International Journal on Advanced Science Engineering Information Technology

Vol.8 (2018) No. 2
ISSN: 2088-5334

Functional Requirements for Adding Digital Forensic Readiness as a Security Component in IoT Environments

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*— For every contact made on a digital device, a trace is left behind; this means that every digital device contains some form of electronic evidence that may be associated to the behaviour of the users in a given environment. This evidence can be used to prove or disprove facts if a cyber-incident is detected. However, the world has seen a shift on how devices communicate and connect as a result of increased devices and connectivity, which has led to the creation of "smart environments" where the Internet of Things (IoT) plays a key role. Still, we can harness this proliferation of digital devices and smart environments to Digital Forensic (DF) technology which might help to solve the puzzle of how proactive strategies can help to minimise the time and cost needed to conduct a digital investigation. This article introduces the Functional Requirements (FRs) and processes needed when Digital Forensic Readiness (DFR) process is employed as a security component in the IoT-based environment. The paper serves as a continuation of the initially proposed architecture for adding DFR as a security component to IoT environment. The aspects and claims presented in this paper can be used as basic building blocks for implementing DFR technologies that guarantee security in the IoT-based environment. It is worth noting again that the processes that have been defined in this paper comply with the ISO/IEC 27043: 2015 International Standard.**

***Keywords*— digital forensic readiness; functional requirements; internet of things**

I. INTRODUCTION

With the ever growing trends in technology and technological devices in the society today, the world has seen a shift in how devices connect and communicate with each other. This revolution has, further, led to the creation of "smart environments" aided by the Internet of Things (IoT).

IoT sometimes referred to as the Internet of Objects as explained by Triawan et al., [1] describes the connection of devices (any devices) which can produce, receive, deliver data or information, as well as connect through a wired or wireless communication between the same or different devices, in order to communicate with each other, without any interaction or human interference [2].

The IoT revolution has made a huge impact on how devices interact with each other as well as with different objects. However, this is not necessarily and completely the best thing that has ever happened in the world of technology. With the growing number of IoT devices in corporate networks based on a survey by Tripwire [3], there is a need for the industry to address the IoT security basics. From the survey, it is evident that less than a third of organisations today are prepared for security risks associated with devices making up the internet of things (IoT). As a way to limit the security risks brought about by IoT devices, it is important that such devices be securely configured, patched for vulnerabilities as well as monitored consistently.

However, an alternative approach to addressing IoT security within organisations is to embrace Digital Forensic Readiness (DFR) as a security component in IoT. For this reason, the authors of this paper introduce the Functional Requirements (FRs) and processes needed when DFR process is employed as a security component in the IoT-based environment. The aspects and claims presented in this paper can be used as basic building blocks for implementing DFR technologies that can guarantee security in the IoT-based environment.

As for the remainder of this paper, Section II presents materials and methods that have been employed in this research study, while Section III the results and discussions made in this paper. Finally, Section IV presents the conclusions made as a result of this study and mentions a possible future work. The next section briefs the reader on the background.

II. Material and Method

In this section, the authors present the background on the Internet of Things (IoT) as well as Digital Forensic Readiness (DFR). IoT 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. DFR is discussed to show the proactive side of Digital Forensics (DF), which can as well be used as an information security component in different organisations.

A. Internet of Things (IoT)

The world as we know it is a collection of very many different things which includes all sorts of physical objects and devices. Creating a communication network around these physical objects and devices brings about the concept of IoT.

IoT, therefore, is a concept that can simply be described as a network of physical objects and devices that contain embedded sensors and actuators to help them communicate and sense or interact with their internal states or their external environment all via the Internet. This also implies that, for the objects to communicate they must feature an IP address for Internet connectivity. The IP address then enables communication between these objects and any other Internet-enabled devices and systems.

However, Barrett [4], describes IoT as a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring Human-to-Human (H2M) or Human-to-Computer interaction (HCI).

With the wide availability of Broadband Internet, Morgan, [5] says that the cost of Internet connections is decreasing by the day. Besides, more devices are being created with Wi-Fi capabilities and sensors and protocols like ZigBee and IEEE 802.14.5 built into them to perform real-time monitoring [22]. In addition, the technology costs are also going down, and smart devices penetration in the society is increasing very steeply. These advances in technology thus create a perfect environment for IoT to thrive.

