprise network as it is unclear whether the connected shadow devices are rogue or not. The flow diagram for the shadow IoT device monitoring is presented in Figure 4. Every shadow IoT device is treated as a potential threat to the organization as it may violate the organization's security policy or potentially perform an untraceable criminal act. The activities of shadow IoT devices are short-lived and will become untraceable if not monitored and logged immediately. Once the shadow IoT devices have been identified and some potential evidence was gathered as discussed in the previous section, it is essential that these devices be monitored. The researcher divided the process of device monitoring into three parts which include feature analysis (step 9), traffic analysis (step 10) and behaviour monitoring (step 11). To monitor these devices, the features of the shadow IoT devices are obtained via a number of processes depicted in the feature analysis function (step 9). These processes are presented in more detail in Section 3.3.1. At the end of the feature analysis stage, a test is carried out to confirm if the features introduced by the shadow IoT device are acceptable to the enterprise network (step 9i). The details of steps 9a–i are discussed in Section 3.3.2.

If the features (packet length, packet statistics, protocol used and packet count among others) are not acceptable, they are captured as potential digital evidence (step 9j). Once all the PDE has been captured, it is sent to stage D (step 12) which follows through to stage F (step 14). The same process as discussed in Section 3.1 is followed for purposes of evidence logging and for future reference.

If the features are acceptable, the shadow IoT device is passed to the traffic analysis stage (step 10), which involves a number of processes presented in this paper as steps 10a–f. Next, the traffic pattern is inspected (step 10d) to check if all activities are in line with the enterprise network policy. If not, such activity is flagged as shadow activity (step 10e) and all the PDE that it presents (i.e., the packet size, packet content and protocol used) is captured (step 10f). All this PDE is sent to stage D (step 12), which follows through to stage F (step 14). The same process as discussed in Section 3.1 is again followed for the purpose of evidence logging, secure storage and future reference.

Moving forward, all rogue devices are automatically disconnected from the enterprise network. However, if the traffic pattern successfully passes the enterprise policy test (step 10d), it is allowed to move on to the behaviour monitoring component (step 11). Just like the feature analysis and traffic analysis components, the behaviour monitoring component involves a number of steps (11a–g) that are further presented in Section 3.3.3 of this paper. The model also determines whether there is communication of any kind among shadow devices on the network (step 11c). Every communication by a shadow device with another device on the network is suspected to be an activity that might be criminal in nature, hence all such activities are logged for further analysis.

For every communication, PDE is captured as indicated in step 11g. Thirteen (13) PDE artefacts are gathered at this stage which are packet length statistics, used protocol, total packet count, packet size, packet content, shadow device name, IP address, MAC address, source and destination frequency, periodicity, data exchange type, and data volume.

