International Journal on Advanced Science Engineering Information Technology

Vol.8 (2018) No. 1
ISSN: 2088-5334

Adding Digital Forensic Readiness as a Security Component to The IoT Domain

Victor R. Kebande [#1], Nickson M.Karie[*], H.S.Venter [#2]

[#] *Department of Computer Science, University of Pretoria, Private Bag X20, Hatfield 0028, Pretoria, South Africa.*
E-mail: [1]vkebande@cs.up.ac.za, [2]hventer@cs.up.ac.za

* *Department of Computer Science, University of Swaziland, Private Bag 4, Kwaluseni. Swaziland*
E-mail: nickson.karie@gmail.com

***Abstract*— The unique identities of remote sensing, monitoring, self-actuating, self–adapting and self-configuring "things" in Internet of Things (IoT) has come out as fundamental building blocks for the development of "smart environments". This experience has begun to be felt across different IoT-based domains like healthcare, surveillance, energy systems, home appliances, industrial machines, smart grids and smart cities. These developments have, however, brought about a more complex and heterogeneous environment which is slowly becoming a home to cyber attackers. Digital Forensic Readiness (DFR) though can be employed as a mechanism for maximizing the potential use of digital evidence while minimizing the cost of conducting a digital forensic investigation process in IoT environments in case of an incidence. The problem addressed in this paper, therefore, is that at the time of writing this paper, there still exist no IoT architectures that have a DFR capability that is able to attain incident preparedness across IoT environments as a mechanism of preparing for post-event response process. It is on this premise, that the authors are proposing an architecture for incorporating DFR to IoT domain for proper planning and preparing in the case of security incidents. It is paramount to note that the DFR mechanism in IoT discussed in this paper complies with ISO/IEC 27043: 2015, 27030:2012 and 27017: 2015 international standards. It is the authors' opinion that the architecture is holistic and very significant in IoT forensics.**

***Keywords*— digital forensic readiness; internet of things; architecture**

INTRODUCTION

The world is currently experiencing a transformation, and at the same time, it is being ushered into a new error of Internet of Things (IoT) technologies. With these transformations, many solutions to existing problems will, therefore, depend on fairly complex architectures [1]. It is for this reason that the European Lighthouse Integrated Project on the IoT Architecture [2] did address for three years the Internet-of-Things Architecture, and created the proposed architectural reference model together with the definition of an initial set of key building blocks. Together the key building blocks are envisioned as foundations that have fostered the emergence of the Internet of Things (IoT) [2].

These initiatives in the IoT domain, however, necessitate the creation of applications and services by exploiting existing physical things. This, further, creates a more complex and heterogeneous environment which is slowly becoming a home to cybercriminals. As a way to counter the cyber-attacks as well as maximize the potential use of digital evidence while minimizing the cost of conducting a digital forensic process in IoT environments; Digital Forensic Readiness (DFR) therefore becomes inevitable in existing IoT environments. Nevertheless, these aspects can also be backed by the top 10 predictions by the International Data Corporation (IDC) [3]. IDC foresees that the growth of IoT will be driven by industries and until 2020 it will grow by a double digit. Nevertheless, a projection on global spending of IoT has been estimated to reach $1.29 trillion by 2020 with "smart home" investments projected to reach $63 billion [3]. This, among other predictions, has shown that IoT is the hot buzzword at the time of writing this paper and therefore the need to come up with proactive and standardized approaches that can help to fight cyber-related incidents.

In this paper, therefore, the authors propose an architecture with the forensic capability of incorporating DFR to the IoT domain for proper planning and preparing for potential security incidents in IoT environments. The primary problem addressed in this study can, therefore, be stated as that: at the time of writing this paper, there still existed no IoT architecture or frameworks that have a capability of incorporating DFR in order to help attain incident preparedness in IoT environments.

The main focus of this research paper is, therefore, to present the architecture in the best way possible such that the IoT environments are able to be forensically prepared for digital investigations. The paper is presented in three folds. Firstly, a high-level of the architecture is presented, which is thereafter followed by a detailed architecture. Later, a hypothetical scenario that addresses the lack of the proposed processes in the architecture is presented. The case scenario has been used as a basis that outlines the impacts of lacking DFR in a given environment and the benefit when the architecture is employed.

As for the remainder of this paper, Section II presents reviews on materials and methods. Thereafter, Section III presents the results and discussion of the proposed Architecture for Adding DFR to the IoT Domain, and finally, Section IV concludes the research work and mentions a possible future work. The next section briefs the reader on the materials and methods used.

MATERIALS AND METHODS

In this section, the authors present a background review of Digital Forensics (DF), Digital Forensic Readiness (DFR), IoT Domain and Architecture (IDA). DF is discussed to show how forensics as science can be used to gather Digital Forensic Evidence (DFE) to be used in both for legal or civil proceedings. DFR is discussed to show the proactive side of DF, IDA is discussed to show a new technology that is being adopted by a majority of organisations to provide interconnectivity of devices, which makes it possible to collect, process, and analyse data from almost every object.

A. Digital Forensics

Digital Forensics (DF) as discussed by Karie and venter [4] is a growing field that is gaining popularity among many computer professionals, Law Enforcement Agencies (LEA), forensic practitioners, and other stakeholders who must always cooperate. According to Desai et al., [5], this field has become very important due to the increase in digital crimes. In the context of this paper, the goal of DF is to examine digital media in a forensically sound manner but with additional standardised guidelines [6] and trusted procedures designed to create legal audit trails [4].

In a growing field like DF, developing practical methodologies and specifications for different areas of application is thus essential and as important as the research itself [7]. It is on these grounds that the authors in this paper are proposing the inclusion of DFR as a security component to the IoT domain. Based on the aspects mentioned beforehand, the next section explains the concept of DFR.

B. Digital Forensic Readiness

DFR, as discussed by Mohay [8], is the extent to which computer systems or computer networks record activities and data. This is done in such a manner that the records are sufficient to their extent for subsequent forensic purposes, and the records are acceptable in terms of their perceived authenticity as evidence in subsequent forensic investigations. However, Cobb [9] adds that DFR sounds like a daunting challenge to many organizations today. As a matter of fact, the emergence of the IoT environments has brought about a more complex and heterogeneous environment which is slowly becoming home to cyber attackers. For this reason, it is necessary for organizations to have some form of forensic readiness so as to help them in planning and preparing for potential cybersecurity incidents. This scenario has motivated this research hence the need to incorporate DFR as a security component to the IoT domain.