It is for this reason that the authors in this paper, as a way to deal with the security risks associated with the IoT-based environment, present the Functional Requirements (FR) for adding DFR as a security component in IoT Environments. This research is motivated by the fact that IoT is a concept 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 hence the need to deal with security problems. DFR concepts are discussed in the next section.

B. Digital Forensic Readiness

Today DFR is rapidly becoming an essential component of many business organisations. This is backed up by the fact that, for every contact made on any digital device used within the organisation, a trace is always left. This means that every digital device contains some form of electronic evidence that may be associated with a particular behaviour of the users in a given environment.

This, therefore, means that a well-coordinated approach to DFR process in any organisation will help in maximising the potentials use of their electronically stored information as well as reduce the cost of conducting digital forensic investigations within the organisation [6].

However, Cobb [7] states that DFR sounds like a daunting challenge to many organisations. 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 organisations to have some form of DFR so as to help them in planning and preparing for potential cybersecurity incidents. This aspect has motivated this research study hence the need to introduce the FRs and processes needed when DFR process is employed as a security component in the IoT-based environment. The next section will briefly highlight the preliminary work that supports this study.

C. Preliminary Work

As mentioned earlier, the study presented in this paper serves as a continuation of an initially proposed architecture for adding DFR to IoT environment (DFR-IoT). Besides, the aspects and claims presented in this paper act as basic building blocks for implementing DFR technologies to help in dealing with security in the IoT-based environment. The preliminary work, however, only proposed an architecture for incorporating DFR to IoT domain for proper planning and preparing in the case of security incidents. This is to mean that the preliminary work did not specifically address the FRs and the processes needed when DFR process is employed as a security component in the IoT-based environment, which is the focus of the current paper. The next section will present related work.

D. Related Work

Research in IoT is currently gaining momentum; however, studies on the integration of IoT and DFR are still wanting. In this section of this paper, therefore, the authors sample some of the existing related research work that has helped in the development of the FRs and processes needed when DFR process is employed as a security component in the IoT-based environment.

To begin with, Van Staden and Venter [8] argue that electronic communication is used in our daily lives. However, unsolicited electronic communication, also known as spam is also on the increase. Tracing the origin of spam by using information contained in SMTP headers, for example, is not possible because SMTP is a clear text protocol and can easily be intercepted and modified. For this reason, these authors proposed, adding DFR to electronic communication using a security monitoring tool. They also add that, during the process of introducing DFR, the amount of information that is gathered is inadvertently increased, to ensure that the information is valid and usable. However, Van Staden and Venter [8], did not address anything close to the FRs and processes needed when DFR process is employed as a security component in an IoT-based environment which is what the current paper focuses on.

In another presentation, Jason [9] talks about how to implement DFR and how to increase operational efficiencies

by implementing a pro-active approach to Digital Forensics (DF) throughout an organisation. His work, demonstrates how DF aligns strategically with an organisation's business operations and information security's program. However, just like Van Staden and Venter [8], Jason [9] also did not specifically address the problem of FRs and processes needed when DFR process is employed as a security component in the IoT-based environment. Jason [9] nonetheless showed in his work how the proper collection, preservation, and presentation of digital evidence is essential for reducing potential business impact as a result of digital crimes, disputes, and incidents. Finally, he concludes by illustrating how using a DFR approach and preparedness as a business goal can enhance the relevance and credibility of digital evidence.

Another study by Reddy and Venter [10] propose some concepts necessary for a Digital Forensic Readiness Management System (DFRMS) with the aim to assist large organisations in achieving an optimal level of management for DFR. The study as well lacked the component that addresses the problem of FRs and processes needed when DFR process is employed as a security component in IoT-based environment.

Although there exist a lot of research and related works on DFR, neither those nor the cited references in this paper have addressed the problem of FRs and processes needed when DFR process is employed as a security component in an IoT-based environment in the way that is introduced in this paper. Nevertheless, we acknowledge the fact that the previous research works have offered useful insights toward the development of the functional requirements in this paper. In the section that follows the authors briefly explain FRs and processes.

III. Results And Discussion

The section presents the Functional Requirements (FRs) as design parameters that can be used in IoT. The FRs has been presented in this research paper in order to bring out the essential requirement analysis approaches that can help Digital Forensic Readiness (DFR) processes to be successfully implemented in an IoT environment. A number of distinct processes have been proposed that may help to achieve this problem. Firstly, an overview of the initially proposed DFR-IoT architecture is shown in Fig. 1, which has in turn been used as a basis for generating the FRs. IoT design requirements allow the DFR-IoT to be implemented at the lowest level possible, which basically means that the FR allows the architecture to have a proper proactive process that is centered on forensic readiness aspects. For example, aspects like the Radio Frequency Identification (RFID), sensing devices, data transmission modes and the controlling units, WANs, LANs, WLANs, Wi-Fi and Ad-hoc networks all provide a holistic-cross platform for effective communication.