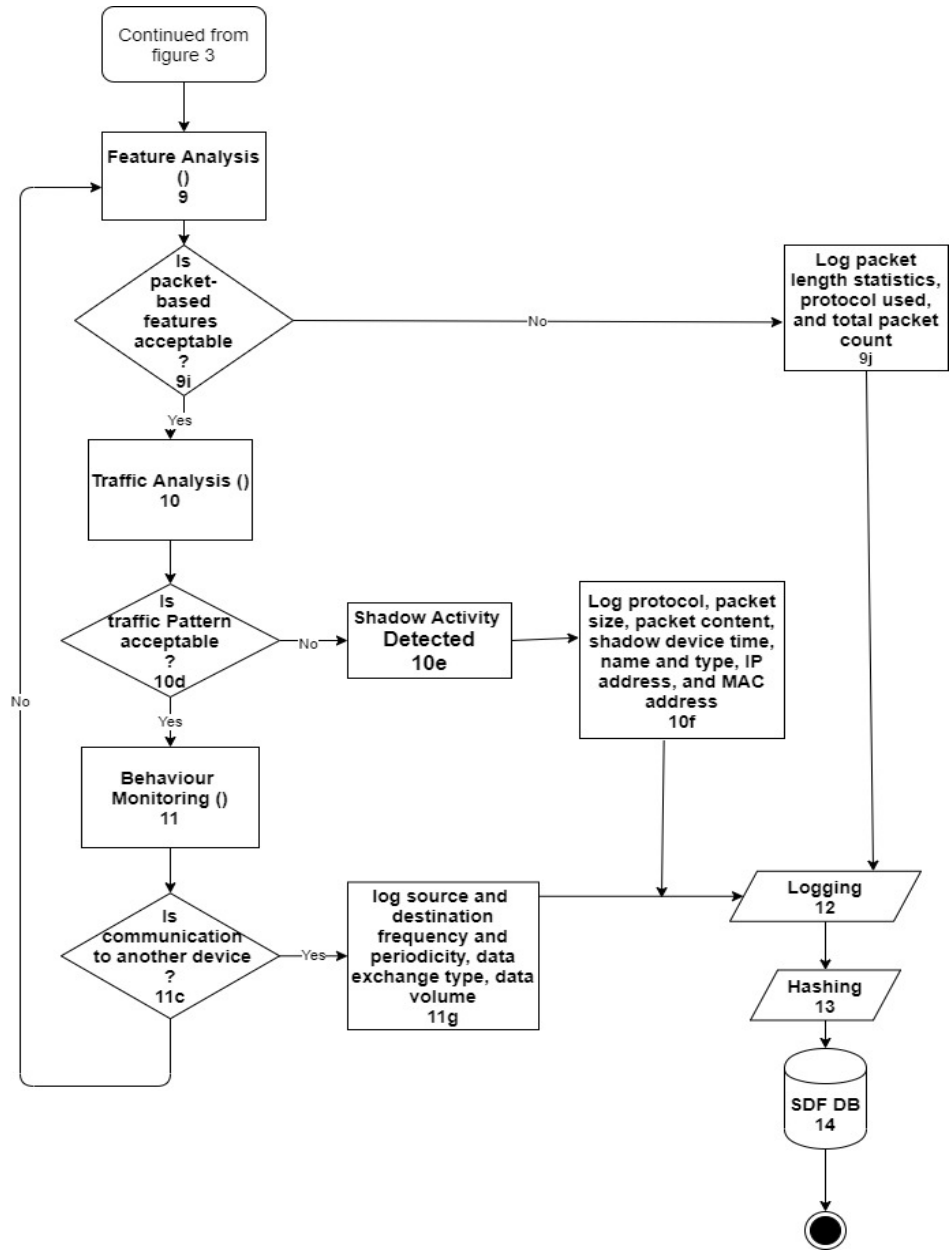

Figure 4. Stage C: Flow diagram of the shadow device monitoring component.

Thereafter, all captured PDE is sent to stage D (step 12) which follows through to stage F (step 14). Again, the same process is followed (as discussed in Section 3.1) for the purpose of evidence logging and future reference.

Otherwise, the SIoTDFR model process follows a cyclic pattern that returns to the feature analysis step (step 9) until the shadow IoT device logs off the enterprise network. The next section contains a description of the shadow IoT device monitoring components.

3.3.1. Shadow IoT Device Feature Analysis

Features of shadow IoT devices can either be physical or packet-based. For instance, some of the physical features of a fitness tracker can be to monitor or track the user's heart rate, calories burnt, sleep moments, etc. Some of the packet-based features are packet length statistics, inter-arrival statistics and total packet count. One shadow IoT device may have similar physical features as another shadow device, yet distinctly possess a unique set of packet-based features. Hence, both the physical and packet-based features are vital for

consideration as PDE for a shadow IoT device. The flow diagram of the shadow IoT device feature analysis is presented in Figure 5. This analysis is a subsystem of the shadow IoT device monitoring stage as mentioned in Section 3.3 and shown in Figure 4, and its flow diagram (as presented in Figure 5) continues from Figure 3 (Stage B: the shadow IoT device identification stage).