DFR as a process has also been explained in the ISO/IEC 27043:2015 standard as a process that occurs before incident identification and involves the collection, preservation, storage, and analysis of digital evidence [6]. ISO/IEC 27043 is an international standard for Information Technology-Security Techniques-Incident Investigation Principles and Processes. An overview of the readiness processes as discussed in the ISO/IEC 27043 standard is briefly explained in the section to follow.

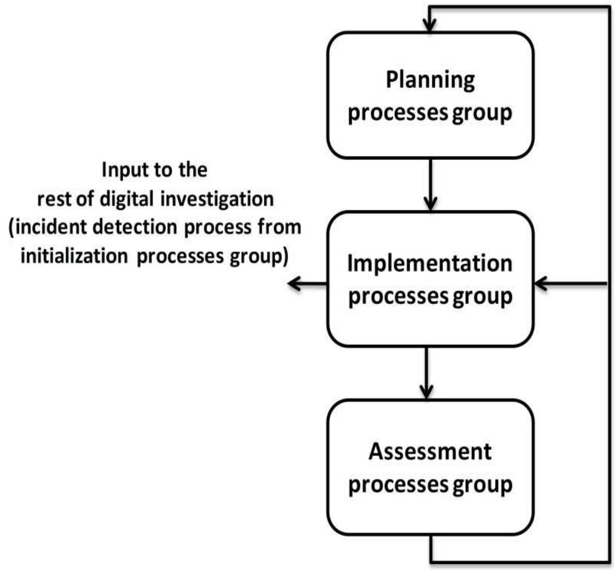

Planning processes group
Input to the rest of digital investigation (incident detection process from initialization processes group)
Implementation processes group
Assessment processes group

Fig. 1 Readiness processes groups (Source [6])

The readiness processes include the class of processes dealing with setting up an organization in such a way that, in the case that a digital forensic investigation is required, such an organization possesses the ability to maximize its potential to use digital evidence whilst minimizing the time and costs of an investigation. This class of processes is optional to the digital investigation processes and is affected by an organization rather than the investigator(s). The aims for having DFR processes in organizations as stated in the ISO/IEC 27043 [6] include:

- To maximize the potential use of digital evidence;
- To minimize the costs of digital investigations incurred either directly onto the organization's system, or related to the system's services;
- To minimize interference with and prevent interruption of the organization's business processes;
- To preserve or improve the current level of information security of systems within the organisation.

Fig. 1 depicts the readiness process groups as described in the ISO/IEC 27043. These process groups include *planning processes group*, *implementation processes group* and *the assessment processes group*.

The planning processes group includes all readiness processes that are concerned with planning activities, including scenario definition, identification of PDE sources, planning pre-incident collection, storage and handling of data representing PDE, planning pre-incident analysis of data representing PDE, planning incident detection, and defining system architecture.

The implementation processes group includes the following readiness processes: implementing system architecture, implementing pre-incident collection, storage and handling of data representing PDE, implementing pre-incident analyses of data representing PDE and implementing incident detection. These processes are concerned with the implementation of the results of the planning processes.

Finally, the assessment processes group includes two readiness processes: assessment of implementation and implementation of assessment results. For a detailed explanation of all the DFR processes and sub-process, we refer the reader to the ISO/IEC 27043. The next section explains the IoT Domain and Architecture.

C. IoT Domain and Architecture

With the dynamism of modern technology, the IoT domain is bound to accommodate a wide range of technologies including but not limited to: stateless and stateful technologies, extremely constrained as well as unconstrained technologies, hard real-time and soft real-time technologies among others. For this reason, single reference architecture may not be used as a representation for all possible implementations. While a reference model can probably be identified, it is likely that several reference architectures will co-exist in the IoT domain.

The word architecture is used in this paper to mean: a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation.

To deliver an end-to-end IoT solution, as stated by Emil [10], architectures will, therefore, require smooth interoperability across the different technology domains.

Some of the technology domains which also comprise a specific set of products, services, and skills are briefly explained below [10]:

1) The Device Domain: This domain encompasses connected assets including sensors, devices, and modules.

2) The Local Network Domain: This domain includes connectivity technologies enabling internal transfer of data from sensors and devices to other devices or a local network gateway.

3) The Wide Area Network Domain: This domain contains connectivity technologies enabling the transfer of data directly from devices or local network gateways to external service enablement domain.

4) The Service Enablement Domain: This domain has platforms and middleware.

5) The Applications And Data Domain: This domain is all about provisioning, development, storage, and management of applications and data.

6) The Enterprise Systems Domain: This domain has the back-end enterprise/ corporate systems.

It is important to note at this point that, the configuration of the named domains may change from use-case to use-case. However, whatever the use-case, organizations have the responsibility to identify the tools and enablers which make implementing IoT solutions across these domains easy and simple. The next section explains the related work in this paper.

D. Related Work

Although research on IoT is currently on the rise, there is, however, little research focus as at the time of conducting this study on architectures that incorporating DFR to IoT environments. Some of the existing literature has mentioned the DFR process explicitly, while others have the DFR process as an implicit process, however, most of them have shown the necessity for a DFR process in the emerging IoT environments. In this section of the paper, therefore, a summary of some of the most prominent efforts in previous research work is presented.

In a paper by Mohamed et al., [11] a description is given about a comprehensive approach to identifying the factors that contribute to DFR and how these factors work together to achieve forensic readiness in an organization. In this research, a conceptual framework for organizational forensic readiness was developed, and a future work towards the empirical validation and refinement of the framework was defined. However, this framework did not have a focus on DFR in IoT environments that could allow proper planning and preparing for potential cyber security incidents as is the case of the current paper.

In another presentation, Groble and Louwrens [12] argue that, in a world where cyber-crime is constantly increasing and pervasive computing is on the rise, information is becoming the most sought-after commodity in the world today, thus, making effective and efficient information security architecture programs is essential. For this reason, the authors then examine the overlap between DF and information security, to determine the relevance of DFR to information security and propose the inclusion of certain aspects of DFR as a component for best practice for information security with a focus to IoT. Groble and Louwrens [12] presentation did not have any component of DFR that was focused towards IoT environments.

More efforts by Pooe and Labuschagne [13] show that the ever-growing threats of fraud and security incidents to law enforcement and organizations present many challenges across the globe. This situation has brought about the need for organizations to build effective incident management strategies, which will enhance the company's reactive capability to security incidents. Their study then proposes proactive activities an organization can undertake in order to increase its ability to respond to security incidents and create a digitally forensic ready workplace environment. While their research focuses on organizations, it does not mention the integration of DFR in IoT environments.

