OPEN ACCESS Freely available online

ISSN: 2684-1304
Journal of
Anthropology Reports

Short Communication

Implementation of Computer System Forensics Approach

Kyra Stull*

Department of Anatomy, University of Pretoria, Pretoria, South Africa

ABOUT THE STUDY

Forensics is indeed a series of activities performed on a potential entity that includes data acquisition, processing, and representation in order to obtain evidence that will be accepted in a court of law. Networking and Cyber security is a field that entails a thorough examination of collected data in order to uncover evidence that can be used in a court of law. The forensic method includes auditing, examining Network and Computer data for information gathering, detecting intrusion, and presenting legal proof. Computer and network forensics is a scientific method for locating, seizing, extracting, analyzing, interpreting, examining, documenting, and presenting cybercrime evidence [1].

The widespread adoption of Information and Communication Technology (ICT) in modern society has resulted in the expansion of the crime domain to include network and computer-related crimes in cyberspace. Forensic analysis is concerned about the growing realm of cybercrime. The traffic generated by network nodes is a rich source of evidence for cyber forensic examination of probable attacks on the privacy and integrity of sensitive data. The purpose of cyber forensics is to present admissible, well-defined, and recorded evidence in a court of law [2]. Computer forensics, often known as cyber forensics, is the act of gathering, retrieving, conserving, and preparing material that has been electronically processed and stored on digital media for presentation in forensic labs.

Cybercrime also known as e-crime or digital technology crime is illegal conduct that uses a network node computer, laptop, or mobile device to target other resources. The target node is hacked, disrupted, or downgraded as a result of cybercrime. Cybercrime is a type of digital crime that uses the internet as a weapon. Over the previous two decades, the scope of cybercrime has expanded from simple credential risks to geopolitical crime. Modern cybercrime strategies have become increasingly sophisticated and marketed over the last decade. Criminals have been running syndicates as professionals using high-speed, easily available, and anonymous technologies [3]. The essential basis of law against criminal offence combines mental and physical factors. The elements of any legal system are mens rea and actusreus.

The actusreus is the act that leads to crime, and Mens rea is the mental condition in which a person intentionally commits a crime. Actusreus is not a crime in and of itself. The problem with cybercrime is that proving both aspects is difficult. The actusreus of cybercrime is a person's act in cyberspace, which laws seek to prevent. It is not a criminal if a person sends an SMS text message and the recipient responds positively. However, it would be illegal if the recipient was insulted and harassed. In this instance, actusreus is sending the message text, and mens rea is 'intention behind stalking.

The goal of a cyber or digital investigation is to identify evidence that can be used in a court of law while maintaining the integrity of the forensic process. An official report has been submitted first Incident Report in India. A notification is issued and a search warrant is requested from competent authority to seize possible evidences if information from third-party agencies or service providers is necessary [4].

Experts from the computer emergency response team arrive at the crime scene and gather potential evidence items, ensuring that collection and packing rules are followed. Cyber forensics labs perform forensics analysis. Witnesses and defendants are interrogated, and their testimonies are recorded. Confessions, forensics laboratory results, and information from 3rd providers are all analyzed together, and a charge sheet is produced in court in an admissibility way [5].

Apart from that, the machine learning technique is essential to achieving high threat detection accuracy. There are three forms of machine learning; supervised learning is predicated on the computer receiving pre-defined data and acting on that data to produce an output [6]. Unsupervised learning is the process of creating outputs by clustering input into classes without using a preexisting dataset. The third one is Reinforcement learning is a sort of machine learning in which the machine learns from its surroundings and continually improves its output.

Correspondence to: Kyra Stull, Department of Anatomy, University of Pretoria, Pretoria, South Africa, Email: kystull@unr.edu

Received: 02-May-2022, Manuscript No. JFA-22-17128; **Editor assigned:** 04-May-2022, PreQC No. JFA-22-17128 (PQ); **Reviewed:** 18-May-2022, QC No. JFA-22-17128; **Revised:** 25-May-2022, Manuscript No. JFA-22-17128 (R); **Published:** 03-Jun-2022, DOI: 10.35248/2684-1304.22.5.130

Citation: Stull K (2022) Implementation of Computer System Forensics Approach. J Anthropology Rep. 5:130.

CONCLUSION

It interacts with apps for updating a repository that enables decision making, rather than using labels as in unsupervised learning. To forecast events, machine learning is utilized to construct a predictive algorithm. The inclusion of data on a distributed file system allows for parallel processing to make intense classification easier by recognizing patterns in the information. This method allows vast amounts of data to be processed in a short amount of time with minimal resources.

REFERENCES

1. Prasanna BM, Vasal SK, Kassahun B, Singh NN. Quality protein maize. Curr Sci. 2001:1308-1319.
2. Mahmood Z, Ajmal SU, Jilani GH, Irfan M, Ashraf MU. Genetic studies for high yield of maize in Chitral valley. Int J Agri Biol. 2004;6(5):788-799.
3. Johnson HW, Robinson HF, Comstock RE. Estimates of genetic and environmental variability in soybeans. Agronomy. 1955;47(7): 314-318.
4. Bello OB, Olaoye G. Combining ability for maize grain yield and other agronomic characters in a typical southern guinea savanna ecology of Nigeria. Afr J Biotechnol. 2009;8(11).
5. Sofi PA, Wani SA, Rather AG, Wani SH. Quality protein maize (QPM): Genetic manipulation for the nutritional fortification of maize. J Plant Breed Crop Sci. 2009;1(6):244-253.
6. Wannows AA, Azzam HK, Al-Ahmad SA. Genetic variances, heritability, correlation and path coefficient analysis in yellow maize crosses (Zea mays L.). J Agric Biol Sci. 2010;1(4):630-637.