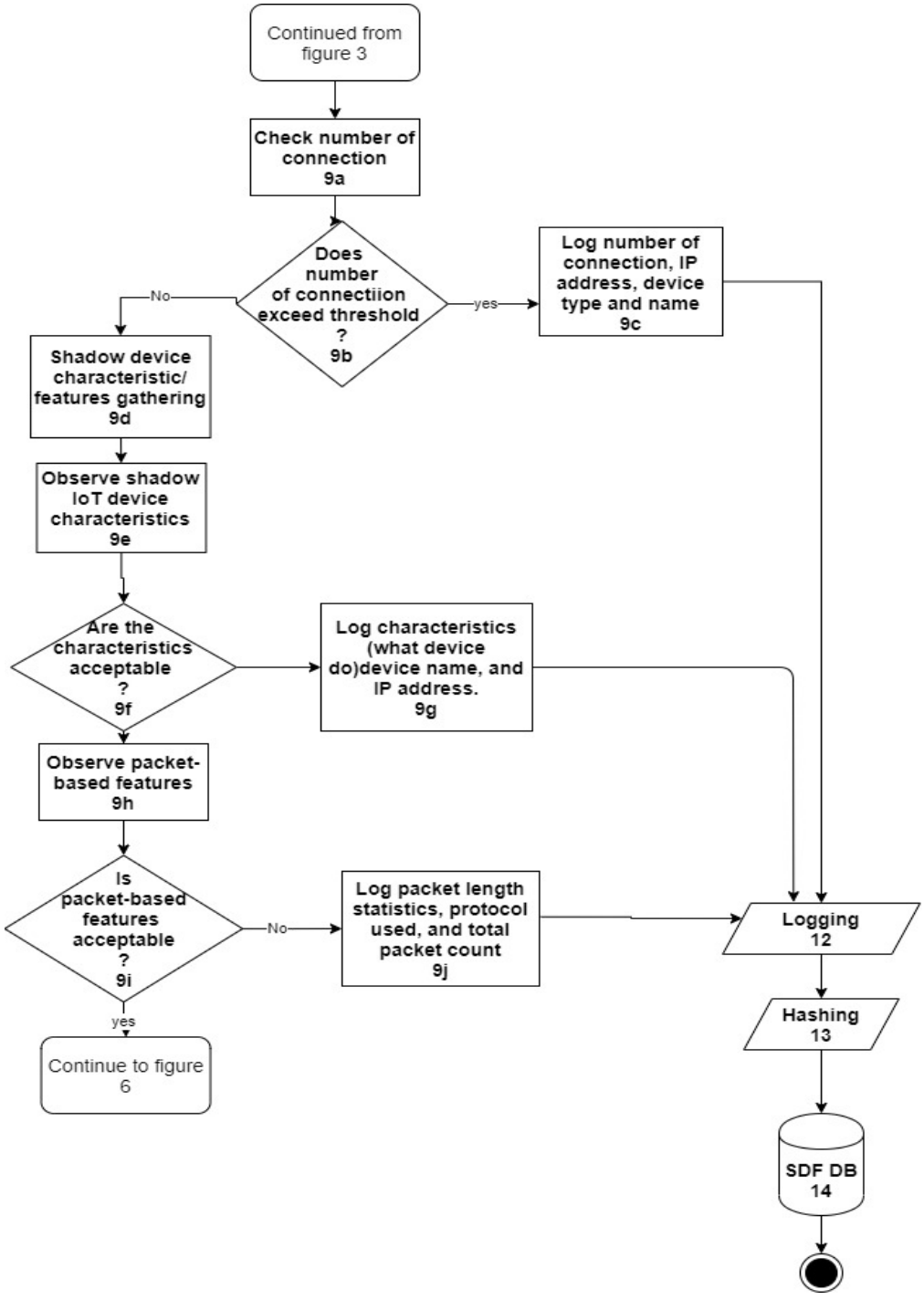

Figure 5. Stage C-1: Flow diagram depicting the shadow device feature analysis.

Step 14 in Figure 5 shows that the gathered PDE of the identified shadow IoT device is securely stored in a database named SDF DB. From this database, some information—such as the name and IP address of the shadow IoT device, the number of shadow device connections and its MAC address—is retrieved as input for the feature analysis component, which is a

part of the shadow device monitoring stage. Using the information extracted from the SDF DB, the number of connections that the shadow IoT device has made will be checked (see step 9a). Subsequently, a decision is made based on whether the number of connections exceeds the threshold laid down by the organization's policy (step 9b). If this is the case, possible PDE is gathered from such devices as depicted in step 9c. Thereafter, all the PDE that has been captured is outputted to stage D (step 12). The process follows through to stage F (step 14) in the same way as discussed in Section 3.1.

Otherwise, the device's features and characteristics are gathered (step 9d) for observation purposes (step 9e). According to [15,19], organizations that wish to achieve DFR are to establish policies that are considered acceptable by their management and that are strictly complied with as binding for legal requirements and evidence gathering. Such a policy should contain a list of acceptable device characteristics and it should treat any deviation as a threat to the network and as a source of potential digital evidence in case of criminal activity. The shadow IoT device characteristics are matched with the slated policy of the organization (step 9f). If there is a deviation, PDE is captured (step 9g).

Thereafter, all the PDE that has been captured is outputted to stage D (step 12) which follows through to stage F (step 14) (adhering to the same process as discussed in Section 3.1 for the purpose of logging and future reference). However, if the characteristics suit the organization's policy, the device's packet-based features that were gathered in step 9d are observed (step 9h). These features are next examined to confirm if they match the acceptable features of the organization (step 9i). Any device that has features that do not comply with the organization's policy will have PDE captured from it. This evidence will serve as the input to stage D (step 12) and then follow through stage F (step 14), following the same process as discussed in Section 3.1 (for the purpose of evidence logging and future reference). A shadow IoT device that complies with the organizational policy is subsequently allowed to pass to the next component of the shadow IoT device monitoring stage, which will be discussed next.

3.3.2. Shadow IoT Device Traffic Analysis

This section is the continuation of the shadow IoT device monitoring stage of which the first component was discussed in the previous subsection. As discussed earlier, any shadow IoT device that has passed the feature analysis of the enterprise network is allowed to move to the next component, namely the shadow IoT device traffic analysis. The flow diagram of this component is presented in Figure 6.

The shadow IoT device's traffic is gathered at this stage (step 10a) in order to inspect the traffic pattern for unacceptable traffic. Alongside, as the traffic is gathered, the device characteristics (i.e., the timestamp of traffic generation, the name of the shadow device and type, the IP address and MAC address of the shadow IoT device) are captured (step 10b). The characteristics are saved as PDE in case of any deviance of the device from its known approved state as discussed in the previous section.

The PDE is passed to stage D (step 12), which follows through to stage F (step 14) for the purpose of logging, integrity preservation, secure storage and future reference. The traffic that has been gathered is subjected to inspection of its pattern (step 10c), after which a decision is made about whether such pattern is acceptable to the enterprise network (step 10d). If it is, the shadow IoT device from which the traffic originated is allowed to pass through to the next component of the shadow IoT device monitoring stage (see Section 3.3.3). Otherwise, it is flagged that the device has produced a shadow activity that is unacceptable (step 10e). PDE such as protocol, traffic packet size, traffic packet content and timestamp, is captured (step 10f) from the device that produced the shadow activities. The evidence is passed on as the output of this component to stage D (step 12), which follows through to stage F (step 14) for the purpose of logging, integrity preservation, secure storage and future reference.