Abdul et al., [14] state that, as of the time of their study, there existed not many discussions on Wireless Body Area Network (WBAN) security impact and security threats. For this reason, they propose a practical approach to assessing WBAN security impact in order to identify, evaluate, and develop a Secure Network Architecture (SNA) complete with DFR capability to secure WBAN implementation. Their architecture, however, did not focus purely on IoT environments as is the case of this paper. Additionally, on IoT, Kebande et al., [19] have proposed countermeasures that can mitigate the "Smart Refrigerator" being used in a clandestine approach to perpetuate cyber-crime. In this study, the authors are able to identify a major weakness that "smart home appliances" possess. Other research in IoT has focussed on public weather and placement of sensor nodes in networks that can be used in IoT-based approach [21], [22].

In research by Editya, Sumpeno and Pratomo [23], the authors tried to use Augmented Reality (AR) to monitor Xbee based IoT device. As a result, they found out that, there is a different result between ZigBee Protocol and IEEE 802.14.5 real-time monitoring system. This research too did not directly mention the integration of DFR in IoT environments as is the case of this paper.

There also exist other related works on DFR models and frameworks, but neither those nor the cited references in this paper have presented DFR architecture for IoT environments in the way that is introduced in this paper. However, we acknowledge the fact that the previously proposed models and frameworks have offered useful insights toward the development of the architecture for adding DFR to the IoT domain in this paper. In the section that follows the authors briefly explain the architecture for adding DFR to the IoT domain.

Results and Discussions

This section presents the architecture for adding DFR to IoT domain as a contribution to how DFR proactive processes can be utilized in the IoT-based environment. The authors concentrate on discussing the important DFR aspects that can forensically prepare an IoT-based environment to be able to manage and possibly thwart potential security incidents. This has been presented using an architecture called DFR for the Internet of Things (DFR-IoT), which is presented in two approaches as shown in Fig. 2 and Fig. 3 respectively. Additionally, based on the functionalities of the DFR-IoT, a hypothetical scenario is also discussed in the later section of this paper. In order for the DFR-IoT architecture to achieve its functionalities, the architecture must satisfy the following aspects:

- Be able to establish a communication mechanism through an interconnection that involves Machine-to-Machine (M-2-M) connectivity.
- Be able to send and receive data from a source to a destination through a well-connected IoT mechanism.
- Be able to transmit data over the web where it also supports the Internet Protocol (IP) addresses.
- Be able to support digital forensic investigative capabilities.

The next subsection will now discuss the high-level view of DFR-IoT Architecture.

A. *High-level Overview of DFR-IoT Architecture*

Fig. 2 shows the high-level view of the architecture which is then followed by an all-inclusive DFR-IoT architecture that is presented later on in Fig. 3. From Fig. 2, the reader can infer that the high-level view of the DFR-IoT architecture consists of three distinct entities namely: Proactive Process (PP), IoT Communication Mechanism (IoT-CM) and Reactive Process (RP).

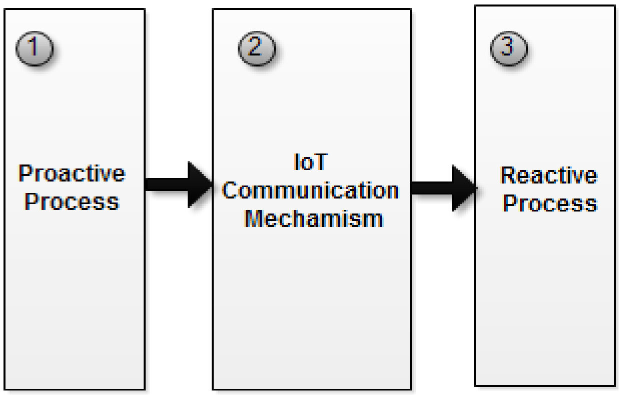


Fig. 2 High-level view of the DFR-IoT architecture

The PP deals with pre-incident detection strategies while the IoT-CM provides smart communication strategies for the M-2-M devices over an intelligent network. Next is the RP which is a post-event response process that deals with digital investigation processes. Each of the entity has been described in detail in the all-inclusive DFR-IoT architecture using Fig. 3.

B. *All-inclusive DFR-IoT Architecture*

In this section, the authors present an all-inclusive DFR-IoT architecture which is an expansion of the initially presented high-level architecture shown in Fig. 2. The high-level architecture in Fig. 2 is divided into three entities, each containing a number of modules as shown in the all-inclusive architecture in Fig. 3. Firstly, the proactive process labeled 1 consists of the ISO/IEC 27043 readiness guidelines, techniques of implementing readiness, readiness processes and readiness reporting. The second process which is labeled 2, is the IoT mechanism, it consists of IoT Intelligent Network (IoT-IN), IoT Operating System (IoT-OS), IoT Network Functionalities (IoT-NF), IoT Device Functionality (IoT-DF) and IoT devices. The third part of the DFR-IoT is the reactive process labeled 3. It is the core Digital Forensic Investigation (DFI) part of the architecture, and it consists of the investigative part of the ISO/IEC 27043 [5]. It comprises of initialization, acquisitive and investigative part. Each of the above-mentioned processes in the architecture has been explained in detail in the sections that follow.

1) *Proactive Process (PP)*: The proactive process has been represented in the first rectangle of Fig. 3 and labeled as 1. It consists of the following modules: readiness guidelines, techniques of achieving forensic readiness, proposed readiness processes and reporting. Each of the proactive process modules has been explained below.

- *Readiness Guidelines*

Note that the concepts that have been proposed in this paper comply and are inclined towards the guidelines that have been mentioned in the ISO/IEC 27043 international standard which is a standard for information technology-security techniques-incident investigation principles and processes. These guidelines are able to encapsulate different models that have been idealized in order for them to enhance a practice that allows forensic processes for capturing digital evidence for purposes of investigation to be implemented (ISO/IEC 27043: 2015). In the context of this paper, the author gives a description based on the following readiness process groups' aspects that are highlighted in ISO/IEC 27043 guidelines. It is important to say that these readiness aspects are treated as functional requirements in any organization.

