DFIM: A NEW DIGITAL FORENSICS INVESTIGATION MODEL FOR INTERNET OF THINGS

MOHAMMAD QATAWNEH [1], WESAM ALMOBAIDEEN[2], MOHAMMED KHANAFSEH[3], IBRAHIM AL QATAWNEH [4]

[1]Professor. The University of Jordan, Department of Computer Science, Jordan
[2]Professor. The University of Jordan, Department of Computer Science, Jordan
[2]Professor. Rochester Institute of Technology, UAE
[3]Ph.D. candidate. The University of Jordan, Department of Computer Science, Jordan
[4]Professor. Al Ain University of Science and Technology College of Law
E-mail: [1]mohd.qat@ju.edu.jo, [2]almobaideen@inf.ju.edu.jo, [2]wxacad@rit.edu, [3]mkhanafsa@gmail.com, [4] Ibrahim.alqatawneh@aau.ac.ae

ABSTRACT

The Internet of Things (IoT) smart devices have been used widely in several applications such as healthcare, education, environment, transportation, smart city, etc. These objects are resource-constrained devices which involve lacks regarding security and may lead to cyber-crime. Therefore, the IoT devices may contain evidence that are considered as an important need to investigators and can be admitted in courts. To tackle this problem most current research focuses on security issues for different IoT architectures rather than approaches and techniques of forensic acquisition and analysis for IoT objects. In this paper, we propose a new Digital Forensics Investigation Model for IoT (DFIM). The DFIM has two main components: The Data Provider Zone (DPZ) which responsible for grouping all data gathered by sensor nodes into a set of groups, where each group contains data or documents related to each other, and the investigation authority which receives the requests from the claimers for investigation, check the validation of the request, and finally select the appropriate investigators. In order to improve the IoT forensics investigation process, the proposed DFIM consists of seven stages and takes into consideration a set of principles such as security, privacy accuracy, performance, data reduction, Openness and transparency.

Keywords: *The Internet Of Things, IOT Forensics, Investigation Authority, Examination Stage, Investigation Process, Committee Of Investigators.*

1. INTRODUCTION

The Internet of Things (IoT) can be viewed as an information system made up of things, networks, data and services. Such things may be wireless sensors, traditional computers, smartphones, cameras, humans, tablets, vehicles, home appliances etc. that are connected over a network. These things may gather, process and upload a huge amount of data to the internet and used to initiate service. The IoT devices can be divided into four main groups: consumer, commercial, industrial, and infrastructure spaces [27]. The number of IoT devices will reach or even exceed 75 billion and enables many applications in different fields [32] as shown in figure 1. Among IoT devices, the wireless sensors are considered the backbone of the IoT because they are part of our life and used in several applications such as smart city, smart home, transportation, environment, military, healthcare, education etc.

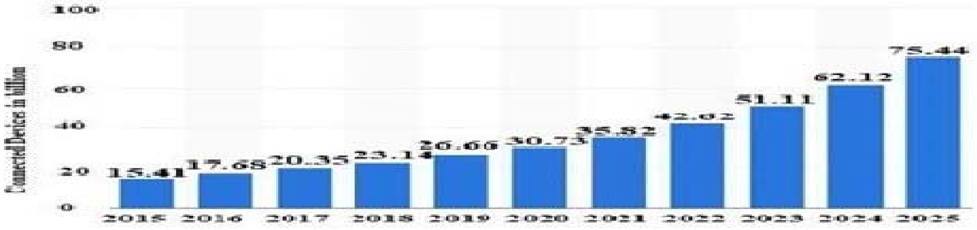


Figure 1: Iot Connected Devices From 2015 To 2019 (In Billions)

However, the wireless sensors are resource-constrained devices which involve shortcomings regarding security and privacy issues thereby

leading to cyber-crime. moreover, IoT is not designed with security in mind, as the main concern was to minimize the cost and size consequently, the IoT is been exposed to the cyber threats and attacks. According to [4], three main sources of threats in IoT has been identified as the following:

- Malicious User: Is the owner or the user of the IoT devices with potential to perform attacks to learn the secrets of the manufacturer, in order to sell secrets to third parties, or attack similar systems.

- Bad Manufacturer: Is the producer of the device with the ability to exploit and use the technology to gain information about the users and revealing it to the outsider.

- External Attacker (Adversary): Known as an outsider entity which is not part of any IoT system and has no authorized to it. He or she then, try to get the sensitive in- formation for malicious purposes.

From the forensics perspective, the IoT devices may contain evidence that is considered as an important need to investigators and courts. Even though IoT has rich sources of evidence, it causes some challenges for forensics investigators including but not limited to the location of data and heterogeneous nature of IoT devices such as differences in operating systems, communication standards, the existing digital forensics tools and approaches which don't fit

with the IoT paradigm. The variety of physical things which get connected with the IoT generate a huge amount of possible evidence bring new challenges to investigators to collect evidence from highly distributed IoT environments [25]. To investigate such evidence a digital IoT forensics is needed because most cur- rent research focuses on security issues for different IoT architecture rather than approaches and techniques of forensic acquisition and analysis for IoT objects [37]. Therefore, in this paper, we discuss the IoT forensics challenges, issues, and forensics frameworks. We propose an IoT Forensics-Model for supporting forensics investigations, where IoT forensics can provide new insights to determine facts about criminal incidents. The rest of this paper is organized as follows: Section II provides the background information about digital forensics, IoT forensics and their challenges, Section III presents the proposed IoT Forensics-Model for supporting forensics investigations, and finally we conclude in Section VI.

2. THEORETICAL BACKGROUND

This section presents an overview of conventional digital forensics and IoT forensics. IoT forensics can be defined as one of the digital forensics branches where the main investigation process must suit with the IoT infrastructure.

2.1 Convention Digital forensics:

The evidence sources in conventional digital forensics could be computers, mobile devices, servers or gateways. Different conventional digital forensics models have been proposed. Each model contains a set of stages. Table 1 shows different frameworks proposed by many researchers.

Table 1: Different Models For Digital Forensics.

Frameworks Names	Initialization stage	Initialization stage	Collection	Reduction	Preservation	Examination	Analysis	Information	Review stage	Documentation Stage	Reporting stage	Presentation	Security Aware	Integrity Aware	Privacy Aware	Complexity Level	Main Comments And Limitations	Framework Contribution
Generic Digital Forensics Framework For IOT [13]	✓	✓	✓	✓	✓	✓	✓	χ	χ	χ		✓	✓	χ	χ	H	The investigation process can be carried out at different IoT levels (Fog level and cloud level). The framework takes security policy into account without any consideration of privacy.	The framework introduced to enhance the security and privacy issues.
Digital Forensics Investigation Model (DFIM) [36]	✓	✓	✓	χ	✓	✓	✓	χ	χ	χ	✓	✓	χ	χ	χ	L	The main drawback of this model refers to the fact that in the investigation process there is no concern about physical evidence, only about digital evidence.	Prang improvement in DF by exposing digital evidence that is hidden, but it does not concern over physical evidence.
Hybrid model for digital forensics investigation model [35]	✓	✓	✓	χ	✓	✓	✓	χ	χ	χ	✓	✓	χ	✓	χ	L	The weak points of this model is that it does not share the investigation report with others and is not aware of privacy and security principles.	This hybrid model was introduced by handling both physical evidence and logic evidence.

