World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:16, No:05, 2022

The Use of Artificial Intelligence in Digital Forensics and Incident Response in a Constrained Environment

Authors : Dipo Dunsin, Mohamed C. Ghanem, Karim Ouazzane

Abstract : Digital investigators often have a hard time spotting evidence in digital information. It has become hard to determine which source of proof relates to a specific investigation. A growing concern is that the various processes, technology, and specific procedures used in the digital investigation are not keeping up with criminal developments. Therefore, criminals are taking advantage of these weaknesses to commit further crimes. In digital forensics investigations, artificial intelligence is invaluable in identifying crime. It has been observed that an algorithm based on artificial intelligence (AI) is highly effective in detecting risks, preventing criminal activity, and forecasting illegal activity. Providing objective data and conducting an assessment is the goal of digital forensics and digital investigation, which will assist in developing a plausible theory that can be presented as evidence in court. Researchers and other authorities have used the available data as evidence in court to convict a person. This research paper aims at developing a multiagent framework for digital investigations using specific intelligent software agents (ISA). The agents communicate to address particular tasks jointly and keep the same objectives in mind during each task. The rules and knowledge contained within each agent are dependent on the investigation type. A criminal investigation is classified quickly and efficiently using the case-based reasoning (CBR) technique. The MADIK is implemented using the Java Agent Development Framework and implemented using Eclipse, Postgres repository, and a rule engine for agent reasoning. The proposed framework was tested using the Lone Wolf image files and datasets. Experiments were conducted using various sets of ISA and VMs. There was a significant reduction in the time taken for the Hash Set Agent to execute. As a result of loading the agents, 5 percent of the time was lost, as the File Path Agent prescribed deleting 1,510, while the Timeline Agent found multiple executable files. In comparison, the integrity check carried out on the Lone Wolf image file using a digital forensic tool kit took approximately 48 minutes (2,880 ms), whereas the MADIK framework accomplished this in 16 minutes (960 ms). The framework is integrated with Python, allowing for further integration of other digital forensic tools, such as AccessData Forensic Toolkit (FTK), Wireshark, Volatility, and Scapy.

Keywords : artificial intelligence, computer science, criminal investigation, digital forensics
Conference Title : ICDFSCC 2022 : International Conference on Digital Forensics and Security of Cloud Computing
Conference Location : Sydney, Australia
Conference Dates : May 16-17, 2022