The DFR-IoT architecture has been presented in the best way possible such that it is able to incorporate the proactive (DFR) approach, IoT communication mechanism and the reactive (Digital Forensic Investigation) process. It is worth noting that the requirements that have been presented in this research are in line with the DFR processes that have also been mentioned in the ISO/IEC 27043: 2015, which is an international standard for Information technology - Security techniques -Incident investigation principles and processes [12]. These processes allow the IoT environment to be forensically prepared before potential security events can occur thus saving cost and time needed for the reactive process.

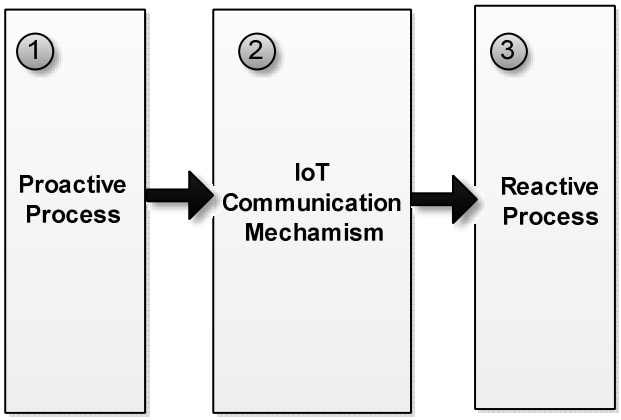

Fig. 1 Overview of DFR-IoT Architecture (Source: [11])

In the most basic approach that has been employed in this section, the FRs should be fulfilled in order for the IoT environment to adapt to the proactive processes. Firstly, it is mandatory for an IoT environment to be subjected to the legal consideration, statutory provisions and digital forensic laws on forensic monitoring and digital forensic evidence collection. These aspects are based on the propositions that have been highlighted by Rowlingson [13], Yansinsac and Manzano [14] as well as Tan [15] on what should be logged, how it should be logged and when logging should be done. The next section gives an explanation of the relationship that exists between the FR and other respective components.

A. Relationship of Functional Components

Based on the previously constructed DFR-IoT architecture [11], this section gives a description of the main FRs of the DFR-IoT that can be used as design facet for the inclusivity of DFR mechanism in IoT. The FRs embodies the concepts of adding DFR in the already existing IoT environment. Additionally, the FRs makes it possible for the DFR-IoT architecture to be able to forensically acquire Potential Digital Evidence (PDE) from distributed and heterogeneous IoT environments. A number of FR's have been considered with respective processes that have also been highlighted in Fig. 2, however, the process flows highlighted in Fig. 2 have also been shown in Fig. 3.

1) IoT Requirements: From Fig. 2, the DFR-IoT architecture allows a forensic user to be able to interact with the first module (IoT Communication Mechanism-IoT-CM labelled *a*) of the DFR-IoT architecture. This interaction happens through the IoT sensor and device monitoring process that is labelled as 1. A detailed explanation of the processes that follows has been explained further in the following sections.

2) Proactive Requirements: The proactive requirements are requirements that are needed in order to enforce DFR in IoT environment. This has been represented

in part labelled b. The components of the proactive requirements include Extraction of digital evidence, parsing forensic logs, digital preservation, creation of hash values, evidence storage, log analysis and characterisation and readiness report. Each of these requirements has been discussed in detail in the section to follow.

