INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 20-23

ROLE OF AI IN DIGITAL FORENSICS

Vratika Singh[1], Dhannjay Singh Pundir[2], Anuvrat Singh[3]

[1,2,3]Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, India.

DOI: https://www.doi.org/10.58257/IJPREMS31763

ABSTRACT

Digital Forensics is one of the fastest growing technologies that had a great impact on the techniques and tools used to analyze, monitor and visualize the crime scene and find the right method to handle the upcoming threats and attacks on the cyber or internet world. The modern use of artificial intelligence to reduce human effort and achieve maximum results with fewer errors has replaced the human ability to perform machine-oriented designed work that has the ability and capacity to minimize errors and improve quality. The use of artificial intelligence in the field of digital forensics can influence the outcome and analyze the evidence in a better and more efficient way to monitor the results.

Keywords: - Artificial Intelligence, Digital Forensics, Evidence, Forensic .

1. INTRODUCTION

Digital forensic is a branch of science which deals with the protection of system and data associated towards its. Digital forensics also deals with occupying the evidence and analyzing of the evidence to know the cause of the attack which part of the system was been attacked. Modern technology has advanced the future in a way that we can predict the future by the use of leading technology. Digital Forensics has a protection system that can determine the evidence and analyze that evidence for future. According to a recent industrial survey, ninety-four percent of the companies didn't respond against potential threat to company and bare a loss of worth $ 35 billion. Digital Forensics is a tool used to learning through which will increase the security and analyzing ability of the system to monitor the risk of information and computer risks.

Digital forensics is defined as the process of preserving, identifying, extracting and documenting computer evidence that can be used by a court of law. It is the science of finding evidence from digital media such as computers, mobile phones, servers or networks. It provides the forensic team with the best techniques and tools to solve complex digital-related cases.

Digital forensics helps forensic teams analyze, inspect, identify and preserve digital evidence residing on a variety of electronic devices.

Technological development, information creation and results can lead to new access for new security users and end-users, without knowing how to end users. When the middle or middle level is known, a safe and secure threat can be found on an incompatible but dangerous computer. It creates a crime and must be investigated and protected through trial proceedings.

The continued increase in digital media storage capabilities and the extensive presence of daily life coverage is increasing demand and verifying the full amount of data. By linking this problem, you analyze the appropriate size and analyze its performance and do not correct the current forensic devices. Thus, computer forensics specialists use more time. The problem with this test is to calculate the required account because most forensic devices do not distribute processing capabilities. The difference in communication for forensic data, criminal investigators and prosecutors, the statistical evidence of the court's misinterpretation can easily led to Wrong decision and suspension of justice or wrong doing. Artificial Intelligence can provide new algorithms and best practices for development and supporting communication between stakeholders. Technology based on artificial intelligence, algorithms can communicate with statistical evidence and equality in construction of Artificial intelligence sample logic and structure illustration. Artificial Intelligence can also be given the model scenario to help making decisions and artificial intelligence enable different judges Test information for some ideas. Artificial Intelligence has developed tools and projects which are practically analyzed through a realistic case study training meeting with the help of forensic law It is expected that this unit will have the final result Analytical tools to prevent legal errors and practical devices The model also allows for the support of legal practitioners Professional exchange between statistical and legal experiments professional. Digital Forensics is a branch of forensic science which includes the identification, collection, analysis and reporting any valuable digital information in the digital devices related to the computer crimes, as a part of the investigation. In simple words, Digital Forensics is the process of identifying, preserving, analyzing and presenting digital evidences. The first computer crimes were recognized in the 1978 Florida computers act and after this, the field of digital forensics grew pretty fast in the late 1980-90's. It includes the area of analysis like storage media, hardware, operating system, network and applications. It consists of 5 steps at high level:

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 07, July 2023, pp : 20-23

Identification of evidence: It includes of identifying evidences related to the digital crime in storage media, hardware, operating system, network and/or applications. It is the most important and basic step.

1. Collection: It includes preserving the digital evidences identified in the first step so that they doesn't degrade to vanish with time. Preserving the digital evidences is very important and crucial.
2. Analysis: It includes analyzing the collected digital evidences of the committed computer crime in order to trace the criminal and possible path used to breach into the system.
3. Documentation: It includes the proper documentation of the whole digital investigation, digital evidences, loop holes of the attacked system etc. so that the case can be studied and analysed in future also and can be presented in the court in a proper format.
4. Presentation: It includes the presentation of all the digital evidences and documentation in the court in order to prove the digital crime committed and identify the criminal.

Branches of Digital Forensics:

Media forensics: It is the branch of digital forensics which includes identification, collection, analysis and presentation of audio, video and image evidences during the investigation process.

Cyber forensics: It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a cyber crime.

Mobile forensics: It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crime committed through a mobile device like mobile phones, GPS device, tablet, laptop.

Software forensics: It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crime related to softwares only

2. DIGITAL FORENSICS AND CONVENTIONAL TOOLS

Digital forensics uses tools and methods to monitor and analyze evidence and files that have been manipulated or traced. Traditional methods collect all possible evidence from various storage locations and present that data for monitoring and analysis. The traditional process involves different types of evidence acquisition from the following such as backup files, logical acquisition and physical acquisition.

Typical Forensics Analysis Step:

- Create timelines of events like the files system, last time file accessed, changed and created. Meta data from the file.
- Mounting of disk image readonly.
- Generating list of all files allocated and deleted
- Analysing the key files
- Recover deleted files
- Files carving by handling the unallocated files.
- Search files inn Disk image.
- Digital Forensics Investigation Process
- Verification
- System description
- Evidence Acquisition
- Timeline analysis
- Media and artefacts analysis
- String or byte search
- Data recovery
- Reporting results.

