CLOUD FORENSICS

Ms. Angela P Johny

Cloud Computing: It is the technology that provides a variety of on-demand computing services to users over the Internet. These services include applications, databases, servers, networks, and more.

Cloud forensics refers to investigations that focus primarily on crimes that occur in the cloud. This could include data breaches and identity theft. With cloud forensics in place, owners are protected, and evidence is better protected. When illegal or criminal activity occurs using the cloud as a medium, cloud forensics professionals use their skills and knowledge to identify the responsible individuals or groups. Cloud forensics involves cloud users, both victims and perpetrators. For example, companies using cloud servers can become victims of data breaches and denial-of-service incidents. Criminals themselves can also use the cloud to launch attacks.

Like other subfields of forensics, cloud forensic scientists must follow strict regulations in order for their work to be admissible in court. This may include obtaining court orders to search cloud servers, verifying that evidence has not been tampered with, and taking other necessary. Digital forensics is a branch of forensics that uses electronic devices and data to uncover crimes, trace criminal paths, and analyse and protect evidence for use by law enforcement and prosecutors.

The area of digital forensics includes various components of the IT (Information Technology) environment; Internet and other networks, email, mobile devices, databases, operating systems, computer memory, etc.

CHALLENGES OF CLOUD FORENSICS

- The storage system is no longer local and may violate jurisdictional law.
- Each cloud server contains files from many tenants.
- Even when data from a particular suspect is identified, it is difficult to distinguish it from his data from other tenants.
- Recovery of deleted data poses problems.
- There is usually no evidence outside of the cloud service provider that a particular file is linked to a particular suspect. In digital forensics, it is difficult to identify information, and if it cannot be identified, it is difficult to acquire it, and without acquisition, there is no analysis.

REFERENCES

- Vaidya, N. (2020). Cloud Forensics: Trends and Challenges. International Journal of Engineering Research & Technology, 9(9). https://www.ijert.org/cloud-forensics-trends-and-challenges
- Digital Forensics: Salary & Career Outlook. (2021, February 11). UCF Online. https://www.ucf.edu/online/criminal-justice/news/digital-forensics-salary/