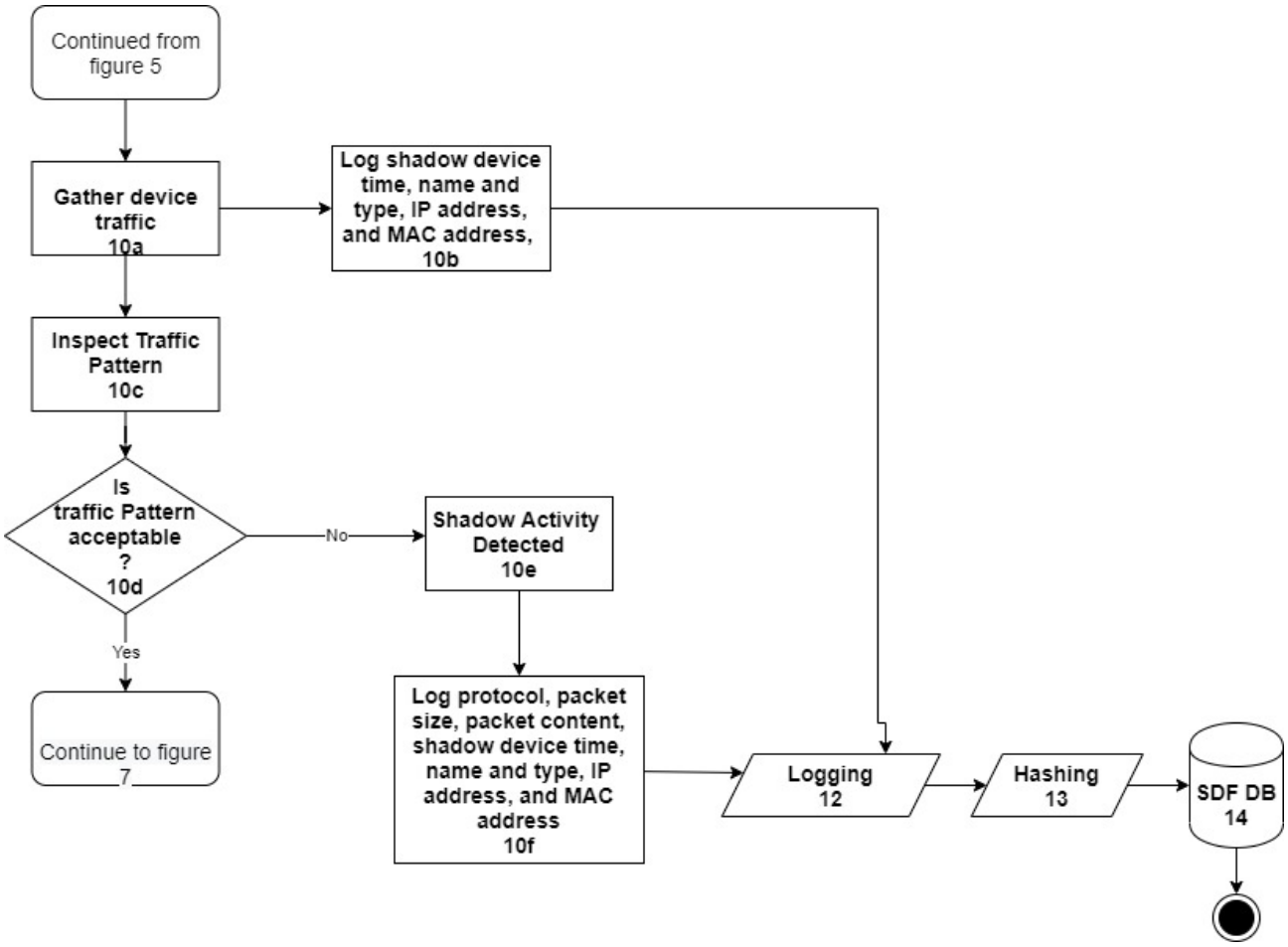

Figure 6. Stage C-2: Flow diagram illustrating the shadow device traffic analysis.

3.3.3. Shadow IoT Device Behaviour Monitoring

To further capture the digital forensic evidence that a shadow IoT device can offer, monitoring of the device's behaviour is essential. The analysis made at this stage involves identifying and monitoring the way a shadow IoT device acts, especially towards another device in the enterprise network. Some of the behavioural characteristics that this research considers are the destination frequency, periodicity, data exchange type, and data volume exchanged. A shadow IoT device that managed to scale through the feature and traffic analysis components presented above is considered fit to continue on the enterprise network. The flow diagram of the shadow IoT device behaviour monitoring component is presented in Figure 7. To monitor the behaviour of the device, it needs to be gathered, which is carried out at step 11a. The behaviour of the captured device triggers an inspection to check if it is communicating with another device (step 11b). This is tested in step 11c, and the truthfulness of this condition leads to checking how often such communication takes place (step 11d). To predict if the particular device can remain on the enterprise network, the frequency of communication is tested next (step 11e). If not exceeding an acceptable threshold, such device is permitted to remain on the network but must continue to be monitored. Hence, the device returns to the feature analysis component (see Figure 6) in a cyclic manner until either the device disconnects from the enterprise network or one of the conditions is not satisfied, which causes the enterprise to halt its connection. However, if the communication frequency is higher than the acceptable threshold, PDE is captured (step 11g). Afterwards, all the PDE that has been captured is outputted to stage D (step 12), which follows through to stage F (step 14). It adhered to the same process as discussed previously in Section 3.1 for the purpose of logging and future reference.