IoT Mobility Forensic[30]	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	M	The main weak points of this framework is that it does not take into consideration any policy for privacy and security through the investigation process.	This framework analyzes the evidence gathered from IoT devices.
IoT Forensic: identification And classification of evidence in criminal investigations [8]	✗	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	L	This framework focuses identification and collection stages	The authors focus on founding enhanced method to identify the right evidence and collect the evidence in a secure and efficient.
IoT forensics framework for smart environment [5]	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	*M*	The framework is lightweight for IoT environment. The main drawback is that it does not take into consideration any principles for privacy and security.	The idea of this framework is to introduce a novel digital forensics framework for smart environment such as smart home, smart office, etc.
IoT forensics framework for smart environment [5]	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	M	The framework is lightweight for IoT environment. The main drawback is that it does not take into consideration any principles for privacy and security.	The idea of this framework is to introduce a novel digital forensics framework for smart environment such as smart home, smart office, etc.

From the table 1, we can conclude that many authors have defined the process of digital forensics into three steps as shown in figure 2, where the acquisition step includes identification and collections stages. The second step deals with examination and analysis of evidence acquired from the crime scene to understand how and by whom the crime was committed. The outcome of the analysis reports including other documentation comprises the presentation step. This step ends with presenting complete analysis re-port in front of the court.

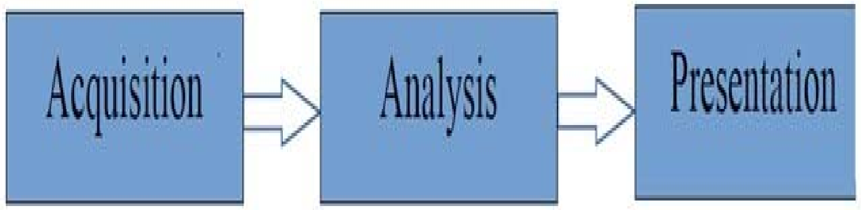


Figure 2: Main Forensics Step

2.2 IoT Forensics

Internet of Things (IoT) devices communicate with each other and interact with users on every day's activity through different sensors for different purposes such as monitoring, collection, and others. These capabilities of IoT devices have also enables the concept of a smart environment. The inter-action process between IoT devices and users in a smart environment generate data with large forensics value, as example for these forensics data in smart environment, the sensors that located at office, the presence on sponsors stat during unauthorized hour mean the existence individual inside the smart office, other example for smart environment forensic data is the data that related to the existence of smoke happening before the fire incident.

Several frameworks have been proposed for IoT forensics purposes [13][8][30][36][35][27][5]. The generic digital forensic framework for IoT that proposed in [13] contains many of advantages such as, it complies with the ISO/IEC 27043: 2015, other it supports security technique and incident investigation support. The proposed framework comprises three main layers, each layer consists of a set of stages as follow: First layer is the Proactive Process layer, which consists of IoT scenario definitions stage, IoT evidence source identification stage, planning incident detection stage, potential digital evidence collection stage, digital preservation stage, and storage for potential evidence. The Second layer which refers to IoT forensics layer, which contains different components that needed for IoT evidence such as cloud server that used as data centers for different evidence collected from IoT devices, Network infrastructure which used to transfer evidences from IoT devices and storage centers, and the last component refers to different IoT devices that responsible for collecting and sensing different forensic information. Finally, the Last layer is Reactive layer, which responsible for reactive between previous layers through different stages such as through initialization stage, acquisition stage, and investigation stages.

The framework proposed in [8] focuses on a specific stages of investigation process such as col- lection stage, the authors define main challenges that can face this stage when implement the investigation process on IoT environment. One of the main problems that can face this stage is finding the best evidence and locating hid- den devices because traditional digital forensic process does not fully fit the IoT environment. Therefore, the authors propose tools and techniques to identify and locate IoT device and the proposed solution for this problem consists of five main phases: The identification phase, the evidence collection phase with specific enhance tools, the preservation stage, the evidence examination and extraction phase, and last phase refers to data analysis and formalization phase. The mobility forensics model proposed in [30] deals with tools and techniques that work to- wards forensically sound recovery of data and evidence from mobile de-vices. The target of this model is to collect evidence from IoT devices in a smart environment, such as smart home to facilitate the investigation process in different crimes such in upper scenarios. This mobility forensics model consists of six stages: identification, collection, interpretation, preservation, analysis, and presentation [30].

In [36] the authors proposed a Digital Forensics

Investigation Model for IoT. The main aim of this model is improving the investigation process by exposing the hidden digital evidence. However, this model does not concern over the physical evidence, and this could be a major drawback when implemented in IoT forensics investigation process, due to the fact that physical evidence is the main concern in all cases of IoT forensics investigation process. The proposed model in [36] consists of the following stages: The initialization and preparation stage, Interaction stage which contains the acquisition stage, re-construction stage, and protection stage. Based on the drawbacks of this model a new hybrid approach was proposed to overcome these problems. The main idea of hybrid approach is to deal with digital and physical evidence. In [35], the author proposes a model for investigating with hybrid evidence which is joins the operations related to digital and physical evidence collection and examination, taking into consideration the special characteristics of each form of evidence. Another IoT framework proposed in [5] which is a light-weight version that suitable for IoT resources. This framework consists of two main components: The modifier which responsible for initialization and acquisition stage, and the second component is the analyzer, where all remaining stages of digital forensics investigation process falls under these two components. Table 2 shows some frameworks for IoT forensics environment.

Table 2. Achieved principles at each stage of DFIM

Stage	Principles
Pre-Investigation Stage	• Security principle by transferring evidence as encrypted format. • The accuracy is achieved by grouping the evidence by DPZ. • Performance is achieved by selecting a professional investigators related to the crime. • Data reduction is achieved by retrieving a group of data. •
Collection and Evaluation Stage	• The accuracy is achieved by collecting only the related evidence. • The privacy is achieved by searching and viewing only in related clusters. •
Preservation Stage	• Integrity is achieved by using a one - way hash function. • Non-repudiation is achieved by using a digital signature.
Examination and Analysis Stage	• Performance and accuracy are achieved dealing with a group of data which save time and resources. • Privacy is achieved by dealing with only related evidence.
Information Sharing Stage	• Accuracy and performance are achieved by requesting other evidence from external resources.

The table contains the framework name, the main stages of the framework, the main contribution and goals of the proposed framework, and the limitations if found in the proposed model.

