PURDUE INNOVATES | Office of Technology Commercialization

StegnoCloud- Automating Digital Forensic Evidence Collection and Analysis: A Deep Learning Approach

A machine learning-based cloud forensic model is designed to detect and analyze illegal activities in cloud storage applications in real-time, enabling Cloud Service Providers to take immediate action and reduce forensic evidence storage.

As an increased amount of private users are adopting cloud applications, there is an increased risk of potential cybercrimes through these cloud applications. Thus, it is crucial to detect illegal cloud activities in motion to reduce the amount of forensic evidence storage. Researchers at Purdue University have developed a cloud forensic model to collect digital evidence related to illegal activities on cloud storage applications using machine learning. This technology accurately identifies and analyzes incidents related to child exploitation, illegal drug trafficking, and illegal firearm transactions uploaded to cloud storage applications in real time. This reduces evidence storage size and the amount of time required to filter out false positives. Through identifying and analyzing these incidents using machine learning, Cloud Service Providers (CSP) can collect alerted logs, block the associated accounts, and report it to law enforcement based on a Cloud Search Warrant (CSW) request. Furthermore, a CSP is able to transport all digital evidence to Evidence Collection and Analysis (ECA) through the cloud. Through tests of over 4500 images for all classes, the model accurately classifies an image roughly 96% of the time.

Advantages:

-Reduce amount of forensic evidence storage

-Efficient

-Accurate

Potential Applications:

-Cloud storage

Technology ID

2019-ROGE-68605

Category

Artificial Intelligence & Machine Learning/Computer Vision & Image Recognition

Authors

Umit Karabiyik

Marcus Kent Rogers

Fahad Salamh

Further information

Matt Halladay

MRHalladay@prf.org

Erinn Frank

EEFrank@prf.org

View online

-Combating child exploitation

-Law enforcement

-Data centers

TRL: 3

Intellectual Property:

Provisional-Patent, 2019-08-31, United States

Utility Patent, 2020-08-28, United States

Keywords: Cloud forensic model, machine learning, cybercrime detection, illegal cloud activities, digital evidence, Cloud Service Providers (CSP), Cloud Search Warrant (CSW), child exploitation, illegal drug trafficking, real-time analysis, Cloud, Computer Technology, Electrical Engineering, Forensics, Machine Learning