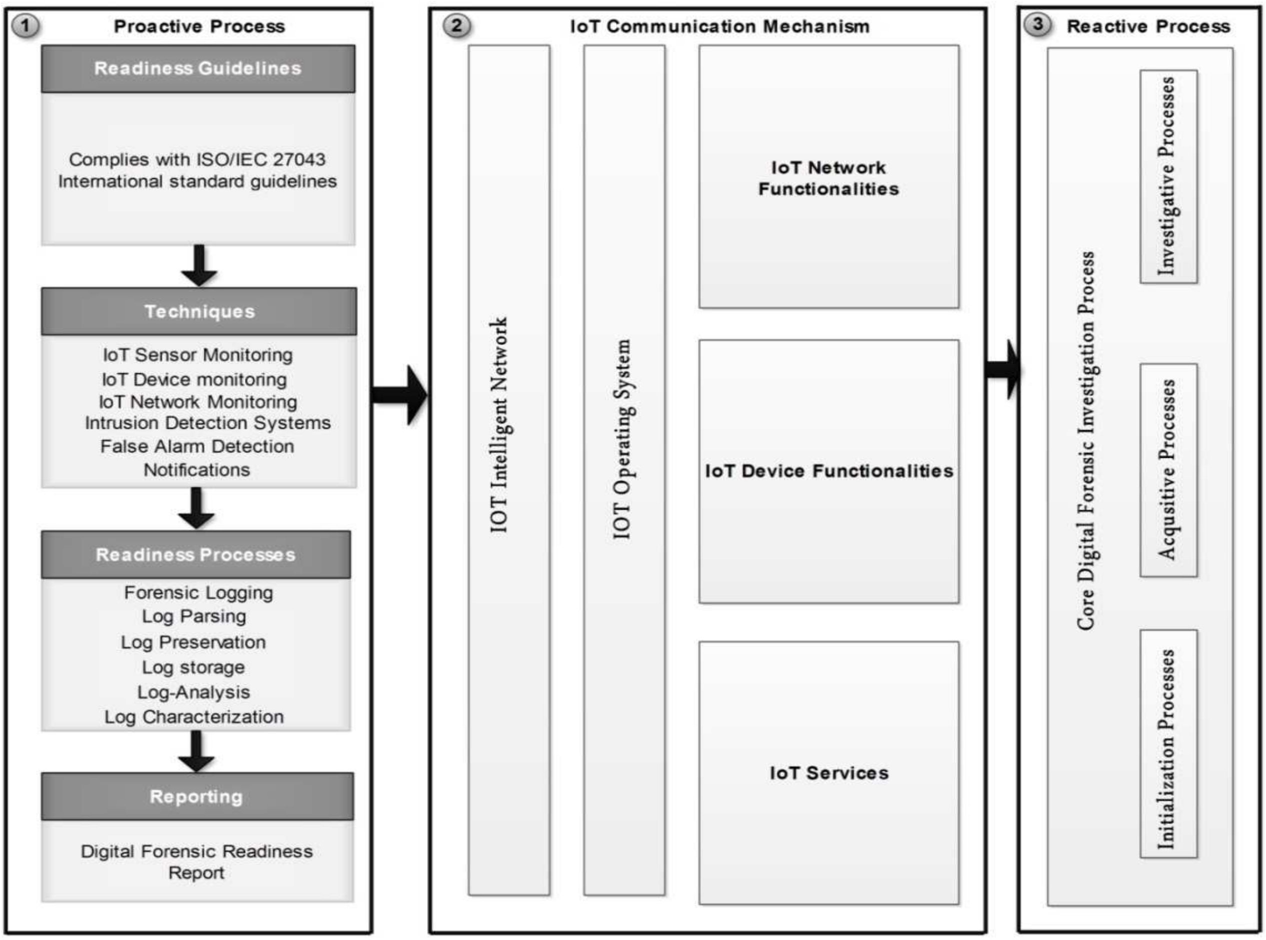


Fig. 3 DFR-IoT architecture

Planning process group- In the perspective of IoT, this group will initiate processes that will define IoT scenarios. The group will identify IoT sources of evidence, plan on how to gather digital evidence that may contain evidence, modes of handling this evidence, analyzing this evidence and defining how pre-incident detection process can be accomplished.

Implementation process group- As a result of implementing the IoT planning activities, this group will provide an implementation of pre-incident gathering process and implement the storage techniques in IoT environment and also implement the pre-incident analysis of the collected PDE from the IoT-based environment. Lastly, an implementation of the pre-incident detection process is achieved in this group.

Assessment process group- This group provides an assessment of the implementation process group. It ensures that the processes conducted in the implementation process group are valid and the results of the implementation are presented.

- *Techniques*

Techniques in the context of this research include modes of achieving DFR from IoT-based environments. The authors have identified various techniques that can be used to perform DFR in order to gather pre-incident information.

IoT Sensor Monitoring- Monitoring systems like ZigBee may be used because it is perceived that they work using light sensors, humid sensors, and temperature sensors. These aspects can forensically be wirelessly transmitted to a centralized center where they can be analyzed for possible incidents.

IoT Device Monitoring- The devices in IoT environment can be monitored based on the network packets they send or receive. The captured packets can also be forwarded to a centralized analysis center. An interpretation of the packets can be useful while trying to uncover a given occurrence.

For example, devices like microcontrollers, power supply, Wi-Fi modules and adapters, Voltage Regulators, Routers can be monitored based on how they are interfaced.

IoT Network Monitoring- Multiple sensors over the network and the network protocols can be assessed and monitored to ascertain how PDE can be excavated. Network services can be monitored too in order for events to be extracted. This is an aspect that facilitates the collection of the comprehensive amount of data about the functioning of the IoT–based networks. The Wireless Sensor Networks (WSN), Interconnected Sensor Nodes (ISN) and Body Sensor Nodes (BSN) can all be monitored so that they can act as potential sources of digital forensic information.

Intrusion Detection Systems (IDS)- Systems that are able to detect different modes of intrusion should also be put as techniques of achieving DFR in IoT based environment. An IDS can seamlessly be deployed anywhere in the IoT environment to protect the smart environments. The role of the IDS would be to send notifications to the administrators whenever an attack or suspicious network activities are detected.

False Alarm Detection and Notifications- False alarms and their notifications can play an important role in preparing the IoT environment for pre-incident detection strategies. This is possible because it is evident that a false alarm might contain some evidence. In previous research, Kebande and Venter [15] [16] have highlighted that to detect the frequency through which incidents occur then the false alarms should be incorporated. This was presented as Equation 1 below:

Based on the Equation (1), it is very evident that the presence of Intrusion Detection Systems (IDS) can generate quite a number of alerts. However, it is the user's task to investigate alerts that are real from the alerts that are false, and how accurate can an alert be. It is a daunting task which is also time-consuming and complicated to be able to filter false alarms from a thousand alarms from the collected information.

This brings about the issue of false positives as a result of forensic logging, which interestingly is not a new thing to the networking domain. More so, there might also be some irrelevant logs and irrelevant alarms that are not false positive or true positive, evidently such do not require attention if there is no vulnerability affected. Significantly, being able to filter traffic is a key attribute for the DFR-IoT architecture.

$$IDR = \frac{No\_I\_D}{No\_R\_I} + \{False\_Alarms\} * 100 \qquad (1)$$

Where IDR is incident detection rate, No_I_D is the number of incidents detected and No_R_I represents the number of incidents that are real. False alarms are incidents that are not treated to have occurred.

