OPEN ACCESS Freely available online

Journal of Information Technology and Software Engineering

Commentary

Healthcare Data Cyber Security Investigations in a Cloud Computing System

Anand Mehta*

Department of Computer Science and Engineering, Jaipur National University, Jaipur, India

ABOUT THE STUDY

The application of cloud computing is widespread across several industries, , and education. The healthcare sector is attracted to cloud services by features including cost reduction, interoperability, data analysis, and data ownership functions. Sensitive healthcare data might attract an outside attacker and internal harmful occurrences, raising security and forensic risks in cloud systems. The most popular service in cloud computing settings is storage. A web browser, a cloud client application, or a mobile application can all be used to access data saved in iCloud (Apple Inc.'s cloud service provider). To sync data from devices like the MacBook, iPhone, iPad, etc., Apple Inc. offers the iCloud service. iCloud allows for the syncing of essential programmes including Mail, Contacts, Calendar, Photos, Notes, Reminders, and Keynote. Editing, deleting, uploading, downloading, and syncing data between devices are just a few of the various actions that may be carried out on cloud data. These processes produce log files and folders, both of which are necessary for an investigation. The taxonomy of iCloud forensic tools presented in this study creates a searchable catalogue for forensic practitioners to locate the tools that satisfy their technical needs. The storage of artefacts linked to environmental data, browser activities (history, cookies, cache), synchronization activities, log files, directories, data content, and iCloud user actions is shown in a case study including the storage of healthcare data on the iCloud service. To assist iCloud forensics, especially the gathering of artefacts from a MacBook machine, a GUI-based dashboard is created.

The importance of health care for people today could be emphasized. Humans are susceptible to several illnesses due to infection, defective diet, inheritance, environment, or deprivation. Traditional technology is unable to maintain and process the health data of such a vast population. Today, healthcare data should be evaluated utilizing cutting-edge technologies like machine learning, deep learning, the Internet of Things, artificial intelligence, image processing, and cloud computing in order to improve everyone's quality of life. The speed at which healthcare data is processed and computed has grown because to these technologies. For research-related discoveries as well as for understanding the patient's medical problems, test results for any disease are required.

Thin-client devices can be used to store healthcare data in the cloud. These devices and cloud user credentials might be accessed by an unauthorized individual, who could then change the cloud-stored record. In order to retrieve the data and determine its use in forensic science, this article investigates thin-client devices and cloud-based synchronized apps. In 2011, Apple Inc. introduced the iCloud storage service, which houses the data from the iPhone®, iPad®, iPod touch®, and Mac®. Apple now offers five different operating systems: iOS, iPadOS, macOS, tvOS, and watchOS. All devices automatically synchronize their data, and any updates can be made.

All devices signed in with the same account ID will automatically sync applications including Mail, Contacts, Calendar, Photos, Notes, Reminders, Pages, Numbers, Keynote, and Keychain. Due to the large number of devices involved and the synchronization of data from several applications, the acquisition and analysis of iCloud-related artefacts is crucial from a forensic standpoint. Evidence such as the account ID, password, data content, timestamps, log files, etc. may be necessary to build a timeline of suspicious behaviour. In order to produce a report on user activity, this research tries to define a recommended practice for iCloud data gathering. This study illustrates how iCloud data is used and where it is stored on the macOS 10.15 file system, as well as where the data is located.

Applications for cloud clients produce a large amount of data that can be used as evidence in forensic investigations. The taxonomy of iCloud forensic techniques described in this study includes potential sources of digital evidence on Apple devices (MacBook, iPhone, iPad, Watch, TV). Multiple sources—including a Web browser, the system setup, user profiles, log files, network packets, and memory analysis—can yield the proof. According to web browser analysis, it is possible to find documents relating to health data that include pertinent details like the filename of a downloaded file and the iCloud Account ID. There is an urgent demand for forensic tools that can quickly

Correspondence to: Anand Mehta, Department of Computer Science and Engineering, Jaipur National University, Jaipur, India, E-mail: anand_m@gmail.com

Received: 18-Nov-2022, Manuscript No. JITSE-22-20959; **Editor assigned:** 21-Nov-2022, Pre QC No. JITSE-22-20959 (PQ); **Reviewed:** 07-Dec-2022, QC No. JITSE-22-20959; **Revised:** 14-Dec-2022, Manuscript No. JITSE-22-20959 (R); **Published:** 21-Dec-2022, DOI: 10.35248/2165-7866.22.12.309.

Citation: Mehta A (2022) Healthcare Data Cyber Security Investigations in a Cloud Computing System.J Inform Tech Softw Eng. 12.309.

and easily retrieve iCloud artefacts from Apple devices. To enable forensic professionals find particular tools that meet their technological needs, the taxonomy of iCloud forensic tools offers a searchable database. The taxonomy may also be crucial in guiding the creation of common forensic tools for cloud systems.

By adding features that span the whole Apple device forensic, including collection, analysis, and attribution, further research will improve the tool taxonomy. In order to assess the postattack investigation and comprehend the attack patterns, it is necessary to create healthcare data sets.