Framework of Confidence Values during Digital Forensic Investigation Processes

NANCY SCHEIDT and MO ADDA
University of Portsmouth
School of Computing
Portland Building, Portland Street, PO1 3AH Portsmouth
UNITED KINGDOM (UK)

Abstract: The advancement of Internet of Things (IoT) devices is continuously progressing and such development also enables a number of issues to arise which increases the complexity in the forensic investigation of the IoT. Globally, investigators are faced with challenges in ways of retrieving evidence from the different areas of the IoT environment, which includes Devices, Networks and the Cloud. One of the most crucial steps during forensic investigations is the writing up and creation of a case report which then needs to be presented in the court of law. In this paper, we propose models to estimate the confidence values of evidence, investigators and case reports to ensure case investigation accuracy and improve the evidential values of case presentation as well as evidence sharing of sensitive data worldwide.

Key Words: confidence value, forensic investigation, IoT server, fuzzy logic, forensic data sensitivity, investigator expertise, forensic report

Received: April 15, 2020. Revised: May 27, 2020. Accepted: May 30, 2020

1 Introduction

The number of Internet of Things (IoT) devices rises rapidly per person and will continue do so, such leads to the fast development and improvement of IoT devices which also opens more doors for the variety of opportunities these devices can offer in terms of usage, commercially, privately or criminally [13, 17]. Therefore, such developments can lead to a variety of challenges in digital and IoT forensics as well as increasing the complexity of accessing information of devices if forensically required. Hence, collecting evidence of the IoT environment (i.e. devices, network, the cloud) is a challenge investigators face worldwide. Research focuses on solutions expediently, however, it mainly addresses solutions to improve cybersecurity in the cloud or focuses on device-specific techniques for investigation purposes [7, 15].

Additionally, research by [18] suggest a server model to ease the investigation process due to IoT devices being registered on and information is stored on such. Managing devices and evidence of these is in need to be managed more efficiently and precisely [4]. If these steps are taken it is crucial to consider how reliable the whole investigation process has been and if sensitive data can be shared securely with other investigators which can include a number of privacy risks in this day and age [14]. Therefore, research by [3] proposes a secure encryption way to ensure data security and privacy. Furthermore, the paper by [16] suggests a data-sharing scheme which is made of 5-steps. If this research regarding data sharing is to be applied into police investigation processes, additional challenges need to be outlined and considered, such as the trust level between different countries when inquiring information for investigation purposes or the abilities of case investigators [9]. These calculations of trust levels have been implemented in research, however, focus on social media and how or if sensitive data can be shared between users [2]. However, this method is not considering the sharing of forensic data and was not applied to investigation processes. Additional research focused on the accuracy of forensic science and witness testimonies [10, 12, 5]. Other research by [5] proposes proficiency tests to assure forensic science results are accurate, however, only provide a theoretical idea by evaluating the benefits of being able to test the accuracy of forensic results. Moreover, [12]'s research focuses on the psychological factor which can influence the accuracy of evidence provided especially in terms of witness testimonies. None of the current research provides models to measure and calculate the accuracy or confidence of forensic investigation aspects, do however, stress its importance. Moreover, fuzzy logic and considering that some aspects cannot be as easily defined as by the Boolean logic 'True' or 'False' has not been linked to previous

mal methods for Security Engineering: ForSE 2019. SciTePress, 2019.

[3] Deyan Chen and Hong Zhao. Data security and privacy protection issues in cloud computing. In *2012 International Conference on Computer Science and Electronics Engineering*, volume 1, pages 647–651. IEEE, 2012.

[4] SangJun Jeon and SangJin Lee. Digital forensics technology management platform. In *2016 International Conference on Platform Technology and Service (PlatCon)*, pages 1–6. IEEE, 2016.

[5] Jonathan J Koehler. Forensics or fauxrensics: Ascertaining accuracy in the forensic sciences. *Ariz. St. LJ*, 49:1369, 2017.

[6] Marylu L Lagunes, Oscar Castillo, Fevrier Valdez, and Jose Soria. Comparison of fuzzy controller optimization with dynamic parameter adjustment based on of type-1 and type-2 fuzzy logic. In *Hybrid Intelligent Systems in Control, Pattern Recognition and Medicine*, pages 47–56. Springer, 2020.

[7] Aine MacDermott, Thar Baker, and Qi Shi. Iot forensics: Challenges for the ioa era. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5. IEEE, 2018.

[8] Ausama Majeed and Adil Al-Yasiri. Formulating a global identifier based on actor relationship for the internet of things. In *Interoperability, Safety and Security in IoT*, pages 79–91. Springer, 2016.

[9] Carole McCartney. Forensic data exchange: ensuring integrity. *Australian Journal of Forensic Sciences*, 47(1):36–48, 2015.

[10] Dawn McQuiston-Surrett and Michael J Saks. Communicating opinion evidence in the forensic identification sciences: Accuracy and impact. *Hastings LJ*, 59:1159, 2007.

[11] Hung T Nguyen, Carol L Walker, and Elbert A Walker. *A first course in fuzzy logic*. CRC press, 2018.

[12] HL Roediger, JH Wixted, and KA DeSoto. The curious complexity between confidence and accuracy in reports from memory. *Memory and law*, page 84, 2012.

[13] Bardia Safaei, Amir Mahdi Monazzah, Milad Bafroei, and Alireza Ejlali. Reliability side-effects in internet of things application layer protocols. 12 2017.

[14] Bruce Schneier. *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company, 2015.

[15] Francesco Servida and Eoghan Casey. Iot forensic challenges and opportunities for digital traces. *Digital Investigation*, 28:S22–S29, 2019.

[16] Jian Shen, Tianqi Zhou, Xiaofeng Chen, Jin Li, and Willy Susilo. Anonymous and traceable group data sharing in cloud computing. *IEEE Transactions on Information Forensics and Security*, 13(4):912–925, 2017.

[17] Sudeep Tanwar, Sudhanshu Tyagi, and Sachin Kumar. The role of internet of things and smart grid for the development of a smart city. In *Intelligent Communication and Computational Technologies*, pages 23–33. Springer, 2018.

[18] Shams Zawoad and Ragib Hasan. Faiot: Towards building a forensics aware eco system for the internet of things. In *2015 IEEE International Conference on Services Computing*, pages 279–284. IEEE, 2015.