To highlight this aspect, the authors present a hypothetical scenario that has been used to bring out the aspects highlighted in Equation 1.

Hypothetical Scenario

X is an organization under a cyber-attack in a span of one week, the attacks that range from intrusion, identity theft, malware attacks, SQL injection, Distributed Denial of Service (DDoS) and web defacement. The attacks on organization X have warranted monitoring connected "things" by the security experts from X. The security experts are not able to determine what kind of attacks is true and which ones are false. As a result, they have come up with a technique of computing data that is verified later (as explained in Section 4.2.1.2).

TABLE I
TABLE DEPICTING TOTAL NUMBER OF INCIDENTS

S.no	Day	DDoS	Identity Theft	Cyber Intrusions	SQL Injection	Web Defacement	Total Incidents
1	**Mon**	2	3	4	0	2	11
2	**Tue**	1	0	4	1	0	6
3	**Wed**	0	0	1	2	0	3
4	**Thu**	0	4	5	4	0	13
5	**Fri**	2	7	0	0	1	10
6	**Sat**	4	10	2	1	2	19
7	**Sun**	5	4	8	1	0	13

Table 1 shows the number type and number of attacks that X has experienced in a span of one week (Monday to Sunday). At the last column, the total number of incidents for each day is highlighted. Based on the data presented in Table 1, there is a need to ascertain whether all the incidents are true or not.

Fig. 4 shows how the incidents appear before detecting the false alarms. This shows that by computing the total incidents that are detected at a given time, then it is possible for one to arrive at the incident response mechanism.

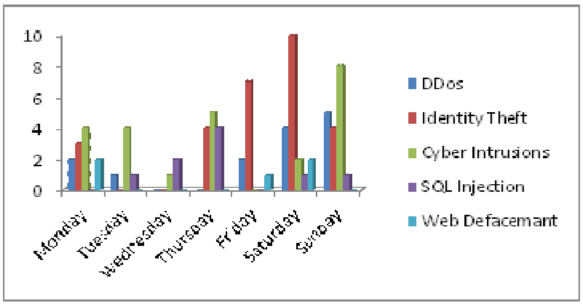


Fig. 4 Graph showing the total number of incidents in a span of one week before verifying collected potential evidence

- *Readiness Processes*

The readiness processes entity that has been presented in Fig. 3 has processes that have been proposed to achieve DFR in IoT-based environments. The following processes have been defined in this entity. Forensic logging, log parsing, log preservation, log storage, log analysis and log characterization. Each of the processes has been explained in sections to follow.

Forensic logging- Forensic logging allows the collection of digital artifacts from the IoT environments. These artifacts can be collected by implementing the techniques that have been proposed previously. Other tools that can be used in the collection of these artifacts can be EnCase, Sleuth Kit or FTK. In this context, the researcher has proposed the techniques of achieving this process as mentioned previously. Artefacts from IoT environment should be centered on sensor communication, packet sending and receiving, real-time data that can help to create a hypothesis that can be used in a court of law to prove or disprove facts.

Log parsing- Generally, logs are used to record information that can help to check the behavior of various events. Log parsing is a technique of packaging the forensic logs that are collected from the IoT-based environment in order to mine or extract specific log event. This helps in characterization which has been explained later on. The main reason for employing log parsing in this context is to be able to distinguish essential logs from non-essential log based on the content.

Log preservation- Preservation which is a way of digitally encoding logs enables the integrity of the collected information to be maintained. This can be done by creating hash values of each collected block of logs through hashing process. Later on, the hashed logs can be verified by comparing the generated hash and the stored hash. This is done to avoid tampering and to maintain the originality of collected forensic logs. Preservation should be done in such a way that the verifier is able to detect the tampered logs and the deleted log data.

If we revisit the hypothetical scenario that has been presented in Section (4.2.1.2), the following can be conducted after verification by matching the stored hashes against the hash values that were stored. The security experts discovered the following incidents. (R) has been used to denote the Real incidents while (F) has been used to denote the False alarms.

TABLE II
TOTAL REAL INCIDENTS AND FALSE ALARMS

No	Day	DDoS		ID Theft		Cyber Intrusions		SQL Injection		Web defacement		Total	
		R	F	R	F	R	F	R	F	R	F	R	F
1	Mon	1	1	2	1	2	2	0	0	1	1	5	5
2	Tue	0	1	0	0	3	1	0	1	0	0	3	3
3	Wed	0	0	0	0	1	0	1	1	0	0	2	1
4	Thu	0	0	2	2	3	2	2	2	0	0	7	6
5	Frid	3	1	5	2	0	0	0	0	0	1	8	4
6	Sat	3	1	6	4	1	1	1	0	0	2	11	8
7	Sun	4	1	3	1	5	3	0	1	0	0	12	6

A total of the real incident and false alarms has been computed as shown in Table 2. Fig. 5 shows the visualization number of real incidents after detecting the false alarms.

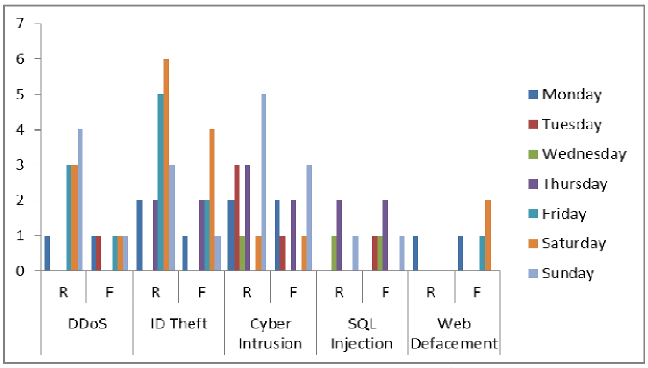


Fig. 5 .Total weekly real incidents and false alarms

From the data on the real incidents and false incidents, it is possible to calculate the Incident Detection Rate (IDR) as highlighted in Equation (1) as follows. Consider an example for S.no 1 as follows:

$$(Monday) Incident\_Detection\_Rate = \{(\frac{11}{5}) + 5) * 100 \tag{2}$$

$$(Tuesday) Incident\_Detection\_Rate = \{(\frac{6}{3}) + 3) * 100 \tag{3}$$

$$(Wednesday) Incident\_Detection\_Rate = \{(\frac{3}{2}) + 1) * 100 \tag{4}$$

$$(Thursday) Incident\_Detection\_Rate = \{(\frac{13}{7}) + 6) * 100 \tag{5}$$

$$(Friday)Incident\_Detection\_Rate = \{(\frac{10}{8}) + 4)*100 \quad (6)$$

$$(Saturday)Incident\_Detection\_Rate = \{(\frac{19}{11}) + 8)*100 \quad (7)$$

$$(Sunday)Incident\_Detection\_Rate = \{(\frac{13}{12}) + 6)*100 \quad (8)$$

TABLE III
INCIDENT DETECTION RATE FOR REAL INCIDENTS AND FALSE ALARMS

S.no	**Day**	**Total Incidents**	**Total Real and False alarms**		**Incident Detection Rate (%)**
			R	**F**	
1	**Monday**	11	5	5	720
2	**Tuesday**	6	3	3	500
3	**Wednesday**	3	2	1	250
4	**Thursday**	13	7	6	785.71
5	**Friday**	10	8	4	525
6	**Saturday**	19	11	8	972.72
7	**Sunday**	13	12	6	708.33

The graph below depicts the total incidents after the false alarms have been detected.

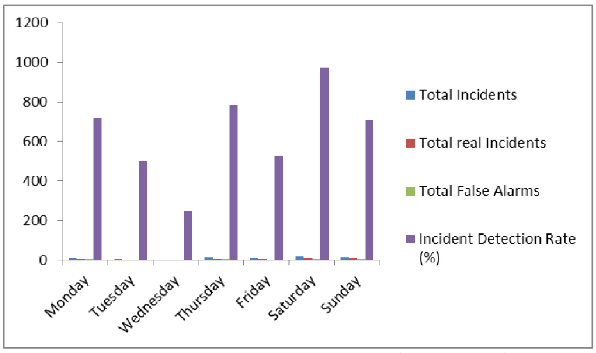


Fig. 6 Graph depicting incident detection rate for real and false alarms

Log storage- Once hash values for the logs have been created the logs are pushed to the forensic database for storage. Logs that are stored can be verified or analyzed. Storage allows the collected logs to accumulate as a centralized location such that if an incident is detected, then the logs can be relied upon for the reactive process that is labeled 3.

Log analysis- Analysis helps to check for possible security incidents. It allows the checking of PDE to ascertain if it contains suspicious events. These events contain common datasets that have user behaviors. This is because most of the time these logs come when they are unordered, analysis helps to group them, for example, based on ID, IP-address or timestamp for proper analysis.

Log characterization- This process allows the user to be able to tell which log comes from what part of the IoT system. Characterisation has been presented by Kebande & Venter [17] [20] in their research as a mechanism that can shorten the process of DFR by checking the characteristics that PDE possesses. By characterizing all the possible evidential activities detection is made more effective for purposes of digital investigation.

- *Forensic Readiness Report*

The readiness report is presented as a very integral part of the proactive process. It is used to show the outcome of the implementation of the readiness processes from the IoT environment. This report may at some point highlight the causality based on the readiness processes implementation.

- *Procedural Flows for the Proactive Phase*

Fig. 7 shows the basic interaction of functional elements of the proactive phase which has been presented as a readiness phase. It consists of five modules namely, readiness guidelines, techniques, readiness process and reporting stage. The obligation of the readiness processes that have been highlighted is to forensically prepare the IoT-based environment.

We consider that each process is enforced, for instance, each process at least requires interacting with the other processes that make a request. Additionally, we consider that each service of the process flow plays an active role in the DFR-IoT architecture.

2) *IoT Communication Mechanism:*

The IoT communication mechanism entity is used to facilitate communication between the network operating system and the IoT devices; this has been shown in the square labeled as 2 of Fig. 2. The mechanism allows data to move across the various channels. For example, power devices, IP connectivity, the functionality of components and node communication are some examples that enable communication of IoT mechanism. The IoT communication mechanism consists of the following modules: IoT Intelligent Network (IoT-IN), IoT Operating System (IoT-OS), IoT Network Functionalities (IoT-NF), IoT Device Functionalities (IoT-DF) and IoT services. Each of the aforementioned modules has been explained in detail below.