In general, every stage of the IoT forensics frameworks faces challenges as follows:

- ✓ Challenges in the Identification Stage: One of the main challenges in this stage is how to find a specific IoT device, which responsible for the data collected [34].
- ✓ Challenges in the Preservation Stage: One of such challenges refer to volatile nature of sensed data, which require a solution to capture the evidence from its resources periodically and transfer it to fog or cloud zones [34].
- ✓ Challenges in the Collection Stage: Such challenges related to device location, da-ta location, limitation of IoT devices, and available tools needed for this stage.
- ✓ Challenges in the Analysis Stage: The challenges in this stage related to different data format and time access to the storage resource. In addition to that the analysis stage suffers from the problem of interaction with the IoT devices which have not graphical user interface [22] [9].

Challenges in the Presentation Stage: This stage faces different challenges such as analytic function that used through analysis stage which can change the structure and the meaning of the collected evidence [34].

3. DIGITAL FORENSICS INVESTIGATION MODEL (DFIM) FOR INTERNET OF THINGS

As previously mentioned in section one, an IoT is an information system made up of things, data, networks and services. Such things or objects may be sensors, traditional computers, smartphones, cameras, humans, tablets, vehicles, home appliances etc. These things are a combination of two types of systems:

1. General Purpose systems such as lap- tops, desktops and servers. Such systems may run a variety of applications, process, store, and upload data to internet. The data may be audio, video and conventional files.

2. Special Purpose Systems whose functions are more limited and whose objective is to deal with limited computation domains. The special purpose systems can be classified into two classes:

(a) Handheld Systems: handheld systems include tablets, IPads, PDAs, smartphones, etc. Hand- held data can be.

(b) Embedded Systems: Unlike general purpose systems and hand- held systems that run a variety of applications, embedded systems are designed for performing specific tasks. The embedded systems are found everywhere, from car engines, and manufacturing robots to DVDs, home appliances, etc.

The IoT architecture may vary from solution to solution, based on the type of solution which we intend to build. Therefore, there is no single consensus on IoT architecture which is agreed universally. Different IoT architectures have been proposed by different researchers like Three-Layer architecture [23] [21], Five-Layer architecture [33], Cloud-based IoT architecture [16] and Fog based IoT architecture [12] [34]. Based on the different IoT architectures, an IoT platform as basically three zones as shown in Figure 3:1. Cloud Zone: Cloud zone contains a group of computers and servers connected together over the internet and have unlimited capabilities in terms of storage and processing power. Cloud zone offers a solution to address the shortcomings issues of IoT objects. Therefore, IoT can benefit from the virtually unlimited capabilities and resources of cloud to compensate its technological constraints (e.g., storage, processing, and energy).2. Fog Zone: The fog is an extension of cloud computing, where the main idea off og computing is to place servers (fogs mini servers) closer to the perception layer to supports delay sensitive, location-aware and mobility-supported applications. It also provides computation, storage, and networking services between end devices and traditional cloud servers.3. Perception Zone: The perception zone contains IoT devices such as sensors, traditional computers, smartphones, cameras, humans, tablets, vehicles, home appliances etc.

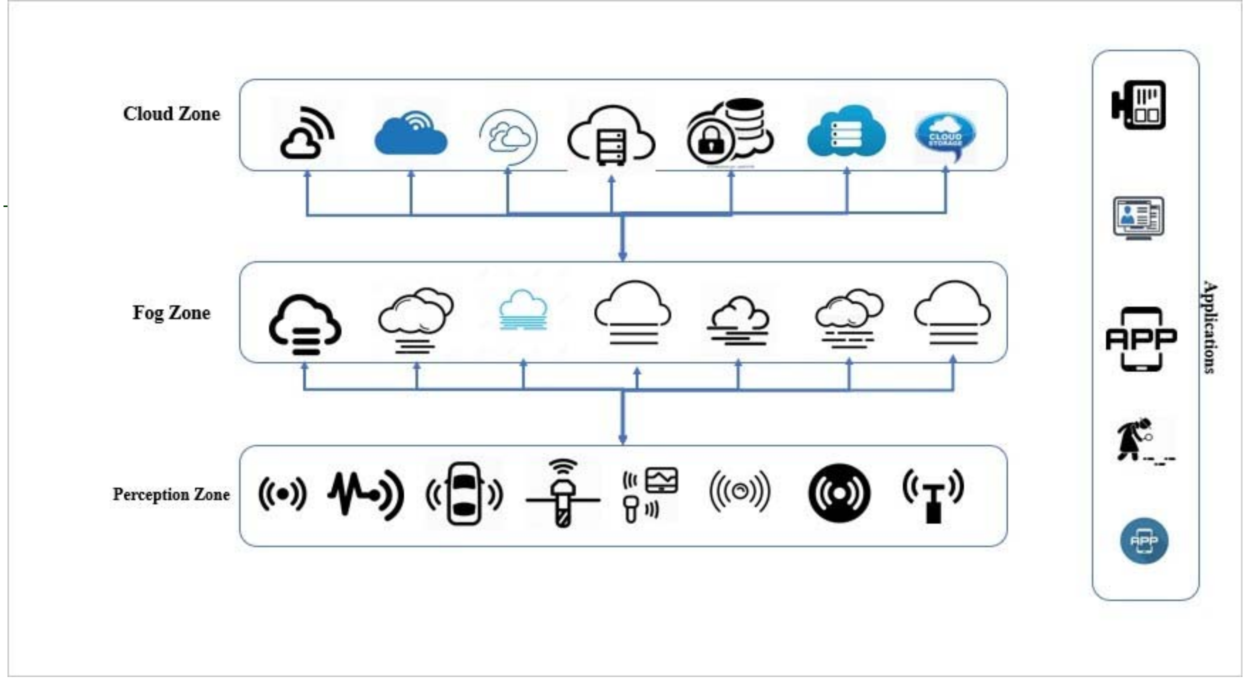


Figure 3: Source Of Iot Digital Evidence.

The above zones can be the source of the IoT evidence as shown in Figure 3. Therefore, our proposed DFIM model takes into consideration the above zones as a crime scene territory, the lo-cation and the type of devices in order to use and equate tool to collect the evidence. The components of the proposed DFIM are as follows: The Data Provider Zone which responsible for grouping all data gathered by sensor nodes into a set of groups, where each group contains data or documents related to each other, the investigation authority which receives the requests from the claimers for investigation, check the validation of the request, and finally select the appropriate investigators as shown in figure 4

