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.

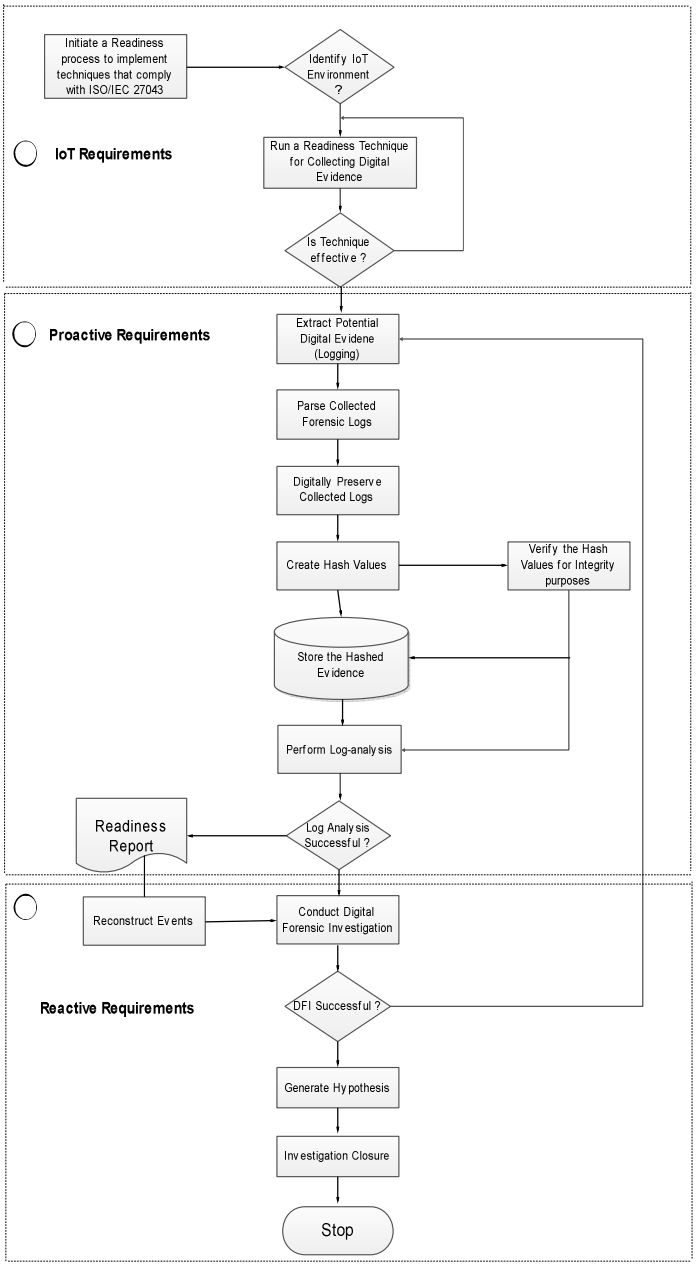

Fig. 3 Flow processes

- *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.