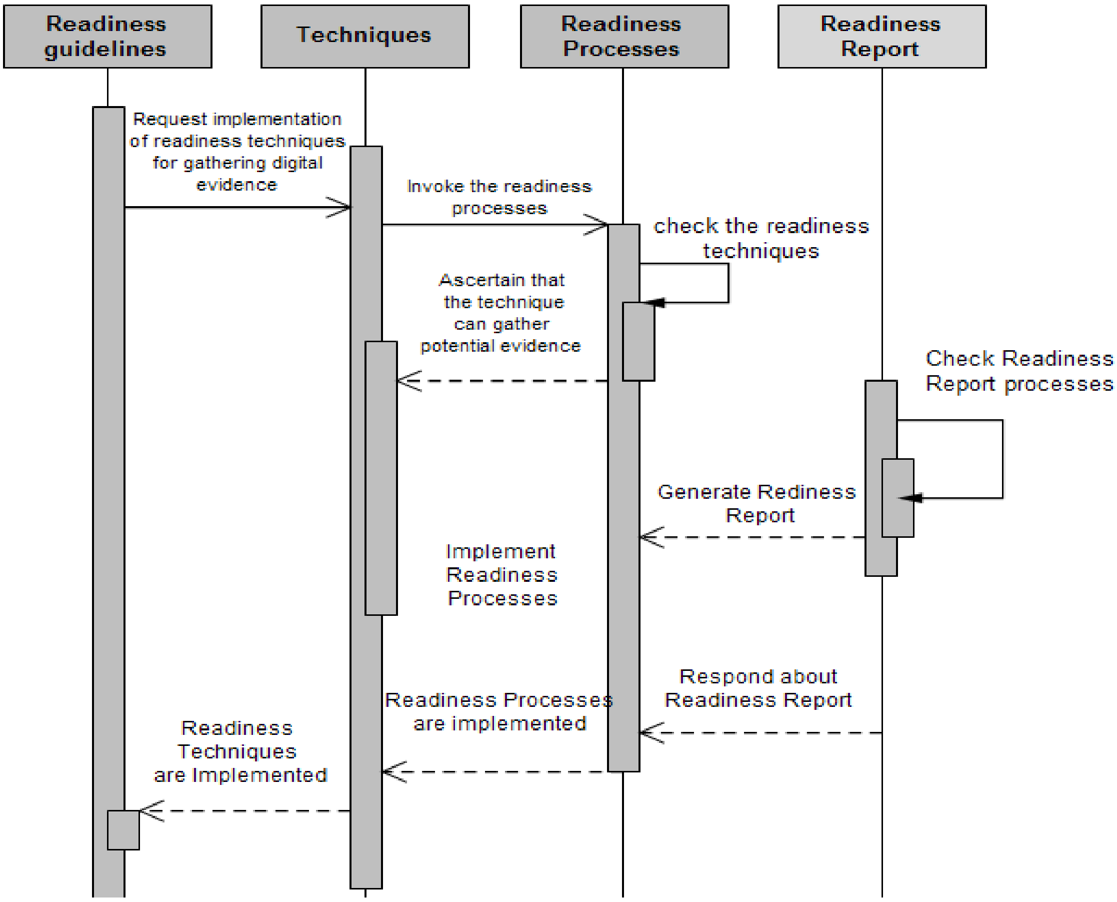
- *IoT Intelligent Network*

Intelligent network paves the way for the functionalities of nodes to be distributed in a flexible manner such that the Operating System (OS) and the devices are able to communicate in order for the IoT tasks to be achieved. IoT-IN should incorporate network elements so that the behavior of the IoT devices and functionalities can be supported. IoT-IN should address the following aspects:

- The IoT-based services that are able to be supported by the connected IoT environment.
- It should be able to trigger the processes and be able to interact with the calling and called processes.
- Should provide a mechanism through which processes are called.
- It should be able to link to the network functions and resources [18]

- *IoT Operating System*

The IoT-OS provides an interface that allows the IoT functionalities to be implemented since a majority of IoT devices are embedded devices that possess wireless sensors. The IoT-OS supports scheduling given that there are many applications running and the time constraint is also limited. The IoT-OS is meant to support network functions of IoT devices. Through the OS it is bound to support WSN protocols, Bluetooth, Z-Wave, Zigbee, IPV6 routing protocols for purposes of seamless communication of large networks.



Readiness guidelines
Techniques
Readiness Processes
Readiness Report
Request implementation of readiness techniques for gathering digital evidence
Invoke the readiness processes
check the readiness techniques
Ascertain that the technique can gather potential evidence
Check Readiness Report processes
Generate Rediness Report
Implement Readiness Processes
Respond about Readiness Report
Readiness Processes are implemented
Readiness Techniques are Implemented

Fig. 7 Procedural flows for the proactive phase of the DFR-IoT

- *IoT Network Functionalities*

The IoT-NF establishes gateway that is able to provide the connectivity of the embedded devices using the IPV6 connectivity. For example, the M-2-M devices are able to establish a protocol that allows them to exchange information in real-time basis over the network domain.

- *IoT Device Functionalities*

IoT-DF allows the connected devices to communicate seamlessly by relying on the interface provided by IoT-OS and the IoT-IN. In this section, the actuators play a role in making the devices and the M-2-M to communicate. Information about every connected device is provided at this phase, and a device management process can help to configure and reconfigure the functionalities over the IoT-OS.

- *IoT Services*

The IoT services are bound to provide information about all the IoT-based components that are connected to the DFR-IoT architecture. For example, the IoT Services is tasked with handling the following tasks: Security of the architecture and components, device communication, authenticity of data being communicated and remote service management.

3) *Reactive Process*

The reactive process provides core Digital Forensic Investigation (DFI) process. This has been presented in the last square that is labeled 3 of Fig. 2. These are processes that rely on the outcome of the proactive processes that have previously been highlighted in Section 4.2 of this research paper. It is worth noting again that the processes in the reactive process have also been mentioned in the ISO/IEC 27043 international standards [5]. The core digital investigation processes mentioned in the DFR-IoT architecture are as follows:

- *Initialisation process:* Whenever there is Potential Digital Evidence (PDE), there is always need to commence an investigation. Therefore, initialization process deals with procedures for commencing an investigation whenever an incident is detected. This is done by handling the post-event response mechanism as a first response and initializing incident detection, planning and preparing a digital investigation process.
- *Acquisitive Process:* This is a process that is concerned with how PDE is acquired from the IoT-based environment. This process concentrates on looking how PDE is identified, techniques that are used to collect these evidence, how this evidence is handled and under which condition this evidence is preserved and stored.
- *Investigative Process:* Once an incident is detected in IoT environment, it is important to identify the causality through proper examination and analysis of collected PDE. The process reports the activities that

have occurred in IoT environment through an interpretation process. The process interprets the activities that have occurred as a result of an incident which is later presented as a hypothesis in a court of law.

C. *Discussions of the Propositions*

The authors have explored the IoT domain, and it is evident that from a security perspective, there are research gaps that exist. The authors have carried out a study on the easiest way through which an IoT-based environment can prepare for potential security incidents. The study presented in this paper would help various researchers in the IoT and forensic community to understand that there are strategies that can be able to thwart cyber-attacks in IoT environments. DFR has a very important aspect in the modern day organizations; this is because it is the only way that an IoT-enabled environment can minimize the potential use of digital evidence while minimizing the cost of conducting a DFI. Compared to the conventional computing devices, IoT has special features which make it important for an IoT environment to be forensically ready for possible cyber-attacks and intrusions.

The mode of operation of the DFR-IoT presents it as a proactively based technique that employs proposed ISO/IEC 27043 International standard in implementing the readiness techniques. The ever-rising demand for smart homes and smart environments in general means that adversaries might also want to target these environments. It is based on this premise that the authors think that adding DFR as a security component to IoT might help in pre-incident detection strategies. The proposed architecture allows the intelligent network to work hand in hand with the IoT communication mechanism in order for all the proposed functions to be achieved.

Taking a closer look at the hypothetical scenario that has been presented in section X, one is able to deduce that implementing readiness aspects can accurately increase the chances of pre-incident detection. This is because, the rate at which the total number of incidents, real incidents, and false alarms occur can easily be computed in order to distinguish the nature of the occurrence. Note that this computation can only occur if the readiness techniques are implemented in the IoT environment. Ultimately, this leads to the reactive process that is characterized by examination and analysis. It is worth noting again that reactive process in the context of this paper differs in terms of wording with the presentation of ISO/IEC 27043 which is presented as a DFI. However roles remain to be the same.

After having presented the hypothetical scenario, it is quite clear that any organization should consider the readiness processes as a business requirement (Rowlingson, 2004). This aspect can only be consolidated based on the readiness processes that have been defined together with the roles, which have presented relationships between the entities, functionalities, and modules. As mentioned earlier, it becomes realistic enough for one to be able to distinguish real incidents from false alarms, which means that the propositions presented in Fig. 1 is entities that every existing organization should consider.