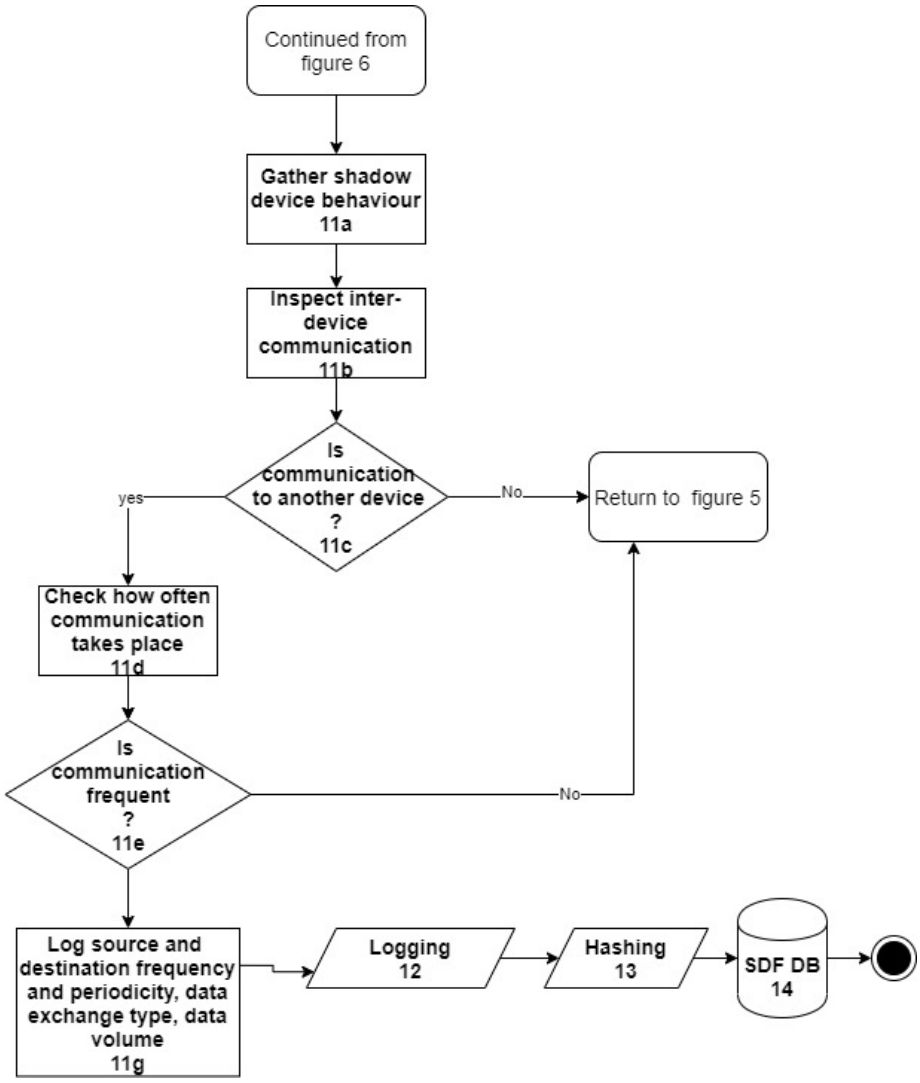

Figure 7. Stage C-3: Flow diagram showing the shadow device behaviour monitoring.

3.4. Stage D: Digital Evidence Gathering

The digital evidence gathering stage (step 12) is a parallel component that accepts digital potential evidence from stages A–C. Stages A–C serve as the components that generate data that can be used as potential digital evidence, such as the timestamp of the connected device, name of the device, device type, data exchange type and data frequency (to name a few). The PDE is the input of this stage, the logging of the potential evidence is the process involved at this stage, and the logged data is now the output that is passed to stage F of the SIoTDFR model.

3.5. Stage E: Digital Evidence Preservation

The digital evidence preservation component helps to maintain the integrity and secure the chain of custody of the potential digital evidence. At this stage, the captured PDE gathered in the previous stage is preserved via hashing. This is essential to ensure potential digital evidence usability, documentation and the preservation of evidence integrity.

3.6. Stage F: Digital Evidence Secure Storage

The last stage of the SIoTDFR model is the digital evidence secure storage (step 14), a parallel component that serves as the database for the gathered PDE in the SIoTDFR model. To securely store the digital evidence, different security techniques are put in place for the database such as sandboxing and access control. An access control strategy helps to restrict

undue access to the database and to ensure data integrity and data confidentiality of the SIoTDFR model. Access control also gives authorization privileges to different levels of users of the enterprise network.

The six stages presented above serve as the proposed conceptual model for shadow IoT devices. The formal specification is presented next.

3.7. Formal Specification of the SIoTDFR Model

This section presents the formal specification of the SIoTDFR model. The definition of notations used in the formal specification is presented in Table 1. Furthermore, definitions of functions called in the formal model specification are presented in Table 2. Lastly, the algorithm that serves as the formal specification for the SIoTDFR model is presented.

Table 1. Notations Table.

