

Mapping the use of expert system as a form of cloud-based digital forensics development

by Erika Ramadhani

Submission date: 23-Oct-2021 11:31AM (UTC+0700)

Submission ID: 1681693099

File name: Paper_Mapping_The_Use_of_Expert_System.pdf (1.02M)


Word count: 2939

Character count: 16167

PAPER · OPEN ACCESS

Mapping the use of expert system as a form of cloud-based digital forensics development

To cite this article: E Ramadhani and S Mulyati 2020 *J. Phys.: Conf. Ser.* **1567** 032032

 View the [article online](#) for updates and enhancements.

You may also like

- [Knot a Bad Idea: Testing BLISS Mapping for Spitzer Space Telescope Photometry](#)
J. C. Schwartz and N. B. Cowan
- [QUASICONFORMAL HOMOTOPIES OF ELEMENTARY SPACE MAPPINGS](#)
I V Abramov and E A Roganov
- [A fast approach to generate large-scale topographic maps based on new Chinese vehicle-borne Lidar system](#)
Han Youmei and Yang Bogang



IOP ebooks™

Bringing together innovative digital publishing with leading authors from the global scientific community.

Start exploring the collection—download the first chapter of every title for free.

Mapping the use of expert system as a form of cloud-based digital forensics development

E Ramadhani^{1*}, S Mulyati¹

¹Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia

*Corresponding Author: erika@uii.ac.id

Abstract. This paper discusses mapping of the use of expert systems for the development of cloud-based digital forensics. Mapping is done to answer the challenges in the development of the amount of data and the types of evidence currently that can affect the process of investigating forensics. The mapping is according to several categories, namely, tools, methods, ontology, and framework. The result is an expert system capable of providing automation to the investigation process, accelerating system performance, becoming a guideline for experts, as a means for investigators, and to get a system that can adapt to the framework.

1. Introduction

With the increasing amount of data, the types of evidence also increased. The digital forensics investigation process will become increasingly complex. As a result, digital forensics systems are developed that use cloud technology called digital forensics as a service (DFaaS). Digital forensics as a service (DFaaS) is the development of a new field of digital forensics. This technology provides services to users based on cloud technology. The difference between conventional digital forensics and DFaaS is the storage and use of tools that are stored centrally, centralized in the cloud. DFaaS was developed to make it easier for investigators, experts, analyzers, and detective to work together without being limited by time and place. Besides, DFaaS is also able to improve performance during the investigation process [1-2].

Digital forensics research is now much in the realm of artificial intelligence (AI), especially in the expert system. Among them is research on data forensics by using expert-system-like rules based on the fuzzy set theory method. Data is taken from databases to look for hidden structures [3]. In addition, K. Barmpatsalou et. al [4] explains f fuzzy systems are used to detect suspicious patterns on mobile forensics evidence. There are also other studies that use expert systems as a support to make the forensic investigation system into an intelligence system as in research [5-7]. In this paper, we discuss mapping regarding the use of expert systems in the process of investigating forensics, especially in DFaaS, which is based on services that use cloud technology. Mapping is based on several important categories, namely tools, methods, ontology, and framework. This category is a category that will continue to change along with the increasing data capacity and diverse types of digital evidence. The selection of this category is also based on the results of a summary of the challenges in digital forensics. Thus, the use of expert systems can be a problem solver of several challenges in the process of digital forensics investigations, especially in DFaaS.

The structure of this paper is as follows: first, discussion of expert systems in general. Then we describe the digital forensic investigation process, which then discusses the challenges of digital



Content from this work may be used under the terms of the [Creative Commons Attribution 3.0 licence](https://creativecommons.org/licenses/by/3.0/). Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

forensics based on the categories of each study. Before mapping, we discuss the DFaaS architecture and the difference with conventional DF. So the next section discusses the expert system mapping of DFaaS development and discussion of the benefits of expert systems. The last section is a conclusion section which summarizes all the results of this paper.

