International Journal of Web Services Research
Volume 16 • Issue 1 • January-March 2019

Ontology-Based Smart Sound Digital Forensics Analysis for Web Services

Aymen Akremi, Umm Al-Qura University (UQU), Makkah, Saudi Arabia
Mohamed-Foued Sriti, Al Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyad, Saudi Arabia
Hassen Sallay, Umm Al-Qura University (UQU), Makkah, Saudi Arabia
Mohsen Rouached, Sultan Qaboos University (SQU), Muscat, Oman

ABSTRACT

The big data generated by today Web services makes very fastidious and time-consuming the investigators logs management and analysis tasks. This is due partly to the lack of an efficient web service dedicated log data representation. We introduce, in this paper, an extensible standard based semantic ontology representation of Web service log data to identify hidden information and extract eventual scenario of Cyber-attacks in the web logs. The proposed ontology supports the Web service specification and it satisfies the forensics and admissibility requirements. Through a friendly graphical user interface, the investigator can define validation rules and queries and execute them using a logical reasoner over the proposed ontology to get some comprehensive forensic report ready to present to the court. We also showed how the proposed ontology can facilitate the investigator analysis task, reduce required time, and enhance the forensics process comprehensiveness.

KEYWORDS

Digital Forensics, Event Tracking, Forensics Investigation, Log Management System, Ontology, OWL, Reasoning, Web Services,

1. INTRODUCTION

Regarding the huge number of communication and commercial transactions through the Internet, the growing size of cybercrimes must be undertaken seriously. Considering this importance, identifying and prosecuting the cyber criminals is a very complicated task. Indeed, Service Oriented Architecture (SOA) and its lead implementation Web Services presents several additional challenges related essentially to the dynamic, autonomy, heterogeneity, self-contained, and their dynamic composition. The data and transaction between Web services grows exponentially making their analysis and events tracking very complicated and fastidious task.

Technically, the data considered in the investigation process are usually recorded in a normal course of actions by the logging systems (e.g. Intrusion Detection System). However, when anomalies or abnormal activities are recorded by such systems, then it will be marked and reported to the Digital Forensic Investigation (human or software) agent to investigate the case and evaluate the impact of the activity on the concerned part from the whole environment. From a company to another, we find that there are differences in the recorded format and used tools. These recorded data present additional

DOI: 10.4018/IJWSR.2019010104

challenges related to the very big data size characterized by its high heterogeneity. In addition, most data format are not extensible in term of providing the ability to make changes or add new security, forensics, or business requirements.

The aforementioned challenges make obstacles in the process of digital forensic analysis. In addition, there is a lack of standardized procedures, lack of forensics knowledge reuse, and lack of sufficient supports for legal criminal/civil prosecution (Hoss & Carver, 2009) especially those related to SOA.

Nevertheless, digital forensics researchers are aware of the importance of providing a standardized representation of the existing and commonly deliberated vocabulary(S. L. Garfinkel, 2010). Adopting a standard and modular forensic data representation is one of the major tasks that should be undertaken seriously throughout the next years, otherwise forensic research will fall behind the market and forensic tools become increasingly obsolete(S. L. Garfinkel, 2010).

In this paper, as an effort to deal with these gaps related to the unreliable and comprehensive-less representation of forensics data and the analysis delays, we promote the usage of the ontology and semantic technologies for providing a standard modeling of the forensic data and set of rules for smartly automating the analysis. We propose new forensics Web services ontology by mapping and extending the Incident Object Description Exchange Format (IODEF/RFC5070) (Danyliw, Meijer, & Demchenko, 2007. This ontology has the advantage to be extensible by new forensics features or domain application specification and will support Web services and forensics requirements management . Our contributions are mainly the following:

1. Design and establishment of new extendable forensics ontology for Web Services that includes all required forensic attributes, business requirements.
2. Automatic forensically sound data analysis through the definition of new rules and policies that identifies forensics breaches and reconstruct the occurred events automatically based on the logged events in the ontology.
3. Simulation case study and test running of forensic violation scenario using the proposed ontology.

The paper is organized as follows. We survey briefly the diplomatic domain, digital forensic investigation (DFI), web services, interesting related works which trying to propose standard data format for DFI, challenges, and requirements of applying forensics in Web Services in Section 2. In Section 3, we present our proposed Web Services Forensic Ontology and its related modules using OWL (Web Ontology Language) in addition to the events reconstructions rules based on the proposed ontology. A simple case study validating our findings is presented in Section 4. Section 5 discusses and concludes the paper.

2. DIGITAL FORENSICS FOR WEB SERVICES: AN OVERVIEW

2.1. Background

Currently, the world witnesses an exponential migration form papers to bits in all domains. This migration is accompanied with many problems related to the electronic record trustworthiness in term of their credibility and ability to convince the court's juries. Electronic records are known as digital data, which represents all files or documents generated by digital devices created by humans or applications. Modifying the content of digital documents means losing both information and admissibility. To make the electronics records admissible for the court, there is a necessity to prove that they are not modified after being generated. The field of preserving the intactness and integrity of digital records is closely related to digital forensics. The digital forensics as defined by Digital Forensics Work Shop (DFWRS)(attendees, 2001) is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and