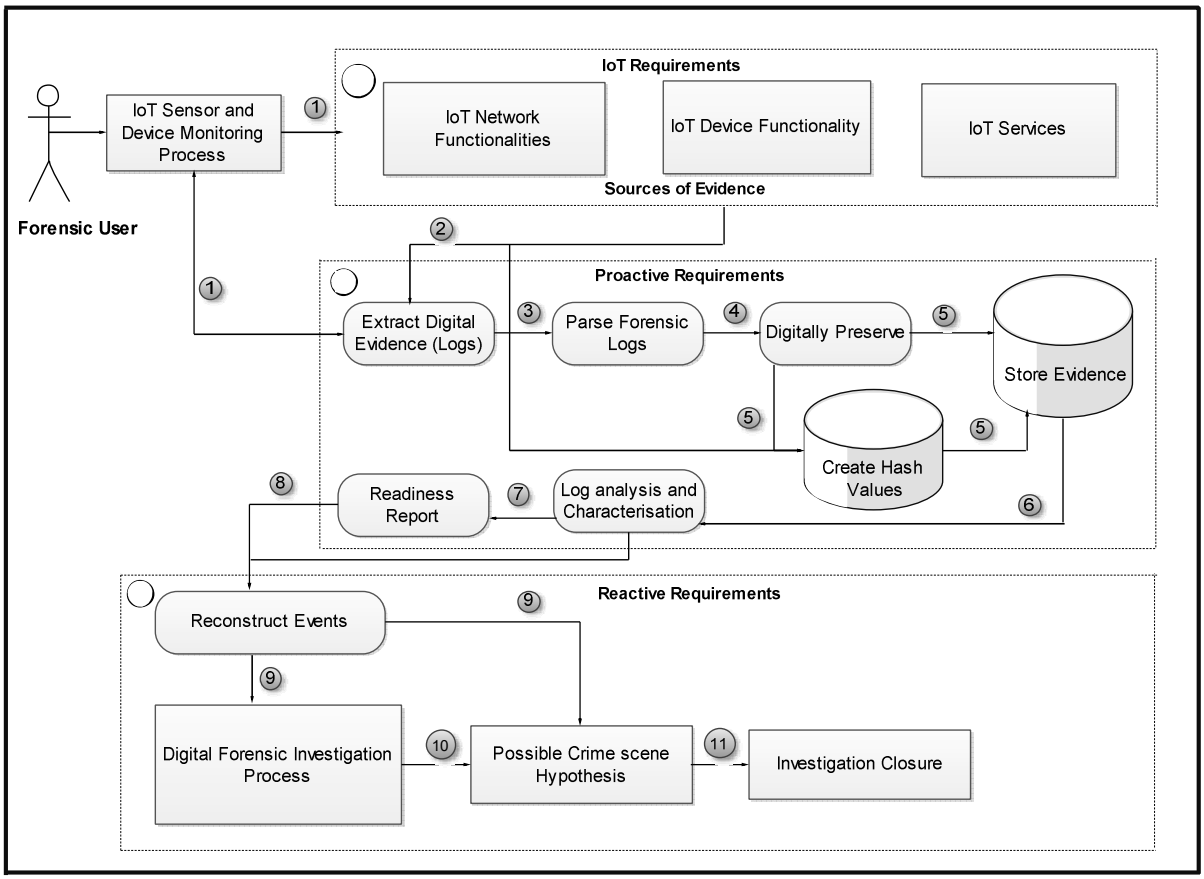

Fig. 2: Requirement and processes

- *Extract Digital Evidence (Logs)*: A link is then created between the IoT-CM and the forensic user which allows the forensic user to be able to access multiple IoT modalities that allows possible digital evidence extraction. In part labelled 2, the IoT-CM connects to a mechanism that allows forensic logging process to be achieved so that the excavation of potential digital evidence is possible.

It is worth noting again that the IoT-CM translates to the first process of the DFR-IoT architecture that was previously highlighted in Fig. 1. Based on the aforementioned explanations the authors have formulated notations and that are employed while extracting forensic logs from IoT-based environments. The following mathematical model has been employed in the extraction of the logs.

$$\sum_{j=1}^{zj} y_j p_j \geq y_j \qquad i = 1,2.....n \qquad (1)$$

and

$$p_j \in \{0,1\}, \quad j = 1.....z_n \qquad (2)$$

Where *n* represents the block of collected forensic logs, y_j is the number of forensic logs collected which may be measured in (KB, MB, TB) from the node *j*. Z_j is a probable number of nodes where logs are extracted from. $p_j = 1$ if the log extractor moves to the node j and $p_j = 0$ otherwise. In order to detect, the IoT nodes through which data is being collected from, the authors have used $y_j p_j \geq y_i$. Based on this aspect, the log extractor, which can be a forensic agent or any other digital information capturing device, can be able to explicitly collect/extract forensic logs from IoT-based nodes. Based on this proposition the concept has been idealised in the parsing phase which is explained in the next section.