2. Expert System

Expert systems are systems based on knowledge [8]. Knowledge of an expert system comes from an expert who is an expert in his field. ES is part of artificial intelligent (AI). The use of expert systems usually integrates on computer programs that have several things to consider, namely knowledge, analytical skills, and experience. The expert system consisting of a knowledge base, inference engine, and user interface. Knowledgebase (KB) is a science that comes from humans or experts to solve problems that require human intelligence. KB accumulates experience and consists of a collection of rules. To represent knowledge using forward and backward chaining are knowledge representations. This knowledge representation will later represent the way of expertise by capturing, coding, and reusing. The inference engine (IE) is the brain of an expert system that interprets the rule and contains methods for reasoning. This interpreter will be in the form of analysis and process rules.

3. Digital Forensics (DF)

Digital forensics is the study of how to find information and data on digital storage media that aims to find evidence of an event. The process of finding information and data on digital devices requires specific methods, usually containing techniques and procedures. This proof can later be used to prove the law when it wants to trap perpetrators of crimes related to technology. The most crucial point in digital forensics is the existence of digital evidence, which is dealing with digital evidence. Forensic experts must understand the procedures in place to maintain the integrity and quality of evidence. The sequence of stages performed in digital forensic are processes, including identifying, acquiring, storage, and reporting [9]. All steps have specific procedures and techniques.

4. Challenges in DF

DF's challenges are divided based on essential points, including architecture, technology, application, IoT, smart devices, and secure computing. The distribution of challenges according to increase storage size, increasing operating system types, file formats, and interfaces, increasing use of encryption, network devices, and cloud resources, malware that uses volatile resources in the work process, as well as challenges to legality [10]. The challenge for digital forensics is also determined based on the topic of big data that is currently developing, along with the increasing data to be analyzed in digital forensics. The challenges based on the digital forensics framework, which consists of several stages, namely preparation, preservation, collection, examination and analysis, and presentation [11]. The exploration of digital forensic challenges is increasing. Along with the changing modern social lifestyles that are heavily dependent on communication, mobile, Internet of Things (IoT), cyber-physical systems (CPS), and cloud-based services. Challenges are not limited to the development of digital forensic frameworks but have thought about security in modern societies and hunting for cybercrime, which is a challenge for security experts and law enforcement agencies [12].

5. Digital Forensics as a Service (DFaaS)

The difference between conventional digital forensics and DFaaS lies in the storage media model used. In the past conventionally, the data stored will be stored separately, whereas by using DFaaS, the data stored centrally. As the name implies, providing services for digital forensics by providing storage services and tools based on cloud technology. H. M. A. Van Beek and R. B. Van Baar [1], [2], DFaaS architecture use cloud technology to provide tool services and storage media. The existence of DFaaS will help the ease of inter-digital communication between investigators, analysts, and detectives. The factors that are the focus of the discussion that influences the efficiency of conventional systems with

DFaaS are resource management, type of questions, time frames needed, research and collaboration, development, and sharing of knowledge.

6. Mapping the use of expert system in cloud-based digital forensics

Mapping the use of expert systems is based on several essential categories in digital forensics, namely, tools, methods, ontologies, and frameworks. The selection of these four categories is because the four parts are parts that always change and develop, along with technological developments. The taxonomies created are related to expert system implementations summarized in Table 1.

6.1. Tool

The tool is the most crucial tool in conducting digital forensics. This type of tool can be either software or hardware. Currently, there are many types of tools used in digital forensics, both open source, and closed source

6.2. Method

With the growing type of technology, there is also an increasing type of digital evidence. It will cause the search for new methods to solve the problems. An investigator must be able to find a new method of investigating a relatively new type of case, whether it is from the kind of evidence, type of electronic device, kind of storage, and so on.