The Forensics Investigation Process

- Early task, will be there be an investigation
- Who will perform the investigation?
- Identification of item of internet

- Preservation of evidence
- Collection and taking control legally
- Examination a time consuming activity
- Analysis must be fully documented
- Presentation in the court of expert witness
- Decision as trail
- Chain Of Custody Of Evidence
- Who obtained the evidence
- Where and when it was obtained
- Who had the control or the position of evidence
- Secure storage in the mounted vault
- Digital Forensics Tools Classification
- Disk and data captured tools
- Files viewer
- File analysis tool
- Registry analysis tool
- Internet analysis tool
- Email analysis tool mobile device analysis tool
- MAC OS analysis tool
- Network forensics tools

Database forensics tools

3. ARTIFICIAL INTELLIGENCE IS ABOUT

Artificial intelligence is the study of intelligent devices and their process of tracking knowledge from the environment and from previous results obtained. Artificial intelligence systems will generally exhibit some of the following behaviors associated with human intelligence: planning, learning, thinking, problem solving, knowledge representation, perception, movement and manipulation, and some knowledge of social intelligence and creativity. At very high levels, artificial intelligence can be divided into two main types: narrow artificial intelligence and general artificial intelligence.

A narrow type of artificial intelligence is what we see around us in today's computers. Intelligent systems that have learned or learned to perform certain tasks without being explicitly programmed to do so. This type of intelligence in the voice recognition and language of Apple's iPhone's default Siri assistant in its self-driving car's vision recognition system is clearly in the suggested engine that suggests the products you love. In the past, unlike humans, this system could only learn to perform certain tasks, which is why it is called narrow artificial intelligence.

In general, AI is quite different because it is a kind of adaptive intelligence in humans that is flexible to intelligence and that is able to learn to perform very different tasks, from cutting hair to scales or thinking about different objects based on accumulated experience.

4. ARTIFICIAL INTELLIGENCE AND ITS IMPLEMENTATION IN DIGITAL FORENSICS

Artificial intelligence is used in the modern world to reduce the input workload to achieve maximum performance and to manage the system by itself taking the correct inputs from previous results and analyzing the resulting values for future course. Artificial intelligence deals with resource management, analysis and adherence to resources and methods in use. Digital forensics spans almost every piece of technology and every application. The use of artificial intelligence in security can help the system analyze a pre-deterministic approach to deal with errors and upcoming errors or security breaches and attacks. Artificial intelligence can also help us predict possible ways to analyze a problem and solve it before security is compromised.

Artificial intelligence can also help the field of digital forensics by incorporating methods and techniques used by artificial intelligence functions to provide the maximum result of analyzed evidence. The need for artificial intelligence in digital forensics is to analyze the data and secondly to predict the possible ways that the computer can be hacked and the possible way to break the computer.

Traditional forensic tools need external input from users to work with the forensic process procedure, but if we use artificial intelligence tools, there is a provision that it can pre-assign the threat or intrusion for the computer to the user so that the security program can be executed and handle the threat. Or in the event that the system is compromised, AI can capture evidence from the source and can keep a record of the attacker.

AI can gather information about the sources of the attack and the attackers, so forensic experts can easily trace back to the source to obtain information and the means by which the attack or breach occurred. The system can analyze evidence and can separate it from other documents. Analysis can also be fast and very reliable if an AI or machine analyzes the machine. Or in other words, if a machine communicates with another machine, the resulting value may be different for a human. Since human errors can occur, the machine is able to perform the task with less errors as designed in the algorithm.

Artificial intelligence can make work easier and more efficient and more reliable compared to humans, but it can also lack supporting files and other evidence for the system, human intervention plays a significant role, but the use of artificial intelligence can cause a fundamental change. . The method of detection and recovery is based on the algorithm designed by the system. The program works according to the design of the system. The chance of predicting who the intruder is becomes easier for the forensic expert.

AI can use any of the forensic tools designed so that an intruder cannot hide evidence anywhere in the system that traditional forensic tools could not analyze. When an intruder breaks into a system, he leaves behind some evidence, and if the intruder knows what type of forensic tool will be used, he hides the information in those memory blocks where the forensic tool cannot find the evidence. The result is no recoverable evidence. However, if the forensic tool is designed intelligently, the remaining memory block can also be analyzed and evidence can be analyzed..

5. CONCLUSION

Digital forensics is an eternal field of study that requires constant changes in functioning to maintain its effectiveness. The right changes should be made and at the appropriate technological peak. To improve the quality of the application, it should be platform-independent and robust. The use of artificial intelligence in digital forensics can cause very broad and recognizable changes in security. Artificial intelligence will help the digital forensics tools to analyze the evidence and make it easier for the forensic expert to analyze the data and make the right conclusion to find the result of the crime scene. It can also help in the practice of preliminary security threat analysis with past threats as well as storing threat logs to update the system for future use. Using a forensic tool, the system can be monitored and treated for possible changes and solutions.

6. REFERENCES

[1] https://www.researchgate.net/publication/220999758Artificialintelligenceappliedtocomputerforensics

[2] https://accessdata.com/blog/the-coming-ai-revolutionindigitalforensics

[3] http://ijarcs.info/index.php/Ijarcs/article/viewFile/4571/4116

[4] https://crimsonpublishers.com/fsar/pdf/FSAR.000554.pdf

[5] http://sas-space.sas.ac.uk/5533/

[6] https://pdfs.semanticscholar.org/5350/676fae09092b42731448acae3469cba8919c.pdf

[7] https://www.deccanherald.com/content/636412/ai-deep-learning-revolution-digital.html
https://resources.infosecinstitute.com/category/computerforensics/introduction/#gref