- *Parsing* Forensic Logs (PFL): This process comes after digital forensic log extraction and is shown in Fig. 2 it has been labelled as step 3. PFL as a process may rely on regular expressions in order to extract a specific log that has a possibility of being used as admissible evidence in a court of law. By undergoing this process, a digital forensic investigator can be able to extract the log pattern and behaviour in order to aid the forensic investigators. A parser may be located in between the log extractor (step 3) and preservation mechanism (step 4).

In addition, this is possible because voluminous logs that are collected are usually in the unstructured format during the acquisition process. We have represented parsing using a set $\sum$ of alphabets or numerical values such that one can

be able to extract specific forensic logs from the collection of the alphabet/numerical.

If $\sum$ is considered to be a se or collection of numerical values or alphabets represented in the form [0,1…..9] and [a,b….z] respectively, we can represent a sequence $\beta = [b_1 b,_2 .....b_n]$ S.T $b_i \in \sum$ for $1 \le i \le n$. Based on this formulation, we can define a sub-sequence of β as follows: $\beta_{xi} = [b_{xi}, b_{xi} .....b_{xk}]$. From the sub-sequence of β, it's evident that $\forall_{xi}$ and $x_i \in \sum$ are represented in the form of $[1 \le x_1 .....x_n] \le n$. To illustrate the concept using the real parsing example we consider the following sequences. If we take four sequences as $\lambda = [2,4,6,8,10]$, $\delta = [2,4,5]$, $\phi = [4,6,9]$ and $\alpha = [6,8,11]$ then we can extract the specific logs based on the specificity of the values that exist commonly between $[\delta, \phi, \alpha]$ and λ. This can be deduced as follows [2, 4], [4, 6] and [6, 8]. Judging from this existence, it is possible to forensically parse logs from existing raw digital information. Nevertheless, according to Du [21], parsing logs in this manner makes log streaming easily due to an easy comparison of logs.

- *Create Hash Values:* Creation of Hash Values (HV) is factored in the process of hashing which in this context has been represented in step 5 of Fig. 2. It allows strings to be transformed into key values in order to represent the original string. Hashing in this context is used for log retrieval purposes for the forensic purposes. Additionally, it allows forensic logs to display HV when retrieved; these hash values can be used as unique keys to match collected logs for verification purposes.

Hash functions can be used as algorithms for verifying this process. The hash function can be represented as a cryptographic algorithm. This can only be possible by encoding the collected logs to form message digest (MD5 or SHA-1) before storing the hash.

HV can easily be created from a Message Digest (MD) or Hash Functions (HF). If x is an MD and *P* is a digital object then we can represent the x in terms of *P* as follows: $f(x) : x \in P$ and also $f(y) : y \in P$ where *P* can easily be preserved. *P* can also be presented as a positive integer and *F* can be represented as a hash function that contains a set of objects S. Given a set of digital objects $w = [w_1, w_2 .....w_t]$ and $x = [x_1, x_2 ....x_n]$ that can be hashed before storage, the following computations have been used to represent this actions.

$$\sum_{i=1}^{t} w_i \text{ and } \sum_{i=1}^{n} x_i \tag{3}$$

Based on this premise, the existence of digital information can be treated as a disjoint subset of and $p = [p_1, p_2 .....p_k]$ which shows that there exists one function $f \in F$ S.T

$$\{f(x) : x \in P_t\} \bigcap \{f(y) : y \in P_k\} = \xi \tag{4}$$

$$\text{for any } t = k$$

This shows that HV and MD can easily be created for digital objects during the process of digital preservation.

- *Storage of Evidence:* The resulting hash from the collected forensic logs (evidence) is stored in a forensic database in step 5 of Fig. 2. To determine if the collected forensic logs are authentic or not verification is done based on the generated hash values. This is because, for example, an attack of Man-In-The-Middle (MIME) attack may have a possibility of compromising the forensic Logs. Due to this hash values are stored with the corresponding file names of each of the message digest (SHA-1 or MD5).

- *Log Analysis and Characterisation:* Log analysis in IoT environment is a process that is done after the potential digital evidence has been collected based on the processes that were previously highlighted in ISO/IECC27043: 2015, it has been shown in step of Fig. 6. Analysis conducted in order to maintain if the collected forensic logs' integrity is maintained or not. This process is achieved based on the possible MD5 and SHA-1 message digest that is stored in the forensic database. Log characterisation as highlighted by Kebande and Venter [16] allows potential digital evidence to be grouped based on file formats.