Name	Notation	Name	Notation
Device	D	Timestamp for device D	T_D
Proprietary network activity monitoring	NM	Device connection	DC()
Device name	Dn	Device type	DT
Potential digital evidence (PDE)	P	MAC address	MAC
Hash function for PDE P_i	Hash(P_i)	Logging function for PDE P_i	$Log_p(P_i)$
Secure Storage for PDE	SStore(P_i)	Shadow Devices	SD
Whitelisted Devices	WD	IP address	IP
ISWD	Is whitelisted device	ISWD()	{True, False} is a Boolean function
GetPDE()	Get PDE for D	C_D	Device connection stage
I_D	Device identification stage	M_{SD}	Shadow device monitoring stage
PF	Packet feature	PF()	{True, False} is a Boolean function
TP	Traffic pattern	TP()	{True, False} is a Boolean function
ISSA	Is shadow activity	ISSA()	{True, False} is a Boolean function
ISCOM	Is communication	ISCOM()	{True, False} is a Boolean function

Table 2. Definitions.

D = {WD, SD}
where WD = {WD_1, WD_2, . . . , WD_n} where nϵN set of whitelisted IoT devices SD = {SD_1, SD_2, . . . , SD_m} where mϵM set of shadow IoT devices ProcessPDE(P) is a 3-staged function defined as ProcessPDE(P) = {Log_p(P), Hash(P), SStore(P)} GetPDE() = {} that collects the PDE The proposed model SIoTDFR is a three (3)—tuple staged model defined as SIoTDFR(SD) = {C_D, I_D, M_{SD}} Where C_D = Device connection stage I_D = Device identification stage M_{SD} = Shadow device monitoring stage

Formal Model Algorithm of SIoTDFR

The algorithm for the formal model of SIoTDFR is given in Algorithm 1. Each stage that makes up SIoTDFR is underlined.

Algorithm 1. Formal model algorithm of SIoTDFR.

```
Device connection stage (C_D)
Start/initiate NM
      If (NM)
Begin
      For any device D_i ϵ D
If DC(D_i)
      PD_i = GetPDE(D_i)
      ProcessPDE(PD_i)
Endif
          End for
End
      End
Device Identification stage (I_D)
      For any Device D_i ϵ D
            If !(D_i ϵ WD)
              Begin
                ISWD(D_i) = false
                PD_i = GetPDE(D_i)
                ProcessPDE(PD_i)
              End
            Endif
        End for
Shadow Device Monitoring (M_SD)
Feature_Analysis (D_i)
      If PF (D_i) == 0
        Begin
            GetPDE(D_i) where PDE = {packet length, protocol used, packet count, total packet}
            ProcessPDE(D_i)
        End
   Else
          Begin
            Traffic_analysis(D_i)
            If TP(D_i)==0
              Begin
                If ISSA(D_i)= True
                    GetPDE(D_i) where PDE = {protocol, packet size, packet content, interarrival
time, DT, DN, T, IP, MAC }
                    ProcessPDE(D_i)
                End
            Else
            Begin
                Behaviour_monitorng()
If ISCOM(D_i) ==True
      GetPDE(D_i) where PDE = {source IP, destination IP, source frequency. source periodicity, data
exchange type, data volume, destination periodicity}
      ProcessPDE(D_i)
                End
                    Endif
          End
Endif
```

The SIoTDFR conceptual model and formal notation have been presented in this section. The evaluation of SIoTDFR model is discussd in the next section.

4. Evaluation of the SIoTDFR Model

The review of the IoT ecosystem indicates that shadow IoT devices have not been catered for from a security and forensic perspective; see Table 3. This study aimed to

address the digital forensic preparedness of shadow IoT devices so as to enable the IoT-based environment to prepare for countering security threats and criminal activities. It is also hoped that this study will help organizations to proactively handle DFIs by minimizing cost and reducing the risk of evidence unavailability or deletion. The SIoTDFR model is robust enough to capture even the minutest PDE, making tracking of criminal activities easy in case of criminal incidents.

Table 3. Comparison of literature survey.

Article	Network Connection Type	Problem Addressed	Captured PDE	Methodology	Standard
[20]	Model for digital forensic readiness	Digital forensic readiness framework		Classification of Organizational process, policy, people, and technology	None
[21]	Smart home network	Forensics Edge Management System (FEMS) for smart IoT home	Events, threshold detection, data compression	Not defined	None
[22]	BYOD inclusive network	Digital forensic readiness model	Not defined	Honeypot technology	ISO/IEC 27043:2015
[23]	IoT network	Flooding attack detection	Attack detection	Test bed	None
[24]	Online social network	Cyberbullying	Tweets, replies, quotes, retweet, profile data, direct message	Formal theory	ISO/IEC 27043:2015, ISO/IEC 27050–1:2016 and ISO/IEC 27050–2:2018
[25]	BYOD for smart city infrastructure	Malicious BYOD activities	BYOD endpoint activities inside the network and VPN connected BYOD interface	Simulated environment	None
[26]	Botnet inclusive network	Identify and classify attack and assist trace of botnet activity on IoT network	Network flow	Decision tree	None
[27]	Financial companies	Identified causes of incidents such as DDoS attack, Data breach, forgery and falsification	Logs, account lists, history of electronic data, remote management history	Conceptualized	ISO/IEC 27043:2015
[28]	IoT network	Forensic readiness model for IoT, link layer dataset	Network parameters and traffic	Simulation on Cooja Provenance graph	None
Our Work	Shadow IoT device inclusive network	IoT Device identification, IoT device monitoring	Device time stamp, IP address, MAC address, device type, protocol, packet size, packet content, device communication frequency, data exchange type, data volume, periodicity, source and destination address	Simulation on Contiki cooja	ISO/IEC:2701573:2015