6.3. Ontology and Framework

Ontology and framework are two interrelated things in digital forensics. To create a new framework, it is necessary to make an ontology first. At present, there are a lot of forensic investigation frameworks that have tested, and none of them have been used as a standard in conducting the investigation process. So, in the absence of these standards, to make a framework, it is essential that we first learn about ontology. Table 1 shows an example of using an expert system that may be implemented into digital forensics.

Table 1. Example of the use of expert system in cloud-based DF

Interest	Example	Illustration
Tool	Determination tool	A system that assist investigators in choosing the right tool when they want to carry out the digital forensic investigation analysis process.
	Detection forgery	The development of a system to assist investigators in forgery detection of digital evidence, usually in the form of multimedia evidence.
	Determination of framework	Database system repositories development that contains a collection of frameworks.
	Searching particular type of file	A system that can parse certain types of files such as parsing data on a hard disk when only looking for files in the form of documents.
Method	Cloud computation	The selection of the use of cloud computing technology suitable for the investigation process
	Service and application	When using DFaaS, the selection of the use of services and applications that are suitable for solving problems needs to be determined
	Remote connection	Security in a DFaaS needs to be considered, especially when connecting remotely. Thus, the selection of communication that established automatically is very necessary.

	Examination of digital evidence	At the examination stage, it is necessary to think about the use of an appropriate examination method when it is intended to be given to the detective, this is adjusted to the use of DFaaS.
	Migration to cloud system	Conventional systems must be able to adapt to the new system, as well as migrating to the cloud system. So that a certain method is needed that allows a system to have an adaptable behaviour.
Ontology	Determination standardization of process investigation	Making the repositories that consist of standard of process investigation, and the selection of the appropriate standard by using an expert knowledge.
	Digital evidence storage	Determination of digital evidence storage by using an ontology based on the expert knowledge
	Chain of custody	Determination of how to know the process of chain of custody by using an ontology based on the expert knowledge
	Best practice investigation	An ontology based on expert knowledge to determine the best practice of any kind of investigation.
Framework	The use of scenario	Making a repositories to choose the right scenerion by using an expert knowledge
	Efficiency of investigation process	Determination of process investigation accroding to the framework that relate to the expert knowledge
	Integration of model to make adaptable to cloud system	Making a framerork that it could as an adaptable cloud system.

Discussion

This section summarizes the use of expert systems in cloud-based DF, namely automation of the forensics stage, the guidelines for experts, the means for investigators, accelerating the process, and get the flexible framework.

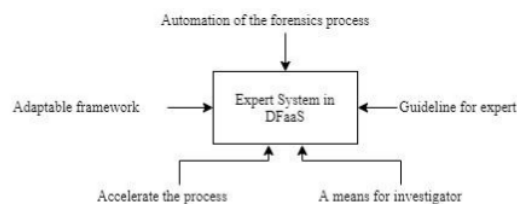


Figure 1. The use of expert system in digital forensics

6.4. Automation and Accelerate the process

Automation systems in digital forensics can use expert systems. Digital Forensics uses system automation in the digital forensic investigation process. So far, the use of the automation process for data representation makes it easier for users to read information and can represent the intent of information and events that occur. At present, the focus of digital forensic automation research is the use of tools that can transform data into information where investigators can use it easily in making decisions. The purpose of this automation is to speed up the investigation process and reduce the number of suspect devices in the lab [13].

6.5. Guidelines for expert

Modeling an expert system on digital forensics is to reevaluate previous cases that have already occurred, which can be an expert guideline in making decisions [14].

6.6. A tool for investigator

Expert systems are useful as a means for investigators to make decisions. For example, there are lots of tools to use when conducting an investigation, but not all of the tools have procedures for their use. It causes the expert to carry out the trial process for each tool. So, a tool that can assist in making decisions about tool selection is needed to speed up the investigation process. Besides, tool selection is more appropriate according to the characteristics of the tool [15].