The analysis in this context can be conducted as a technique through which a forensic analyst tries to proof if the collected (Hashed Log, HL) is what it was in order to maintain integrity. For example, a forensic expert may pick the HL as $HL \in X_n$ and computes it by selecting a key $< K_s, Y_s >$ in order for it to produce a signature that will be used during the verification process. Each HL has a unique identifier (U_ID) and a timestamp t_i. *For i=1 to n* to n a forensic analyst is able to generate a signature based on the following equation:

$$\psi = [HL]_{ti}^{U\_ID} \| < K_s, Y_s > \tag{5}$$

Where U_ID is the unique identifier used to represent the hashed HL and t_i represents the time stamp of the HL. $< K_s, Y_s >$ represent the key that will be used together with the signature for verification. In this process, the forensic analyst is able to check the file metadata in a retrieval process that involves checking the HL's t_i and the U_ID, through which the HL is picked given that $HL \in X_n$. It is worth noting that HL can be any random hashed log that has a t_i and a U_ID respectively.

To provide proof-by-verification by checking the HL and the signature in order to determine the integrity, a forensic analyst should perform a computation for HL as follows:

$$C = \sum_{i=1}^{n} HL \in X_n \quad (6)$$

This information may be used by a forensic analyst to compute the hash value for the HL and its properties. Therefore, the overall computation of the hash towards verification can be represented as follows:

$$C = \sum HL \in X_n = H_{sh} = \prod_{HL \in X_n} [U\_ID, t_i] \quad (7)$$

The above equation is the verification equation, which is invoked to provide the proof of HL and to show after analysis that the integrity of HL is maintained. After invocation the proof is provided as follows:

$$HL \xleftarrow{SIGNATURE} VERIFY < K_S, Y_S >= PROOF \quad (8)$$

- *Forensic Readiness Report:* A readiness report is an outline that consists of the examination notes that shows the processes that have been undertaken to excavate potential evidence. This has been shown as the last process of Fig. 2. Reporting has also been mentioned in the ISO/IEC 27043 as an integral process that gives the results that emanate from analysis and characterisation process. The importance of reporting is that it is useful during the reconstruction of events, a process that is very useful for the reactive (digital investigation) process.

Fig. 3 represents the flow processes that as depicted previously in Fig. 2. Fig. 3 has been used to systematically show how each requirement is succeeded in each module. For purposes of simplicity, the processes start from the module *a* to *b* to *c*. It is worth noting once again that a number of the process that is shown in Fig. 3 have been mentioned in the ISO/IEC 27043 international standard. Additionally, the processes have been idealised in the DFR-IoT architecture, and they are being used as high-level concepts for digital forensic investigation processes.

3) Reactive Requirements

Reactive requirements are forensic requirements that act as a post-event response techniques to the available potential digital evidence. The reactive requirements that have been considered in this context are discussed in the sections to follow.

- Reconstruction of Events: Reconstruction of events ensures that the collected potential evidence exists in an acceptable manner such that it can be admissible in a court of law if an incident is detected in IoT environments. This may include incident scenarios, system calls, and other proactive strategies. The design goals for reconstruction according to Liao & Langweg [17] are completeness, pertinence, reliability and privacy preservation. Nevertheless, Kebande and Venter [18], have also proposed the addition of reconstruction to a cloud forensic readiness model which appears to be a similar requirement. This mechanism allows the retrieval of the forensically logged information in order to search for events that can be reconstructed.