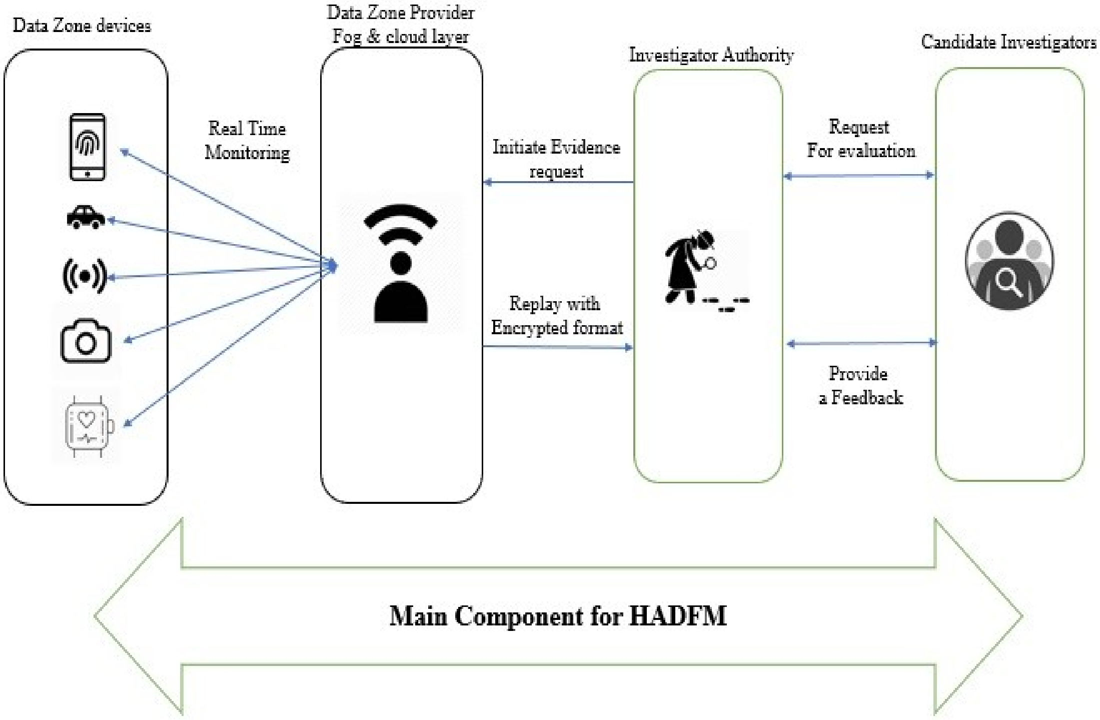


Figure 4: Main Components Of DFIM.

The Proposed DFIM consists of the following seven stages as shown in figure 6:

1. Pre-Investigation stage: This stage comprises the following four steps:
   A. Initialization Step: The aim of this step is to collect all needed information related to the crime such as location of the crime (zones and devices), and sent a report to investigation authority to initiate the investigation process.
   B. Validation Step: The function of this step is to validate the incoming re-port/request by the investigation authority (not malicious report) to start the investigation process.
   C. Selection Step: After validation the incoming request a professional committee will be selected to deal with the crime
   D. Preparation the Data Zone Step: The IoT zones can be the crime scene territory. Therefore, preparing devices in different zones for data collection is important, this can be done by the Data Provider Zone (DPZ) in fog or cloud zones which responsible for grouping all data gathered by sensor nodes into a set of groups, where each group contains data or documents related to each other.
2. Collection and Evaluation Stage: After preparation the devices in all IoT zones for evidence collection by DPZ, the investigators can start collecting the evidence from different groups located in different devices by using an appropriate tool which starts searching for a required evidence in a specific group that contains a high level of similarity with the tampered document based on Jaccard similarity measure. The groups that contain evidence are marked as a required group and sent back to investigation authority in a cipher format to achieve high levels of evidence security and privacy. The next process is the evaluation of collected evidence by the investigation authority to make sure that these evidence are fair enough to be accepted in the court, if the collected evidence are not enough then the investigators go back to collection stage for searching other evidence.
3. Preservation Stage: The goal of preservation stage is to achieve the integrity of collected evidence, to make sure that these evidences cannot be changed through the next stages of investigation process. The preservation process in the proposed DFIM uses a one-way hash algorithm to achieve the integrity.
4. Examination and Analysis Stage: The gathered evidence should be examined and analyzed by using one of the matching algorithms to define and extract the appropriate evidence related to the crime. During this stage the investigators can decide if the they need to search for another evidence or not. If the evidence provided by the DPZ at specific zone or device does not provide an enough evidence, then the solution is to go through the information sharing stage, which allows investigators to request help from out sources as dis-cussed in the next stage.
5. Information Sharing Stage: This stage involves remote entities for sharing the evidence between different investigators and data zone providers based on the nature of the crime and for a specific purpose and with limited permission over these evidences as shown in figure 5.