Shadow IoT devices are the target of the conceptualized model presented in this article. Any IoT device that joins an organization's network in which it is unknown is regarded as a shadow device in that network. The SIoTDFR model follows a layered architecture where each layer is independent. This implies that each component of the model can be implemented separately for IoT device identification and IoT device monitoring. Furthermore, this concept is an adaptive model for the IoT ecosystem as it can be used as a passive monitor for any IoT network. Additionally, the conceptual model will be beneficial to the organization in that it can identify IoT devices that connect per time to their network. The

SIoTDFR model can be used to track the availability and connection of the IoT devices in an organization, thus rendering information that can serve several purposes.

Moving forward, this study also considered privacy issues related to IoT devices as most of these devices are used to communicate personal data. The SIoTDFR model uses IoT device features, traffic patterns, and behaviour as PDE. However, since the model is targeted at the organization's digital forensic readiness, the data gathered (PDE) are meant strictly for legal use and should be made available only to authorized personnel. This is in line with some of the legislation that governs the use of IoT and PDE admissibility. Examples are the Internet of Things (IoT) Cybersecurity Improvement Act of 2020 (USA), the Protection of Personal Information (POPI) Act (South Africa), the Association of Chief Police Officers (ACPO) guidelines (UK), the Criminal Procedure Act (CPA) (South Africa) and the Data Protection Act (UK) [12,29,30]. Additionally, it is expected of the organization that implements the SIoTDFR model to flag rules, policies and regulations that govern their network. Such policy must state clearly that data will, for forensic purposes, be captured from devices that connect to their network.

The short lifespan of shadow IoT devices on networks makes the activities of such devices very difficult to trace. This is because there exist no historical data that can prove that such a device ever joined the network or participated in any criminal activity on the enterprise network. It is imperative that the activities of such devices be tracked and logged, as they have high tendencies to inflict security attacks on the network when connected. This concern will be dealt with by the SIoTDFR model as every shadow device and its activities will be captured.

One of the main characteristics of an IoT device is the fact that it has many special features. This implies that conventional forensic readiness techniques may not be efficient to handle such devices in terms of gathering PDE. The SIoTDFR model has purposefully considered these special features and characteristics in gathering PDE. The next section presents a brief discussion of future works and concludes this paper.

5. Conclusions

This paper proposed a model towards implementing DFR in a shadow IoT device inclusive network. A shadow IoT device-inclusive network is a network that has shadow IoT devices connected to it. This paper introduced a generic model that is capable of gathering potential digital evidence by taking the special functionalities, features and behaviour of IoT devices into consideration. The SIoTDFR model can be adopted in smart homes, smart cities, as well as organizations with IoT networks to ensure their forensic readiness when shadow IoT devices have been included into such IoT networks. The model presented in this paper consists of six phases that identify and manage the activities and behaviour of the overwhelmingly growing number of shadow IoT devices that connect with enterprise networks. Furthermore, potential digital evidence is gathered from the connection of the shadow IoT devices, and such evidence is logged and preserved for the purpose of digital forensic readiness. The concept of shadow IoT device digital forensic readiness is vital as a complementary approach towards shadow Internet of Things forensics, investigation and attack prevention. For future work, the authors plan to simulate an organizational IoT network with shadow IoT device inclusion in the network using the Contiki Cooja simulator. This will be used to implement each stage of this model as a prototype to critically evaluate it for organizational use. In addition, the authors will conduct research to assess the vulnerability of shadow IoT devices before they are permitted to join an enterprise network.