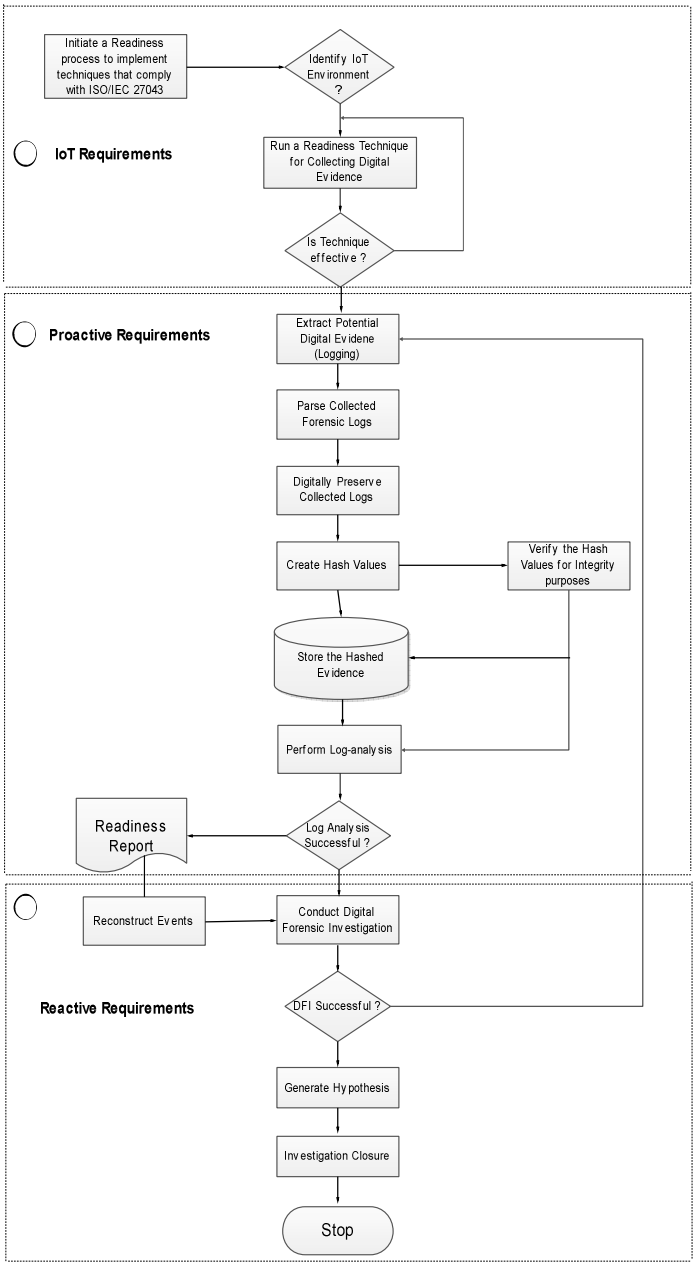

Fig. 3 Flow processes

- *Digital Forensic Investigation Process:* Digital Forensic Investigation Process (DFIP) is the actual investigation process which also translates to the investigative process of the ISO/IEC 27043. It ensures that all the activities dealing with DFI, examination, and analysis are successfully conducted in IoT environments.

- *Possible Crime Scene Hypothesis:* A hypothesis will generally be used to prove or disprove a fact in a court of law. Generally, a hypothesis that is based on the activities that have been highlighted in the parts labelled *a* and *b* of Fig. 2 ensures that there always will exist a link between an incident and a perpetrator. Carrier and Spafford [19] have argued that a hypothesis may be used to examine and analyse traces which can help investigation processes.

- *Investigation Closure:* This represents the closing of pertinent cases that are focused on IoT incidents. It is worth noting again that investigation closure has also been mentioned as a very integral process in ISO/IEC 27043 that allows termination of the investigation processes.

B. Discussion of the Propositions

The authors have proposed the Functional Requirements (FRs) that are needed when DFR is added to IoT environment as a security component. The study has introduced essential requirements to the initially proposed DFR-IoT architecture. Additionally, the proposition that has been presented in this paper provides a generic approach, however, it is a much better approach given that at the time of writing this research paper, there existed no IoT environment that had a forensic capability that has a focus on ISO/IEC 27043 expect the DFIF-IoT, that was proposed by Kebande and Ray [20] which was able to incorporate the classes of digital investigation processes.

The work that has been reported in this paper could act as a guide toward the development of DFR-IoT architecture which will easily enable compatibility with other components and devices. We have further addressed the need for (reactive requirements) forensic investigation process, which in a real sense is not the focal part of the study; however, it is an indicator that depends on DFR, since it falls under post-incident response.

It is worth noting too that the requirements have been developed to suit Human to Machine (H2M) interaction, however, from this simplicity, it can also be applied to Machine to Machine (M2M) communication. This aspect can only be achieved by writing and running scripts that can enable effective communication between human and machines.

Consequently, our solution makes it possible for the implementation of DFR-IoT during the design and development process. This is important because it will spearhead the identification of cyber-security based incidents in the IoT-based environment. Even though the study has been presented as a theoretical concept, it has an inherent applicability to the development of the DFR-IoT prototype. Precisely, if this notion would be falsified, then the DFR-IoT would not have a degree of communication between the different modules that were proposed in this research paper, otherwise, the notion holds.