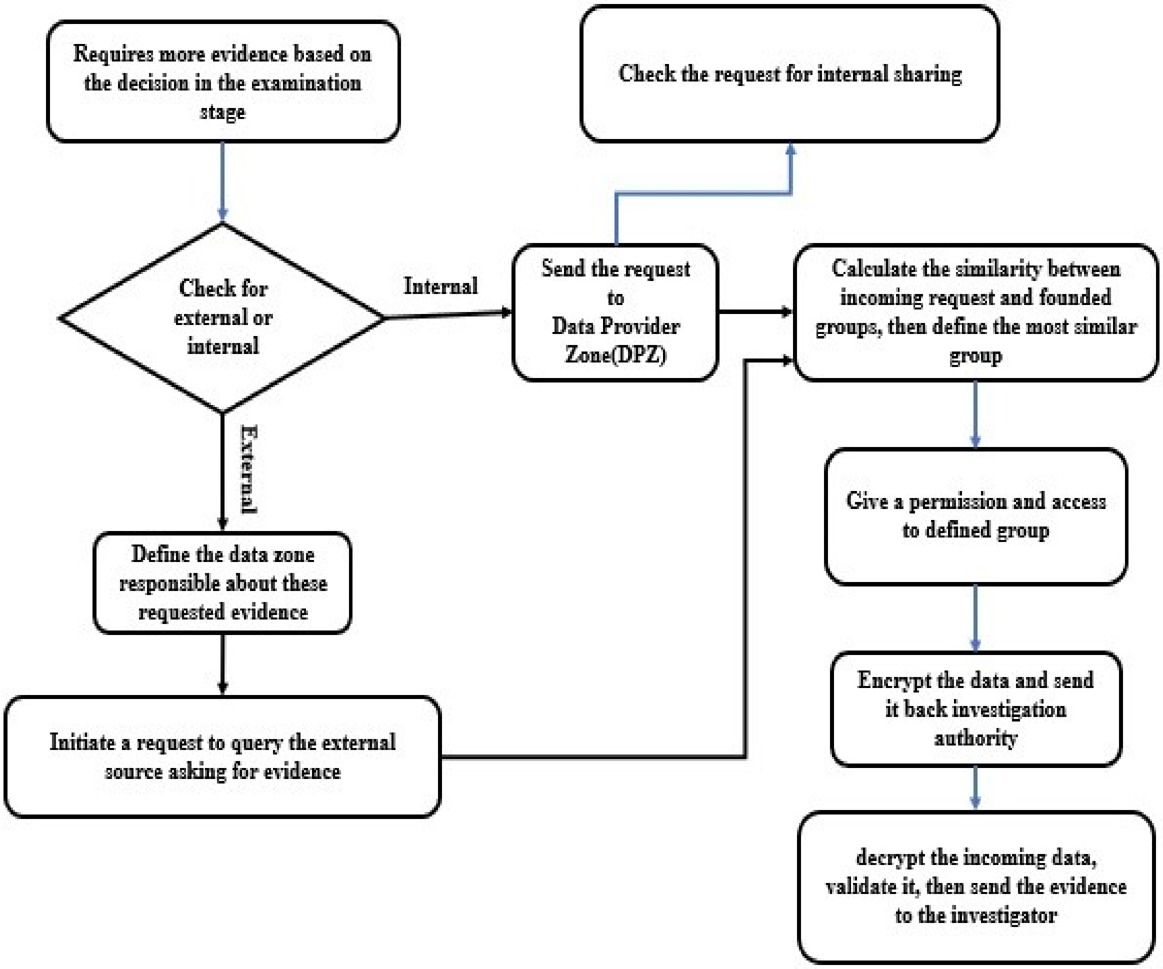
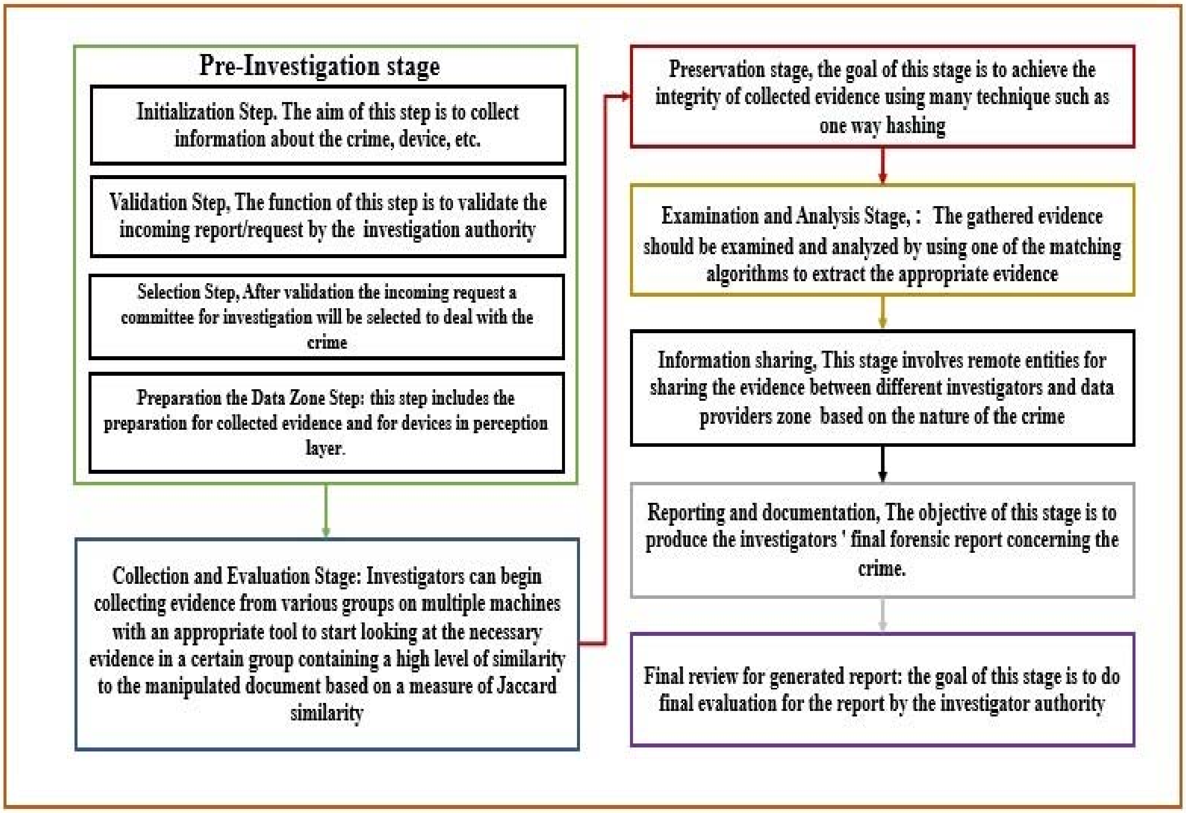

Requires more evidence based on the decision in the examination stage
Check the request for internal sharing
Check for external or internal
Internal
Send the request to Data Provider Zone(DPZ)
Calculate the similarity between incoming request and founded groups, then define the most similar group
External
Give a permission and access to defined group
Define the data zone responsible about these requested evidence
Encrypt the data and send it back investigation authority
Initiate a request to query the external source asking for evidence
decrypt the incoming data, validate it, then send the evidence to the investigator

Figure 5: The Process Of Requesting Internal And External Evidence.

6. Report and Documentation Stage: The goal of this stage is to generate a final forensics report related to the crime by the investigators. The final forensics report should contain information such as these tags taken during the investigation process, what tools were used, how the analysis was done, short description of phase s taken during the evaluation, examination, and analyzing such as string searches, recovering erased data, and finally the conclusion.

7. Final Review Stage: In this stage the investigation authority take a final decision represents the if the report formatted by the investigators is ready to submit to the court or not.



Pre-Investigation stage

Initialization Step. The aim of this step is to collect information about the crime, device, etc.

Validation Step. The function of this step is to validate the incoming report/request by the investigation authority

Selection Step, After validation the incoming request a committee for investigation will be selected to deal with the crime

Preparation the Data Zone Step: this step includes the preparation for collected evidence and for devices in perception layer.

Collection and Evaluation Stage: Investigators can begin collecting evidence from various groups on multiple machines with an appropriate tool to start looking at the necessary evidence in a certain group containing a high level of similarity to the manipulated document based on a measure of Jaccard similarity

Preservation stage, the goal of this stage is to achieve the integrity of collected evidence using many technique such as one way hashing

Examination and Analysis Stage, : The gathered evidence should be examined and analyzed by using one of the matching algorithms to extract the appropriate evidence

Information sharing, This stage involves remote entities for sharing the evidence between different investigators and data providers zone based on the nature of the crime

Reporting and documentation, The objective of this stage is to produce the investigators ' final forensic report concerning the crime.

Final review for generated report: the goal of this stage is to do final evaluation for the report by the investigator authority

Figure 6: Stages Of DFIM.