On the basis of the mapping that we did with the ISO/IEC 27043 guidelines, the DFR-IOT architecture is able to be mapped with the readiness process groups namely planning implementation and assessment and the reactive processes namely initialization, acquisitive and implementation. The biggest advantage as compared to any other architecture is the aspect of usability in an organization and being able to use standardized processes thereof.

Besides, enterprises running services and applications over the cloud can be able to technically implement these processes without having to disrupt the business processes. The next section presents a conclusion and future work.

IV. Conclusion

The study has proposed the addition of DFR to the smart environments of IoT by employing standardized processes that have been mentioned in the ISO/IEC 27043 international standard. This has been done with the convenience that allows the IoT-based environment to be forensically prepared for possible cybersecurity incidents. The proposed DFR-IoT architecture starts from the readiness guidelines, and then moves to techniques, readiness processes and reporting phase. Thereafter, the author describes the IoT communication mechanism and the reactive process. It is expected that the proposed architecture can be very useful when applied in smart IoT platforms.

For future work, the authors plan to propose the functional requirements that are needed in order to fully implement the DFR-IoT in a smart environment, based on this aspect; a prototype would provide proof of the propositions. Also, the authors will be able to come up with propositions that will allow organizations to be able to customize the architecture in order for the proposed processes to fit their organizational structures.

References

[1] Unknown (2015). Identifying the Technological Building Blocks in an Enterprise IoT Architecture. Available at: https://www.smartindustry.com/blog/smart-industry-connect/identifying-the-technological-building-blocks-in-an-enterprise-iot-architecture/ [Accessed June 03, 2016].

[2] IoT-A, (2013). Internet-of-Things Architecture (IoT-A). Available at: http://www.iot a.eu/public [Accessed June 03, 2016].

[3] IDC(2017) “Internet of Things spending 2017-2020: IoT industry drivers and investments”[online], Accessed February 2017. Available at-https://www.i-scoop.eu/internet-of-things-guide/iot-spending-2020/

[4] N.M. Karie, and H.S. Venter, “Taxonomy of Challenges for Digital Forensics.” Journal of Forensic Sciences. Doi: 10.1111/1556-4029, 2015.

[5] A.M. Desai, D. Fitzgerald, B. Hoanca, “Offering a digital forensics course in Anchorage”, Alaska. Inform Syst Edu J; Vol 7(35); http://isedj.org/7/35/, 2009

[6] ISO/IEC 27043: 2015: Information technology -- Security techniques -- Incident investigation principles and processes

[7] N.M. Karie, and H.S. Venter, “Toward a General Ontology for Digital Forensic Disciplines.” Journal of Forensic Sciences, Vol. 59, No. 5 Doi: 10.1111/1556-4029, 2014.

[8] G. Mohay, “Technical challenges and directions for digital forensics. Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering; 2005 Nov. 7–9; Taipei, Taiwan. Piscataway, NJ: IEEE Computer Society Publishers,;155–61, 2005.

[9] M. Cobb, “Digital forensic investigation procedure: form a computer forensics policy”. http://www.computerweekly.com/tip/Digital-forensicinvestigation-procedure-Form-a-computer-forensics-policy [Accessed February 18, 2013].

[10] E. Berthelsen, “Identifying the Major Technological Domains in an IoT Architecture.” Avilable online at: https://www.thingworx.com/blog/identifying-the-major-technological-domains-in-an-iot-architecture/ [Accessed June, 30th 2015]

[11] E. Mohamed, B.M. Sean, A. Atif and L. Andrew, “Towards A Systemic Framework for Digital Forensic Readiness.” Journal of Computer Information Systems 54(3):97-105. DOI: 10.1080/08874417.2014.11645708, 2014.

[12] T. Grobler and B. Louwrens, “Digital Forensic Readiness as a Component of Information Security Best Practice”, in IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds, in Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), pp. 13-24, 2007.

[13] A. Pooe, and L. Labuschagne, “A conceptual model for digital forensic readiness. Information Security for South Africa, Johannesburg, Gauteng. pp. 1-8, 2012”.

[14] F.A.R. Abdul, A. Rabiah, and Z.M. Madihah, “Developing Forensic Readiness Secure Network Architecture for Wireless Body Area Network (WBAN).” International Journal of Security and Its Applications. Vol.8, No.5 pp.403-420. http://dx.doi.org/10.14257/ijsia.2014.8.5.35, 2014).

[15] V. R. Kebande, and I. Ray, “A Generic Digital Forensic Investigation Framework for Internet of Things (IoT).” In Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on (pp. 356-362). IEEE, 2016.

[16] V. R. Kebande and H. S. Venter, “Novel digital forensic readiness technique in the cloud environment”, Australian Journal of Forensic Sciences, DOI: 10.1080/00450618.2016.1267797, 2017.

[17] V. R. Kebande and H. S.Venter, “Towards a Model for Characterizing Potential Digital Evidence in the Cloud Environment during Digital Forensic Readiness Process.” In ICCSM2015-3rd International Conference on Cloud Security and Management: ICCSM2015 (p. 151). Academic Conferences and publishing limited, 2015.

[18] O. Martikainen, J. Lipiäinen and K. Molin, “Tutorial on intelligent networks” Lappeenranta University of Technology, 1994.

[19] V. R Kebande, N.M. Karie, Michael, A, Semaka, M & Venter, H.S(2017, Ma). How an IoT-enabled “Smart Refrigerator” can play a Clandestine Role in Perpetuating Cyber-crime. In IST-Africa, 2017 IEEE International Conference on. IEEE-To appear.

[20] V. R. Kebande and H. S Venter, “Adding event reconstruction to a Cloud Forensic Readiness model.” In *Information Security for South Africa (ISSA), 2015* (pp. 1-9). IEEE, 2015.

[21] G. B. Satrya, H. T. Reda, K. J. Woo, P. T. Daely, U. K. Latif, S. Y. Shin and S.Chae, “IoT and Public Weather Data Based Monitoring & Control Software Development for Variable Color Temperature LED Street Lights.” *International Journal on Advanced Science, Engineering and Information Technology*, *7*(2), 2017.

[22] H. Z. Abidin, N. M. Din, N.A.M Radzi and Z. I Rizman, " A Review on Sensor Node Placement Techniques in Wireless Sensor Networks," International Journal on Advanced Science, Engineering and Information Technology, vol. 7, pp. 190–197, 2017.

[23] Editya,A.S, Sumpeno, S. and Pratomo, I.,(2017).Performance of IEEE 802.14.5 and ZigBee protocol on realtime monitoring augmented reality based wireless sensor network system. International Journal of Advances in Intelligent Informatics.Vol.3, No 2,pp. 90-97