6.7. Adaptable framework

With the existence of DFaaS, of course, making the system must be able to accept all forms of digital evidence for processing. It makes the system required to be able to adapt to various types of the framework in the process of digital forensic investigation [9].

7. Conclusion

This paper introduces the use of expert systems in digital forensics, especially in DFaaS. The increasing number of data challenges and the increasingly diverse types of evidence require a system that provides better performance system performance. To answer these challenges, the use of expert systems can help in developing DFaaS. Some of the benefits of an expert system integrated with DFaaS include system automation, accelerate the process, guidelines for experts, a means for investigators, and to get the flexible framework. However, this paper has not explicitly explained the implementation of the use of the expert system method in digital forensics cases. In the future, this research will discuss the use of expert system methods that implement to solve problems faced by DFaaS.

References

- [1] Van Beek HMA, Van Eijk EJ, Van Baar RB, Ugen M, Bodde JNC and Siemelink A J 2015 *Digit. Investig.* **15** 20
- [2] Van Baar RB, Van Beek HMA and Van Eijk EJ 2014 *Digit. Investig.* **11** S54
- [3] Stoffel K and Cotofrei P 2010 Fuzzy Methods for Forensic Data Analysis *Proceedings of the 2010 International Conference of Soft Computing and Pattern Recognition.*, pp. 23–28
- [4] Barmpatsalou K, Cruz TJ, Monteiro E, and Simoes P 2017 Fuzzy System-based Suspicious Pattern Detection in Mobile Forensic Evidence Fuzzy System-based Suspicious Pattern Detection in Mobile Forensic Evidence *9th EAI International Conference on Digital Forensics and Cybercrime*. October, 2017
- [5] Irons A and Lallie HS 2014 *Future Internet.* **6** 584
- [6] Franke K 2014 Computational Forensics : Towards Hybrid-Intelligent Crime Investigation Computational Forensics : Towards Hybrid-Intelligent Crime Investigation Katrin Franke and Sargur Srihari TR-05-07 June 2007 Center of Excellence for Document Analysis and Recognition *Proceedings of the Third International Symposium on Information Assurance and Security*. May 2014
- [7] Mansourvar M, Mahmud R and Karemm SA 2012 A Computer-Based System To Support Intelligent Forensic Study *Proceedings of Computational Intelligent.* 2012
- [8] Munaiseche CPC, Kaparang DR, and Rompas PTD., "An Expert System for Diagnosing Eye Diseases using Forward Chaining Method," in *IOP Conference Series: Materials Science and Engineering*, 2018, v306, no. 1
- [9] Du X and Scanlon M, "Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service," 2016
- [10] Waqar A. and Aslam B, Zareen MS 2013 Digital Forensics : Latest Challenges and Response in *2nd International Conference on Information Assurance (NCIA)* pp. 21–29

- [11] Adedayo OM 2016 Big data and digital forensics, Rethinking Digital Forensics in 2016 *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF) 2016* pp. 1–7.
- [12] Caviglione L, National I, Wendzel S and Mazurczyk W 2017 The Future of Digital Forensics : Challenges and the Road Ahead *IEEE Security and Privacy Magazine* December 2017
- [13] James JI and Gladyshev P 2013 Challenges with Automation in Digital Forensic Investigations
- [14] Duce DA, Mitchell FR, Turner P, Merabti M, and Security C 2010 *Digit. Evid. Electron. Signat. Law Rev.* 7 35
- [15] Kiper JR 2018 Pick a Tool , the Right Tool : Developing a Practical Topology for Selecting Digital Forensics Tools

Mapping the use of expert system as a form of cloud-based digital forensics development

ORIGINALITY REPORT

13%

SIMILARITY INDEX

8%

INTERNET SOURCES

8%

PUBLICATIONS

8%

STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

6%

★ Submitted to Universitas Negeri Surabaya The State University of Surabaya

Student Paper

Exclude quotes On

Exclude matches < 1%

Exclude bibliography On