4. Evaluation

this section explains how does DFIM work through applying its stages by presenting an at-tack scenario in a smart environment such as library, hospital, etc. where a number of IoT devices and different technologies are used to manage and control this environment. The administrator of this environment have a so-called Digital Witness Device (DWD), which capable to detect and sore information initiated by any attack from any neighboring device. Suppose that the administrator's digital witness device detects an attack attempt initiated by a device nearby and stores all information related to this attack. Consider the administrator decides to request an investigation, then the administrator should send the evidence stored in the digital witness device to the investigation authority to investigate in happened cyber-crime. Applying the DFIM, the investigation process is as follows as shown in figure 7

- ✓ The investigation authority should validate the received request for starting the investigation process.
- ✓ Formatting a committee (investigators) for investigation based on the type of the crime.
- ✓ The investigators will send a request to the DPZ asking for evidence related to the tampered file.
- ✓ After approving the request, the DPZ will apply the appropriate tools to retrieve the evidence related to the tempered file.
- ✓ The collected evidence by the DPZ sends back to the investigation authority applying security techniques to achieve security principles, usually using digital signature and lightweight encryption algorithm.
- ✓ The investigation authority evaluates the received evidence to make sure that such evidence is fair enough to be accepted by the court, if the collected evidence is not enough then the investigators go back to collection stage for searching for another evidence. To make sure that the evaluated evidence cannot be changed through the next stages of investigation process, the preservation process is applied using a one-way hash algorithm to achieve the integrity.
- ✓ The evaluated evidence should examine and analyze using different matching

techniques to extract useful information related to the crime. If the extracted data cannot be useful or not enough to be presented to the court, then the information sharing stage in DFIM should be used to collect other related evidence from DPZ.

✓ The investigator committee generates the final report as mentioned in DFIM.

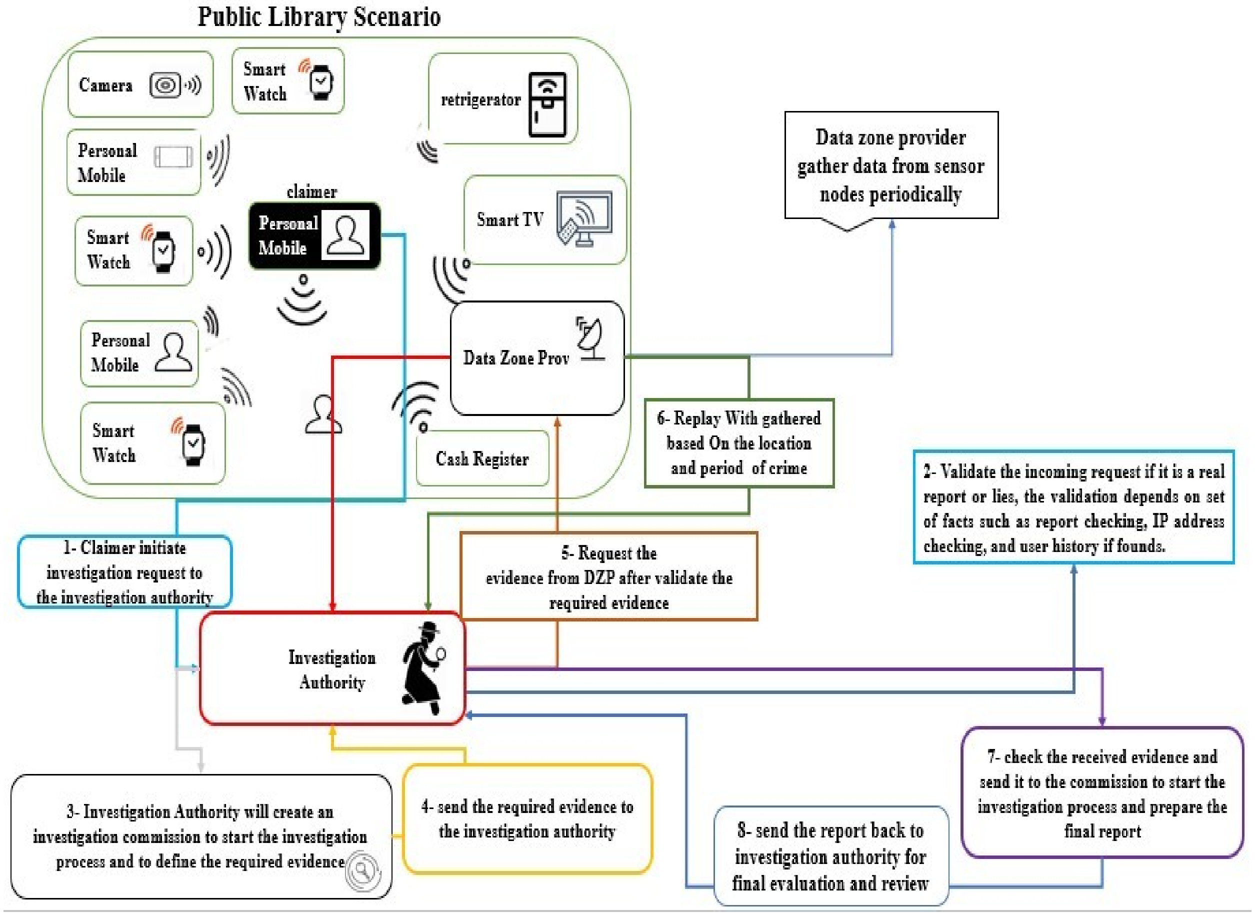

Public Library Scenario
Camera
Smart Watch
retrigerator
Personal Mobile
claimer
Personal Mobile
Smart TV
Smart Watch
Personal Mobile
Data Zone Prov
Smart Watch
Cash Register
Data zone provider gather data from sensor nodes periodically
6- Replay With gathered based On the location and period of crime
2- Validate the incoming request if it is a real report or lies, the validation depends on set of facts such as report checking, IP address checking, and user history if founds.
1- Claimer initiate investigation request to the investigation authority
5- Request the evidence from DZP after validate the required evidence
Investigation Authority
7- check the received evidence and send it to the commission to start the investigation process and prepare the final report
3- Investigation Authority will create an investigation commission to start the investigation process and to define the required evidence
4- send the required evidence to the investigation authority
8- send the report back to investigation authority for final evaluation and review

Figure 7: Main Stages For Proposed Model When Applied In A Public Library Scenario.

The proposed DFIM for IoT forensics takes into consideration the following security and privacy principles based in ISO/IEC 29100:2011 [24] [20] [19], and applies them during the lifecycle of investigation process as follows:

1. Availability: Availability ensures that the data is available to users at a required range of performance in any situation [10] [11] [28]. The availability in the DFIM can be achieved by grouping the data related to each other in one cluster.

2. Authentication: This principle can be achieved by adding a so called data zone provider in fog and cloud layers which acts as an authenticator for both investigators and devices in perception layer [3] [2] [31].

3. Integrity: Integrity can be achieved through the preservation phase which depends on using a signature technique to ensure the integrity of the evidence in all stages.

4. Authorization: The Investigators do not start the investigation process unless the legal

authority is obtained from the relevant authorities such as the court and investigation authority.

5. Non-repudiation: In the proposed DFIM non-repudiation can be achieved via a secure chain of custody, which uses a digital signature for all documents used in the process of investigation. vi) Confidentiality: Confidentiality can be achieved by using a lightweight encryption algorithm specified for IoT devices.

Table 3 shows how the DFIM can achieve the security, privacy and other principles such ac-curacy, performance, data reduction, Openness and transparency at each stage of DFIM.

Table 3: Different frameworks for digital forensics.