Author Contributions: Conceptualization, F.I.F. and H.S.V.; supervision, H.S.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Gupta, A. IoT—Connected Devices Network. Available online: https://jktech.com/insight/blogs/ (accessed on 4 August 2021).
2. Onag, G. *Analysts Say COVID-19 Pandemic Will Spur IoT Adoption*; FutureIoT: Singapore, 2020.
3. Cox, G. Managing the risks of shadow IoT. *Netw. Secur.* **2019**, *2019*, 14–17. [CrossRef]
4. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Alshdadi, A.A.; Wills, G.B. Security, cybercrime and digital forensics for IoT. In *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*; Springer International Publishing: Cham, Switzerland, 2020; pp. 551–577.
5. Karabiyik, U.; Akkaya, K. Digital forensics for IoT and WSNS. In *Mission-Oriented Sensor Networks and Systems: Art and Science*; Springer International Publishing: Cham, Switzerland, 2019; pp. 171–207.
6. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
7. Leiner, B.M.; Cerf, V.G.; Clark, D.D.; Kahn, R.E.; Kleinrock, L.; Lynch, D.C.; Postel, J.; Roberts, L.G.; Wolff, S. A brief history of the Internet. *ACM SIGCOMM Comput. Commun. Rev.* **2009**, *39*, 22–31. [CrossRef]
8. Stoyanova, M.; Nikoloudakis, Y.; Panagiotakis, S.; Pallis, E.; Markakis, E.K. A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1191–1221. [CrossRef]
9. Kumar, R.; Goyal, R. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Comput. Sci. Rev.* **2019**, *33*, 1–48. [CrossRef]
10. Alabdulsalam, S.; Schaefer, K.; Kechadi, T.; Le-Khac, N.-A. Internet of Things Forensics—Challenges and a Case Study. In *Advances in Digital Forensics XIV*; Springer International Publishing: Cham, Switzerland, 2018; pp. 35–48.
11. Hameed, S.; Khan, F.I.; Hameed, B. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. *J. Comput. Netw. Commun.* **2019**, *2019*, 9629381. [CrossRef]
12. Kigwana, I.; Venter, H.S. A Digital Forensic Readiness Architecture for Online Examinations. *S. Afr. Comput. J.* **2018**, *30*, 1–39. [CrossRef]
13. Zulkipli, N.H.N.; Wills, G.B. An Exploratory Study on Readiness Framework in IoT Forensics. *Procedia Comput. Sci.* **2021**, *179*, 966–973. [CrossRef]
14. Collie, J. A Strategic Model for Forensic Readiness. *Athens J. Sci.* **2018**, *5*, 167–182. [CrossRef]
15. Kebande, V.R.; Mudau, P.P.; Ikuesan, R.A.; Venter, H.S.; Choo, K.-K.R. Holistic digital forensic readiness framework for IoT-enabled organizations. *Forensic Sci. Int. Rep.* **2020**, *2*, 100117. [CrossRef]
16. Kebande, V.R.; Ray, A. 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; pp. 356–362.
17. Valjarević, A.; Venter, H.; Petrović, R. ISO/IEC 27043: 2015—Role and application. In Proceedings of the 2016 24th Telecommunications Forum (TELFOR), Belgrade, Serbia, 22–23 November 2016; pp. 1–4.
18. Kebande, V.R.; Karie, N.M.; Venter, H.S. Adding Digital Forensic Readiness as a Security Component to the IoT Domain. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2018**, *8*, 1–11. [CrossRef]
19. Moussa, A.N.; Ithnin, N.B.; Miaikil, O.A. Conceptual forensic readiness framework for infrastructure as a service consumers. In Proceedings of the 2014 IEEE Conference on Systems, Process and Control (ICSPC 2014), Kuala Lumpur, Malaysia, 12–14 December 2014; pp. 162–167.
20. Pooe, A.; Labuschagne, L. A conceptual model for digital forensic readiness. In Proceedings of the 2012 Information Security for South Africa, Johannesberg, South Africa, 15–17 August 2012; pp. 1–8. [CrossRef]
21. Oriwoh, E.; Sant, P. The forensics edge management system: A concept and design. In Proceedings of the 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, Vietri sul Mare, Italy, 18–21 December 2013; pp. 544–550.
22. Kebande, V.R.; Karie, N.M.; Venter, H. A generic Digital Forensic Readiness model for BYOD using honeypot technology. In Proceedings of the 2016 IST-Africa Week Conference, Durban, South Africa, 11–13 May 2016; pp. 1–12.
23. Rizal, R.; Hikmatyar, M. Investigation Internet of Things (IoT) Device using Integrated Digital Forensics Investigation Framework (IDFIF). *J. Phys. Conf. Ser.* **2019**, *1179*. [CrossRef]
24. Arshad, H.; Omlara, E.; Abiodun, I.O.; Aminu, A. A semi-automated forensic investigation model for online social networks. *Comput. Secur.* **2020**, *97*, 101946. [CrossRef]
25. Ali, M.I.; Kaur, S.; Khamparia, A.; Gupta, D.; Kumar, S.; Khanna, A.; Al-Turjman, F. Security challenges and cyber forensic ecosystem in IOT driven BYOD environment. *IEEE Access* **2020**, *8*, 172770–172782. [CrossRef]
26. Wiyono, R.T.; Cahyani, N.D.W. Performance Analysis of Decision Tree C4. 5 as a Classification Technique to Conduct Network Forensics for Botnet Activities in Internet of Things. In Proceedings of the 2020 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 5–6 August 2020; pp. 1–5.

27. Lee, S.J.; Kim, G.B. K-FFRaaS: A Generic Model for Financial Forensic Readiness as a Service in Korea. *IEEE Access* **2021**, *9*, 130094–130110. [CrossRef]
28. Sadineni, L.; Pilli, E.S.; Battula, R.B. Ready-IoT: A Novel Forensic Readiness Model for Internet of Things. In Proceedings of the 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 14 June–31 July 2021; pp. 89–94.
29. Nortje, J.G.; Myburgh, D.C. The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa. *Potchefstroom Electron. Law J. Potchefstroomse Elektron. Regsblad* **2019**, *22*, 1–42. [CrossRef]
30. Losavio, M.M.; Chow, K.P.; Koltay, A.; James, J. The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. *Secur. Priv.* **2018**, *1*, e23. [CrossRef]