IV. CONCLUSIONS

In this paper, the authors have discussed the functional requirements that are needed when adding DFR as a security component into IoT environment. The authors presented this using three approaches namely, IoT requirements, proactive requirements and reactive requirements. Being able to identify requirements is a crucial and a starting stage in the process of software development. This aspect is able to deal with the needs that are needed in order to design the software in the best way possible. With the current trends of innovative technologies, IoT technologies have started penetrating into every part of our daily lives, it is, therefore, important to build architecture with a forensic capability that can support the forensic community. Requirement gathering has been employed as a very important part towards the design of the DFR-IoT architecture.

Nevertheless, having pointed out the requirements that are needed, this research, therefore, mentions future work that will involve the development of a DFR-IoT prototype. The focus of this prototype will be how contextual data can be gathered that can help to proactively prepare the IoT environments for digital forensic investigations.

REFERENCES

[1] M. Triawan, H. Hindersah, D.Yolanda, and F. Hadiatna, “Internet of Things using Publish and Subscribe Method Cloud-based Application to NFT-based Hydroponic System”, In the 2016 IEEE, Proceedings of the 6th International Conference on System Engineering and Technology(ICSET) Oct, 3-4, 2016 Bandung – Indonesia, 2016.

[2] M. Al-Fuqaha, M. Guizani, M. Mohammadi, Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourthquarter, 2015.

[3] Tripwire,” Survey: Less Than One-Third of Organizations Prepared for IoT Security Risks”, Available at: http://www.tripwire.com/company/news/press-release/survey-less-than-one-third-of-organizations-prepared-for-iot-security-risks/ [Accessed on 23 -Feb- 2016].

[4] J. Barrett, “Internet of Things (IoT)”, 2016 Available at: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT [Accessed on 24th Feb. 2017]

[5] J. Morgan, “A Simple Explanation of 'The Internet of Thing”, 2014. Available at: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#1734f7081d09 [Accessed on 24th Feb. 2017]

[6] S. Jason, “How ‘Digital Forensic Readiness’ Reduces Business Risk” Available at: http://www.darkreading.com/attacks-breaches/how-digital-forensic-readiness-reduces-business-risk/a/d-id/1323508, 2015 [Accessed March 18, 2017]

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

[8] F. R. Van Staden and H. S. Venter,"Adding digital forensic readiness to electronic communication using a security monitoring tool," 2011 Information Security for South Africa, Johannesburg, 2011, pp. 1-5. doi: 10.1109/ISSA.2011.6027537.

[9] S. Jason , “Implementing Digital Forensic Readiness: From Reactive to Proactive Process:, 1st Edition. EBook ISBN: 9780128045015. Copyright: © Syngress 2016.

[10] K. Reddy, and H. S. Venter, “The architecture of a digital forensic readiness management system”, *Computers & security*, *32*, 73-89, 2013.

[11] Victor R Kebande,Nickson M Karie and H S Venter,"Adding Digital Forensic Readiness as a Security Component to the IoT Domain," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 1, pp. 1-11, 2018. [Online]. Available: http://dx.doi.org/10.18517/ijaseit.8.1.2115.

[12] ISO/IEC 27043: 2015, Information technology -- Security techniques -- Incident investigation principles and processes, [online],Accessed at https://www.iso.org/standard/44407.html

[13] R. Rowlingson, “A ten step process for forensic readiness”, *International Journal of Digital Evidence*, *2*(3), 1-28, 2004.

[14] A. Yasinsac and Y. Manzano, “Policies to enhance computer and network forensics. In *Proceedings of the 2001 IEEE workshop on information assurance and security* (pp. 289-295), 2001.

[15] J. Tan, “Forensic readiness. *Cambridge, MA:@ Stake*, 1-23, 2001.

[16] 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)., 2015 Academic Conferences and publishing limited.

[17] Y. C. Liao and H. Langweg," Resource-Based Event Reconstruction of Digital Crime Scenes", In *Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint* (pp. 129-136). IEEE, 2014.

[18] 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.

[19] B. D Carrier and E. H Spafford, "Defining event reconstruction of digital crime scenes", *Journal of Forensic Science*, *49*(6), JFS2004127-8, 2004.

[20] 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.

[21] Du, M., & Li, F. Spell: Streaming Parsing of System Event Logs.

[22] A. S. Editya, S. Sumpeno, I, Pratomo, " 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, 2017.