Framework	Comments	Stage1	Stage2	Stage3	Stage4	Stage5	Stage6	Stage7
VMcKemmish [18]	McKemmish is the first proposed model for digital forensics. This framework does not maintain the reduction and reviewing stages for the collected evidence.	Identification And Collection	Preservation	Examination	Presentation			
NIST [14]	The NIST model contains the basic stages of investigation process. It does not take into consideration security and privacy principles.	Collection	Identification And preservation	Examination	Analysis	Reporting		
Martini [17]	This framework does not have any stage for evaluation, either at initial stages or at later stages. proposed framework does not take the privacy of the collected evidence into consideration because there is no stage or action to give permission for collected data for authorized investigator.	Identification	Preservation	Collection	Examination And Analysis	Reporting and Presentation		

Beebe [7]	Beebe framework contains the main stages of standard digital forensics with some additional stages such as the preparation stage to prepare the report which contains the request order for investigation. This model does not have any suggestion to enhance the security for collected evidence neither on the level of transferring evidence from side to side or on the level of storing evidence. Another weak point of this model is the limitation in the accuracy for investigation process Preparati on Incident Response	Collection	Preservation and store	Analysis	Presentatio n	Incident Closer		
IDIP [6]	The model proposed differs from standard models, starting with the readiness stage, which presents the preparation of operations and infrastructure. Then the next stage refers to the deployment stage that can be part of the readiness stage, this stage of installing all the necessary software and discovering the crime. After that, the main stages of the standard investigation process begin. And the final phase refers to the results of the investigation.	Readiness	Deployment	Trace-back	Dynamite	Review		

Cohn [15]	The Cohen model does not take into consideration any of security and privacy principles such evaluation for the collected evidence, evaluation for the selected investigator. Other comment here is the evaluation for the produced report before presenting to the court	Identification	Collection	Collection And Preservation	Transportation Storage	Analysis	Interpretation And Attributes	Presentation
Agrawal Framework [1]	This framework consists of the main stages of digital forensics process. One of comments on this model is the needs for an initial evaluation stage for collected evidence before starting the examination process, another comment refers to achieve the security principles either through the transporting for collected evidence or at the place of storing evidence Preparation Securing and recognition.	Preparation	Securing and recognition.	Evidence Collection	Preservation	Analysis	Presentation	Result And Review
Perumal [26]	This framework does not have any evaluation stage to evaluate collected evidence or produced report from the investigation process.	Planning	Identification	Collection	Analysis	Proof and Defense Result	Review	
Perumal [27]	Perumal framework does not set any criteria to collect evidence from the identified device. No any action to achieve the security in this framework. There is no any suggestion to ensure the conditionality and privacy for the collected evidence.	Planning	Device Identification Triage	Examination Router or Fog or getaways servers	Lab analysis	Archive and Storage		
Quick and Choo Framework [29]	This framework is considered as one of the strongest frameworks in digital forensics. In addition to standard stages of forensics process, this	Commence	Preparation	Identify and collection.	Reduction and reviewing.	Evidence analysis.	Presentation-on.	Complete

	framework has a review stage for collected evidence in order to enhance the accuracy and performance for the investigation process.							

5. Important questions

5.1 What is new in proposed solution?

Proposed idea to investigate in the crimes happened in IoT devices added a lot of new stages for evaluation and validation purposes. Such as the pre-investigation stage, the information sharing stage, evaluation stage, and final review stage. Each of these stages is important to enhance the investigation process.

5.2 What are the points which distinguish the proposed model from the existing models?

The proposed model characterized by the ability to verify and test collected evidence, where the stage of validation of evidence in the proposed model was implemented in the initial stage before beginning the investigation process, which called the pre-investigation stage in the proposed model. The stage which responsible for evaluation for collected evidence was applied through the stage of collection in proposed model, these two stages distinguish the proposed solution from other solutions that proposed to investigate in IoT forensics. Another important point distinguishing the solution proposed applies to the final review before sending the final report to the court, which it is important to assess the document to ensure that the report is approved in court, this point is different and evolves over all prior approaches that do not take any strategy to evaluate the investigation report before submitting it to the court.

5.3 What is the contribution for the proposed model?

As a summary, the proposed solutions differ from the previous solutions since the proposed solution overcomes all the shortcomings and issues facing previous solutions such as the validity of the evidence gathered, and the validity of the tools and third parties involved in the investigation process and other points listed in the previous question. Moreover, the proposed solution is made up of two main components, the data zone provider and the investigation authority, where each component has its own responsibility to improve the investigation process from the validation and evaluation side, as stated in the previous sections.

5.4 What is the validity of the study?

The aim of this study is to find a comprehensive solution for the investigation of crimes committed in the IoT environment, where the proposed solution has added a number of stages to overcome all issues facing the IoT investigation framework. The proposed model consists of two main components of the investigation authority and the data zone provider, each of which has a set of responsibilities to enhance and improve the investigation process. The solution overcomes many of the issues facing the related framework in the IoT forensics file based on the new stages added and the components used.

6. Conclusion

In this paper, we propose a New Digital Forensics Investigation Model for Internet of Things (DFIM) which has two main components: The Data Zone Provider which responsible for grouping all data gathered by sensor nodes into a set of groups, where each group contains data or documents related to each other, and the investigation authority which receives the requests from the claimers for investigation, check the validation of the request, and finally select the appropriate investigators. The DFIM consists of seven stages and takes into consideration a set of principles such as security, privacy and other principles such accuracy, performance, data reduction, Openness and transparency in order to improve the IoT forensics investigation process. proposed solution achieve the security and privacy through adding a pre-investigation stage which responsible about validation for the evidence which will sent back to the investigation authority. The principle of data reduction and accuracy other achieved through the new stages which added through proposed solution by filtering the evidence collected and evaluation for these evidence if it has a direct relation with the crime or not, and the accuracy achieved from multi-level of validation for collected evidence.

REFERENCES

[1] Ankit Agarwal, Megha Gupta, Saurabh Gupta, and Subhash Chandra Gupta. Sys-tematic digital forensic investigation model.International Journal of Computer Scienceand Security (IJCSS), 5(1):118–131, 2011.

[2] Areej Al-Shorman and Mohammad Qatawneh. Performance of parallel rsa oniman1 super computer. International Journal of Computer Applications, 180:31–36,04 2018.

[3] Mohammed Alkhanafseh and Mohammad Qatawneh. A parallel chemical reaction optimization algorithm for maxflow prob-lem.International Journal of ComputerScience and Information Security,, 15:19–32, 06 2017.

[4] Ahmad W Atamli and Andrew Martin. Threat-based security analysis for the inter-net of things. In2014 International Work-shop on Secure Internet of Things, pages35–43. IEEE, 2014.

[5] Leonardo Babun, Amit Kumar Sikder, Abbas Acar, and A Selcuk Uluagac.Iotdots: A digital forensics frameworkfor smart environments.arXiv preprintarXiv:1809.00745, 2018.

[6] Venansius Baryamureeba and Florence Tushabe. The enhanced digital investigation process model. InProceedings ofthe Fourth Digital Forensic Research Work-shop, pages 1–9, 2004.

[7] Nicole Lang Beebe and Jan Guynes Clark. A hierarchical, objectives-based framework for the digital investigations process. Digi-tal Investigation, 2(2):147–167, 2005.

[8] François Bouchaud, Gilles Grimaud, and Thomas Vantroys. Iot forensic: identification and classification of evidence in criminal investigations. In Proceedings of the13th International Conference on Availability, Reliability and Security, page 60. ACM,2018.

[9] Stephen D Burd, Darrin E Jones, and Alessandro F Seazzu. Bridging differences in digital forensics for law enforcement and national security. In2011 44th Hawaii International Conference on System Sciences, pages 1–6. IEEE, 2011.

[10] Ahmad Bany Doumi and Mohammad Qatawneh. Performance evaluation of parallel international data encryption algorithm on iman1 super computer. Available at SSRN 3350418, 2019.

[11] Heba Harahsheh and Mohammad Qatawneh. Performance evaluation of two fish algorithm on iman1 supercomputer. International Journal of Computer Applications, 179:1–7, 06 2018.

[12] Pengfei Hu, Sahraoui Dhelim, Huansheng Ning, and Tie Qiu. Survey on fog computing: architecture, key technologies, applications and open issues. Journal of network and computer applications, 98:27–42, 2017.

[13] Victor R Kebande and Indrakshi Ray. Ageneric digital forensic investigation frame-work for internet of things (iot). In2016IEEE 4th International Conference on Future Internet of Things and Cloud (Fi-Cloud), pages 356–362. IEEE, 2016.

[14] Karen Kent, Suzanne Chevalier, Tim Grance, and Hung Dang. Guide to integrating forensic techniques into incident response. NIST Special Publication,10(14):800–86, 2006.

[15] Michael Donovan Kohn, Mariki M Eloff, and Jan HP Eloff. Integrated digital forensic process model. Computers & Security,38:103–115, 2013.

[16] Yang Liu, Jonathan E Fieldsend, and Geyong Min. A framework of fog computing: Architecture, challenges, and optimization. IEEE Access, 5:25445–25454, 2017.

[17] Ben Martini and Kim-Kwang Raymond Choo. An integrated conceptual digital forensic framework for cloud computing.Digital Investigation, 9(2):71–80, 2012.

[18] Rodney McKemmish. What is forensic computing? Australian Institute of Criminology Canberra, 1999.

[19] Alexandra Michota and Sokratis Katsikas. Compliance of the LinkedIn privacy pol-icy with the principles of the iso 29100:2011 standard. In International Conference on Web Information Systems Engineering, pages 72–83. Springer, 2014.

[20] Chris Mitchell. Privacy, compliance and the cloud. In Guide to Security As surancefor Cloud Computing, pages 3–14. Springer,2015.

[21] Mainak Mukherjee, Isha Adhikary, Surajit Mondal, Amit Kumar Mondal, Meen akshiPundir, and Vinay Chow dary. A vision of iot: Applications, challenges, and opportunities with dehradun perspective. In Proceeding of International Conference on

Intelligent Communication, Control and Devices, pages 553–559. Springer, 2017.

[22] Syed Naqvi, Gautier Dallons, and Christophe Ponsard. Applying digital forensics in the future internet enterprise systems-european sme’s perspective. In2010 Fifth IEEE International Workshopon Systematic Approaches to DigitalForensic Engineering, pages 89–93. IEEE,2010.

[23] Anne H Ngu, Mario Gutierrez, VangelisMetsis, Surya Nepal, and Quan Z Sheng.Iot middleware: A survey on issues andenabling technologies.IEEE Internet ofThings Journal, 4(1):1–20, 2017.

[24] Nicolás Notario, Alberto Crespo, Yod-Samuel Martín, Jose M Del Alamo, DanielLe Métayer, Thibaud Antignac, AntonioKung, Inga Kroener, and David Wright. Pripare: integrating privacy best practicesinto a privacy engineering methodology. In2015 IEEE Security and Privacy Work-shops, pages 151–158. IEEE, 2015.

[25] Edewede Oriwoh, David Jazani, Gregory Epiphaniou, and Paul Sant. Internet of things forensics: Challenges and approaches. In9th IEEE International Conference on Collaborative computing: networking, Applications and Worksharing, pages 608–615. IEEE, 2013.

[26] Sundresan Perumal. Digital forensic model based on Malaysian investigation process.International Journal of Computer Scienceand Network Security, 9(8):38–44, 2009.

[27] Sanderson Perumal, Norita Md Norwawi,and Valliappan Raman. Internet of things(iot) digital forensic investigation model: Top-down forensic approach methodology. In2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), pages 19–23. IEEE,2015.

[28] Mais Haj Qasem and Mohammad Qatawneh. Parallel hill cipher encryption algorithm. International Journal of Computer Applications, 179(19):16–24,2018.

[29] Darren Quick and Kim-Kwang Raymond Choo. Data reduction and data mining framework for digital forensic evidence: storage, intelligence, review and archive. Trends & Issues in Crime and Criminal Justice, 480:1–11, 2014.

[30] KM Sabidur Rahman, Matt Bishop, and Albert Holt. Internet of things mobilityforensics.de Proceedings of the 2016 In-formation Security Research and Education(INSuRE), 2016.

[31] Mahmoud Rajallah Asassfeh, Mohammad Qatawneh, and Feras Alazzeh. Performance evaluation of blowfish algorithm on supercomputer iman1.International jour-nal of Computer Networks Communications, 10:43–53, 03 2018.

[32] Maha Saadeh, Azzam Sleit, Mohammed Qatawneh, and Wesam Almobaideen. Authentication techniques for the internet of things: A survey. In2016 Cyber security and Cyber forensics Conference (CCC),pages 28–34. IEEE, 2016.

[33] Bhagya Nathali Silva, Murad Khan, and Kijun Han. Internet of things: A comprehensive review of enabling technologies, architecture, and challenges. IETE Technical review, 35(2):205–220, 2018.

[34] Sunu Thomas, KK Sherly, and S Dija. Extraction of memory forensic artifacts from windows 7 ram image. In2013 IEEE Conference on Information & Communication Technologies, pages 937–942. IEEE, 2013.

[35] Konstantinos Vlachopoulos, Emmanouil Magkos, and Vassileios Chrissikopoulos. A model for hybrid evidence investigation. International Journal of Digital Crime and Forensics (IJDCF), 4(4):47–62, 2012.

[36] Yunus Yusoff, Roslan Ismail, and Zainud-din Hassan. Common phases of computerforensics investigation models. International Journal of Computer Science & In-formation Technology, 3(3):17–31, 2011.

[37] Nurul Huda Nik Zulkipli, Ahmed Alenezi,and Gary B Wills. Iot forensic: Bridging the challenges in digital forensic and the internet of things. In International Conference on Internet of Things, Big Data and Security, volume 2, pages 315–324.SCITEPRESS, 2017.